Teoría de grupos

Teoría de cuerpos y teoría de Galois

Representaciones de grupos finitos

Notas ampliadas de un curso de álgebra
Versión preliminar

Bruno Stonek
bruno@stonek.com

23 de octubre de 2012

Índice general

Capítulo 1

Teoría de grupos

1.1. Definiciones básicas

Damos ahora las definiciones y propiedades básicas de los grupos. Los detalles (sencillas manipulaciones algebraicas) quedan a cargo del lector.

Definición. Sea G un conjunto, $* : G \times G \to G$ una función. Consideremos las siguientes propiedades de $*$:

1. $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$ (asociatividad)
2. $\exists e \in G : a * e = a = e * a \quad \forall a \in G$ (existencia de neutro)
3. $\forall g \in G \, \exists g^{-1} \in G : g * g^{-1} = e = g^{-1} * g$ (existencia de inverso)
4. $\forall a, b \in G \quad a * b = b * a$ (conmutatividad)

Si $(G, *)$ satisface 1, es un *semigrupo*.
Si $(G, *)$ satisface 1 y 2, es un *monoide*.
Si $(G, *)$ satisface 1, 2 y 3 es un *grupo*. Si además satisface 4, se dice *abeliano* o *conmutativo*.

El *orden* del grupo $(G, *)$, notado $|G|$, es el cardinal del conjunto G.[1] El grupo es *finito* si lo es su orden, en caso contrario es *infinito*.
Si $|G| = n$ y $G = \{a_1, \ldots, a_n\}$, su *tabla de multiplicación* es la matriz $n \times n$ con coeficientes en G que en la entrada (i, j) consiste del producto $a_i a_j$.

Notación. Cuando un grupo es abeliano, a menudo adoptaremos la *notación aditiva*, escribiendo $a + b$ en vez de ab, 0 en vez de e, y $-a$ en vez de a^{-1}.

Observación 1.1.1.
- Escribiremos ab en vez de $a * b$, y diremos que "G es un grupo" sobreentendiendo la operación y el neutro (análogamente con semigrupo y monoide).
- La asociatividad nos permite escribir abc. Por inducción, se prueba que todas las maneras de asociar n factores dan el mismo resultado, permitiéndonos escribir en general $a_1 \ldots a_n$ (ver [J] pp. 39-40 para más detalles).

[1] También usaremos esta notación para notar el cardinal de un conjunto cualquiera.

- El neutro, si existe, es único.
- Para poder escribir g^{-1} hay primero que verificar que el inverso, si existe, es único.
- Si a es invertible, $(a^{-1})^{-1} = a$.
- Si a y b son invertibles, cumplen $(ab)^{-1} = b^{-1}a^{-1}$.
- Si a es invertible entonces $ab = ac \Rightarrow b = c$. En particular, si $a^2 = a$, entonces $a = e$. Análogamente, si a es invertible entonces $ba = ca \Rightarrow b = c$.

Definición. Sea G un grupo. Si $n \in \mathbb{Z}^+$, definimos $a^n := \overbrace{a \dots a}^{n \text{ veces}}$, y $a^{-n} := \overbrace{a^{-1} \dots a^{-1}}^{n \text{ veces}}$. Si $n = 0$, $a^n := e$.

El *orden* de un elemento $a \in G$ es $|a| := \text{ínf}\{n \in \mathbb{Z}^+ : a^n = e\}$. Si no existe un tal n, decimos que $|a| = \infty$.

Notación. En notación aditiva, a^n se vuelve na, y $a^{-n} = -na$.

Observación 1.1.2.
- $a^n a^m = a^{n+m}$ y $(a^n)^m = a^{nm}$, $\forall n, m \in \mathbb{Z}$.
- Si $a, b \in G$ conmutan (i.e. $ab = ba$), entonces $(ab)^n = a^n b^n$.

Definición. Sea G un grupo. Un subconjunto $H \subset G$ es un *subgrupo*, y lo notamos $H < G$, si:

- $e \in H$
- $a, b \in H \Rightarrow ab \in H$
- $a \in H \Rightarrow a^{-1} \in H$

Un subgrupo $H < G$ es *propio* si $\{e\} \subsetneq H \subsetneq G$.

Observación 1.1.3. Sea G grupo, $H \subset G$. Son equivalentes:

- $H < G$,
- $H \neq \varnothing$ y $a, b \in H \Rightarrow ab^{-1} \in H$,
- $e \in H$ y H con la operación de G restringida a H es un grupo,

Observación 1.1.4. La intersección de una familia no vacía de subgrupos de un grupo es un subgrupo. Esto nos permite hacer la siguiente

Definición. Sea G grupo, $S \subset G$ subconjunto. El *subgrupo generado* por S es la intersección de los subgrupos de G que contienen a S, i.e.

$$\langle S \rangle := \bigcap_{S \subset H < G} H$$

Si $G = \langle S \rangle$, decimos que S es un *generador* de G. Si existe $S \subset G$ finito tal que $G = \langle S \rangle$, entonces decimos que G es *finitamente generado*. En este caso, si $S = \{a_1, \dots, a_n\}$ notamos $\langle a_1, \dots, a_n \rangle = \langle \{a_1, \dots, a_n\} \rangle$.

Observación 1.1.5.

- $\langle S \rangle$ es el menor subgrupo de G que contiene a S.
- $\langle S \rangle = \{s_1^{n_1} \dots s_k^{n_k} : s_i \in S, n_i \in \mathbb{Z}, k \in \mathbb{N}\}$.

Definición. Sean G_1, G_2 grupos. Una función $\varphi : G_1 \to G_2$ es un *homomorfismo de grupos* (cuando quede claro abreviaremos simplemente por *morfismo*) si cumple:

$$\varphi(ab) = \varphi(a)\varphi(b), \quad \forall a, b \in G_1$$

El *núcleo* de φ es $\ker \varphi := \{a \in G_1 : \varphi(a) = e\}$.
La *imagen* de φ es $\text{Im } \varphi := \{b \in G_2 : \exists\, a \in G : \varphi(a) = b\}$.
Notaremos por $\text{Hom}(G_1, G_2) := \{\varphi : G_1 \to G_2 : \varphi \text{ es morfismo de grupos}\}$

Observación 1.1.6. Sea $\varphi : G_1 \to G_2$ morfismo de grupos.

- φ es inyectiva $\iff \ker \varphi = \{e\}$,
- φ es sobreyectiva $\iff \text{Im } \varphi = G_2$,
- $\varphi(e) = e$,
- $\varphi(a^{-1}) = \varphi(a)^{-1}$, $\forall a \in G_1$; en general $\varphi(a^n) = \varphi(a)^n$, $\forall n \in \mathbb{Z}$,
- La imagen de un subgrupo es un subgrupo, i.e. $H_1 < G_1 \Rightarrow \varphi(H_1) < G_2$. En particular, $\varphi(G_1) = \text{Im } \varphi < G_2$.
- La preimagen de un subgrupo es un subgrupo, i.e. $H_2 < G_2 \Rightarrow \varphi^{-1}(H_2) < G_1$. En particular, $\varphi^{-1}(\{e\}) = \ker \varphi < G_1$.
- Si φ es biyectiva, entonces su inversa $\varphi^{-1} : G_2 \to G_1$ también es un morfismo de grupos.
- La composición de morfismos es un morfismo.
- Es lo mismo dar un subgrupo de G que dar una sucesión exacta[2] de grupos $e \longrightarrow H \longrightarrow G$.

Definición. Sea $\varphi : G_1 \to G_2$ morfismo.

- Si φ es inyectiva, decimos que es un *monomorfismo*.
- Si φ es sobreyectiva, decimos que es un *epimorfismo*.
- Si φ es biyectiva, decimos que es un *isomorfismo*. Si existe un isomorfismo entre dos grupos, diremos que son *isomorfos*.
- Si $\varphi : G \to G$, i.e. si $G_2 = G_1 =: G$ decimos que φ es un *endomorfismo* de G.
- Un endomorfismo de G que es un isomorfismo se dice un *automorfismo* de G.

[2]Remitimos al lector olvidado de sucesiones exactas a 1.7 para un breve repaso.

Observación 1.1.7. Una imagen homomórfica de un grupo G es una impresión más o menos borrosa de algunas propiedades del grupo G. Si el núcleo es trivial entonces la impresión es perfecta. En el otro extremo, si el núcleo es todo G entonces lo único que aprendemos de G a través de su imagen es que tiene un elemento identidad. Por lo tanto estudiar imágenes homomórficas de un grupo es una manera de estudiar al grupo, máxime si estudiamos varias a la vez. Por ejemplo, si sabemos que $\mathbb{Z}_2, \mathbb{Z}_3, \ldots$ (ver ejemplo 5 de 1.1.8) son todos imágenes homomórficas de G entonces G debe ser infinito.

Pasamos ahora a dar algunos ejemplos.

Ejemplo 1.1.8.

1. El *grupo trivial* es el grupo que sólo consiste del neutro. Usamos el artículo definido "el" porque son obviamente todos isomorfos. En general lo notaremos $\{e\}$. Cualquier grupo admite un único morfismo hacia el grupo trivial y desde el grupo trivial: llamaremos a ambos *morfismo trivial* y también los notaremos e.

2. Si G es un grupo, $\{e\}$ y G son subgrupos. Llamamos al primero el *subgrupo trivial*.

3. El *centro* de un grupo G, notado $Z(G)$, consiste de los elementos de G que conmutan con todo G:
$$Z(G) := \{x \in G : xg = gx \ \forall g \in G\}$$
Es un subgrupo conmutativo de G. Un grupo G es abeliano si y sólo si $G = Z(G)$.

4. $(\mathbb{C}, +)$ es un grupo abeliano, y $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ son subgrupos.

5. Los subgrupos de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$, $m \in \mathbb{N}$.

6. $(\mathbb{N}, +)$ es un monoide que no es un grupo, y $(2\mathbb{N}, +)$ es un semigrupo que no es un monoide.

7. Notamos $\mathbb{Z}_n := \frac{\mathbb{Z}}{n\mathbb{Z}}$ a los enteros módulo n: son un grupo abeliano con la suma.
El grupo $\mathbb{Z}_n$ puede verse como el grupo de rotaciones de un n-ágono regular. Analizaremos esto en la observación 1.2.3.

8. El grupo abeliano $\mathbb{Z}_2 \times \mathbb{Z}_2$ se llama 4-*grupo de Klein*, o *Vierergruppe*, y se suele notar $\mathbf{V}$. Es importante observar que $\mathbb{Z}_2 \times \mathbb{Z}_2$ no es isomorfo a $\mathbb{Z}_4$: el primero tiene tres elementos de orden 2 mientras que el segundo tiene un elemento de orden 4. Es un ejercicio sencillo probar que todo grupo de orden 4 es isomorfo a $\mathbb{Z}_4$ o a $\mathbf{V}$ (sólo hay dos tablas de multiplcación posibles).
El 4-grupo de Klein se corresponde con el grupo de reflexiones respecto de tres ejes cartesianos en el espacio.

9. Si R es un anillo (en particular si $R = k$ es un cuerpo), entonces $(R, +)$ es un grupo abeliano, y $(R, \cdot)$ es un monoide.

10. Si k es un cuerpo, $(k\backslash\{0\}, \cdot)$ es un grupo abeliano, que se llama *grupo multiplicativo* de k y denotaremos k^*. El grupo abeliano $(k, +)$ se llama *grupo aditivo* de k.

11. Más en general, si R es un anillo, notamos por R^* al conjunto de elementos invertibles de R (*unidades* del anillo), forman un grupo con el producto.

12. Si R es un anillo y M un R-módulo (en particular, si $R = k$ es un cuerpo y $M = V$ un k-espacio vectorial) entonces $(M, +)$ es un grupo abeliano.

13. Si G es un grupo, sea $\mathrm{End}(G) := \{\varphi : G \to G : \varphi \text{ es endomorfismo}\} \subset \mathrm{Aut}(G) := \{\varphi : G \to G : \varphi \text{ es automorfismo}\}$. Se tiene que, con la composición como operación, $\mathrm{End}(G)$ es un monoide, y $\mathrm{Aut}(G)$ es un grupo (generalmente no abeliano).

14. Si k es un cuerpo, el conjunto $\mathrm{M_n(k)}$ de matrices $n \times n$ es un monoide con la multiplicación. El *submonoide* $\mathrm{GL_n(k)}$ de matrices $n \times n$ invertibles es un grupo, llamado *grupo general lineal*. El determinante, $\det : \mathrm{GL_n(k)} \to \mathrm{k^*}$ toma valores en el grupo multiplicativo del cuerpo, y es un morfismo. Su núcleo $\mathrm{SL_n(k)}$ es el grupo de matrices $n \times n$ con determinante 1, llamado *grupo especial lineal*.

    Es sabido que $Z(\mathrm{GL_n(k)}) = \{\lambda \mathrm{I_n} : \lambda \in \mathrm{k^*}\}$, i.e. las matrices escalares no nulas.

15. Sea X un conjunto. Definimos el *grupo simétrico* de X como el conjunto de biyecciones de X:

$$\mathrm{Sym}(X) := \{f : X \to X : f \text{ es una biyección}\}$$

    Los elementos de $\mathrm{Sym}(X)$ se llaman *permutaciones*. Cuando $X = \{1, \dots, n\}$, $n \geqslant 2$ el grupo simétrico *en n letras* $\mathrm{Sym}(\{1, \dots, n\})$ se nota S_n: tiene orden $n!$. Estudiaremos en profundidad este grupo en la sección 1.10.

16. Sea $n \geqslant 3$. El *grupo diedral* D_n es el grupo de reflexiones y rotaciones de los vértices de un n-ágono regular. Consiste de n rotaciones y n simetrías, y por lo tanto $|D_n| = 2n$ (ver Figura 1.1).

    Sea R una rotación de ángulo $\frac{2\pi}{n}$, y S una simetría. Satisfacen las siguientes relaciones:

$$R^n = e, \qquad S^2 = e, \qquad RSRS = e$$

    Las tres relaciones juntas implican $SR = R^{n-1}S$. Por lo tanto

$$D_n = \{e, R, \dots, R^{n-1}, S, RS, \dots, R^{n-1}S\}$$

    Dijimos que $\mathbb{Z}_n$ podía verse como el grupo de rotaciones de un n-ágono regular. Ahora estamos añadiendo una nueva operación, la de reflexión respecto de un eje (orientado) formado por dos vértices, para cada vértice. Estas reflexiones tienen orden 2. Esto nos lleva a pensar que D_n está formado de alguna manera de $\mathbb{Z}_n$ y de $\mathbb{Z}_2$. Podremos especificar de qué manera cuando estudiemos el producto semidirecto: ver ejercicio 26.

17. Sean $a = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$, $b = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. El *grupo de los cuaterniones* Q es el subgrupo de $\mathrm{GL_2}(\mathbb{C})$ generado por a y b. Estos elemetos satisfacen las siguientes relaciones:

$$a^4 = e, \qquad a^2 = b^2, \qquad bab^{-1} = a^3$$

    La última relación implica $ba = a^3 b$. Por lo tanto

$$Q = \{\mathrm{id}, a, a^2, a^3, b, ab, a^2 b, a^3 b\}$$

    Recordemos que el *anillo de los cuaterniones* $\mathbb{H}$ es $\mathbb{R}^4$ con la suma punto a punto y el producto definido de la siguiente manera: sea $\{1, i, j, k\}$ una base de $\mathbb{R}^4$. Entonces todo

Figura 1.1: Las dieciséis simetrías de D_8

elemento h de $\mathbb{H}$ se escribe como $h = a1 + bi + cj + dk$. El elemento 1 será la identidad de $\mathbb{H}$, entonces $h = a + bi + cj + dk$. Definimos el producto de dos cuaterniones en la base y extendemos por asociatividad. La ecuación

$$i^2 = j^2 = k^2 = ijk = -1$$

determina todos los posibles productos de i, j, k. Queda como ejercicio probar que el *grupo* de los cuaterniones es isomorfo a $\{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$ con el producto.

1.1.1. Teorema fundamental de los grupos abelianos

Recordemos que dar un grupo abeliano "es lo mismo" que dar un $\mathbb{Z}$-módulo, y podemos definir por ejemplo un *grupo abeliano libre* como un $\mathbb{Z}$-módulo libre, i.e. que tiene una base (no hay que confundir esta noción con la de *grupo libre* que estudiaremos más tarde).

Como $\mathbb{Z}$ es un dominio de ideales principales, se aplica el teorema de estructura para módulos finitamente generados:

Teorema 1.1. *Sea G un grupo abeliano finitamente generado. Existe un único $r \in \mathbb{N}$ tal que:*

- *existen únicos $n_1, \dots, n_k$ llamados* factores invariantes *de G tales que*

  $$G \simeq \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

  con $n_1 \geqslant 2$ y $n_1 \mid \cdots \mid n_k$.

- *existe un único $s \in \mathbb{N}$ tal que existen únicos primos $p_1, \dots, p_s$ y naturales $e_1, \dots, e_s$ tales que*

  $$G \simeq \mathbb{Z}^r \times \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}}$$

  Los $p_i^{e_i}$, $i = 1, \dots, s$ son los divisores elementales *de G.*

Ejercicios

Ej. 1 — Un semigrupo G es un grupo si y sólo si :

I. Existe un $e \in G$ tal que $ea = a$ para todo $a \in G$ (neutro por izquierda)

II. Para todo $a \in G$ existe $a^{-1} \in G$ tal que $a^{-1}a = e$ (inversa por izquierda)

Ej. 2 — Si todos los elementos de un grupo son involuciones (i.e. $a^2 = e$ para todo a) entonces el grupo es abeliano.

Ej. 3 — Un grupo no puede ser unión de dos subgrupos propios.

Ej. 4 — Un grupo con sólo un número finito de subgrupos debe ser finito.

Ej. 5 — Si $H, K < G$ entonces $HK := \{hk : h \in H, k \in K\}$ es un subgrupo si y sólo si $HK = KH$.

Ej. 6 — ¿Cuándo es $x \mapsto x^{-1}$ un automorfismo de G?

Ej. 7 — Los axiomas de grupo son independientes. Esto es, existe un conjunto con una operación que satisface una propiedad y no las otras dos, para cualquiera de las tres propiedades de grupo.

1.2. Grupos cíclicos y orden

Definición. Sea G grupo, $a \in G$. El *subgrupo cíclico* generado por a es $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$. Un grupo G es *cíclico* si existe $a \in G$ tal que $G = \langle a \rangle$.

Observación 1.2.1. Un grupo cíclico siempre es abeliano.

Proposición 1.2.
- *La imagen de un grupo cíclico es cíclica.*
- *Un subgrupo de un grupo cíclico es cíclico. Más aún: si $H < \langle a \rangle$, entonces $H = \langle a^m \rangle$ donde $m = \min\{n \in \mathbb{Z}^+ : a^n \in H\}$*

Demostración.
- $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$ pues $\varphi(a)^n = \varphi(a^n)$, $\forall n \in \mathbb{Z}$.
- $H = \langle a^m \rangle$: $(\supset)$ es obvia. $(\subset)$: si $b = a^n \in H$, entonces $n = mq + r$, $0 \leqslant r < m$. Entonces
$$a^n = (a^m)^q a^r \Rightarrow a^r = a^n a^{-mq} \Rightarrow a^r \in H \Rightarrow r = 0$$
por minimalidad de m, luego $n = mq$, por lo tanto $b = a^{mq} = (a^m)^q \Rightarrow b \in \langle a^m \rangle$. □

La siguiente proposición nos dice que si un grupo cíclico es infinito, es isomorfo a $\mathbb{Z}$, y si es finito, es isomorfo a $\mathbb{Z}_m$ para un único $m \geqslant 2$.

Proposición 1.3. *Sea G un grupo cíclico. Si $|G| = \infty$ entonces $G \simeq \mathbb{Z}$; si $|G| = m < \infty$, entonces $G \simeq \mathbb{Z}_m$.*

Demostración. Sea $a \in G$ tal que $G = \langle a \rangle$. Tenemos un epimorfismo $\varphi : \mathbb{Z} \to G$, $k \mapsto a^k$. El núcleo $\ker \varphi$ es un subgrupo de $\mathbb{Z}$, luego:
$\ker \varphi = \{0\} \Rightarrow G \simeq \mathbb{Z}$;
$\ker \varphi \neq \{0\} \Rightarrow \ker \varphi = m\mathbb{Z} \Rightarrow G \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z}_m$.[3] □

Proposición 1.4. *Sea G grupo, $a \in G$. Si $|a| = m < \infty$, entonces:*
- $a^k = e \iff m \mid k$,
- $a^k = a^l \iff k \equiv l$ *(mód m)*,
- $\langle a \rangle = \{e, a, \ldots, a^{m-1}\}$, *en particular* $|\langle a \rangle| = m$,
- $k \mid m \Rightarrow |a^k| = \frac{m}{k}$.

Demostración. La prueba es sencilla y se deja como ejercicio para el lector. □

Corolario 1.5. *Sea $\varphi : G_1 \to G_2$ morfismo de grupos y $a \in G_1$ tal que $|a| < \infty$. Entonces $|\varphi(a)| < \infty$, y $|\varphi(a)| \mid |a|$.*

Demostración. Si $|a| = n < \infty$, entonces
$$e = \varphi(e) = \varphi(a^n) = \varphi(a)^n$$
y por lo tanto $|\varphi(a)| < \infty$ y $|\varphi(a)| \mid n$. □

[3] Hemos usado el *primer teorema de isomorfismo* para grupos abelianos, que ya lo conocemos del curso de Álgebra I. Lo volveremos a ver en breve para grupos no abelianos.

Proposición 1.6.
- *Si* $|\langle a\rangle| = \infty$ *entonces* a *y* a^{-1} *son los únicos generadores de* $\langle a\rangle$.
- *Si* $|\langle a\rangle| = m$, *entonces* a^k *genera* $\langle a\rangle \iff mcd(m,k) = 1$.

Demostración.
- $\langle a\rangle \simeq \mathbb{Z}$ a través del isomorfismo $a^k \mapsto k$. Como 1 y -1 son los únicos generadores de $\mathbb{Z}$ y se corresponden con a y a^{-1}, entonces éstos son los únicos generadores de $\langle a\rangle$.
- $|\langle a\rangle| = m \Rightarrow \langle a\rangle \simeq \mathbb{Z}_m$. Ahora,

$$\begin{aligned} \text{mcd}(m,k) = 1 &\iff \exists\, r,s \in \mathbb{Z} : 1 = mr + ks \iff 1 \equiv sk(\text{mód } m) \\ &\iff \mathbb{Z}_m = \langle 1\rangle < \langle k\rangle < \mathbb{Z}_m \iff \mathbb{Z}_m = \langle k\rangle \\ &\iff \langle a\rangle = \langle a^k\rangle \end{aligned}$$

□

Definición. La *función* φ *de Euler* se define como $\varphi : \mathbb{N} \to \mathbb{N}$,

$$\varphi(m) = |\{0 \leqslant k < m : \text{mcd}(m,k) = 1\}|$$

Observación 1.2.2. Por la proposición anterior, hay $\varphi(n)$ generadores de $\mathbb{Z}_n$.

Definición. Consideremos el *grupo circular* $\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\} < (\mathbb{C}^*, \cdot)$.
Dado $n \in \mathbb{N}$,

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} : z^n = 1\} < \mathbb{T} < \mathbb{C}^*$$

es el grupo de *raíces n-ésimas de la unidad*.

Los generadores de $\mu_n(\mathbb{C})$, i.e. los $e^{\frac{2k\pi i}{n}}$ con $\text{mcd}(n,k) = 1$ son las *raíces primitivas n-ésimas de la unidad*.

Observación 1.2.3.
- $\mu_n(\mathbb{C}) = \langle e^{\frac{2\pi i}{n}}\rangle$. Geométricamente, $\mu_n(\mathbb{C})$ consiste de los vértices de un n-ágono regular inscrito en el círculo unidad.
- $\mu_n(\mathbb{C}) \simeq \mathbb{Z}_n$, a través de $e^{\frac{2k\pi i}{n}} \mapsto k$.[4] En particular hay $\varphi(n)$ raíces n-ésimas primitivas de la unidad.

  Esto nos permite ver $\mathbb{Z}_n$ como el grupo de rotaciones de un n-ágono regular.
- Una raíz n-ésima de la unidad es primitiva si y sólo si no es una raíz m-ésima de la unidad para ningún $0 < m < n$.
- Podemos considerar más en general el grupo $\mu_n(k)$ de raíces n-ésimas de la unidad de un cuerpo k cualquiera; son un subgrupo de k^*.

Ejemplo 1.2.4. El centro de $\text{SL}_n(\text{k})$ son las matrices escalares con determinante 1, por lo tanto, son las matrices escalares con una raíz n-ésima de la unidad en la diagonal: $Z(\text{SL}_n(\text{k})) = \mu_n(\text{k})\text{I}_n$.

El siguiente teorema nos será de utilidad más adelante.

[4] Atención: $\mu_n(\mathbb{C}) < (\mathbb{C}^*, \cdot)$ es multiplicativo mientras que $\mathbb{Z}_n = (\mathbb{Z}_n, +)$ es aditivo.

Teorema 1.7. *Todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico. En particular, el grupo multiplicativo de un cuerpo finito es cíclico.*

Demostración. Sea F un cuerpo y G un subgrupo finito de F^*. En particular G es abeliano finito, por lo tanto por el teorema fundamental de los grupos abelianos, $G \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$, donde $1 < m_1 \mid \cdots \mid m_k$. Entonces todos los elementos de G son raíces del polinomio $X^{m_k} - 1 \in F[X]$ que tiene grado m_k, por lo tanto tiene a lo sumo m_k raíces $\Rightarrow |G| \leqslant m_k$.

Por otro lado $|G| = m_1 \dots m_k$: si fuera $k > 1$ tendríamos $|G| > m_k$, absurdo. Por lo tanto $k = 1$ y $G \simeq \mathbb{Z}_{m_1}$. □

Observación 1.2.5. $(\mathbb{Z}_p)^*$ es cíclico de orden $p - 1$. Es cíclico por el teorema anterior, y es de orden $p - 1$ porque al ser $\mathbb{Z}_p$ un cuerpo, todos sus elementos menos 0 son invertibles.

Ejercicios

Ej. 8 — Si $a, b \in G$ entonces $|a| = |a^{-1}|$, $|ab| = |ba|$, $|a| = |bab^{-1}|$.

Ej. 9 — El producto de elementos de orden finito puede tener orden infinito: considerar $\mathbb{Z}_2 \times \mathbb{Z}$.

Ej. 10 — Un grupo cíclico finito tiene un único subgrupo de orden n para cada n que divide al orden del grupo.

Ej. 11 — Sea G un grupo cíclico, $a, b \in G$ generadores. Existe un automorfismo φ de G tal que $\varphi(a) = b$. Recíprocamente, todo automorfismo de G lleva un generador en otro generador. Deducir que $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}_2$.

Ej. 12 — El producto de elementos de orden finito puede tener orden infinito: considerar $A = \left(\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ y $B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ en $\mathrm{GL}_2(\mathbb{Q})$.

Ej. 13 — El producto de elementos de orden 2 puede tener cualquier orden m (Sugerencia: considerar las matrices del ejercicio anterior en $\mathrm{GL}_2(\mathbb{Z}_m)$).

Ej. 14 — En un grupo finito no trivial G, si todos los elementos (salvo el neutro) tienen el mismo orden entonces $|G|$ es primo.

Ej. 15 — En un grupo abeliano el producto de elementos de orden finito tiene orden finito.

Ej. 16 — En $(\mathbb{Z}_p)^*$ el producto de dos elementos que no son cuadrados es un cuadrado.

Ej. 17 — Si dos elementos conmutan y tienen orden coprimo, entonces el producto de los elementos tiene orden el producto de los órdenes. Recíprocamente, si $g \in G$ tiene orden n y $n = n_1 n_2$ con $\mathrm{mcd}(n_1, n_2) = 1$ entonces existe una única descomposición $g = g_1 g_2$ con $|g_1| = n_1$, $|g_2| = n_2$, y tal que g_1 y g_2 conmutan.

Ej. 18 — Si a, b conmutan entonces G tiene un elemento de orden $\mathrm{mcm}(|a|, |b|)$. (Sugerencia: probarlo primero para el caso $\mathrm{mcd}(|a|, |b|) = 1$, en cuyo caso el elemento buscado es

el producto ab.) En particular, si G es un grupo abeliano finito entonces el orden de todo elemento divide al elemento de orden maximal en G.

Ej. 19 — Si G es un grupo abeliano finito con a lo sumo un subgrupo de cada orden, entonces es cíclico. (El resultado vale para cualquier grupo finito, pero la prueba es más complicada).

Ej. 20 — Un grupo infinito es cíclico si y sólo si es isomorfo a todo subgrupo propio.

1.3. Coclases y normalidad

Definición. Sea G grupo, $H < G$. Definimos las relaciones binarias en G de *congruencia a derecha módulo H* y *congruencia a izquierda módulo H*, notadas respectivamente $\equiv_r$ y $\equiv_l$, tales que para todo $a, b \in G$:

$$a \equiv_r b \text{ (mód } H) \text{ si } ab^{-1} \in H \qquad\qquad a \equiv_l b \text{ (mód } H) \text{ si } a^{-1}b \in H$$

Observación 1.3.1. Una manera sencilla de acordarse cuál es la derecha y cuál es la izquierda es recordando que es la indicación del lado de la congruencia del que queda la identidad, i.e. $a \equiv_r b \iff ab^{-1} \equiv e$, $a \equiv_l b \iff e \equiv a^{-1}b$.

Proposición 1.8. *Sea G grupo, $H < G$, $a \in G$.*

- *Las relaciones $\equiv_r$ (mód H) y $\equiv_l$ (mód H) son de equivalencia.*
- *La clase de equivalencia de a bajo $\equiv_r$ (mód H) es $Ha := \{ha : h \in H\}$ y se llama* coclase derecha de a.

  La clase de equivalencia de a bajo $\equiv_l$ (mód H) es $aH := \{ah : h \in H\}$ y se llama coclase izquierda de a.
- $|Ha| = |H| = |aH|$.

Demostración. Lo demostramos para $\equiv_r$, para $\equiv_l$ es análogo.

- Reflexiva: $a \equiv_r a$ pues $aa^{-1} = e \in H$.

  Simétrica: $a \equiv_r b \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H \Rightarrow b \equiv_r a$.

  Transitiva: $a \equiv_r b, b \equiv_r c \Rightarrow ab^{-1}, bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} = ac^{-1} \in H \Rightarrow a \equiv_r c$.
- La clase de equivalencia de a es

$$\begin{aligned}\{x \in G : x \equiv_r a\} &= \{x \in G : xa^{-1} \in H\} = \{x \in G : xa^{-1} = h \text{ para cierto } h \in H\} \\ &= \{x \in G : x = ha \text{ para cierto } h \in H\} = Ha\end{aligned}$$

- El mapa $Ha \to H$, $ha \mapsto h$ es una biyección. □

Observación 1.3.2. Las coclases de H en G no son generalmente subgrupos de G. La coclase de la identidad, H, siempre es un subgrupo de G. Las otras coclases pueden pensarse como *trasladados* del subgrupo.

Notación. Si el grupo es abeliano, la coclase izquierda de a se suele notar $a + H$, y la coclase derecha $H + a$.

Ejemplo 1.3.3.

- En $\mathbb{Z}$, si consideramos el subgrupo $3\mathbb{Z}$, tenemos tres coclases izquierdas: $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, $2 + 3\mathbb{Z}$.
- Un ejemplo más geométrico: consideramos $G = \mathbb{R}^2$, y $H = \mathbb{R}e_1$ el eje x. La coclase izquierda módulo H de un punto $p \in \mathbb{R}^2$ es

  $$p + \mathbb{R}e_1 = \{p + \alpha e_1 : \alpha \in \mathbb{R}\}$$

  Las coclases son pues las rectas paralelas al eje x. Observar que las únicas que son subgrupos son las que corresponden a puntos p de la forma $p = (x, 0)$.

- La solución general de una ecuación lineal $Ax = b$ no homogénea es de la forma: una solución particular más la solución general de la ecuación homogénea $Ax = 0$. Las soluciones de la ecuación $Ax = b$ se pueden ver como coclases, de esta manera:

  Sea $V = \{x \in \mathbb{R}^n : Ax = 0\}$, es un grupo con la suma. Si $b \neq 0$, si la ecuación $Ax = b$ tiene una solución x_0, entonces el conjunto de soluciones de $Ax = b$ es la coclase $x_0 + V$. En efecto,

$$Ax = b \iff Ax = Ax_0 \iff A(x - x_0) = 0 \iff x - x_0 \in V \iff x \in x_0 + V$$

Corolario 1.9.

- $Ha = Hb \iff ab^{-1} \in H, \quad aH = bH \iff a^{-1}b \in H.$
- *Dos coclases del mismo lado son disjuntas o iguales.*
- $|\{\text{coclases izquierdas de } H \text{ en } G\}| = |\{\text{coclases derechas de } H \text{ en } G\}|$, *mediante la biyección* $Ha \mapsto a^{-1}H$.

Definición. Sea G grupo, $H < G$. El *índice* de H en G es el número de coclases izquierdas diferentes de H en G. Lo notamos $|G : H|$.

Observación 1.3.4.

- Por el corolario anterior, $|G : H|$ también es igual al número de coclases *derechas* diferentes de H en G.
- $|G : \{e\}| = |G|$.
- $|G : H| = 1 \iff H = G$.

Teorema 1.10 (Transitividad de índices)**.** *Sea G grupo. Si $K < H < G$, entonces*

$$|G : K| = |G : H||H : K|$$

Demostración. Escribamos[5] $G = \bigsqcup_{i \in I} Ha_i, \quad H = \bigsqcup_{j \in J} Kb_j$. Se tiene entonces:

$$G = \bigsqcup_{i \in I} \left(\bigsqcup_{j \in J} Kb_j \right) a_i = \bigcup_{(i,j) \in I \times J} Kb_j a_i$$

Basta probar que esta última unión es disjunta, pues entonces

$$|G : K| = |I \times J| = |I||J| = |G : H||H : K|$$

Probemos que la unión es disjunta:

$$Kb_j a_i = Kb_r a_t \Rightarrow b_j a_i = k b_r a_t \Rightarrow H \overbrace{b_j}^{\in H} a_i = H \overbrace{k b_r}^{\in H} a_t \Rightarrow Ha_i = Ha_t \Rightarrow i = t$$

$$\Rightarrow b_j = k b_r \Rightarrow Kb_j = K \overbrace{k}^{\in K} b_r \Rightarrow Kb_j = Kb_r \Rightarrow j = r \qquad \square$$

Corolario 1.11. (Teorema de Lagrange). *Sea G grupo.*

[5] Usaremos el símbolo $\sqcup$ para notar una unión que es disjunta.

- *Si $H < G$, entonces $|G| = |G : H||H|$. En particular, si G es finito, $|G : H| = \frac{|G|}{|H|}$.*
- *Si G es finito entonces $|a| \mid |G|$, para todo $a \in G$. Equivalentemente, $a^{|G|} = e$ para todo $a \in G$.*

Demostración.
- $\{e\} < H < G \Rightarrow |G : \{e\}| = |G : H||H : \{e\}| \Rightarrow |G| = |G : H||H|$.
- $\{e\} < \langle a \rangle < G \Rightarrow |G| = |G : \langle a \rangle||\langle a \rangle| \Rightarrow |a| \mid |G|$. Esto es equivalente con $a^{|G|} = e$ para todo $a \in G$ por la proposición 1.4.

□

Observación 1.3.5.
- La primera parte del teorema de Lagrange, i.e. el orden del grupo es el producto del índice y el orden de un subgrupo, se puede probar directamente con un sencillo argumento de conteo: el índice $|G : H|$ es la cantidad de coclases de H en G, que forman una partición de G y son todas de orden $|H|$, de donde $|G| = |G : H||H|$.

  Además, nos dice que $|H| \mid |G|$, y $|G : H| \mid |G|$, resultado que usaremos a menudo.
- Si $H < G$, entonces $|H| \mid |G|$, pero el recíproco es falso. Esto es, si $n \mid |G|$, no necesariamente existe un subgrupo de G de orden n (los grupos que cumplen esto se dicen *Lagrangianos*). Daremos un ejemplo más adelante, en 1.68 (o en 1.72).
- El teorema de Lagrange nos dice que el orden y el índice de un subgrupo son "recíprocos" en $|G|$: a mayor orden, menor índice, y viceversa.

Corolario 1.12. *Si G tiene orden p entonces es cíclico y cualquier elemento no trivial es un generador de orden p.*

Demostración. Por Lagrange todo elemento no trivial g tiene orden p. Entonces $|\langle g \rangle| = p$, luego $\langle g \rangle = G$. □

Observación 1.3.6. No es cierto que si todo elemento no trivial tiene orden p entonces el grupo es cíclico, tomar por ejemplo $\mathbb{Z}_p \times \mathbb{Z}_p$ (no tiene elementos de orden p^2).

Corolario 1.13. *Dos subgrupos de orden primo p diferentes se intersectan trivialmente.*

Demostración. Sean $H, K < G$, $H \neq K$, $|H| = |K| = p$. Si $x \in H \cap K$, entonces $|x| \mid p$. Si $|x|$ fuera p, entonces $H = K$ pues $x \in H$, $x \in K$, y cualquier elemento de orden p en un grupo de orden p genera el grupo. Por lo tanto $|x| = 1$ y $x = e$. □

Corolario 1.14 (Teorema de Fermat)**.** *Si p es primo y $a \not\equiv 0$ (mód p), entonces $a^{p-1} \equiv 1$ (mód p).*

Demostración. Tomemos $G = (\mathbb{Z}_p)^*$. Si $a \in G$ entonces como $|G| = p - 1$, por Lagrange se tiene $a^{p-1} = 1$ en $(\mathbb{Z}_p)^*$, i.e. $a^{p-1} \equiv 1$ (mód p). □

Corolario 1.15 (Teorema de Euler)**.** *Si a es coprimo con m entonces $a^{\varphi(m)} \equiv 1$ (mód m).*

Demostración. Tomemos $G = (\mathbb{Z}_m)^*$. Si a es coprimo con m entonces $a \in G$. Como $|G| = \varphi(m)$, por Lagrange se tiene $a^{\varphi(m)} = 1$ en $(\mathbb{Z}_m)^*$, i.e. $a^{\varphi(m)} \equiv 1$ (mód m). □

Corolario 1.16. *Sean H, K subgrupos finitos de un grupo dado. Si $mcd(|H|, |K|) = 1$, entonces $H \cap K = \{e\}$ y $\mathrm{Hom}(H, K) = \{e\}$. En particular, si $mcd(m, n) = 1$ entonces $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) = \{0\}$.*

Demostración. Si $x \in H \cap K$, entonces por Lagrange $|x| \mid |H|$ y $|x| \mid |K|$ que son coprimos, luego $|x| = 1$ y $x = e$.

Sea $\varphi : H \to K$, $a \in H$. Entonces $|\varphi(a)| \mid |K|$ por el teorema de Lagrange. Además, por el corolario 1.5, $|\varphi(a)| \mid |a| \mid |H|$ de nuevo por Lagrange, luego $|\varphi(a)| \mid |H|$ y $|\varphi(a)| \mid |K|$: como $\mathrm{mcd}(|H|, |K|) = 1$ entonces $|\varphi(a)| = 1$ para todo $a \in H$, luego φ es el morfismo trivial. □

Proposición 1.17. *Sea G grupo, $N < G$. Son equivalentes:*

I. *$\equiv_l$ (mód N) y $\equiv_r$ (mód N) definen la misma relación de equivalencia en G, llamada* congruencia módulo N,

II. *Toda coclase izquierda de N en G es una coclase derecha de N en G,*

III. $aN = Na \ \forall a \in G$,

IV. $aNa^{-1} \subset N \ \forall a \in G$,

V. $aNa^{-1} = N \ \forall a \in G$.

Demostración. Se deja como sencillo ejercicio para el lector. □

Definición. Sea G grupo, $N < G$. Decimos que N es *normal* en G, y lo notamos $N \lhd G$, si satisface la proposición anterior. Un grupo es *simple* si no tiene subgrupos normales propios.

El siguiente resultado nos dice que si tenemos un subgrupo propio "lo más grande posible" (de índice 2) entonces debe ser normal. Generalizaremos este resultado en la proposición 1.55.

Proposición 1.18. *Todo subgrupo de índice 2 es normal.*

Demostración. Sea $N < G$, $|G : N| = 2$. Sea $g \in G \backslash N$. Entonces $G = N \sqcup gN$, y gN es el complemento de N en G. También es $G = N \sqcup Ng$, luego Ng también es el complemento de N en G, por lo tanto $Ng = gN$ para todo $g \in G \backslash N$ y trivialmente para todo $g \in N$, por lo tanto N es normal en G. □

Observación 1.3.7.

- Sean $N < H < G$. Si $N \lhd G$ entonces $N \lhd H$, pero puede pasar $N \lhd H \lhd G$ sin que $N \lhd G$. Consideremos $G = D_4$, con R y S como en el ejemplo 16 de 1.1.8. Sea
$$H = \langle RS, SR \rangle = \{e, RS, R^2, SR\} \simeq \mathbf{V}$$
$H \lhd G$ pues $|G : H| = 2$. Sea ahora $K = \langle RS \rangle = \{1, RS\}$. Ahora, $K \lhd H$, pues $|H : K| = 2$. Tenemos $K \lhd H \lhd G$, pero $K \not\lhd G$. En efecto, como $S^2 = e$ entonces $S = S^{-1}$, luego
$$S^{-1} \circ RS \circ S = S \circ RS \circ S^{-1} = SR \notin K$$

- La definición de grupo simple sugiere que no todo subgrupo es normal, y esto lo vimos efectivamente en el ítem anterior. En general, hay muchos subgrupos (cualquier elemento de un grupo genera un subgrupo), pero no así subgrupos normales.

- Si G es abeliano, todo subgrupo es normal (trivialmente es $aN = Na$ para todo $a \in G$). En particular, los únicos grupos abelianos simples son el trivial y los grupos cíclicos de orden primo.

- En un grupo abeliano todo subgrupo es normal, pero el recíproco *no* vale. Existen grupos, llamados *Hamiltonianos*, que no son abelianos pero todo subgrupo es normal. Un ejemplo es el del grupo de los cuaterniones (ver ejemplo 17 de 1.1.8). Está generado por dos elementos de orden 4: a y b. Luego $|Q : \langle a \rangle| = |Q : \langle b \rangle| = 2$ y por lo tanto $\langle a \rangle$ y $\langle b \rangle$ son normales en Q. Tenemos sólo otro subgrupo no trivial, que es $\langle a^2 \rangle = \{\mathrm{id}, a^2\}$, y es fácil verificar a mano que es normal en Q.

Proposición 1.19. *Sea G grupo, $N \lhd G$, y $G/N = \{aN : a \in G\}$ el conjunto cociente de la relación de congruencia módulo N. Entonces la operación $aN \cdot bN := (ab)N$ dota a G/N de una estructura de grupo, que llamamos* grupo cociente*, tal que la aplicación canónica $\pi : G \to G/N$ es un epimorfismo de grupos.*

Demostración. Lo único que no es trivial de verificar es que la operación está bien definida. Supongamos que $aN = a'N$ y $bN = b'N$, veamos que $(ab)N = (a'b')N$.

$$(ab)N = \{abn : n \in N\} \overset{bN=b'N}{=} \{ab'n : n \in N\} \overset{N\lhd G}{=} \{an'b' : n' \in N\} \overset{aN=a'N}{=} \{a'n'b' : n' \in N\}$$
$$\overset{N\lhd G}{=} \{a'b'n'' : n'' \in N\} = (a'b')N$$ □

Observación 1.3.8. Hay tantos elementos del grupo cociente como hay coclases, por lo tanto $|G/N| = |G : N|$.

Corolario 1.20. *Si $\varphi : G_1 \to G_2$ es morfismo de grupos, entonces* $\ker \varphi \lhd G_1$*. Recíprocamente, todo subgrupo normal es el núcleo de un homomorfismo.*

Demostración. Ya sabemos que $\ker \varphi < G_1$. Es normal: sea $a \in \ker \varphi$, $g \in G_1$:

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e \Rightarrow gag^{-1} \in \ker \varphi$$

Recíprocamente, si $N \lhd G$, entonces $N = \ker \pi$, siendo $\pi : G \to G/N$ la aplicación canónica. □

Ejemplo 1.3.9. $\mathrm{SL_n(k)} \lhd \mathrm{GL_n(k)}$, pues $\mathrm{SL_n(k)} = \ker \det$, donde $\det: \mathrm{GL_n(k)} \to \mathrm{k^*}$ es el determinante. El primer teorema de isomorfismo (ver teorema 1.23) nos da un isomorfismo $\mathrm{GL_n(k)/SL_n(k)} \simeq \mathrm{k^*}$.

Definimos el *grupo general lineal proyectivo* como $\mathrm{PGL_n(k)} := \mathrm{GL_n(k)/Z(GL_n(k))}$, y el *grupo especial lineal proyectivo* como $\mathrm{PSL_n(k)} := \mathrm{SL_n(k)/Z(SL_n(k))}$.

Observación 1.3.10. "Es lo mismo" dar:

1. Un subgrupo normal de G,
2. Un grupo cociente de G,
3. Una sucesión exacta corta de grupos con G en medio,
4. Un epimorfismo desde G.

En efecto, si tenemos $N \lhd G$, o G/N grupo, tenemos una sucesión exacta

$$e \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \longrightarrow e$$

y si la sucesión

$$e \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow e$$

es exacta entonces $N \simeq i(N) = \ker p \lhd G$, y $Q \simeq G/\ker p \simeq G/N$.

Por otro lado, si tenemos un epimorfismo $G \xrightarrow{p} Q \longrightarrow e$ entonces lo podemos completar a una sucesión exacta corta de grupos

$$e \longrightarrow \ker p \longrightarrow G \xrightarrow{p} Q \longrightarrow e$$

Observar que todo esto *no* es lo mismo que dar un monomorfismo desde G, pues si bien los núcleos son siempre normales, las imágenes no. Es decir, así como completamos la sucesión anterior con un núcleo, podríamos pensar en completar la sucesión exacta $e \longrightarrow H \xrightarrow{i} G$ con el *conúcleo*, i.e. en formar la sucesión exacta corta $e \longrightarrow H \xrightarrow{i} G \xrightarrow{\tilde{p}} G/\mathrm{Im}\ p \longrightarrow e$, pero $G/\mathrm{Im}\ p$ no tiene por qué ser un grupo.

Proposición 1.21. *Sea G grupo, $H, N < G$. Si $N \lhd G$ entonces $HN := \{hn \in G : h \in H, n \in N\} < G$. Si también $H \lhd G$, entonces $HN \lhd G$.*

Demostración. Obviamente $e \in HN$. Además:

$$\begin{aligned}(hn)(h'n') &= h(nh')n' \overset{Nh'=h'N}{=} hh'n''n' \in HN \\ (hn)^{-1} &= n^{-1}h^{-1} \overset{Nh^{-1}=h^{-1}N}{=} h^{-1}n' \in HN\end{aligned}$$

Por lo tanto $HN < G$. Si además $H \lhd G$, entonces

$$gHNg^{-1} = gH\overbrace{g^{-1}g}^{=e}Ng^{-1} = HN$$

de donde $HN \lhd G$. □

Cerramos la sección con una discusión sobre cocientes en general. Los detalles quedan a cargo del lector.

Definición. Una relación de equivalencia $\sim$ en un grupo G es una *congruencia* si es compatible con el producto, i.e. si

$$a \sim b, a' \sim b' \Rightarrow aa' \sim bb'$$

De esta manera, el producto de dos clases de congruencia es de nuevo una clase de congruencia. El conjunto cociente $G/_\sim$ es un grupo bajo multiplicación de clases. Observemos que las congruencias en un grupo G están en biyección con los subgrupos normales de G. En efecto, si $N \lhd G$ entonces $a \sim b \iff a^{-1}b \in N$ es una congruencia cuyas clases de congruencia son las coclases de N en G. Recíprocamente, si $\sim$ es una congruencia en G, entonces el conjunto N de elementos congruentes a la identidad es un subgrupo normal de G; sus coclases son las clases de congruencia. De esta manera si $\sim$ y N se corresponden

por la biyección, generan mismos grupos cociente, i.e. el grupo $G/_\sim$ y el grupo G/N son iguales.

Lo interesante de esta discusión es que el concepto de congruencia es fácilmente generalizable a otras estructuras algebraicas (una relación de equivalencia compatible con la (o las) operación (u operaciones)), mientras que la de subgrupo normal no tan fácilmente. Por lo tanto si queremos averiguar por qué tipo de subconjuntos podemos cocientar, tenemos que poder describir al conjunto de elementos congruentes a la identidad, dada cualquier congruencia en el objeto. Queda como ejercicio para el lector el descubrir de esta manera que los subconjuntos por los que podemos cocientar un anillo son los ideales bilaterales.

1.3.1. Teoremas de isomorfismo

Enunciamos ahora los clásicos *teoremas de isomorfismo* sin demostración pues se trata de los mismos argumentos que ya usamos para espacios vectoriales, módulos, anillos, grupos abelianos...

Proposición 1.22 (Propiedad universal del cociente)**.** *Sea $\varphi : G \to H$ morfismo de grupos, $N \lhd G$ tal que $N \subset \ker \varphi$. Entonces φ pasa al cociente de manera única, esto es, existe un único morfismo $\tilde{\varphi} : G/N \to H$ tal que el siguiente diagrama conmuta:*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi}\downarrow & \nearrow_{\tilde{\varphi}} & \\ G/N & & \end{array}$$

Corolario 1.23 (Primer teorema de isomorfismo)**.** *Sea $\varphi : G \to H$ morfismo de grupos. Entonces φ induce un isomorfismo*

$$G/\ker \varphi \simeq \operatorname{Im} \varphi$$

Corolario 1.24. *Sea $\varphi : G_1 \to G_2$ morfismo de grupos, $N_1 \lhd G_1$, $N_2 \lhd G_2$ tales que $\varphi(N_1) < N_2$. Entonces existe un único morfismo $\tilde{\varphi}$ tal que el siguiente diagrama conmnuta:*

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ {\scriptstyle\pi_1}\downarrow & & \downarrow{\scriptstyle\pi_2} \\ G_1/N_1 & \xrightarrow[\tilde{\varphi}]{} & G_2/N_2 \end{array}$$

Corolario 1.25 (Segundo teorema de isomorfismo)**.** *Sea G grupo, $N \lhd G$, $H < G$. Entonces $N \lhd HN$, $H \cap N \lhd H$ y*

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}$$

Corolario 1.26 (Tercer teorema de isomorfismo)**.** *Sea G grupo, $M < N < G$ tales que $N \lhd G$, $M \lhd G$. Entonces $N/M \lhd G/M$ y*

$$\frac{G/M}{N/M} \simeq \frac{G}{N}$$

Teorema 1.27 (de correspondencia)**.** *Si $N \lhd G$, entonces hay una biyección entre los subgrupos de G que contienen a N y los subgrupos del cociente G/N:*

$$\{\text{subgrupos de } G \text{ que contienen a } N\} \underset{H \hookleftarrow H/N}{\overset{H \mapsto H/N}{\longleftrightarrow}} \{\text{subgrupos de } G/N\}$$

Todo subgrupo de G/N es de la forma H/N donde $N < H < G$. Además

$$H/N \lhd G/N \iff H \lhd G$$

y si H, K son subgrupos de G que contienen a N, entonces $H/N \subset K/N$ si y sólo si $H \subset K$, y en este caso

$$|K/N : H/N| = |K : H|$$

Ejercicios

Ej. 21 — Q y D_4 no son isomorfos. (Sugerencia: D_4 tiene 5 elementos de orden 2, mientras que Q tiene sólo uno.)

Ej. 22 — Sean $H, K < G$.

1. Existe $\varphi : H/H \cap K \to G/K$ inyectiva, y por lo tanto $|H : H \cap K| \leqslant |G : K|$.
2. Si $|G : K| < \infty$ entonces $|H : H \cap K| = |G : K| \Leftrightarrow G = HK$.

Ej. 23 — Sean $H, K < G$ de índice finito.

1. $|G : H \cap K| < \infty$ y $|G : H \cap K| \leqslant |G : H||G : K|$.
2. $|G : H \cap K| = |G : H||G : K|$ si y sólo si $G = HK$.

Ej. 24 — Si $H, K < G$ tales que $|G : H|$ y $|G : K|$ son finitos y coprimos, entonces $G = HK$.

Ej. 25 — Si $H \lhd G$ es tal que H y G/H son finitamente generados, entonces G es finitamente generado.

1.4. Producto directo

Dados dos grupos, veamos una primera manera de juntarlos para formar otro grupo.

Definición. Sean $G_1, \dots, G_k$ grupos. Definimos el *producto directo externo* de $G_1, \dots, G_k$ como el conjunto $G_1 \times \cdots \times G_k$ con la operación

$$(g_1, \dots, g_k)(g_1', \dots, g_k') = (g_1 g_1', \dots, g_k g_k')$$

Observación 1.4.1. Pongamos $k = 2$ por simplicidad. En $G_1 \times G_2$, las inyecciones $G_1 \to G_1 \times G_2$, $g_1 \mapsto (g_1, e)$ y $G_2 \to G_1 \times G_2$, $g_2 \mapsto (e, g_2)$ nos dan copias $\tilde{G_1}, \tilde{G_2} < G_1 \times G_2$ de G_1 y G_2 en $G_1 \times G_2$, que a menudo identificaremos con los originales, escribiendo $G_1, G_2 \subset G_1 \times G_2$. Además los elementos de estas copias conmutan entre ellos, la intersección de las copias es la identidad y $G_1 \times G_2 = \tilde{G_1}\tilde{G_2}$. Estas tres condiciones son necesarias y suficientes para que un grupo *sea un producto directo interno*, como veremos en la proposición 1.28.

Recién vimos cómo a partir de k grupos construir uno nuevo. Ahora hagámonos la pregunta inversa y veamos cuándo un grupo nos viene dado como producto directo de k subgrupos.

Definición. Sea G grupo, $H_1, \dots, H_k < G$. Decimos que G es *producto directo interno* de $H_1, \dots, H_k$ si el mapa

$$\varphi : H_1 \times \cdots \times H_k \to G, (h_1, \dots, h_k) \mapsto h_1 \cdots h_k$$

es un isomorfismo de grupos. En particular G es isomorfo al producto directo externo de $H_1, \dots, H_k$.

Observación 1.4.2. Una reformulación de la definición es la siguiente: G es producto directo interno de $H_1, \dots, H_k$ si y sólo si todo $g \in G$ se escribe de manera única como $g = h_1 \cdots h_k$ y además si $g = h_1 \cdots h_k$ y $g' = h_1' \cdots h_k'$ entonces $gg' = (h_1 h_1') \cdots (h_k h_k')$.

Proposición 1.28. *G es producto directo interno de H_1 y H_2 si y sólo si:*

- $G = H_1 H_2$,
- $H_1 \cap H_2 = \{e\}$,
- *todo elemento de H_1 conmuta con todo elemento de H_2.*

Demostración. ($\Rightarrow$) a) pues φ es sobreyectiva.
b) si $h \in H_1 \cap H_2$, entonces $\varphi(h, h^{-1}) = e$ y como φ es inyectiva entonces $h = e$.
c) Si $h_1 \in H_1$, $h_2 \in H_2$ entonces

$$h_1 h_2 = \varphi(h_1, h_2) = \varphi((h_1, e)(e, h_2)) = \varphi((e, h_2)(h_1, e)) = h_2 h_1$$

($\Leftarrow$) φ es morfismo:

$$\varphi((h_1, h_2)(h_1', h_2')) = \varphi(h_1 h_1', h_2 h_2') = h_1 h_1' h_2 h_2' \overset{c)}{=} h_1 h_2 h_1' h_2' = \varphi(h_1, h_2)\varphi(h_1', h_2')$$

Es sobreyectivo por a), y es inyectivo:

$$\varphi(h_1, h_2) = h_1 h_2 = e \Rightarrow h_1 = h_2^{-1} \in H_1 \cap H_2 \overset{b)}{=} \{e\} \Rightarrow h_1 = h_2 = e$$

□

Proposición 1.29. *G es producto directo interno de H_1 y H_2 si y sólo si:*

- $G = H_1H_2$,
- $H_1 \cap H_2 = \{e\}$,
- $H_1, H_2 \lhd G$.

No estamos diciendo que la propiedad c) de esta proposición y de la anterior sean equivalentes en general: lo son en la presencia de a) y b).

Demostración. ($\Rightarrow$) En virtud de la proposición anterior, resta verificar el tercer ítem. Sea $g \in G, h \in H_1$. Como $G = H_1H_2$, existen $h_1 \in H_1, h_2 \in H_2$ tales que $g = h_1h_2$. Entonces:

$$ghg^{-1} = h_1h_2hh_2^{-1}h_1^{-1} = h_1hh_1^{-1} \in H_1$$

ya que los elementos de H_1 conmutan con aquellos de H_2. Entonces $H_1 \lhd G$. Análogamente $H_2 \lhd G$.

($\Leftarrow$) $h_1h_2 = h_2h_1 \iff h_1h_2h_1^{-1}h_2^{-1} = e$, pero

$$h_1h_2h_1^{-1}h_2^{-1} \overset{H_1 \lhd G}{=} h_1 \overbrace{(h_2h_1^{-1}h_2^{-1})}^{\in H_1} \overset{H_2 \lhd G}{=} \overbrace{(h_1h_2h_1^{-1})}^{\in H_2} h_2^{-1} \in H_1 \cap H_2 = \{e\} \qquad \square$$

Enunciamos ahora sin demostración (pues es una sencilla aplicación de las dos proposiciones anteriores y un poco de inducción) los criterios análogos para más cantidad de subgrupos.

Proposición 1.30. *G es producto directo interno de $H_1, \ldots, H_k$ si y sólo si:*

- $G = H_1 \ldots H_k$
- *Para cada $i = 1, \ldots, k$ se tiene $H_i \cap (H_1 \ldots H_{i-1}H_{i+1} \ldots H_k) = \{e\}$,*
- *Todo elemento de H_i conmuta con todo elemento de H_j, $\forall i, j = 1, \ldots, k$, con $i \neq j$.*

Proposición 1.31. *G es producto directo interno de $H_1, \ldots, H_k$ si y sólo si:*

- $G = H_1 \ldots H_k$
- *Para cada $i = 1, \ldots, k$ se tiene $H_i \cap (H_1 \ldots H_{i-1}H_{i+1} \ldots H_k) = \{e\}$,*
- $H_1, \ldots, H_k \lhd G$.

1.5. Automorfismos

Definición. Sea G grupo, $g \in G$. El mapa $i_g : G \to G$, $x \mapsto gxg^{-1}$ se llama *conjugación por* g. Es un automorfismo, y todo automorfismo de esta forma se dice *interno*. Notamos $\mathrm{Inn}(G)$ al conjunto de automorfismos internos de G. Si un automorfismo no es interno, se dice *externo*.

De esta manera, un subgrupo es normal si y sólo si queda invariante por conjugación.

Proposición 1.32. *Sea G grupo. Se tiene que $\varphi : G \to Aut(G)$, $g \mapsto i_g$ es un morfismo de grupos, cuyo núcleo es $Z(G)$ y su imagen $Inn(G)$. Por lo tanto $Z(G) \lhd G$, $Inn(G) < Aut(G)$ y*

$$\frac{G}{Z(G)} \simeq Inn(G)$$

Además $Inn(G) \lhd Aut(G)$.

Demostración. φ es morfismo:

$$\begin{aligned}\varphi(gg')(x) = i_{gg'}(x) = gg'x(gg')^{-1} = gg'xg'^{-1}g^{-1} \\ = gi_{g'}(x)g^{-1} = i_g \circ i_{g'}(x) = \varphi(g)\varphi(g')(x)\end{aligned}$$

para todo $x \in G$, luego $\varphi(gg') = \varphi(g)\varphi(g')$.

$\ker \varphi = Z(G)$:

$$\begin{aligned}g \in \ker \varphi &\iff i_g = \mathrm{id} \iff i_g(x) = x \quad \forall x \in G \\ &\iff gxg^{-1} = x \quad \forall x \in G \iff gx = xg \quad \forall x \in G\end{aligned}$$

Además $\mathrm{Im}\ \varphi = \mathrm{Inn}(G)$ por definición, y el primer teorema de isomorfismo da el isomorfismo buscado.

$\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$:

$$(\alpha \circ i_g \circ \alpha^{-1})(x) = \alpha(g\alpha^{-1}(x)g^{-1}) = \alpha(g)x\alpha(g^{-1}) = i_{\alpha(g)}(x) \qquad \square$$

Observación 1.5.1. La proposición anterior nos dice, intuitivamente, que la cantidad de automorfismos internos que tiene un grupo es una "medida" de cuán lejos está el grupo de ser abeliano. En un grupo abeliano todos los automorfismos (salvo la identidad) son externos.

Definición. Un grupo G es *completo* si $\varphi : G \to \mathrm{Aut}(G)$, $g \mapsto i_g$ es un isomorfismo.

Corolario 1.33. *Un grupo es completo si y sólo si su centro es trivial y todos sus automorfismos son internos. En particular, un grupo completo G cumple $Aut(G) \simeq G$.*

Calculemos el grupo de automorfismos de $\mathbb{Z}_n$.

Teorema 1.34. *$Aut(\mathbb{Z}_n) \simeq (\mathbb{Z}_n)^*$.*

Demostración. Escribamos $\mathbb{Z}_n = \langle a \rangle$. Si $\phi \in \mathrm{Aut}(\mathbb{Z}_n)$, entonces $\phi(a) = a^m$ para cierto $m \in \mathbb{Z}$ (único módulo n), y esto define completamente ϕ, que notamos ψ_m.

ψ_m es un automorfismo, entonces lleva generadores en generadores, por lo tanto a^m genera $\mathbb{Z}_n$ y por lo tanto $\text{mcd}(m,n) = 1$. Como $(\mathbb{Z}_n)^* = \{m \in \mathbb{Z}_n : \text{mcd}(m,n) = 1\}$ tenemos bien definido

$$\psi : \text{Aut}(\mathbb{Z}_n) \to (\mathbb{Z}_n)^*, \quad \psi_m \mapsto m$$

Es obviamente inyectivo, y es sobreyectivo pues para cada m coprimo con n, ψ_m es un automorfismo. Además es un morfismo:

$$(\psi_m \circ \psi_r)(a) = \psi_m(a^r) = (a^r)^m = a^{mr} = \psi_{mr}(a)$$

por lo tanto $\psi(\psi_m \circ \psi_r) = \psi(\psi_{mr}) = mr = \psi(\psi_m)\psi(\psi_r)$. Entonces ψ es el isomorfismo buscado. □

Teorema 1.35. *Si $n = p_1^{r_1} \dots p_s^{r_s}$ es la descomposición en primos de n, entonces*

$$(\mathbb{Z}_n)^* \simeq (\mathbb{Z}_{p_1^{r_1}})^* \times \cdots \times (\mathbb{Z}_{p_s^{r_s}})^*, \ y\ (\mathbb{Z}_{p^r})^* = \begin{cases} \mathbb{Z}_{(p-1)p^{r-1}} & \text{si } p \neq 2 \\ \mathbb{Z}_2 & \text{si } p^r = 4 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}} & \text{si } p = 2,\ r > 2 \end{cases}$$

Demostración. Ver [DF] p.314, o [M1] p.40-41. □

Comparar el resultado anterior con la observación 1.2.5.

Definición. Un subgrupo $H < G$ es *característico* si $\alpha(H) = H$ para todo $\alpha \in \text{Aut}(G)$. Notamos H char G.

Observación 1.5.2. Un subgrupo es normal si es invariante por automorfismos internos, y un subgrupo es característico si es invariante por todos los automorfismos. Por lo tanto un subgrupo característico es normal. El recíproco es falso. Por ejemplo, si H es un grupo y $G = H \times H$, entonces el subgrupo $H \times \{e\}$ es normal pero no característico, pues no es es invariante por el automorfismo $(x,y) \mapsto (y,x)$.

Observación 1.5.3.

- El centro de un grupo G es un subgrupo característico: si $x \in Z(G)$, $\alpha \in \text{Aut}(G)$:

$$\begin{aligned} xg = gx \ \ \forall g \in G &\Rightarrow \alpha(xg) = \alpha(gx) \ \ \forall g \in G \Rightarrow \alpha(x)\alpha(g) = \alpha(g)\alpha(x) \ \ \forall g \in G \\ &\Rightarrow \alpha(x)y = y\alpha(x) \ \ \forall y \in G \Rightarrow \alpha(x) \in Z(G) \end{aligned}$$

  pues como α es un automorfismo de G, $\alpha(g)$ es un elemento arbitrario y de G.

- Ya vimos que "ser normal" no es transitivo, pero ser característico sí lo es: K char H char $G \Rightarrow K$ char G, pues todo automorfismo de G se restringe a un automorfismo de H. Más aún, K char $H \lhd G \Rightarrow K \lhd G$. [6]

- Todo subgrupo de un grupo abeliano es normal, pero no necesariamente característico. Por ejemplo, un subespacio de dimensión 1 en el $\mathbb{Z}_p$-espacio vectorial $\mathbb{Z}_p \times \mathbb{Z}_p$ no es invariante por $\text{Aut}(\mathbb{Z}_p) \simeq \text{GL}_2(\mathbb{Z}_p)$ (tomar una rotación).

- Si H es el único subgrupo de G de orden m, entonces es característico, pues $\alpha(H)$ es también un subgrupo de G de orden m.

[6] Ahora vemos en términos de automorfismos la obstrucción a que la normalidad sea transitiva: al restringir un automorfismo interno de G a H, resulta un automorfismo de H que no tiene por qué ser interno.

1.6. Producto semidirecto

Observación 1.6.1 (Transporte de estructura). Sean G grupo, X conjunto y $\varphi : X \to G$ una biyección. Podemos dotar a X de una estructura de grupo de manera que φ sea un isomorfismo: definimos

$$x \star y := \varphi^{-1}(\varphi(x)\varphi(y))$$

Se verifica fácilmente que $(X, \star)$ es un grupo, y que φ es un isomorfismo de grupos.

Aplicaremos esta observación para motivar la definición de *producto semidirecto*.

Sea G grupo y sean $N \lhd G$, $Q < G$ tales que $N \cap Q = \{e\}$ y $G = NQ$. Si Q no es normal en G, entonces G no será el producto directo interno de N y Q (proposición 1.29).

Es decir, la función $\varphi : N \times Q \to G$, $\varphi(n, q) = nq$ no será en este caso un isomorfismo de grupos, a menos que Q sea normal en G.

Las condiciones $G = NQ$ y $N \cap Q = \{e\}$ garantizan que φ sea una función biyectiva; el problema pasa por la preservación de la estructura de grupo.

Utilicemos la biyección φ para transportar la estructura de grupo de G al conjunto $N \times Q$, consiguiendo que φ sea un isomorfismo de grupos. Veamos cómo luce explícitamente el nuevo producto en $N \times Q$:

$$\begin{aligned}\varphi^{-1}(\varphi(n_1, q_1)\varphi(n_2, q_2)) &= \varphi^{-1}(n_1 q_1 n_2 q_2) \\ &= \varphi^{-1}(n_1 q_1 n_2 \overbrace{q_1^{-1} q_1}^{=e} q_2) \\ &= (n_1 q_1 n_2 q_1^{-1}, q_1 q_2)\end{aligned}$$

donde en el último paso utilizamos que $q_1 n_2 q_1^{-1} \in N$ por ser N normal en G, y por lo tanto se tiene $\overbrace{n_1 q_1 n_2 q_1^{-1}}^{\in N}\overbrace{q_1 q_2}^{\in Q}$.

Si definimos $\theta : Q \to \mathrm{Aut}(N)$ como $\theta(q)(n) = qnq^{-1}$, entonces el nuevo producto en $N \times Q$ resulta ser

$$(n_1, q_1)(n_2, q_2) = (n_1 \theta(q_1)(n_2), q_1 q_2)$$

Podemos ahora abstraer esta definición a una definición *externa*, donde N y Q no son subgrupos de un grupo dado, etc.

Definición. Sean N, Q grupos, $\theta : Q \to \mathrm{Aut}(N)$ morfismo. El *producto semidirecto externo* de N con Q es el conjunto $N \times Q$ con el producto:

$$(n_1, q_1)(n_2, q_2) = (n_1 \theta(q_1)(n_2), q_1 q_2)$$

Lo notamos $N \rtimes_\theta Q$.[7] Decimos que Q actúa sobre N por automorfismos.[8] El neutro es (e, e) y el inverso $(n, q)^{-1} = (\theta(q^{-1})(n^{-1}), q^{-1})$.

Ejemplo 1.6.2. Dado un cuerpo k, el *grupo afín* es $\mathrm{Aff}_n(\mathrm{k}) = \mathrm{k}^n \rtimes_\theta \mathrm{GL}_n(\mathrm{k})$, donde $\theta(A)(v) = Av$. Es el grupo de transformaciones afines del espacio afín k^n.[9]

[7] Es el producto semidirecto de N con Q, y esto no es reflexivo.

[8] Comparar con la proposición 1.48: en este caso, es lo mismo dar un morfismo $Q \to \mathrm{Aut}(N)$ que dar una acción $Q \times N \to N$ tal que $q.-$ sea morfismo de grupos para todo $q \in Q$.

[9] Recordemos que una transformación afín es de la forma $x \mapsto ax + b$.

Proposición 1.36. *El producto semidirecto externo $N \rtimes_\theta Q$ es un grupo tal que, si $\tilde{N} = N \times \{e\}$, $\tilde{Q} = \{e\} \times Q$, entonces:*

- $\tilde{N} \simeq N$, $\tilde{Q} \simeq Q$ *y* $\tilde{N}, \tilde{Q} < N \rtimes_\theta Q$,
- $\tilde{N} \lhd N \rtimes_\theta Q$,
- $\tilde{N} \cap \tilde{Q} = \{(e, e)\}$,
- $\tilde{N}\tilde{Q} = N \rtimes_\theta Q$.

Recíprocamente, si G es un grupo que es producto semidirecto interno *de subgrupos $N, Q < G$, i.e. si $N \lhd G$, $N \cap Q = \{e\}$ y $NQ = G$ entonces si $\theta : Q \to Aut(N)$ es $\theta(q)(n) = qnq^{-1}$, se tiene que $\eta : N \rtimes_\theta Q \to G$, $(n, q) \mapsto nq$ es un isomorfismo.*

Demostración. ($\Rightarrow$) El primer y el tercer ítem son obvios. Verifiquemos la normalidad de $\tilde{N}$.

$$\begin{aligned}(n_1, q_1)(n_2, e)(n_1, q_1)^{-1} &= (n_1\theta(q_1)(n_2), q_1)(\theta(q_1^{-1})(n_1^{-1}), q_1^{-1}) \\ &= (n_1\theta(q_1)(n_2)\theta(q_1)(\theta(q_1^{-1})(n_1^{-1})), q_1 q_1^{-1}) \\ &= (n_1\theta(q_1)(n_2)n_1^{-1}, e) \in \tilde{N}\end{aligned}$$

$\tilde{N}\tilde{Q} = N \rtimes_\theta Q$: sea $(n, q) \in N \rtimes_\theta Q$. Entonces

$$(n, q) = (n\theta(e)(e), q) = (n, e)(e, q) \in \tilde{N}\tilde{Q}$$

($\Leftarrow$) Este es el contenido de la discusión anterior a la definición. □

Observación 1.6.3. Podría parecernos a priori que la construcción externa es más general, pues estamos partiendo de una acción por un automorfismo arbitrario, mientras que en el producto semidirecto interno consideramos una acción por automorfismos internos. Esto es ilusorio: cuando pasamos de la construcción externa a la interna, siempre terminamos con una acción por conjugación.

En efecto, se cumple "$\theta(q)(n) = qnq^{-1}$", donde estamos identificando N con $\tilde{N}$ y Q con $\tilde{Q}$.

Más formalmente, si $n \in N$, notemos $\tilde{n} = (n, e) \in \tilde{N}$, y si $q \in Q$, notemos $\tilde{q} = (e, q) \in \tilde{Q}$.

Se cumple $\tilde{q}\tilde{n}\tilde{q}^{-1} = \theta(\tilde{q})(n)$. En otras palabras, si $\tilde{\theta} : \tilde{Q} \to \mathrm{Aut}(\tilde{N})$ se define como $\tilde{\theta}(\tilde{q})(\tilde{n}) = (\theta(q)(n), e)$, entonces $\tilde{\theta}(\tilde{q})(\tilde{n}) = \tilde{q}\tilde{n}\tilde{q}^{-1}$.

$$\begin{aligned}\tilde{q}\tilde{n}\tilde{q}^{-1} &= (e, q)(n, 1)(e, q) \\ &= (\theta(q)(n), q)(e, q^{-1}) \\ &= (\theta(q)(n)\theta(q)(e), qq^{-1}) \\ &= (\theta(q)(n), e) \\ &= \theta(\tilde{q})(n)\end{aligned}$$

Proposición 1.37. *Sean Q, N grupos. Entonces*

$$\theta : Q \to \mathrm{Aut}(N) \text{ es el morfismo trivial} \iff N \rtimes_\theta Q = N \times Q$$

Demostración.

$$(n_1, q_1)(n_2, q_2) = (n_1\theta(q_1)(n_2), q_1q_2) = (n_1n_2, q_1q_2) \quad \forall n_1, n_2 \in N, q_1, q_2 \in Q$$
$$\iff \theta(q_1) = \mathrm{id}_N \quad \forall q_1 \in Q \iff \theta \text{ es el morfismo trivial} \qquad \square$$

El producto directo de grupos abelianos es abeliano. Ahora vemos que nuestra nueva construcción, a menos que sea el producto directo, no es abeliana.

Proposición 1.38. *Sean Q, N grupos. Si $\theta : Q \to \mathrm{Aut}(N)$ no es el morfismo trivial, entonces el producto semidirecto $N \rtimes_\theta Q$ no es abeliano.*

Demostración. Si θ no es trivial entonces existe $q \in Q$ tal que $\theta(q) \neq \mathrm{id}_N$, por lo tanto existe $n \in N$ tal que $\theta(q)(n) \neq n$.

$$(n, e)(e, q) = (n\theta(e)(e), eq) = (n, q)$$
$$(e, q)(n, e) = (e\theta(q)(n), qe) = (\theta(q)(n), q)$$

Tenemos entonces que existen n, q tales que $(n, e)(e, q) \neq (e, q)(n, e)$, luego $N \rtimes_\theta Q$ no es abeliano. $\square$

Enunciamos ahora sin demostración un teorema que permite reconocer un producto semidirecto. Parte de premisas en N y en G/N para concluir algo sobre G. Esto es algo que se repite a menudo en teoría de grupos: trabajando por inducción en $|G|$, se tiene que $|N|, |G/N| < |G|$ y se puede aplicar la hipótesis de inducción a estos grupos, lo cual puede ser fructífero. Usaremos esta técnica más adelante (y de hecho ya apareció en el ejercicio 25).

Teorema 1.39 (Schur-Zassenhaus)**.** *Todo grupo finito G con subgrupo normal N tal que su orden $|N|$ es coprimo con su índice $|G : N|$ es producto semidirecto de N con G/N.*

Ejercicios

Ej. 26 — $D_n \simeq \mathbb{Z}_n \rtimes \mathbb{Z}_2$.

Ej. 27 — El grupo de los cuaterniones no es un producto semidirecto (Sugerencia: contar elementos de orden 2). Por lo tanto que $Q \not\simeq D_4$ (esto ya apareció en el ejercicio 21).

Ej. 28 — $\mathrm{GL}_n(\mathrm{k}) \simeq \mathrm{SL}_n(\mathrm{k}) \rtimes \mathrm{k}^*$.

Ej. 29 — Sean N, Q grupos y $N \rtimes_{\theta_1} Q$, $N \rtimes_{\theta_2} Q$ dos productos semidirectos. Si existe $\phi \in \mathrm{Aut}(N)$ tal que $\theta_1 = \phi \circ \theta_2$, entonces $N \rtimes_{\theta_1} Q \simeq N \rtimes_{\theta_2} Q$.

1.7. Extensiones de grupos y sucesiones exactas

Definición. Una sucesión de grupos y morfismos de grupos

$$\ldots \xrightarrow{\varphi_{n+1}} G_{n+1} \xrightarrow{\varphi_n} G_n \xrightarrow{\varphi_{n-1}} \ldots$$

es *exacta* si $\operatorname{Im} \varphi_{i+1} = \ker \varphi_i$ para todo i. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$e \longrightarrow H \xrightarrow{i} G \xrightarrow{p} K \longrightarrow e \tag{1.1}$$

donde e denota el grupo trivial, y los morfismos inicial y final son los únicos posibles. De esta manera, una sucesión de la forma (1.1) es exacta si y sólo si i es inyectiva, p es sobreyectiva e $\operatorname{Im} i = \ker p$. Por lo tanto cumple $pi = 0$.

Definición. Una *extensión* de un grupo Q por un grupo N es una sucesión exacta corta

$$e \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow e$$

Diremos también que G es una extensión de Q por N.

Observación 1.7.1. En este caso se tiene $N \simeq i(N) = \ker p$ luego $i(N) \lhd G$, y $Q \simeq G/N$. Podemos pensar entonces que N es un subgrupo normal de G y que Q es el cociente de G por N. De esta manera, el problema de conocer un grupo G conociendo un subgrupo normal N y el cociente G/N se traduce al problema de conocer las extensiones de Q por N: es el llamado *problema de la extensión*. El problema de la extensión intenta explicitar las extensiones de un grupo Q en términos manejables, i.e. a través de construcciones conocidas, y en general no está resuelto.

Ejemplo 1.7.2. Sea $N \lhd G$, entonces tenemos una sucesión exacta corta

$$e \longrightarrow N \xrightarrow{i} G \xrightarrow{p} G/N \longrightarrow e \tag{1.2}$$

donde i es la inclusión y p la proyección.

Definición. Dos sucesiones exactas cortas (las filas del diagrama siguiente) son *equivalentes* si existen isomorfismos (las columnas) tales que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} e & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & e \\ & & \simeq\downarrow & & \simeq\downarrow & & \downarrow\simeq & & \\ e & \longrightarrow & H' & \xrightarrow{i'} & G' & \xrightarrow{p'} & K' & \longrightarrow & e \end{array}$$

Observación 1.7.3.

- Decir que dos sucesiones exactas cortas son equivalentes no es sólo decir que los grupos son uno a uno isomorfos. Lo adicional es la conmutatividad del diagrama, que nos dice informalmente que H se inyecta en G de la misma manera que H' en G', y que K es cociente de G de la misma manera que K' lo es de G'.
- Dar una sucesión exacta corta es lo mismo que dar un subgrupo normal de G; esto ya lo justificamos en 1.3.10, pero ahora lo podemos decir con otro lenguaje. Toda sucesión exacta corta es equivalente a una de la forma (1.2):

$$\begin{array}{ccccccccc} e & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & e \\ & & \alpha\downarrow & & \mathrm{id}\downarrow & & \downarrow\tilde{\beta} & & \\ e & \longrightarrow & \alpha(H) & \xrightarrow{i} & G & \xrightarrow{p} & G/\ker\,\beta & \longrightarrow & e \end{array}$$

- Dos pares de grupos isomorfos Q, Q' y N, N' pueden dar lugar a extensiones G, G' no isomorfas. Por ejemplo, consideremos D_4 y Q que no son isomorfos (ver ejercicio 27). Sin embargo, $\langle R^2\rangle \simeq \langle \pm 1\rangle$ y $D_4/\langle R^2\rangle \simeq Q/\langle \pm 1\rangle$, i.e. se tienen sucesiones exactas cortas

$$e \longrightarrow \langle R^2\rangle \longrightarrow D_4 \longrightarrow D_4/\langle R^2\rangle \longrightarrow e$$

$$e \longrightarrow \langle \pm 1\rangle \longrightarrow Q \longrightarrow Q/\langle \pm 1\rangle \longrightarrow e \tag{1.3}$$

  con primer y último grupo isomorfos, pero el del medio no. Esto nos dice que conocer N y G/N no es suficiente en general para conocer G.

Ejemplo 1.7.4. Dados H y K grupos, tenemos una sucesión exacta corta

$$e \longrightarrow H \longrightarrow H \times K \longrightarrow K \longrightarrow e \tag{1.4}$$

donde el primer mapa es la inyección y el segundo la proyección. Más en general, si $\theta : Q \to \mathrm{Aut}(N)$, entonces los mismos mapas determinan otra sucesión exacta corta

$$e \longrightarrow H \longrightarrow H \rtimes_\theta K \longrightarrow K \longrightarrow e \tag{1.5}$$

Uno podría preguntarse si todas las extensiones son isomorfas a esta sucesión exacta corta. O, en otras palabras, si toda extensión es un producto semidirecto. Pero no es así, por ejemplo, la sucesión (1.3) no lo satisface por el ejercicio 27. Rápidamente vemos que el problema de la extensión *no* es trivial.

El grupo afín (ver ejemplo 1.6.2) es una extensión de $\mathrm{GL_n(k)}$ por k^n.

Teorema 1.40. *Sea* $e \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow e$ *una sucesión exacta corta. Son equivalentes:*

1. *Existe* $\alpha' : G \to H$ *morfismo tal que* $\alpha'\alpha = \mathrm{id}_H$.[10]

$$e \longrightarrow H \underset{\alpha'}{\overset{\alpha}{\rightleftarrows}} G \xrightarrow{\beta} K \longrightarrow e \tag{1.6}$$

2. *La sucesión es equivalente a (1.4), de esta manera: existe un isomorfismo* $\phi : G \to H \times K$ *tal que el siguiente diagrama conmuta:*

$$\begin{array}{ccccccccc} e & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & e \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ e & \longrightarrow & H & \xrightarrow{i} & H \times K & \xrightarrow{p} & K & \longrightarrow & e \end{array} \tag{1.7}$$

Demostración. $(1 \Rightarrow 2)$ Definimos ϕ de la manera más sensata: $\phi(g) = (\alpha'(g), \beta(g))$, para todo $g \in G$.

Hace conmutar el diagrama de la izquierda:
$\phi(\alpha(g)) = (\alpha'(\alpha(g)), \alpha(\beta(g))) = (g, e) = i(g)$ y el de la derecha:

[10] Siempre existe una tal *función*, pues al ser α inyectiva tiene inversa por izquierda. Lo importante es que exista una que sea un *morfismo*.

$p(\phi(g)) = \beta(g)$.

ϕ es inyectiva: supongamos que $\phi(g) = (e, e)$. Entonces $\alpha'(g) = e = \beta(g)$. Luego $g \in \ker \beta = \operatorname{Im} \alpha$, por lo tanto existe $h \in H$ tal que $g = \alpha(h)$. Pero entonces $\alpha'(\alpha(h)) = e$, de donde $h = e$ y $g = \alpha(e) = e$.

ϕ es sobreyectiva: sea $(h, k) \in H \times K$. Existe $g_0 \in G$ tal que $k = \beta(g_0)$. Ahora, si $x \in H$ entonces $\beta(g_0\alpha(x)) = k$. Por lo tanto si hallo x tal que $\alpha'(g_0\alpha(x)) = h$, ya está. Pero

$$\alpha'(g_0\alpha(x)) = h \iff \alpha'(g_0)x = h \iff x = (\alpha'(g_0))^{-1}h$$

por lo tanto $x = (\alpha'(g_0))^{-1}h$ e $y = g_0\alpha(x)$ cumplen $\phi(y) = (h, k)$.

$(2 \Rightarrow 1)$ Sea $\pi : H \times K \to H$ la proyección sobre la primera coordenada. Definamos entonces $\alpha'(g) = \pi\phi(g)$ para todo $g \in G$. Es un morfismo que cumple

$$\alpha'(\alpha(h)) = \pi(\phi(\alpha(h))) = \pi i(h) = h \qquad \square$$

Teorema 1.41. *Sea* $e \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow e$ *una sucesión exacta corta. Son equivalentes:*

1. *Existe* $\beta' : K \to G$ *morfismo tal que* $\beta\beta' = \mathrm{id}_K$.[11]

$$e \longrightarrow H \xrightarrow{\alpha} G \underset{\beta'}{\overset{\beta}{\rightleftarrows}} K \longrightarrow e \tag{1.8}$$

2. *La sucesión es equivalente a (1.5), de esta manera: existen un morfismo* $\theta : K \to \mathrm{Aut}(H)$ *y un isomorfismo* $\phi : G \to H \rtimes_\theta K$ *tales que el siguiente diagrama conmuta:*

$$\begin{array}{ccccccccc} e & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & e \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ e & \longrightarrow & H & \xrightarrow{i} & H \rtimes_\theta K & \xrightarrow{p} & K & \longrightarrow & e \end{array} \tag{1.9}$$

Observación 1.7.5. En la categoría R-Mód de R-módulos, las condiciones del teorema 1.40 y del teorema 1.41 son equivalentes, no así en la categoría Grp de grupos en donde estamos trabajando: ver ejercicio 30. Si quisiéramos probar como con módulos que (1.8) implica (1.7), intentaríamos definir el morfismo más sensato $\gamma : H \times K \to G$, $\gamma(h, k) = \alpha(h)\beta'(k)$. Pero al no tener conmutatividad, esto no define un *morfismo*, por cómo es el producto en el producto directo $H \times K$. Este problema se soluciona usando el mismo morfismo pero cambiando el producto de $H \times K$ y poniendo el producto semidirecto. Veremos en la demostración cómo de esta manera γ resulta un morfismo.

[11] Como en el teorema anterior, siempre existe una tal *función*, pues al ser β sobreyectiva tiene inversa por derecha. Lo importante es que exista una que sea un *morfismo*.

Demostración. $(1 \Rightarrow 2)$ Definamos una acción θ de K en H por automorfismos internos. Si $k \in K$, $h \in H$, conjuguemos $\alpha(h)$ por $\beta'(k)$. Se tiene que $\beta'(k)\alpha(h)\beta'(k^{-1}) \in \ker \beta$, pues

$$\beta(\beta'(k)\alpha(h)\beta'(k^{-1})) = kek^{-1} = e$$

por lo tanto $\beta'(k)\alpha(h)\beta'(k^{-1}) = \alpha(h')$ para un $h' \in H$ que es único por inyectividad de α. Definimos $\theta(k)(h) = h'$, i.e. $\theta(k)(h)$ es el único elemento de H tal que

$$\beta'(k)\alpha(h)\beta'(k)^{-1} = \alpha(\theta(k)(h)) \tag{1.10}$$

Primero observamos que para $k = 1$ se obtiene $\alpha(h) = \alpha(\theta_1(h))$ para todo $h \in H$; como α es inyectiva esto significa que $\theta_1 = \mathrm{id}_H$.

Veamos que $\theta : K \to \mathrm{Aut}(H)$ es un morfismo de grupos. Notamos $\theta_k = \theta(k) : H \to H$.

Primero tenemos que verificar que θ_k es un morfismo de grupos. $\theta_k(h_1h_2)$ está caracterizado por la ecuación

$$\beta'(k)\alpha(h_1h_2)\beta'(k)^{-1} = \alpha(\theta_k(h_1h_2))$$

El miembro izquierdo de la ecuación es

$$\begin{aligned}\beta'(k)\alpha(h_1)\alpha(h_2)\beta'(k)^{-1} &= (\beta'(k)\alpha(h_1)\overbrace{\beta'(k)^{-1})(\beta'(k)}^{=e}\alpha(h_2)\beta'(k)^{-1}) \\ &= \alpha(\theta_k(h_1))\alpha(\theta_k(h_2)) \\ &= \alpha(\theta_k(h_1)\theta_k(h_2))\end{aligned}$$

Tenemos entonces $\alpha(\theta_k(h_1)\theta_k(h_2)) = \alpha(\theta_k(h_1h_2))$, pero α es inyectiva, luego $\theta_k(h_1)\theta_k(h_2) = \theta_k(h_1h_2)$ y θ_k es morfismo.

Ahora veamos que θ_k es invertible y que θ es un morfismo. Probemos primero que $\theta_{k_1}\theta_{k_2} = \theta_{k_1k_2}$. Ahora, $\theta_{k_1k_2}(h)$ está caracterizado por la ecuación

$$\beta'(k_1k_2)\alpha(h)\beta'(k_1k_2)^{-1} = \alpha(\theta_{k_1k_2}(h))$$

El miembro izquierdo de la ecuación es

$$\begin{aligned}\beta'(k_1)\beta'(k_2)\alpha(h)\beta'(k_2)^{-1}\beta'(k_1)^{-1} &= \beta'(k_1)\alpha(\theta_{k_2}(h))\beta'(k_1)^{-1} \\ &= \alpha(\theta_{k_1}(\theta_{k_2}(h)))\end{aligned}$$

Tenemos entonces $\alpha(\theta_{k_1}(\theta_{k_2}(h))) = \alpha(\theta_{k_1k_2}(h))$, pero α es inyectiva, luego $\theta_{k_1}(\theta_{k_2}(h)) = \theta_{k_1k_2}(h)$ para todo $h \in H$, i.e.

$$\theta_{k_1}\theta_{k_2} = \theta_{k_1k_2} \tag{1.11}$$

Dado $k \in K$, tomando $k_1 = k$, $k_2 = k^{-1}$ obtenemos $\theta_k\theta_{k^{-1}} = \theta_1 = \mathrm{id}_H$, y tomando $k_2 = k$, $k_1 = k^{-1}$ obtenemos $\theta_{k^{-1}}\theta_k = \theta_1 = \mathrm{id}_H$. Por lo tanto θ_k es un automorfismo, luego θ está bien definido, y la ecuación (1.11) nos dice que es un morfismo de grupos.

Ahora tenemos que construir un isomorfismo entre G y $H \rtimes_\theta K$. Sea $\gamma : H \rtimes_\theta K \to G$ definido como

$$\gamma(h, k) = \alpha(h)\beta'(k)$$

γ es un morfismo de grupos:

$$\begin{aligned}\gamma((h_1,k_1)(h_2,k_2)) &= \gamma(h_1\theta_{k_1}(h_2),k_1k_2)\\ &= \alpha(h_1\theta_{k_1}(h_2))\beta'(k_1k_2)\\ &= \alpha(h_1)\alpha(\theta_{k_1}(h_2))\beta'(k_1)\beta'(k_2)\\ &= \alpha(h_1)(\beta'(k_1)\alpha(h_2)\beta'(k_1)^{-1})\beta'(k_1)\beta'(k_2)\\ &= \alpha(h_1)\beta'(k_1)\alpha(h_2)\beta'(k_2)\\ &= \gamma(h_1,k_1)\gamma(h_2,k_2)\end{aligned}$$

γ es inyectiva: si $\gamma(h,k)=e$ entonces $\alpha(h)\beta'(k)=e$, por lo tanto

$$\beta(\alpha(h)\beta'(k))=\beta(e)\Rightarrow \overbrace{\beta(\alpha(h))}^{=e}\overbrace{\beta(\beta'(k))}^{=k}=e\Rightarrow k=e$$

luego $\beta'(k)=e$, por lo tanto $\alpha(h)=e$ y como α es inyectiva, $h=e$.

γ es sobreyectiva: sea $g\in G$. Queremos hallar h,k para que $g=\alpha(h)\beta'(k)$. Aplicándole β a esta igualdad se obtiene $\beta(\alpha(h))\beta(\beta'(k))=\beta(g)\Rightarrow k=\beta(g)$. Entonces k debe ser necesariamente $\beta(g)$. Por lo tanto

$$\begin{aligned}\exists h: g=\alpha(h)\beta'(k) &\iff \exists h: g=\alpha(h)\beta'(\beta(g))\\ &\iff \exists h: \alpha(h)=g\beta'(\beta(g))^{-1}\\ &\iff g\beta'(\beta(g))^{-1}\in \operatorname{Im}\alpha=\ker\beta\end{aligned}$$

Verifiquemos esto:

$$\beta(g\beta'(\beta(g))^{-1})=\beta(g)\beta\beta'(\beta(g)^{-1})=\beta(g)\beta(g)^{-1}=e$$

Por lo tanto γ es un isomorfismo. Definimos $\phi=\gamma^{-1}$. Queremos ver que ϕ hace conmutar el diagrama (1.9). Es lo mismo que verificar que γ hace conmutar el diagrama

$$\begin{array}{ccccccccc} e & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & e\\ & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \mathrm{id}} & & \\ e & \longrightarrow & H & \xrightarrow{i} & H\rtimes_\theta K & \xrightarrow{p} & K & \longrightarrow & e\end{array}$$

$\gamma(i(h))=\gamma(h,e)=\alpha(h)\beta'(e)=\alpha(h)$ luego el cuadrado de la izquierda conmuta.
$\beta(\gamma(h,k))=\beta(\alpha(h)\beta'(k))=\beta(\alpha(h))\beta\beta'(k)=k=p(h,k)$ luego el cuadrado de la derecha conmuta.

$(2\Rightarrow 1)$ ¿Cómo podríamos definir β'? Si miramos cómo definimos γ en la prueba de la otra implicación, entonces tomando $h=e$ se obtiene que $\gamma(e,k)=\beta'(k)$. Esto nos sugiere que definamos

$$\beta'(k)=\phi^{-1}(e,k)$$

β' es la composición de la inyección $K\to H\rtimes_\theta K$ con ϕ^{-1}, luego es un morfismo. Ahora la conmutatividad del cuadrado de la derecha de (1.9) nos da la conmutatividad del cuadrado

inverso

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ {\scriptstyle \phi^{-1}}\uparrow & & \uparrow{\scriptstyle \mathrm{id}} \\ H \rtimes_\theta K & \longrightarrow & K \end{array}$$

Esto nos dice que $\beta\phi^{-1}(h,k) = k$, por lo tanto por definición de ϕ se tiene $\beta\beta'(k) = k$ para todo $k \in K$, i.e. $\beta\beta' = \mathrm{id}_K$. □

Definición. Una sucesión exacta corta de grupos *se escinde* si satisface las condiciones del teorema anterior, y en este caso decimos que la extensión de K por H es una *extensión trivial*.

Ahora podemos expresar el teorema de Schur-Zassenhaus de esta manera:

Teorema 1.42 (Schur-Zassenhaus)**.** *Toda extensión de grupos finitos de orden coprimo se escinde.*

Ejercicios

Ej. 30 — La sucesión exacta[12]

$$\mathrm{id} \longrightarrow A_3 \xrightarrow{\iota} S_3 \xrightarrow{\epsilon} \{\pm 1\} \longrightarrow \mathrm{id}$$

cumple que existe un morfismo $\eta : \{\pm 1\} \to S_3$ tal que $\epsilon\eta = \mathrm{id}_{\{\pm 1\}}$, pero no existe un morfismo $\psi : S_3 \to A_3$ tal que $\psi\iota = \mathrm{id}_{A_3}$.

Ej. 31 — La equivalencia de sucesiones exactas cortas tiene las propiedades de una relación de equivalencia.
Aquí termina el ejercicio; lo siguiente es un comentario. Las clases de equivalencia de las extensiones de un grupo abeliano Q por otro grupo abeliano N son un grupo abeliano isomorfo al grupo abeliano $\mathrm{Ext}^1(Q,N)$ estudiado en álgebra homológica. Por ejemplo, decir que toda extensión grupos abelianos de Q por N es trivial es decir que $\mathrm{Ext}^1(Q,N) = \{0\}$. El problema de la extensión en el caso abeliano se traduce entonces en el estudio del grupo $\mathrm{Ext}^1(Q,N)$.[13]

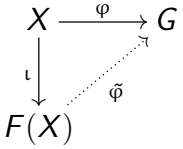
[12] Ver sección 1.10 para la definición de S_n y de A_n.

[13] Se puede probar que si A es un grupo abeliano numerable, entonces $\mathrm{Ext}^1(A,\mathbb{Z}) = \{0\}$ implica que A es un grupo abeliano libre. El *problema de Whitehead* es si esto vale en general para grupos de cardinal arbitrario. Shelah (1974) probó que este problema es indecidible en la teoría axiomática usual de conjuntos, ZFC. Fue el primer resultado indecidible que se encontró fuera de la teoría de conjuntos en sí, y en particular dentro del álgebra.

1.8. Grupos libres y presentaciones

Supongamos que tenemos un conjunto X. No hay ninguna operación en juego así que los elementos no están relacionados de ninguna manera. Si consideramos los elementos del conjunto como letras, podemos empezar a concatenarlos para formar palabras, de manera totalmente "libre", i.e. nunca va a haber cancelaciones. Ésta es la idea de un grupo libre de base X: va a ser el mayor grupo que tenga como generadores a los elementos de X.

Teorema 1.43. *Sea X un conjunto. Existe un grupo $F(X)$ y una función inyectiva $\iota : X \to F(X)$ tal que para todo grupo G y toda función $\varphi : X \to G$ existe un único morfismo de grupos $\tilde{\varphi} : F(X) \to G$ tal que el siguiente diagrama conmuta:*



En otras palabras, $F(X)$ es un grupo tal que para definir un morfismo desde él hacia otro grupo G, basta definir una función desde X hacia G. En aún otras palabras, toda función definida sobre X hacia G se extiende a un único morfismo de $F(X)$ hacia G.

Definición. $F(X)$ se llama *grupo libre* de base X. Un grupo H es *libre* si existe un conjunto X tal que $H = F(X)$.

Demostración. Llamamos a X el conjunto de *letras*. Sea X^{-1} otro conjunto tal que $X \cap X^{-1} = \varnothing$ y $|X^{-1}| = |X|$. Elegimos una biyección $X \to X^{-1}$, y a la imagen de x por esta biyección la denotamos x^{-1}.

Elegimos un elemento que no pertenezca a $X \cup X^{-1}$: lo denotamos 1 (la *letra vacía*).

Una *palabra* en X es una sucesión $(a_1, a_2, \dots) \subset X \cup X^{-1} \cup \{1\}$ tal que existe $n \in \mathbb{Z}^+$ de manera que $a_i = 1$ para todo $i \geqslant n$ (las palabras son sucesiones "finitas" de letras). Los elementos a_i y a_{i+1} se dicen *adyacentes* para todo i.

La palabra constante $(1, 1, \dots)$ es la *palabra vacía* y por abuso de notación la notamos 1.

Una palabra $(a_1, a_2, \dots)$ es *reducida* si:

I. $\forall x \in X$, x y x^{-1} no son adyacentes en $(a_1, a_2, \dots)$.

II. Si $k \in \mathbb{N}$ es tal que $a_k = 1$ entonces $a_i = 1 \quad \forall i \geqslant k$.

El primer ítem es que queremos tratar a x^{-1} como la inversa de x; el segundo ítem es que no queremos frases sino sólo palabras. Observar que 1 es una palabra reducida.

Definiendo x^{+1} como x, toda palabra reducida es de la forma $(x_1^{\lambda_1}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$, donde $\lambda_i = \pm 1$ para todo $i = 1, \dots, n$. La escribiremos como $x_1^{\lambda_1} \dots x_n^{\lambda_n}$. Observar que $x_1^{\lambda_1} \dots x_n^{\lambda_n} = y_1^{\delta_1} \dots y_m^{\delta_m}$ si y sólo si $n = m, x_i = y_i, \lambda_i = \delta_i$ para todo $i = 1, \dots, n$.

Sea $F(X) = \{\text{palabras reducidas en } X\}$. Definimos el producto $F(X) \times F(X) \to F(X)$ mediante:

si $p = x_1^{\lambda_1} \dots x_n^{\lambda_n}$, $q = y_1^{\delta_1} \dots y_n^{\delta_n}$, entonces pq es el resultado de reducir la concatenación $x_1^{\lambda_1} \dots x_n^{\lambda_n} y_1^{\delta_1} \dots y_n^{\delta_n}$. El neutro es la palabra vacía 1, y el inverso de p es $p^{-1} = x_n^{-\lambda_n} \dots x_1^{-\lambda_1}$.

Es tedioso pero evidente cómo verificar que esto define un grupo, lo dejamos como ejercicio para el lector escéptico.

Definimos $\iota : X \to F(X)$ como $x \mapsto (x, 1, 1, \dots) = x$. Es una función inyectiva. Veamos que $(F(X), \iota)$ verifica la propiedad universal: sea G grupo, $\varphi : X \to G$ función.

Si $\tilde{\varphi} : F(X) \to G$ es un morfismo tal que $\tilde{\varphi} \circ \iota = \varphi$, entonces $\tilde{\varphi}(x^1) = \varphi(x)$ para todo x, luego $\tilde{\varphi}(x^{-1}) = \tilde{\varphi}(x^1)^{-1} = \varphi(x)^{-1}$, por lo tanto

$$\tilde{\varphi}(x_1^{\lambda_1} \dots x_n^{\lambda_n}) = \varphi(x_1)^{\lambda_1} \dots \varphi(x_n)^{\lambda_n}$$

Entonces todo elemento en $F(X)$ es de la forma $x_1^{\lambda_1} \dots x_n^{\lambda_n}$, esto determina $\tilde{\varphi}$ de manera única. Es directo verificar que esta fórmula define efectivamente un morfismo. □

Observación 1.8.1.

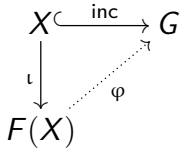
- Como ι es inyectiva, identificamos X con $\iota(X)$ en $F(X)$. De esta manera, $X \subset F(X)$ y X genera $F(X)$ como grupo.
- Si $|X| = 1$ entonces $F(X) \simeq \mathbb{Z}$. En efecto, si $X = \{a\}$, la función $X \to \mathbb{Z}$, $a \mapsto 1$ se extiende a un isomorfismo $F(X) \to \mathbb{Z}$.
- Si $|X| \geqslant 2$ entonces $F(X)$ no es abeliano. En efecto, sean $x, y \in X$, $x \neq y$. Entonces $xy \neq yx$. Formalmente, $xyx^{-1}y^{-1} \in F(X)$ por ser una palabra reducida; además $xyx^{-1}y^{-1} = (x, y, x^{-1}, y^{-1}, 1, 1, \dots) \neq (1, 1, \dots) = 1$ luego $xyx^{-1}y^{-1} \neq 1$.
- Si $|X| = 0$, i.e. si $X = \varnothing$, entonces $F(X) \simeq \{0\}$.

El siguiente teorema no tiene ninguna demostración de nivel adecuado al curso. Una posible demostración se encuentra en [Rot1], página 383.

Teorema 1.44 (Nielsen-Schreier)**.** *Todo subgrupo de un grupo libre es libre.*

Proposición 1.45. *Todo grupo es cociente de un grupo libre.*

Demostración. Sea G grupo, y X un generador de G (por ejemplo, $X = G$). Considero la inclusión inc de X en G. Por definición de $F(X)$ existe un único $\varphi : F(X) \to G$ morfismo tal que $\varphi(\iota(x)) = \text{inc}(x) = x$.



φ es sobreyectiva: $\text{Im}\,\varphi \supset \text{Im inc} = X$, y X genera G, por lo tanto $\text{Im}\,\varphi$ genera G. Pero $\text{Im}\,\varphi < G$, luego $\text{Im}\,\varphi = G$. Entonces φ es un epimorfismo, y se tiene $G \simeq F(X)/\ker\varphi$ (recordemos la observación 1.3.10). □

Observar que la φ anterior es $\varphi(x_1^{\lambda_1} \dots x_n^{\lambda_n}) = x_1^{\lambda_1} \dots x_n^{\lambda_n}$, donde a la izquierda no hay relaciones y a la derecha puede haberlas. Si nunca las hay es $\ker \varphi = \{e\}$ y G es libre.

Definición. Sea G grupo, $S \subset G$ subconjunto. El *subgrupo normal generado por* S es la intersección de todos los subgrupos normales de G que contienen a S. Explícitamente, es el subgrupo generado por $\{asa^{-1} : a \in G, s \in S\}$.

A continuación damos una nueva manera de especificar un grupo. Consideremos un conjunto de letras X; en vez de formar el grupo libre de base X formando palabras sin cancelaciones, ahora pasamos a especificar algunas cancelaciones. Por ejemplo, podemos querer especificar el grupo que tiene como generadores a dos elementos a, b sujetos sólo a la condición de que conmutan, i.e. $ab = ba$. Esto es lo mismo que decir que $aba^{-1}b^{-1} = e$. Es así como especificaremos las *relaciones* entre los elementos.

Definición. Sea X conjunto, $P \subset F(X)$ subconjunto. Un grupo G está definido por los *generadores* $x \in X$ y las *relaciones* $p = e, p \in P$ si $G \simeq F(X)/N$ donde N es el subgrupo normal de $F(X)$ generado por P.

Decimos que $\langle X \mid P \rangle$ es una *presentación* de G.

Observación 1.8.2. Como todo grupo es cociente de un grupo libre, entonces todo grupo admite una presentación.

Ejemplo 1.8.3.
- Si $P = \varnothing$, entonces $N = \{e\}$, luego $F(X)/N \simeq F(X)$ y $\langle X \mid \varnothing \rangle$ es una presentación de $F(X)$. Esto es predecible, $\langle X \mid \varnothing \rangle$ es el grupo "libre de relaciones" entre sus elementos (ninguna palabra se reduce), como lo es $F(X)$.

- El producto tensorial de R-módulos M, N es un grupo abeliano dado por generadores los elementos de $M \times N$ y ciertas relaciones.

Definición. Un grupo es *finitamente generado* si admite un generador finito.

Un grupo es *finitamente presentado* si admite una presentación $\langle X \mid P \rangle$ donde X, P son conjuntos finitos.

El "problema de la palabra" es el siguiente: dado un grupo G finitamente presentado por $\langle X \mid P \rangle$, y una palabra en $F(X)$, ¿existe un algoritmo para determinar si se puede reducir la palabra a 1 en G? La respuesta es que *no*. Por lo tanto, la impresión de que dar una presentación finita de un grupo debería ser algo que convierte al grupo en algo "manejable" es ilusoria.

Observación 1.8.4.
- "Es lo mismo" dar una presentación de G que dar un epimorfismo desde un libre, i.e. una sucesión exacta $F \longrightarrow G \longrightarrow e$ donde F es un grupo libre.

- "Es lo mismo" dar un grupo finitamente generado G que dar un epimorfismo desde un libre finitamente generado, i.e. una sucesión exacta $F \longrightarrow G \longrightarrow e$ donde F es libre finitamente generado.

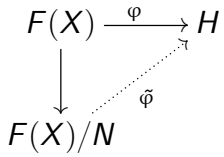
- "Es lo mismo" dar una presentación finita de G que dar una sucesión exacta $R \longrightarrow F \longrightarrow G \longrightarrow e$, donde F y R son grupos libres finitamente generados.

Teorema 1.46 (Von Dyck)**.** *Si G está presentado por $\langle X \mid P\rangle$ y H es otro grupo generado por X que satisface las relaciones $p = e, p \in P$ (pero puede verificar otras), entonces es un cociente de G.*[14] *Más formalmente:*

Si H está generado por $Y = \{y_i\}_{i\in I}$, i.e. $H = \langle Y\rangle$, y los elementos de Y satisfacen relaciones $y_{i_1}^{\alpha_{i_1}} \dots y_{i_l}^{\alpha_{i_l}}$, $i_1, \dots, i_l \in I$, $\alpha_{i_1}, \dots, \alpha_{i_l} \in \mathbb{Z}$ para ciertas palabras reducidas $y_{i_1}^{\alpha_{i_1}} \dots y_{i_l}^{\alpha_{i_l}}$, y G está presentado por $\langle X \mid P\rangle$ donde $X = \{x_i\}_{i\in I}$, $|X| = |Y|$ y $P = \{x_{i_1}^{\alpha_{i_1}} \dots x_{i_l}^{\alpha_{i_l}}\}$, entonces existe un epimorfismo

$$G \to H, \quad \overline{x_i} \mapsto y_i$$

Demostración. Sea $\varphi : F(X) \to H$ definida por $\varphi(x_i) = y_i$. Como $H = \langle Y\rangle$ entonces $\operatorname{Im}\varphi = H$. Sea N el subgrupo normal de $F(X)$ generado por P.



Para ver que $N \subset \ker\varphi$, basta ver que $P \subset \ker\varphi$, pues $\ker\varphi \lhd F(X)$ y N es el menor subgrupo normal que contiene P. Pero $\varphi(x_{i_1}^{\alpha_{i_1}} \dots x_{i_l}^{\alpha_{i_l}}) = y_{i_1}^{\alpha_{i_1}} \dots y_{i_l}^{\alpha_{i_l}} = e$. Entonces por la propiedad universal del cociente, φ se extiende a $\tilde{\varphi} : F(X)/N \to H$ tal que $\tilde{\varphi}(\overline{x_i}) = \varphi(x_i) = y_i$, y $\tilde{\varphi}$ es claramente sobreyectiva. □

Ejemplo 1.8.5. Probemos formalmente que $D_n \simeq \langle R, S \mid R^n, S^2, SRSR\rangle$. De D_n sabemos que $|D_n| = 2n$ y que es generado por la rotación R y la reflexión S que satisfacen $R^n = S^2 = \mathrm{id}$, $RS = SR^{n-1} = SR^{-1}$ y por lo tanto $SRSR = \mathrm{id}$.

Sea $X = \{a, b\}$ y $G = F(X)/N$ donde $N \subset F(X)$ es el subgrupo normal de $F(X)$ generado por $P = \{a^n, b^2, baba\}$.

Como $\pi : F(X) \to F(X)/N$ es un epimorfismo, entonces $\{\overline{a}, \overline{b}\}$ genera G. Queremos probar que $G \simeq D_n$.

$P \subset N \Rightarrow \overline{a}^n = \overline{b}^2 = \overline{b}\overline{a}\overline{b}\overline{a} = \overline{e}$. Además:

- $\overline{b}^2 = \overline{e} \Rightarrow \overline{b}^{-1} = \overline{b} \Rightarrow \overline{b}^n = \overline{b}^{\pm 1} \quad \forall n \in \mathbb{Z}$.
- $\overline{a}^n = \overline{e} \Rightarrow \{\overline{a}^m : m \in \mathbb{Z}\} = \{\overline{e}, \overline{a}, \dots, \overline{a}^{n-1}\}$.
- $\overline{b}\overline{a}\overline{b}\overline{a} = \overline{e} \Rightarrow \overline{b}\overline{a} = \overline{a}^{-1}\overline{b}^{-1} \Rightarrow \overline{b}\overline{a} = \overline{a}^{-1}\overline{b}$.

Por lo tanto en G las únicas palabras que quedan son: $\{\overline{e}, \overline{a}, \dots, \overline{a}^{n-1}, \overline{b}, \overline{a}\overline{b}, \dots, \overline{a}^{n-1}\overline{b}\}$. Entonces $|G| \leqslant 2n$ ($\leqslant$ pues a priori no sabemos si no hay más relaciones).

Por el teorema de Von Dyck, como D_n satisface las relaciones que G satisface, existe $\psi : G \to D_n$ epimorfismo, $\overline{a} \mapsto R$, $\overline{b} \mapsto S$. Por lo tanto $|G| \geqslant |D_n| = 2n$, luego $|G| = |D_n|$ y ψ es el isomorfismo deseado.

Teorema 1.47. *Todo grupo no abeliano de orden 8 es isomorfo a D_4 o a Q (que no son isomorfos, ver ejercicios 21 o 27).*

[14] El grupo que nos da la presentación es el "más grande" que satisface las relaciones dadas, en el sentido que cualquier otro grupo que las satisface es un cociente.

Demostración. Sea G no abeliano de orden 8. Por Lagrange, todo elemento no trivial de G tiene orden 2 o 4. Por el ejercicio 2, existe $x \in G$ de orden 4.

Sea $y \in G \backslash \langle x \rangle$. Como $\langle x \rangle \subsetneq \langle x, y \rangle$ y $|\langle x \rangle| = 4$, entonces $G = \langle x, y \rangle$. Como G no es abeliano entonces x e y no conmutan.

$\langle x \rangle \lhd G$ pues tiene índice 2. En particular $yxy^{-1} \in \langle x \rangle = \{e, x, x^2, x^3\}$.

Como yxy^{-1} tiene orden 4 (ver ejercicio 8), entonces $yxy^{-1} = x$ o $yxy^{-1} = x^3 = x^{-1}$. La primera opción no es posible pues en ese caso $yx = xy$, pero x e y no conmutan. Por lo tanto $yxy^{-1} = x^{-1}$.

Se tiene que $G/\langle x \rangle = \{\overline{e}, \overline{y}\}$ pues tiene orden 2, por lo tanto $\overline{y^2} = \overline{e}$. Se tiene entonces $y^2 \in \langle x \rangle = \{1, x, x^2, x^3\}$.

Como y tiene orden 2 o 4, entonces y^2 tiene orden 1 o 2, luego $y^2 = e$ o $y^2 = x^2$.

Tenemos entonces que $G = \langle x, y \rangle$, con dos posibilidades:

$$x^4 = e, \;\; y^2 = e, \;\; yxy^{-1} = x^{-1}$$

o

$$x^4 = e, \;\; y^2 = x^2, \;\; yxy^{-1} = x^{-1}$$

y no se satisfacen más relaciones pues G tiene orden 8. En el primer caso, $G \simeq D_4$ por el ejemplo anterior. En el segundo caso, $G \simeq Q$ por el ejercicio 32. □

Ejercicios

Ej. 32 — El grupo de los cuaterniones Q está dado por la presentación

$$\langle a, b \mid a^4, a^2 b^{-2}, bab^{-1}a \rangle$$

Ej. 33 — $D_n \simeq \langle a, b \mid a^2, b^2, (ab)^n \rangle$. Esta presentación motiva la introducción del *grupo diedral infinito*, "haciendo tender $n \to \infty$": es el grupo D_∞ presentado por $\langle a, b \mid a^2, abab \rangle$. Tiene orden infinito.

1.9. Acciones

En esta sección estudiamos el primer ejemplo de *representación* de un grupo: describiremos nuestro grupo como un grupo de permutaciones (ver ejemplo 15).

Definición. Sea G grupo, X conjunto. Una *acción* (o *representación conjuntista*, o *representación por permutaciones*) de G en X es una función $\cdot : G \times X \to X$, $(g, x) \mapsto g \cdot x$ que verifica:

I. $e \cdot x = x \quad \forall x \in X$,

II. $g_1 \cdot (g_2 \cdot x) = g_1 g_2 \cdot x \quad \forall x \in X, g_1, g_2 \in G$.

Decimos que G *actúa* en X y que X *soporta* una acción de G. Esta acción convierte a X en un G-*conjunto*. Dado $g \in G$ notaremos por $g \cdot -$ a la función $X \to X$, $x \mapsto g \cdot x$.

Observación 1.9.1. Si G actúa en X y $H < G$ entonces H actúa en X por restricción de la acción de G.

La siguiente proposición nos dice por qué una acción describe nuestro grupo como un grupo de permutaciones. De esta manera podemos pensar que cada elemento de G nos da una permutación de los elementos de X. Otra idea interesante es pensar que los elementos de X son personas que se van a sacar una foto grupal pero no se deciden en qué orden ponerse, entonces están en movimiento; y que la acción de G es sacar fotografías de X en cada momento diferente $g \in G$.

Proposición 1.48. *"Es lo mismo" dar una acción de G en X que dar un morfismo de grupos $\rho : G \to \mathrm{Sym}(X)$.*

Demostración. La relación fundamental es $g \cdot - = \rho(g)$.

($\Rightarrow$) Definamos $\rho : G \to \mathrm{Sym}(X)$, $\rho(g) = g_L$ donde $g_L = g \cdot -$.

g_L es una biyección de X: en efecto, tiene como inversa a g_L^{-1},

$$g_L \circ g_L^{-1}(x) = g \cdot (g^{-1} \cdot x) = g g^{-1} \cdot x = e \cdot x = x, \quad \forall x \in X$$

por lo tanto $g_L \circ g_L^{-1} = \mathrm{id}$, análogamente se verifica $g_L^{-1} \circ g_L = \mathrm{id}$.

ρ es morfismo:

$$\begin{aligned} \rho(g_1 g_2)(x) = (g_1 g_2)_L(x) &= g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x) \\ &= g_{1L}(g_{2L}(x)) = \rho(g_1)(\rho(g_2)(x)), \quad \forall x \in X \end{aligned}$$

por lo tanto $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$.

($\Leftarrow$) Definamos $\cdot : G \times X \to X$ mediante $g \cdot x = \rho(g)(x)$. Es una acción:

I. $e \cdot x = \rho(e)(x) = \mathrm{id}(x) = x$,

II. $g_1 \cdot (g_2 \cdot x) = \rho(g_1)(\rho(g_2)(x)) = \rho(g_1) \circ \rho(g_2)(x) = \rho(g_1 g_2)(x) = g_1 g_2 \cdot x$. □

Observación 1.9.2. $g \cdot x = g \cdot y \Rightarrow x = y$, pues $g \cdot - = \rho(g) \in \mathrm{Sym}(X)$, en particular es inyectiva. Esto es una trivialidad en términos de fotografías: si en un momento dado dos personas ocupan el mismo lugar, entonces son la misma. Que $\rho(g)$ sea sobreyectiva para todo $g \in G$ nos dice que nadie en ningún momento se pone tímido y abandona el encuadre de la fotografía.

Si el núcleo del morfismo ρ es trivial, nuestra representación es muy buena; esto es reminiscente de nuestra observación 1.1.7 y motiva la siguiente

Definición. Una acción $\cdot : G \times X \to X$ es *fiel* si $g \cdot x = x \quad \forall x \in X \Rightarrow g = e$. Equivalentemente, una acción $\rho : G \to \mathrm{Sym}(X)$ es fiel si ρ es inyectivo.

Observación 1.9.3. Una acción es fiel si y sólo si dados distintos $g, h \in G$ se tiene que existe $x \in X$ tal que $g \cdot x \neq h \cdot x$. Esto nos dice que si la acción es fiel, las fotografías de X que nos ofrecen los elementos de G son todas diferentes, i.e. en dos momentos diferentes las fotografías son diferentes.

Definición. Una acción $\cdot : G \times X \to X$ es *transitiva* si para todo $x, y \in X$ existe $g \in G$ tal que $g \cdot x = y$. Decimos que G *actúa transitivamente* en X.

Una acción es *doblemente transitiva* si para todo $(x_1, x_2), (y_1, y_2) \in X \times X, x_1 \neq x_2, y_1 \neq y_2$ existe $g \in G$ tal que $g \cdot x_1 = y_1$, $g \cdot x_2 = y_2$. Análogamente se define una acción k-transitiva, para todo $k \geqslant 3$.

Si $G \times X \to X$ es una acción, y $H < G$ es tal que la acción restringida $H \times X \to X$ es una acción transitiva, diremos que H es un *subgrupo transitivo* de G.

Observación 1.9.4. Una acción es transitiva si dados dos elementos del conjunto existe un elemento del grupo que lleva el uno en el otro. O sea, dadas dos personas diferentes de X, en algún momento una estuvo en la posición de la otra. Una acción es doblemente transitiva si dados dos pares de personas, hay un momento en el que los del primer par ocuparon las posiciones de las del segundo par.

Ejemplo 1.9.5.

1. G actúa sobre sí mismo por conjugación: $G \times G \to G$, $g \cdot x = gxg^{-1}$.
2. La *acción trivial* de G en X es $G \times X \to X$, $g \cdot x = x$ para todo $g \in G, x \in X$.
3. Una acción de G en X induce una acción en $\mathcal{P}(X)$, definida como $g \cdot A := \{g \cdot x : x \in A\}$ si $A \neq \varnothing$, y $g \cdot \varnothing := \varnothing$.
4. $\mathrm{Aut}(G) \times G \to G$, $\varphi \cdot x = \varphi(x)$ es una acción tal que la acción por conjugación es su restricción a $\mathrm{Inn}(G)$.
5. $\mathrm{Sym}(X)$ actúa fiel y transitivamente en X.
6. Todo subgrupo $H < G$ actúa fielmente en G con la acción $h \cdot g = hg$.
7. $\mathrm{GL}_n(\mathrm{k}) \times \mathrm{k}^n \to \mathrm{k}^n$, $A \cdot v = Av$ es una acción fiel.

Definición. Dados X e Y G-conjuntos, un *G-mapa* (o *morfismo de G-conjuntos*) es una función $\varphi : X \to Y$ que respeta la acción de G, i.e. $\varphi(g \cdot x) = g \cdot \varphi(x)$ para todo $g \in G, x \in X$.

Un *isomorfismo* de G-conjuntos es un G-mapa biyectivo (la inversa de un G-mapa siempre es un G-mapa).

Definición. Sea X un G-conjunto. Un subconjunto $Y \subset X$ es *G-estable* si $g \cdot y \in Y$, para todo $g \in G, y \in Y$. En esta situación Y es un G-conjunto por restricción.

Proposición 1.49. *Sea $G \times X \to X$ una acción. La relación $\sim$ en X definida como*

$$x \sim x' \iff \exists g \in G : g \cdot x = x'$$

es una relación de equivalencia.

Demostración.
- $x \sim x$ pues $e \cdot x = x$.
- $x \sim x' \Rightarrow \exists g \in G : g \cdot x = x' \Rightarrow g^{-1} \cdot x' = g^{-1} \cdot g \cdot x = g^{-1} g \cdot x = e \cdot x = x \Rightarrow x' \sim x$.
- $x \sim y, y \sim z \Rightarrow \exists g_1, g_2 \in G, g_1 \cdot x = y, g_2 \cdot y = z$. Entonces

$$(g_2 g_1) \cdot x = g_2 \cdot (g_1 \cdot x) = g_2 \cdot y = z$$

luego $x \sim z$. □

Definición. Sea X un G-conjunto. Las clases de equivalencia de $\sim$ en X se dicen *órbitas* de la acción. La órbita de un elemento $x \in X$ es

$$o(x) := \{g \cdot x : g \in G\}$$

Si $o(x) = \{x\}$ decimos que es una órbita *unitaria*.

El conjunto cociente se denota X/G y se llama *espacio de órbitas*.

Cuando la acción es de un grupo sobre sí mismo por conjugación, las órbitas se llaman *clases de conjugación*: la clase de conjugación de $x \in G$ es

$$GxG^{-1} = \{gxg^{-1} : g \in G\}$$

Observación 1.9.6.
- Para todo $x \in X$, $o(x) \subset X$ es el menor subconjunto G-estable que contiene a x, y $G \times o(x) \to o(x)$ es una acción transitiva.
- Una acción es transitiva si y sólo si tiene una sola órbita.
- Como las órbitas son una partición de X, entonces $o(x) \cap o(y) \neq \varnothing \Rightarrow o(x) = o(y)$.
- Un subconjunto $Y \subset X$ es G-estable si y sólo si para todo $y \in Y$, $o(y) \subset Y$.
- La clase de conjugación de $x \in G$ es $\{x\}$ si y sólo si $x \in Z(G)$.

Proposición 1.50. *Sea X un G-conjunto. Un subconjunto $Y \subset X$ es G-estable si y sólo si Y es unión de órbitas.*

Demostración. Se deduce a partir del cuarto ítem de la observación anterior. □

Corolario 1.51. *Un subgrupo $H < G$ es normal si y sólo si es unión de clases de conjugación.*

Demostración. Considerar la acción por conjugación de G en G. Entonces si $H < G$, H es G-estable si y sólo si es unión de órbitas, i.e. si y sólo si es unión de clases de conjugación. Por otro lado H es G-estable si y sólo si

$$\forall x \in H \;\; o(x) \subset H \iff \forall x \in H \;\; \{gxg^{-1} : g \in G\} \subset H \iff H \lhd G \qquad \square$$

Definición. Sea X un G-conjunto. El *estabilizador* o *grupo de isotropía* de un elemento $x \in X$ es

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

$x \in X$ es un *punto fijo* para la acción si $g \cdot x = x$ para todo $g \in G$. Notamos

$$X_0 := \{x \in X : g \cdot x = x \;\; \forall g \in G\}$$

al conjunto de los puntos fijos de la acción.

Observación 1.9.7.

- $x \in X$ es un punto fijo $\iff o(x) = \{x\} \iff G_x = G$.
- X_0 es un subconjunto G-estable, y la restricción $G \times X_0 \to X_0$ es la acción trivial.
- Si $X = G$ y consideramos la acción por conjugación, entonces $X_0 = Z(G)$.

Proposición 1.52. *Sea X un G-conjunto. Si $x \in X$ entonces $G_x < G$. Además G_x y $G_{g\cdot x}$ se relacionan mediante $G_{g\cdot x} = gG_xg^{-1}$.*

Demostración. $G_x < G$: obviamente $e \in G_x$ y si $g, h \in G_x$ entonces

$$gh^{-1} \cdot x = g \cdot (h^{-1} \cdot x) \overset{x=h\cdot x}{=} g \cdot (h^{-1} \cdot h \cdot x) = g \cdot x = x$$

$G_{g\cdot x} = gG_xg^{-1}$:

($\subset$) Si $h \in G_{g\cdot x}$ entonces $h \cdot (g \cdot x) = g \cdot x$. Observo que $h \in gG_xg^{-1} \iff g^{-1}hg \in G_x$:

$$g^{-1}hg \cdot x = g^{-1} \cdot (h \cdot g \cdot x) = g^{-1} \cdot g \cdot x = x \Rightarrow g^{-1}hg \in G_x$$

($\supset$) Sea $ghg^{-1} \in gG_xg^{-1}$, i.e. $h \cdot x = x$. Entonces

$$ghg^{-1} \cdot (g \cdot x) = gh \cdot x = g \cdot x \Rightarrow ghg^{-1} \in G_{g\cdot x} \qquad \square$$

Ejemplo 1.9.8. Si $H < G$, entonces G actúa en el conjunto cociente G/H de coclases izquierdas de H en G mediante $G \times G/H \to G/H$, $g \cdot aH = gaH$. En este caso se tiene $G_H = H$, y en general $G_{gH} = gHg^{-1}$.

Observación 1.9.9.

$$\bigcap_{x\in X} G_x = \{g \in G : g \cdot x = x \;\; \forall x \in X\} = \{g \in G : \rho(g) = \mathrm{id} \;\; \forall g \in G\} = \ker \rho \lhd G$$

Definición. Sea X un G-conjunto y $S \subset X$ un subconjunto. El *estabilizador* de S es $\mathrm{Stab}(S) = \{g \in G : gS = S\}$.

Análogamente que con $\mathrm{Stab}(x)$ se prueba que $\mathrm{Stab}(S) < G$ y que $\mathrm{Stab}(gS) = g\mathrm{Stab(S)}g^{-1}$.

Teorema 1.53 (de la órbita y el estabilizador)**.** *Sea X un G-conjunto, $x \in X$. Entonces la función*

$$\varphi : G/G_x \to o(x), \quad gG_x \mapsto g \cdot x$$

es una isomorfismo de G-conjuntos; en particular, $|o(x)| = |G : G_x|$.

Demostración. Es sobreyectiva por definición. Está bien definida y es inyectiva pues si $g, h \in G$, $x \in X$:

$$\begin{aligned} g \cdot x = h \cdot x &\iff h^{-1} \cdot g \cdot x = x \iff h^{-1}g \cdot x = x \\ &\iff h^{-1}g \in G_x \iff gG_x = hG_x \end{aligned}$$

□

Es fácil verificar que φ es un G-mapa, donde G/G_x tiene la acción del ejemplo 1.9.8.

Corolario 1.54. *Si G es un grupo finito y X es un G-conjunto, entonces $|o(x)| \mid |G|$ para todo $x \in X$.*

Definición. Si G actúa sobre sí mismo por conjugación, entonces el estabilizador de $x \in G$ es

$$C_G(x) := G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

y se llama *centralizador* de x en G.

Observación 1.9.10.

- $C_G(x)$ consiste de los elementos de G que conmutan con x.
- $Z(G) = \bigcap_{x \in G} C_G(x) \trianglelefteq G$.
- El teorema anterior nos da, para $x \in G$:

  $$|GxG^{-1}| = |G : C_G(x)|$$

  O sea, la cantidad de elementos de la clase de conjugación de x es el índice del centralizador de x en G. En particular $|GxG^{-1}| \mid |G|$.

Definición. Sea $\mathrm{Subg}(G) = \{H : H < G\}$. Entonces $G \times \mathrm{Subg}(G) \to \mathrm{Subg}(G)$, $g \cdot H = gHg^{-1}$ es una acción. El estabilizador de $H \in \mathrm{Subg}(G)$ es

$$N_G(H) := G_H = \{g \in G : gHg^{-1} = H\} = \{g \in G : gH = Hg\}$$

y se llama *normalizador* de H en G.

Si $H, K < G$ y $H < N_G(K)$, decimos que H *normaliza* a K.

Observación 1.9.11.

- Sea $H < G$. Entonces $H \trianglelefteq G$ si y sólo si H es un punto fijo de esta acción, si y sólo si $N_G(H) = G$.
- $N_G(H)$ es el mayor subgrupo de G que tiene a H como subgrupo normal.
- El teorema anterior nos da, para $K < G$:

  $$|\{H < G : H \text{ es conjugado de } K\}| = |G : N_G(K)|$$

  O sea, la cantidad de subgrupos conjugados de K en G es el índice del normalizador de K en G. En particular, la cantidad de subgrupos conjugados de K divide $|G|$.

Proposición 1.55. *Sea G un grupo finito. Si $H < G$ es tal que $|G : H| = p$ donde p es el menor primo que divide $|G|$, entonces $H \lhd G$.*

Demostración. Hacemos actuar G en el conjunto G/H de coclases izquierdas de H en G, $G \times G/H \to G/H$, $g \cdot aH = gaH$. Observar que $|G/H| = p$; tenemos entonces un morfismo $\rho : G \to \mathrm{Sym}(G/H) \simeq S_p$. Sea $K = \ker \rho$. Si mostramos que $H = K$ ya está. Como $K \subset H$, basta ver que $|G : K| = |G : H|$.

Aplicando la propiedad universal del cociente a ρ, obtenemos una inyección de G/K en S_p, por lo tanto $|G : K| \mid |S_p| = p!$.

Por otro lado, por Lagrange $|G : K| \mid |G|$, y en la descomposición de $|G|$ aparece p como menor primo, por lo tanto $|G : K| = p$. □

Ecuación de clases Sea X un G-conjunto, donde $|X| < \infty$ (o más en general, donde $|X/G| < \infty$). Si tomamos $\{x_1, \ldots, x_n\}$ un conjunto de representantes de las órbitas, i.e. $\{o(x) : x \in X\} = \{o(x_1), \ldots, o(x_n)\}$ con $o(x_i) \cap o(x_j) = \varnothing$ si $i \neq j$, se tiene

$$X = \bigsqcup_{i=1}^{n} o(x_i) \;\Rightarrow\; |X| = \sum_{i=1}^{n} |o(x_i)| = \sum_{i=1}^{n} |G : G_{x_i}|$$

Como los puntos fijos son aquellos tales que $o(x) = \{x\}$, entonces necesariamente $X_0 \subset \{x_1, \ldots, x_n\}$. Escribiendo $\{x_1, \ldots, x_n\} = X_0 \sqcup (\{x_1, \ldots, x_n\} \backslash X_0)$, la ecuación de arriba queda:

$$|X| = |X_0| + \sum_{|G:G_{x_i}|>1} |G : G_{x_i}| \tag{1.12}$$

Cuando G es un grupo finito que actúa sobre sí mismo por conjugación, esta ecuación queda

$$|G| = |Z(G)| + \sum |G : C_G(x)|$$

donde x recorre un conjunto de representantes de las clases de conjugación con más de un elemento. Esta ecuación se llama *ecuación de clases*.

Teorema 1.56 (de Cauchy)**.** *Sea G un grupo finito, $p \mid |G|$. Entonces G tiene un elemento de orden p.*

Demostración. Por inducción en $|G|$.

Caso 1: $\exists y \in G \backslash Z(G) : p \nmid |G : C_G(y)|$.
$p \mid |G| = |G : C_G(y)||C_G(y)|$, entonces $p \mid |C_G(y)|$. Como $y \notin Z(G)$, entonces $C_G(y) \subsetneq G$, luego $|C_G(y)| < |G|$. Por hipótesis de inducción, $C_G(y)$ tiene un elemento de orden p, luego G también.

Caso 2: $\forall y \in G \backslash Z(G) : p \mid |G : C_G(y)|$.
Además $p \mid |G|$, luego por la ecuación de clases $|G| = |Z(G)| + \sum |G : C_G(y)|$, se tiene que $p \mid |Z(G)|$. Pero $Z(G)$ es un grupo abeliano, luego por el teorema fundamental de los grupos abelianos, existe $n \in \mathbb{Z}^+$ y otro grupo K tal que $Z(G) = \mathbb{Z}_{p^n} \times K$. Entonces $Z(G)$ (y por lo tanto G) tiene un elemento de orden p, por ejemplo (p^{n-1}, e). □

Corolario 1.57 (Grupos de orden 6)**.** *Todo grupo de orden 6 es isomorfo a S_3 (si no es abeliano) o a $\mathbb{Z}_6$ (si es abeliano).*

Demostración. Sea G un grupo de orden 6. Por Cauchy, G tiene un elemento a de orden 2 y un elemento b de orden 3. Si $ab = ba$, entonces $|ab| = 6$. En efecto, $(ab)^2 = b^2 \neq e$ y $(ab)^3 = a \neq e$, luego por Lagrange ab tiene orden 6. Se tendría entonces $G = \langle ab \rangle$, y G sería cíclico, luego isomorfo a $\mathbb{Z}_6$.

Supongamos entonces que $ab \neq ba$, en particular $bab^{-1} \neq a$. Además $a \neq e \Rightarrow bab^{-1} \neq e$. Entonces si $H = \langle a \rangle = \{1, a\}$, se tiene que $bab^{-1} \notin H$, por lo tanto $H \not\lhd G$.

Hacemos actuar G en G/H por multiplicación a izquierda. Esto nos da un morfismo $\rho : G \to \mathrm{Sym}(G/H) \simeq S_3$. Si $g \in \ker \rho$, entonces $gH = H$, luego $g \in H$. Como el núcleo es un subgrupo, debe ser $\ker \rho = \{e\}$ o $\ker \rho = H$. Pero no puede ser todo H, pues el núcleo siempre es un subgrupo normal y H no lo es, luego es $\ker \rho = \{e\}$ y ρ es inyectiva. Además tanto G como S_3 tienen orden 6, luego ρ es un isomorfismo. □

El corolario anterior es un caso particular del siguiente, que a su vez son casos particulares de la clasificación de grupos de orden pq, pero las pruebas nos parecieron interesantes de por sí.

Corolario 1.58. *Todo grupo finito de orden $2p$, con $p \neq 2$ primo, es cíclico o diedral.*

Demostración. Por Cauchy, el grupo G contiene elementos s y r de órdenes 2 y p respectivamente. Sea $H = \langle r \rangle$, entonces $|G : H| = 2$ luego $H \lhd G$. Como $s \notin H$, se tiene $G = H \cup Hs$, por lo tanto

$$G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}$$

Como H es normal, entonces $srs^{-1} = r^i$ para algún i. Teniendo en cuenta que $s = s^{-1}$ y que $srs^{-1} = r^i$, se obtiene

$$r = s^{-1}r^i s = sr^i s^{-1} = (r^i)^i = r^{i^2}$$

por lo tanto $i^2 \equiv 1$ (mód p). Es decir, $p \mid (i-1)(i+1)$, y por lo tanto $i \equiv \pm 1$ (mód p).

Si $i \equiv 1$ (mód p), entonces $sr = rs$, luego G es conmutativo, de orden $2p$, con mcd(p,2)=1, luego $G \simeq \mathbb{Z}_{2p}$.

Si $i \equiv -1$ (mód p), se tiene $srs^{-1} = r^{-1}$, luego $G \simeq \langle r, s \mid r^p, s^2, srsr \rangle \simeq D_p$. □

Ejercicios

Ej. 34 — $\mathrm{GL_n(k)}$ actúa en $\mathrm{M_n(k)}$ por conjugación. ¿Es una acción fiel? ¿Cuáles son sus puntos fijos? ¿Cómo es un conjunto de representantes de las órbitas?

Ej. 35 — El único grupo finito con dos clases de conjugación es $\mathbb{Z}_2$ (recordar el ejercicio 8).

Ej. 36 — Sean $g_1, \ldots, g_n$ representantes de las clases de conjugación de un grupo finito G. Para probar que G es abeliano basta probar que los g_i conmutan dos a dos.

Ej. 37 — Si G es un grupo de orden impar, entonces todo $x \in G$, $x \neq e$ no es conjugado a x^{-1}.

Ej. 38 — Una acción de G en X es *primitiva* si sólo preserva las particiones triviales de X. Más formalmente, consideremos la acción inducida $G \times \mathcal{P}(X) \to \mathcal{P}(X)$. Decimos que una partición $\pi(X)$ es *estabilizada* por G si $g \cdot A \in \pi(X)$ para todo $g \in G$ y $A \in \pi(X)$. De esta manera, la acción de G en X se dice primitiva si las únicas particiones de X estabilizadas por G son $\{X\}$ y $\{\{x\} : x \in X\}$.
Toda acción doblemente transitiva es primitiva.

Ej. 39 — Si una acción de G en X es primitiva y fiel, entonces la acción por restricción de H en X es transitiva, para cualquier subgrupo normal $H \lhd G$, $H \neq \{e\}$.

1.10. El grupo simétrico

En esta sección estudiamos uno de los más importantes ejemplos de grupo. La primera razón es histórica. Antes de llegar a la definición de grupo, Galois (∼1830) estudió los grupos de permutaciones de las raíces de polinomios de grado mayor que cuatro en búsqueda de una fórmula para estas raíces. Cauchy estudió poco después los grupos de permutaciones en general, y recién en 1854 Cayley dio la primera definición de grupo abstracto.

Definición. Sea X un conjunto. Definimos el *grupo simétrico* de X como el conjunto de biyecciones de X:

$$\mathrm{Sym}(X) := \{f : X \to X : f \text{ es una biyección}\}$$

Los elementos de $\mathrm{Sym}(X)$ se llaman *permutaciones*. Un subgrupo de un grupo simétrico se llama *grupo de permutaciones*. Cuando $X = \{1, \dots, n\}$, $n \geqslant 2$ el grupo simétrico *en n letras* $\mathrm{Sym}(\{1, \dots, n\})$ se nota S_n.

Notación. Dada una permutación $\sigma \in S_n$ adoptamos la notación

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

Observación 1.10.1. El orden de S_n es $n!$, por un sencillo argumento combinatorio.

Definición. Un r-ciclo, $2 \leqslant r \leqslant n$ es una permutación $\sigma \in S_n$ tal que:

- existen $i_1, \dots, i_r \in \{1, \dots, n\}$ distintos dos a dos tales que $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\dots$, $\sigma(i_r) = i_1$,
- $\sigma(x) = x$ para todo $x \in \{1, \dots, n\} \backslash \{i_1, \dots, i_r\}$

Notamos $\sigma = (i_1 \dots i_r)$. Decimos que r es la *longitud* del ciclo. Un 2-ciclo se llama una *transposición*.

Observación 1.10.2.

- $(i_1 \dots i_r) = (i_2 \dots i_r i_1) = \cdots = (i_r i_1 \dots i_{r-1})$,
- Si $\sigma = (i_1 \dots i_r)$ entonces $|\sigma| = r$ y $\sigma^{-1} = (i_r \dots i_1)$,
- Si $\sigma \in S_n$ es un r-ciclo y $x \in \{1, \dots, n\}$ es tal que $\sigma(x) \neq x$, entonces

$$\sigma = (x\, \sigma(x) \dots \sigma^{r-1}(x))$$

- Hay $\dfrac{n(n-1)\dots(n-r+1)}{r}$ r-ciclos diferentes en S_n. El factor $\frac{1}{r}$ se debe al primer ítem de esta observación.

Definición. Dos ciclos $(i_1 \dots i_r)$, $(j_1 \dots j_s)$ se dicen *disjuntos* si mueven lugares diferentes, i.e. si

$$\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \varnothing$$

Observación 1.10.3. Dos ciclos disjuntos conmutan.

Teorema 1.59. *Si $\sigma \in S_n$, $\sigma \neq id$ entonces σ se escribe en forma única (a menos de orden) como producto de ciclos disjuntos.*

Demostración. Sea $G = \langle \sigma \rangle$, y notemos $I_n = \{1, \ldots, n\}$. Tenemos una acción

$$G \times I_n \to I_n, \quad \sigma^j \cdot i \mapsto \sigma^j(i)$$

I_n se descompone como unión disjunta de órbitas:

$$I_n = I_n^\sigma \sqcup \bigsqcup_{i=1}^{t} o(x_i)$$

donde I_n^σ es el conjunto de puntos fijos, y $|o(x_i)| > 1$, $\forall i = 1, \ldots, t$. Pero

$$o(x_i) \approx G/G_{x_i}, \quad \sigma^r(x_i) \leftrightarrow \overline{\sigma^r}$$

y como $G_{x_i} < G = \langle \sigma \rangle$ entonces existe $m_i \in \mathbb{Z}^+$ tal que $G_{x_i} = \{\sigma^{m_i}\}$, de donde $G/G_{x_i} = \{\overline{\mathrm{id}}, \overline{\sigma}, \ldots, \overline{\sigma^{m_i-1}}\}$. Por lo tanto a través de la biyección,

$$o(x_i) = \{x_i, \sigma(x_i) \ldots, \sigma^{m_i-1}(x_i)\}$$

Para todo $i = 1, \ldots, t$ considere $\sigma_i = (x_i \sigma(x_i) \ldots \sigma^{m_i-1}(x_i))$, son ciclos disjuntos pues las órbitas lo son, y se tiene $\sigma = \sigma_1 \ldots \sigma_t$.

Unicidad: una descomposición $\sigma = \sigma_1 \ldots \sigma_t$ en producto de ciclos disjuntos se corresponde con una descomposición de I_n en órbitas (ignorando ciclos de largo 1 y órbitas con un solo elemento). Podemos olvidarnos los ciclos de largo 1, cambiar el orden de los ciclos, y cambiar cómo escribimos los ciclos (escogiendo diferentes posiciones iniciales, i.e. representantes para las órbitas) pero nada más, pues por la correspondencia las órbitas de σ deben ser respetadas. □

La prueba describe un algoritmo para hallar la descomposición: miro adónde va a parar el 1, luego adónde va a parar $\sigma(1)$, luego $\sigma^2(1)$ hasta que se cierre el ciclo. Luego tomo un elemento que no haya tocado en el ciclo recién construido, y repito el procedimiento. Así hasta agotar los elementos de la permutación.

Ejemplo 1.10.4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (13)(245)$.

Observación 1.10.5. Como los ciclos disjuntos conmutan (luego $(\sigma_i \sigma_j)^n = \sigma_i^n \sigma_j^n$), se deduce (ejercicio) que si $\sigma = \sigma_1 \ldots \sigma_r$ es la descomposición en ciclos disjuntos, entonces

$$|\sigma| = \mathrm{mcm}(|\sigma_1|, \ldots, |\sigma_r|)$$

Corolario 1.60. *Toda permutación se escribe como producto de transposiciones (no necesariamente de forma única).*

Demostración. Basta ver que todo ciclo lo verifica, pero

$$(i_1 \ldots i_r) = (i_1 i_r)(i_1 i_{r-1}) \ldots (i_1 i_3)(i_1 i_2)$$ □

Observación 1.10.6. Analicemos este ejemplo para clarificar cómo se lee un producto de ciclos. Empezamos de derecha a izquierda. Primero vemos que i_1 va a parar a i_2. Ahora buscamos si i_2 aparece alguna vez más en los ciclos posteriores. Como no aparece, entonces i_1 va a parar a i_2. Ahora, i_2 en el primer ciclo va a parar a i_1, y en el segundo ciclo i_1 va a parar a i_3, que no vuelve a aparecer, luego i_2 va a parar a i_3, y así sucesivamente.

El siguiente teorema es de un alto interés teórico. Nos dice que un grupo cualquiera puede ser pensado como subgrupo de un grupo de permutaciones. Un ejemplo claro de este fenómeno es el grupo diedral D_n, que podemos pensar como subgrupo (propio) de S_n.

Teorema 1.61 (Cayley)**.** *Sea G grupo. Existe un monomorfismo $\alpha : G \to \mathrm{Sym}(G)$.*

Demostración. Definimos $\alpha(g)(x) = gx$, i.e. $\alpha(g)$ es multiplicar a la izquierda por g: es la *representación regular* de G. $\alpha(g) \in \mathrm{Sym}(G)$ pues tiene como inversa a $\alpha(g^{-1})$. α es un morfismo:

$$\alpha(gg')(x) = (gg')x = g(g'x) = \alpha(g)(\alpha(g')(x)) \quad \forall x \in G \Rightarrow \alpha(gg') = \alpha(g)\alpha(g')$$

Es inyectiva: $\alpha(g) = \alpha(g') \Rightarrow gx = g'x \quad \forall x \in G$, en particular para e, luego $g = g'$. □

Observación 1.10.7. Podemos ver entonces a un grupo G de orden n como subgrupo de S_n, pero a lo mejor podemos verlo como subgrupo de un grupo simétrico más pequeño. Por ejemplo, D_n tiene orden $2n$. Cayley nos dice que podemos verlo como subgrupo de S_{2n}, pero D_n puede verse como subgrupo de S_n, enumerando los vértices del n-ágono.

Por otro lado, hay ejemplos de grupos donde el orden del grupo simétrico dado por Cayley no puede disminuirse. Tomemos el grupo de los cuaterniones Q, y veamos que no es subgrupo de S_i para cualquier $i \leqslant 7$. En otras palabras, veamos que no existe una acción fiel de Q sobre un conjunto A de i elementos, para $i \leqslant 7$.

En efecto, sea $\rho : Q \to \mathrm{Sym}(A)$ un morfismo. Si $a \in A$, entonces $|Q : Q_a| = |o(a)| \leqslant 7$, luego por Lagrange $|Q : Q_a| \in \{1, 2, 4\}$, i.e. $|Q_a| \in \{2, 4, 8\}$ y Q_a es un subgrupo no trivial de Q.

Ahora, recordemos que $\ker \rho = \bigcap_{x \in A} Q_x$ (observación 1.9.9). Por otro lado, es sencillo observar que todo subgrupo no trivial de Q contiene al subgrupo $\langle -1 \rangle$, por lo tanto el núcleo de ρ no es trivial, luego ρ no puede ser inyectiva.

1.10.1. Conjugación en S_n

La conjugación en S_n tiene una interpretación sencilla y similar a la conjugación de matrices. Dos permutaciones serán conjugadas si y sólo si "hacen lo mismo" pero en lugares diferentes. Pensemos en lo que sucede con las matrices. La matriz conjugada BAB^{-1} especifica la misma transformación lineal que A pero sobre una base nueva. En efecto, BAB^{-1} actúa de esta manera sobre los vectores vistos como combinación lineal de la base nueva:

- B^{-1} expresa el vector en la base original,
- A hace la transformación original,
- B expresa los vectores transformados a la base nueva.

Lo mismo va a estar sucediendo con las permutaciones en S_n. Consideremos $\sigma\tau\sigma^{-1}$. Podemos pensar que tenemos n cosas con etiquetas viejas $1, \ldots, n$ y $\sigma\tau\sigma^{-1}$ es la misma permutación pero reetiquetando las cosas: se la aplicamos a una permutación con las nuevas etiquetas,

- σ^{-1} convierte las etiquetas nuevas a las viejas,

- τ hace la transformación original,
- σ reetiqueta las cosas transformadas con las etiquetas nuevas.

De esta manera podemos pasar por ejemplo de $(123)(45)$ a $(513)(24)$ con $\sigma = (235)$ (verificarlo).

Definición. Decimos que dos permutaciones *son del mismo tipo* si consisten del mismo número de ciclos disjuntos del mismo largo.

Adoptaremos una notación para el tipo de una permutación que es más sencillo de describir mediante un ejemplo:

Ejemplo 1.10.8.
- $(12)(3456)$ y $(123)(456)$ no son del mismo tipo.
- (12) y (34) son del mismo tipo que notamos 2,
- $(12)(34)$ y $(13)(24)$ son del mismo tipo que notamos 2 2,
- $(523)(14)$ y $(617)(32)$ son del mismo tipo que notamos 3 2, etc.

Proposición 1.62. *Dos permutaciones en S_n son conjugadas en S_n si y sólo si son del mismo tipo. En particular, todos los r-ciclos son conjugados en S_n.*

Demostración. ($\Rightarrow$) Basta ver que conjugar un r-ciclo es un r-ciclo. Sea $\sigma \in S_n$, entonces

$$\sigma\,(i_1 \dots i_r) = (\sigma(i_1) \dots \sigma(i_r))\,\sigma \Rightarrow \sigma\,(i_1 \dots i_r)\,\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_r)) \tag{1.13}$$

La primera igualdad es un juego de palabras: primero mover las letras y luego aplicar σ es lo mismo que primero aplicar σ y luego mover las letras movidas por σ.

($\Leftarrow$) Escribo $\tau = (i_1 \dots i_r) \dots (j_1 \dots j_s)$, $\eta = (i'_1 \dots i'_r) \dots (j'_1 \dots j'_s)$. Definamos σ:

$$\sigma = \begin{pmatrix} i_1 & \dots & i_r & \dots & j_1 & \dots & j_s \\ i'_1 & \dots & i'_r & \dots & j'_1 & \dots & j'_s \end{pmatrix}$$

y se tiene que $\sigma\tau\sigma^{-1} = \eta$, como queríamos. Observar que σ hace lo que describíamos en la discusión informal anterior: "reetiquetar las cosas transformadas con las etiquetas nuevas". □

Observación 1.10.9. La igualdad (1.13) es interesante. No sólo nos dice que conjugar un ciclo τ es un ciclo, sino además *qué* ciclo. En particular si τ manda k en l entonces la conjugación $\sigma\tau\sigma^{-1}$ manda $\sigma(k)$ en $\sigma(l)$.

Miremos la ecuación de clases en este caso particular. Si la cantidad de clases de conjugación de S_n es k y x_i son representantes (por lo tanto aparece una permutación de cada tipo), notando $c(x_i)$ la clase de conjugación de x_i:

$$|S_n| = 1 + \sum_{i=1}^{k} |c(x_i)|$$

Analicemos el caso particular de S_4: tenemos 4 clases de conjugación no triviales,[15]

[15] Ignorar la última columna hasta no haber leído la sección 1.10.2.

Tipo de permutación	Representante	# en la clase de conj.	Paridad
1	id	1	par
2	(12)	6	impar
3	(123)	8	par
2 2	(12)(34)	3	par
4	(1234)	6	impar

Observación 1.10.10.

- La tercera columna corresponde a la ecuación de clases.
- Es fácil verificar que los elementos de tipo 2 2 junto con la identidad forman un subgrupo de S_4 (y de A_4, ver sección 1.10.3). Siendo además unión de clases de conjugación, es por lo tanto un subgrupo normal de orden 4 (de A_4 y de S_4), sin elementos de orden 4 y por lo tanto isomorfo a $\mathbf{V}$. Esto muestra que S_4 (y A_4) no son simples.

1.10.2. Signo de una permutación

Teorema 1.63. *Si $\sigma \in S_n$ se descompone como dos productos de transposiciones:*

$$\sigma = \tau_1 \dots \tau_r = \tau'_1 \dots \tau'_{r'}$$

entonces $r \equiv r'$ (mód 2).

Demostración. Observemos primero que $\tau^{-1} = \tau$ para cualquier transposición τ. Entonces combinando las dos igualdades obtenemos una representación de la permutación identidad como producto de $r + r'$ transposiciones:

$$\mathrm{id} = \sigma\sigma^{-1} = \tau_1 \dots \tau_r \tau'_{r'} \dots \tau'_1$$

Basta entonces probar que la identidad sólo se puede escribir como un número par de transposiciones, pues entonces $r + r'$ es par y se deduce la tesis. Escribamos pues

$$\mathrm{id} = (a_1 b_1) \dots (a_k b_k)$$

con $k \geqslant 1$ y $a_i \neq b_i$. Veamos que k es par por inducción en k.

El caso $k = 1$ no se puede dar pues la identidad no se puede escribir como una transposición no trivial. Supongamos entonces que si la identidad se escribe como producto de menos de k transposiciones entonces k es par.

Alguna de las $(a_i b_i)$ para $i \geqslant 2$ debe mover a_1 si queremos que ese producto sea la identidad. Esto es, algún $(a_i b_i)$ tiene a a_1, podemos suponer que algún $a_i = a_1$.

Afirmo que podemos suponer $i = 2$, en cuyo caso

$$\mathrm{id} = (a_1 b_1)(a_1 b_2)\sigma' \tag{1.14}$$

En efecto, si i no es 2 entonces de todas maneras podemos correr $(a_1 b_i)$ hasta el comienzo: si a, b, c, d son números diferentes entonces las fórmulas

$$(cd)(ab) = (ab)(cd), \quad (bc)(ab) = (ac)(bc)$$

muestran que cualquier producto de dos transposiciones en el que el segundo factor mueve a y el primero no, puede ser escrito como producto de dos transposiciones en las que el primer factor mueve a y el segundo no. Aplicamos esto $i-2$ veces y obtenemos la forma deseada.

Suponemos entonces $i=2$. Si $b_2=b_1$ entonces la ecuación (1.14) reduce la identidad a un producto de $k-2$ transposiciones. Por hipótesis de inducción $k-2$ es par, luego k es par, y terminamos.

En el caso $b_2 \neq b_1$ se tiene $(a_1b_1)(a_1b_2)=(a_1b_2)(b_1b_2)$, y por lo tanto

$$\mathrm{id}=(a_1b_2)(b_1b_2)(a_3b_3)\dots(a_kb_k)$$

Repetimos el argumento anterior: alguno de los a_i para $i\geqslant 4$ debe mover a_3. O reducimos el número de transposiciones en dos en una descomposición de la identidad, y terminamos por hipótesis de inducción, o de nuevo reescribimos la descomposición con el mismo número de transposiciones pero con una transposición menos que mueve a_1.

Este proceso debe terminar llegando al caso en que dos transposiciones se cancelan, porque no podemos terminar con una descomposición de la identidad como producto de transposiciones en que solo la primera mueve a_1. Por lo tanto k es par. □

El teorema anterior nos permite hacer la siguiente

Definición. Si $\sigma\in S_n$ se escribe como producto de r transposiciones, definimos su *signo* como $\epsilon(\sigma)=(-1)^r$. Decimos que σ es *par* si tiene signo 1, de lo contrario es *impar*.

Ejemplo 1.10.11.

- Una transposición tiene signo -1.
- La identidad se escribe como $(12)(12)$, por lo tanto tiene signo 1.
- La descomposición de un r-ciclo en $r-1$ transposiciones

$$(i_1\dots i_r)=(i_1i_r)(i_1i_{r-1})\dots(i_1i_3)(i_1i_2)$$

  muestra que un r-ciclo es par si y sólo si r es impar.

Teorema 1.64. *Existe un único morfismo no trivial $S_n\to\mathbb{Z}^*=\{\pm1\}$, y este morfismo es $\epsilon: S_n\to\{\pm1\}$.*

Demostración. Existencia: Ya sabemos que ϵ no es trivial pues vale -1 en toda transposición. Es morfismo: sean $\sigma,\sigma'\in S_n$ tales que se escriben como producto de k,k' transposiciones respectivamente. Entonces $\sigma\sigma'$ se escribe como producto de $k+k'$ transposiciones, por lo tanto

$$\epsilon(\sigma\sigma')=(-1)^{k+k'}=(-1)^k(-1)^{k'}=\epsilon(\sigma)\epsilon(\sigma')$$

Unicidad:

Paso 1: Si $\tau\in S_n$ es una transposición, entonces $h(\tau)=h(12)$.

Si $\tau=(12)$ ya está.

Si τ mueve o 1 o 2 (no ambos): supongo que mueve a 1, el otro caso es análogo. Entonces $\tau=(1b)$, $b>2$. Observar que

$$(1b)=(2b)(12)(2b)$$

y si le aplicamos h a la ecuación, nos queda

$$h(1b)=h(2b)h(12)h(2b)=[h(2b)]^2h(12)=h(12)$$

usando que $h(12)$ y $h(2b)$ conmutan pues $\{\pm 1\}$ es conmutativo, y que en $\{\pm 1\}$ todo elemento es idempotente (i.e. $1^2 = (-1)^2 = 1$).

Si τ no mueve ni a 1 ni a 2, entonces $\tau = (ab)$, $a, b > 2$. Observar que

$$(ab) = (1a)(2b)(12)(2b)(1a)$$

y si le aplicamos h a la ecuación, nos queda

$$h(ab) = h(1a)h(2b)h(12)h(2b)h(1a) = [h(1a)]^2[h(2b)]^2 h(12) = h(12)$$

por las mismas razones de antes.

Paso 2: El valor de $h(\sigma)$ para cualquier permutación σ.

Escribo σ como producto de k transposiciones. Por el Paso 1, las k transposiciones tienen la misma imagen por h, llamémosle $u \in \{\pm 1\}$, luego $h(\sigma) = u^k$.

Si $u = 1$, h es trivial, y si $u = -1$ entonces $h(\sigma) = (-1)^k = \epsilon(\sigma)$ para todo $\sigma \in S_n$. □

1.10.3. El grupo alternado

Definición. Sea $n \geqslant 3$. El *grupo alternado en n letras*, notado A_n, es el subgrupo de S_n que consiste de las permutaciones pares.

Observación 1.10.12.

- $A_n = \ker \epsilon$, por lo tanto $A_n \lhd S_n$.
- Más aún, es de índice 2: $\epsilon : S_n \to \{\pm 1\}$ es un morfismo sobreyectivo, por lo tanto $\frac{S_n}{A_n} \simeq \{\pm 1\}$, luego $|S_n : A_n| = |\frac{S_n}{A_n}| = 2 \Rightarrow |A_n| = \frac{n!}{2}$.

Proposición 1.65. *El grupo alternado A_n está generado por los 3-ciclos.*

Demostración. Si $\sigma \in A_n$, $\sigma \neq \mathrm{id}$ entonces σ es producto de un número par de transposiciones. Veamos entonces que el producto no trivial de dos transposiciones puede ser escrito como producto de 3-ciclos:

$$(ij)(kl) = \begin{cases} (ijl) & \text{si } j = k \\ (ijk)(jkl) & \text{si } i, j, k, l \text{ son distintas} \end{cases}$$

que son todos los casos posibles de un producto de dos transposiciones, i.e. o todas las letras son distintas, o podemos suponer que las de en medio son las iguales. □

Lema 1.66. *Si G es un grupo finito y $N \lhd G$ entonces todo elemento de G con orden coprimo a $|G : N|$ está en N. En particular, si N tiene índice 2 entonces todo elemento de G con orden impar está en N.*

Demostración. Sea $g \in G$ de orden m coprimo con $|G : N|$. La ecuación $g^m = e$ se transforma en $\overline{g}^m = \overline{e}$ en G/N. Además $\overline{g}^{|G/N|} = \overline{g}^{|G:N|} = \overline{e}$, luego el orden de $\overline{g}$ en G/N divide a m y a $|G : N|$, que son coprimos, por lo tanto $\overline{g} = \overline{e}$, i.e. $g \in N$. □

Veamos ahora que A_4 no es Lagrangiano:

Proposición 1.67. *Ningún subgrupo de A_4 tiene índice 2.*

Demostración. Si A_4 tiene un subgrupo de índice 2, entonces tiene orden 6. Por otro lado, por el lema anterior tiene a todo elemento de A_4 de orden impar. Pero hay 8 elementos de orden 3 en A_4 (los 8 diferentes 3-ciclos), absurdo. □

Ya vimos en 1.10.10 que A_4 no es simple. Veamos que es la excepción. Para ello, probamos primero algunos lemas.

Por la proposición 1.62, ya sabemos que los 3-ciclos son conjugados en S_n. Ahora nos preguntamos si son conjugados *como elementos de* A_n. Cuando $n = 4$ no, por ejemplo (123) y (132) no son conjugados en A_4. Pero para $n \geqslant 5$ sí:

Lema 1.68. *Si $n \geqslant 5$, los 3-ciclos son conjugados en A_n.*

Demostración. Como la conjugación es una relación de equivalencia, basta ver que cualquier 3-ciclo $\sigma \in A_n$ es conjugado a (123) en A_n. Por la proposición 1.62, existe $\pi \in S_n$ tal que

$$(123) = \pi\sigma\pi^{-1}$$

Si $\pi \in A_n$ ya está. Si no, sea $\pi' = (45)\pi \in A_n$: como $(45)^{-1} = (45)$ entonces

$$\pi'\sigma\pi'^{-1} = (45)\pi\sigma\pi^{-1}(45) = (45)(123)(45) = (123)$$ □

Lema 1.69. *A_5 es simple.*

Demostración. Sea $N \lhd A_5$, $N \neq \{\mathrm{id}\}$. Si probamos que N contiene un 3-ciclo terminamos, pues por normalidad de N y el lema 1.69, N los contiene a todos, y por 1.66 se tiene que $N = A_n$.

Sea $\sigma \in N$, $\sigma \neq \mathrm{id}$. Entonces σ tiene orden 3, 4 o 5, luego es de tipo 3, 2 2, o 5. Si σ es de tipo 3 ya está. Si $\sigma = (ab)(cd)$, entonces N contiene

$$\overbrace{((abe)(ab)(cd)(abe)^{-1})}^{\in N \text{ pues } N\lhd A_5}(ab)(cd) = (be)(cd)(ab)(cd) = (aeb)$$

Si $\sigma = (abcde)$ entonces N contiene

$$\overbrace{((abc)(abcde)(abc)^{-1})}^{\in N \text{ pues } N\lhd A_5}(abcde)^{-1} = (adebc)(aedcb) = (abd)$$

En cualquier caso N contiene un 3-ciclo, y ya está. □

Lema 1.70. *Si $n \geqslant 5$ entonces toda $\sigma \in A_n$, $\sigma \neq id$ tiene una conjugada $\sigma' \neq \sigma$ que coincide con σ en algún i, i.e. tal que $\sigma(i) = \sigma'(i)$ para algún $i = 1, \ldots, n$.*

Demostración. Sea $\sigma \in A_n$, $\sigma \neq \mathrm{id}$. Escribimos σ como producto de ciclos disjuntos y notamos r a la mayor longitud de ciclo que aparece en la descomposición. Reetiquetando los índices podemos suponer

$$\sigma = (1 \ldots r)\pi$$

donde $(1 \ldots r)$ y π son disjuntos.

Si $r \geqslant 3$, sea $\tau = (345)$ y $\sigma' = \tau\sigma\tau^{-1}$. Entonces

$$\sigma'(1) = \tau\sigma\tau^{-1}(1) = \tau\sigma(1) = \tau(2) = 2 = \sigma(1)$$
$$\sigma'(2) = \tau\sigma\tau^{-1}(2) = \tau\sigma(2) = \tau(3) = 4 \neq 3 = \sigma(2)$$

y ya está. Si $r = 2$ entonces σ es producto de transposiciones disjuntas. Si es producto de al menos tres, entonces $n \geqslant 6$ y reetiquetando (ver observación 1.10.13) podemos suponer

$$\sigma = (12)(34)(56)\dots$$

Sea $\tau = (12)(35)$ y $\sigma' = \tau\tilde{\sigma}\tau^{-1}$. Entonces

$$\sigma'(1) = \tau\sigma\tau^{-1}(1) = \tau\sigma(2) = \tau(1) = 2 = \sigma(1)$$
$$\sigma'(3) = \tau\sigma\tau^{-1}(3) = \tau\sigma(5) = \tau(6) = 6 \neq 4 = \sigma(3)$$

y ya está. Si es producto de dos transposiciones disjuntas, entonces reetiquetando podemos suponer

$$\sigma = (12)(34)\dots$$

Sea $\tau = (132)$ y $\sigma' = \tau\sigma\tau^{-1} = (13)(24)$. Entonces $\sigma' \neq \sigma$ y ambos fijan 5. □

Observación 1.10.13. ¿Por qué podemos hacer esas suposiciones acerca de cómo es σ? Es decir, si σ tiene un ciclo $(i_1 \dots i_r)$, ¿por qué podemos suponer que es $(1 \dots r)$? Si el lector ya está convencido, sírvase seguir adelante con su lectura. De lo contrario, aquí va una explicación más formal.

Consideremos una permutación $\tau \in S_n$ tal que $1 \mapsto i_1, \dots, r \mapsto i_r$. Consideremos

$$\tau A_n \tau^{-1} = \{\tau\psi\tau^{-1} : \psi \in A_n\}$$

Definamos el isomorfismo $\phi : A_n \to \tau A_n \tau^{-1}$, $\psi \mapsto \tau\psi\tau^{-1}$. $\phi : \sigma \mapsto \tau\sigma\tau^{-1}$, y como $(i_1 \dots i_r)$ es el ciclo más largo de σ en A_n, entonces

$$\tau\sigma\tau^{-1}(i_1 \dots i_r) \overset{1,13}{=} (\tau(i_1) \dots \tau(i_r)) = (1 \dots r)$$

es el ciclo más largo de $\tau\sigma\tau^{-1}$ en $\tau A_n \tau^{-1}$. Entonces, "reetiquetando σ" significa trabajar mediante el isomorfismo ϕ con $\sigma\tau\sigma^{-1}$ en $\tau A_n \tau^{-1}$.

Teorema 1.71. *A_n es simple si y sólo si $n = 3$ o $n \geqslant 5$. En particular, para estos n A_n no tiene subgrupos de índice 2.*

Demostración. Ya vimos en el ejemplo 1.10.10 que A_4 no es simple. Además A_3 es simple porque es de orden 3. Basta ver que si $n \geqslant 5$ entonces A_n es simple.

Por inducción en n. Por el lema 1.70, podemos suponer $n \geqslant 6$. Consideremos la acción natural $A_n \times \{1, \dots, n\} \to \{1, \dots, n\}$, y consideremos los subgrupos estabilizadores G_i que fijan i, de manera que $G_i \simeq A_{n-1}$ que es simple por hipótesis de inducción (y porque $n \geqslant 6$).

Sea $N \lhd A_n$, $N \neq \{\mathrm{id}\}$. Veremos que $N = A_n$ probando que N contiene un 3-ciclo. Sea $\sigma \in N$, $\sigma \neq \mathrm{id}$. Por el lema 1.71, existe σ' conjugada de σ tal que $\sigma' \neq \sigma$, $\sigma'(i) = \sigma(i)$ para algún i. Como $N \lhd A_n$ entonces $\sigma' \in N$.

Entonces $\sigma^{-1}\sigma' \in N$ no es la identidad y fija i:

$$\sigma^{-1}\sigma'(i) = \sigma^{-1}(\sigma(i)) = i$$

por lo tanto $N \cap G_i$ es un subgrupo no trivial de G_i, y es normal en G_i pues lo es en A_n. Pero G_i es simple, luego $N \cap G_i = G_i$, por lo tanto $G_i \subset N$. Pero G_i contiene un 3-ciclo (construido con 3 índices cualesquiera diferentes de i), entonces N también contiene un 3-ciclo y ya está. □

Corolario 1.72. *Si $n \geqslant 5$, el único subgrupo normal propio de S_n es A_n. En particular S_n tiene un único subgrupo de índice 2, que es A_n.*

Demostración. Sea $N \lhd S_n$ propio. Entonces $N \cap A_n \lhd A_n$, que es simple.

Si $N \cap A_n = A_n$, entonces $N \supset A_n$ que tiene índice 2 en S_n, luego $N = A_n$ o $N = S_n$.

Si $N \cap A_n = \{e\}$, el mapa $\pi|_N \colon N \to \frac{S_n}{A_n}$, $n \mapsto \overline{n}$ es inyectivo, luego N tiene orden 1 o 2. Pero N no puede tener orden 2, pues al ser normal es unión de clases de conjugación, y no hay una clase de conjugación unitaria no trivial en S_n por el corolario 1.63 (recordando que una clase de conjugación es unitaria si y sólo si el elemento está en el centro, ver observación 1.9.6). Entonces $N = \{e\}$. □

1.11. Series subnormales

Definición. Sea G grupo. Una cadena de subgrupos

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G \tag{1.15}$$

donde cada uno es normal en el siguiente, se llama una *serie subnormal* de G. Decimos que los subgrupos G_i son *subnormales* en G. Si además cada $G_i \lhd G$, entonces (1.15) se llama *serie normal* de G.

Los grupos cociente G_{i+1}/G_i son los *factores* de la serie.

Una serie subnormal es más una "filtración" de G que una descomposición: si leemos (1.15) de derecha a izquierda, es como ir imponiendo filtros cada vez más rigurosos a G.

Ejemplo 1.11.1.

1. Todo grupo tiene al menos una serie subnormal, que es la trivial $\{e\} \lhd G$. Si G es simple, entonces es la única.

2. Un grupo puede tener series subnormales con factores no isomorfos, por ejemplo $\{0\} \lhd \langle 2\rangle \lhd \mathbb{Z}_6$ y $\{0\} \lhd \langle 3\rangle \lhd \mathbb{Z}_6$.

3. Dos grupos no isomorfos pueden tener series subnormales con factores isomorfos. Por ejemplo, $\{0\} \lhd \langle 2\rangle \lhd \mathbb{Z}_{2n}$ y $\{1\} \lhd \langle R\rangle \lhd D_n$ son series subnormales de $\mathbb{Z}_{2n}$ y de D_n respectivamente, con factores cíclicos de orden n y 2. Observar además que si n es una potencia de 2 entonces $\mathbb{Z}_{2n}$ no es un producto semidirecto de $\mathbb{Z}_2$ con $\mathbb{Z}_n$.

4. Si G es un producto directo, entonces induce una serie subnormal con factores isomorfos a los factores del producto. Por ejemplo, si $G = H_1 \times H_2 \times H_3$, entonces

   $$\{(e,e,e)\} \lhd H_1 \times \{e\} \times \{e\} \lhd H_1 \times H_2 \times \{e\} \lhd H_1 \times H_2 \times H_3$$

   es una serie subnormal de G con factores isomorfos a H_1, H_2 y H_3.

   Sin embargo, no toda serie subnormal proviene de una descomposición del grupo en factores isomorfos a los factores de la serie. En el ejemplo anterior, los factores de D_n son $\mathbb{Z}_n$ y $\mathbb{Z}_2$, y D_n no es producto directo de éstos pues no es abeliano.

Definición. Una serie subnormal de G es un *refinamiento* de otra si introdujo más subgrupos subnormales en medio. Si ninguno de los nuevos factores es el grupo trivial, entonces el refinamiento es *no trivial*.

Proposición 1.73. *1. Si $H < G$, entonces si intersectamos una serie subnormal de G como (1.15) con H, obtenemos una serie subnormal para H:*

$$\{e\} = H \cap G_0 \lhd H \cap G_1 \lhd \cdots \lhd H \cap G_r = H$$

Además los factores sucesivos de esta serie son isomorfos a subgrupos de los factores sucesivos de (1.15).

2. Si $N \lhd G$, entonces si (1.15) es una serie subnormal de G, obtenemos una serie subnormal para G/N:

$$\{\overline{e}\} = \overline{G}_0 \lhd \overline{G}_1 \lhd \cdots \lhd \overline{G}_r = G/N \tag{1.16}$$

donde $\overline{G}_i := (NG_i)/N$. Además los factores sucesivos son isomorfos a cocientes de los factores sucesivos de (1.15).

Demostración. 1. Consideremos el morfismo obvio (incluir y proyectar): $\pi : H_{i+1} := H \cap G_{i+1} \to G_{i+1}/G_i$. Entonces

$$\ker \pi = H_{i+1} \cap G_i = (H \cap G_{i+1}) \cap G_i = H \cap G_i = H_i$$

Entonces $H_i \lhd H_{i+1}$, y además H_{i+1}/H_i es isomorfo a un subgrupo de G_{i+1}/G_i.

2. Al ser $N \lhd G$ y $G_i < G$ obtenemos $NG_i < G$ para todo i.

   Tenemos que $N \lhd NG_i$ pues $N \lhd G$. Entonces $NG_i/N \lhd NG_{i+1}/N$ pues $G_i \lhd G_{i+1}$. Obtenemos entonces que (1.16) es una serie subnormal para G/N.

   Combinando los teoremas de isomorfismo con la observación $NG_{i+1} = (NG_i)G_{i+1}$ se obtiene

$$\frac{NG_{i+1}/N}{NG_i/N} \overset{3^{\text{er}}\text{teo.}}{\simeq} \frac{NG_{i+1}}{NG_i} = \frac{(NG_i)G_{i+1}}{NG_i} \overset{2^{\circ}\text{teo.}}{\simeq} \frac{G_{i+1}}{G_{i+1} \cap G_iN} \overset{3^{\text{er}}\text{teo.}}{\simeq} \frac{G_{i+1}/G_i}{(G_{i+1} \cap NG_i)/G_i}$$

   luego los factores de (1.16) son isomorfos a cocientes de (1.15). □

A continuación consideramos las series subnormales *maximales*:

Definición. Una serie subnormal que no se puede refinar no trivialmente y no tiene repeticiones se llama *serie de composición*. La cantidad de subgrupos subnormales (descontando el trivial) que aparecen en la descomposición es el *largo* de la serie de composición, por ejemplo r en (1.15) si es una serie de composición.

Observación 1.11.2. Una serie subnormal no se puede refinar no trivialmente si y sólo si todos los factores son simples. Esto se deduce de la correspondencia entre los subgupos normales de un cociente H/N y los subgrupos normales de H.

Por lo tanto, una serie es de composición si y sólo si todos sus factores son simples y no triviales.

De esta manera, una serie de un grupo abeliano es de composición si y sólo si sus factores tienen orden primo.

Si pensamos en una serie subnormal como una "factorización" del grupo, un refinamiento sería una factorización mayor, y una serie de composición sería como una factorización en factores primos. Evitar las repeticiones sería como evitar unos en una factorización.

Ejemplo 1.11.3. 1. Un refinamiento no trivial de $\{1\} \lhd \langle R^2 \rangle \lhd D_n$ es $\{1\} \lhd \langle R^2 \rangle \lhd \langle R \rangle \lhd D_n$. Si $n = 4$ esta serie no se puede refinar más pues todos los factores tienen orden 2: es una serie de composición para D_4. Otra serie de composición para D_4 es $\{1\} \lhd \langle S \rangle \lhd \langle R^2, S \rangle \lhd D_4$. Ambas series de composición tienen los mismos factores.

2. $\{1\} \lhd \langle R^2 \rangle \lhd \langle R \rangle \lhd D_6$ y $\{1\} \lhd \langle R^3 \rangle \lhd \langle R^3, S \rangle \lhd D_6$ son dos series de composición de D_6. Ambas tienen factores una vez $\mathbb{Z}_3$ y dos veces $\mathbb{Z}_2$, pero aparecen en otro orden. Probaremos que esto ocurre en general.

3. Una serie subnormal para S_4 es $\{1\} \lhd A_4 \lhd S_4$, que a su vez podemos refinar (recordar observación 1.10.10) a

$$\{1\} \lhd \mathbf{V} \lhd A_4 \lhd S_4 \tag{1.17}$$

$\mathbf{V}$ tiene como subgrupo normal al subgrupo cíclico U generado por un elemento de orden 2, y obtenemos entonces la serie

$$\{1\} \lhd U \lhd \mathbf{V} \lhd A_4 \lhd S_4 \tag{1.18}$$

que no se puede refinar no trivialmente porque cada subgrupo tiene índice primo en el subgrupo siguiente. Ésta es entonces una serie de composición para S_4 de largo 4.

Proposición 1.74. *Todo grupo finito no trivial tiene una serie de composición.*

Demostración. Por inducción en $|G|$. Empezamos con la serie subnormal trivial $\{e\} \lhd G$. Si G es simple entonces es una serie de composición y ya está. Si no, G tiene un subgrupo normal no trivial N, y obtenemos $\{e\} \lhd N \lhd G/N$.

Si N y G/N son simples, entonces es de composición y ya está. Si no, continuamos refinando no trivialmente. Este proceso debe parar, pues G es finito y se tiene, por transitividad de índices:

$$|G| = |G_r : G_{r-1}| \dots |G_2 : G_1||G_1 : G_0| \geqslant 2^r \qquad \square$$

Observación 1.11.4. Los grupos infinitos pueden no tener una serie de composición. Por ejemplo $\mathbb{Z}$ no tiene. En efecto, si $\{0\} \lhd m\mathbb{Z} \lhd \cdots \lhd \mathbb{Z}$ es una serie subnormal, entonces por ejemplo $\{0\} \lhd 2m\mathbb{Z} \lhd m\mathbb{Z} \lhd \cdots \lhd \mathbb{Z}$ también lo es.

Teorema 1.75 (Jordan-Hölder)**.** *Si G es un grupo no trivial y*

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

$$\{e\} = \tilde{G}_0 \lhd \tilde{G}_1 \lhd \cdots \lhd \tilde{G}_s = G$$

son dos series de composición para G, entonces $r = s$ y para alguna permutación $\pi \in S_r$ se tiene $\tilde{G}_i/\tilde{G_{i-1}} \simeq G_{\pi(i)}/G_{\pi(i)-1}$ para $1 \leqslant i \leqslant r$.

En otras palabras, el largo de una serie de composición para G es único, y los factores (con multiplicidades) también (aunque no necesariamente aparecen en el mismo orden).

Observación 1.11.5. Esto nos permite especificar cómo "todo grupo finito (o más en general, todo grupo que admite una serie de composición) está construido a partir de grupos simples". Dado un grupo G con una serie de composición, los factores determinan ciertos (únicos por Jordan-Hölder) grupos simples H_i. Ya vimos en el tercer ejemplo de 1.11.1 que no podemos esperar recuperar un único grupo solamente a partir del largo de una serie de composición y de sus factores. Hay que especificar *cómo* los factores se juntan para formar un grupo mayor. Hacer esta descripción equivale a describir las posibles extensiones de H_i,

$$e \longrightarrow K_i \longrightarrow G_i \longrightarrow H_i \longrightarrow e$$

donde G_i son los subgrupos subnormales de la serie de composición, $H_i = G_i/G_{i-1}$, y $K_i \simeq G_{i-1}$. Por lo tanto, sabemos que un grupo que admite una serie de composición se construye tomando extensiones de ciertos grupos simples, pero saber exactamente *cómo* es el problema de la extensión que ya comentamos. El tercer ejemplo de 1.11.1 nos muestra que el problema de la extensión no se resuelve con algo tan sencillo como un producto semidirecto.

Este problema está ausente en la analogía con los números primos, pues determinan un único número que es la multiplicación.

Para probar el teorema, empezamos con un lema técnico.

Lema 1.76 (Zassenhaus)**.** *Sea G grupo, $A \lhd A^* < G$, $B \lhd B^* < G$. Entonces se tiene $A(A^* \cap B) \lhd A(A^* \cap B^*)$ y $B(B^* \cap A) \lhd B(B^* \cap A^*)$, y hay un isomorfismo*

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \simeq \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$$

Demostración. Probemos primero que $A \cap B^* \lhd A^* \cap B^*$; intercambiando las letras obtenemos también $A^* \cap B \lhd A^* \cap B^*$.

Sea $c \in A \cap B^*$, $x \in A^* \cap B^*$. Entonces $xcx^{-1} \in A$ pues $c \in A$ y $x \in A^* \rhd A$. También $xcx^{-1} \in B^*$ pues $c, x \in B^*$. Por lo tanto $xcx^{-1} \in A \cap B^*$, y ya está.

Por lo tanto se tiene $D := (A \cap B^*)(A^* \cap B) \lhd A^* \cap B^*$. Definamos ahora un isomorfismo

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \simeq \frac{A^* \cap B^*}{D}$$

en cuyo caso ya está, pues intercambiando las letras obtenemos otro isomorfismo

$$\frac{B(A^* \cap B^*)}{B(A \cap B^*)} \simeq \frac{A^* \cap B^*}{D}$$

y componiendo isomorfismos obtenemos el deseado.

Sea $\varphi : A(A^* \cap B^*) \to (A^* \cap B^*)/D$, $ax \mapsto xD$, donde $a \in A$ y $x \in A^* \cap B^*$.

φ está bien definida: si $ax = a'x'$, entonces $(a')^{-1}a = x'x^{-1} \in A \cap (A^* \cap B^*) = A \cap B^* < D$, luego $x'x^{-1} \in D$, i.e. $xD = x'D$.

φ es morfismo: $\varphi(axa'x') \overset{A \lhd A'}{=} \varphi(a''xx') = xx'D = \varphi(ax)\varphi(a'x)$.

Es un ejercicio sencillo verificar que φ es sobreyectiva y que $\ker \varphi = A(A^* \cap B)$; el primer teorema de isomorfismo concluye la demostración. □

Teorema 1.77 (de refinamiento de Schreier)**.** *Dos series subnormales de un grupo admiten refinamientos equivalentes, i.e. con mismos factores. Esto es, dadas dos series subnormales, podemos insertar subgrupos subnormales de manera que los factores sean isomorfos, contando multiplicidades.*

Demostración. Sean

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

y

$$\{e\} = \tilde{G}_0 \lhd \tilde{G}_1 \lhd \cdots \lhd \tilde{G}_s = G$$

series subnormales para G. La idea es insertar una copia de la segunda serie entre cada G_i y G_{i+1} de la primera serie, y una copia de la primera serie entre cada G_j y G_{j+1} de la segunda serie. El lema de Zassenhaus nos va a permitir probar que estas nuevas series largas son series subnormales, refinamientos de las originales con factores isomorfos.

Sea $G_{ij} = G_i(G_{i+1} \cap \tilde{G}_j)$. Se tiene que $G_{ij} < G_{i+1}$ pues $G_i \lhd G_{i+1}$, luego $G_{ij} < G_{i(j+1)}$. Obtenemos entonces la serie

$$\cdots < G_i < G_{i1} < \cdots < G_{is} = G_{i+1} < \ldots$$

Análogamente, si $\tilde{G}_{pq} = \tilde{G}_p(\tilde{G}_{p+1} \cap G_q)$, se obtiene la serie

$$\cdots < \tilde{G}_p < \tilde{G}_{p1} < \cdots < \tilde{G}_{ps} = \tilde{G}_{r+1} < \dots$$

Ambas series largas tienen rs términos. Para cada i, j aplicamos el lema de Zassenhaus a los subgrupos $G_i \lhd G_{i+1}$ y $\tilde{G}_j \lhd \tilde{G}_{j+1}$: nos dice que las dos series largas son series subnormales, por lo tanto refinamientos de las series originales; y que hay un isomorfismo

$$\frac{G_{ij}}{G_{i(j+1)}} = \frac{G_i(G_{i+1} \cap \tilde{G}_{j+1})}{G_i(G_{i+1} \cap \tilde{G}_j)} \simeq \frac{\tilde{G}_j(\tilde{G}_{j+1} \cap G_{i+1})}{\tilde{G}_j(\tilde{G}_{j+1} \cap G_i)} = \frac{\tilde{G}_{ij}}{\tilde{G}_{i(j+1)}}$$

La asociación $G_{ij}/G_{i(j+1)} \mapsto \tilde{G}_{ij}/\tilde{G}_{i(j+1)}$ es una biyección, por lo tanto los dos refinamientos son equivalentes. □

Ahora el teorema de Jordan-Hölder es un sencillo corolario:

Demostración. Sea G un grupo con dos series de composición. Como una serie de composición sólo se puede refinar de manera trivial, el teorema de Schreier nos dice entonces que ambas series tienen factores isomorfos, contando multiplicidades. □

Damos otro corolario del teorema de Schreier:

Corolario 1.78. *Si G es un grupo con una serie de composición, entonces toda serie subnormal se puede refinar a una serie de composición.*

Demostración. Refinamos la serie subnormal y la serie de composición a un refinamiento equivalente por Schreier. De nuevo, una serie de composición sólo se puede refinar trivialmente, luego la serie subnormal se refina a una serie de composición. □

Observación 1.11.6. La factorización única en números primos es un caso particular del teorema de Jordan-Hölder para grupos cíclicos finitos:

Sea $n \geqslant 2$. Como $\mathbb{Z}_n$ es abeliano, una serie de composición de $\mathbb{Z}_n$ tendrá factores cíclicos de orden primo. Por lo tanto si (1.15) es una serie de composición para $G = \mathbb{Z}_n$, y si $p_i = |G_{i+1} : G_i|$, entonces se tiene $n = p_1 \dots p_r$, y obtenemos una factorización en primos de n. Esto prueba la existencia de una factorización.

Si $n = p_1 \dots p_r$ es una factorización de n en números primos, entonces la serie

$$\{0\} \lhd \langle p_1 \dots p_r \rangle \lhd \langle p_2 \dots p_r \rangle \lhd \cdots \lhd \langle p_r \rangle \lhd \langle 1 \rangle = \mathbb{Z}_n$$

es una serie de composición para $\mathbb{Z}_n$ con factores primos de orden $p_1, \dots, p_r$. Comparando esta serie con una serie subnormal arbitraria como (1.15) para $G = \mathbb{Z}_n$, se tiene entonces, por Jordan-Hölder, que dos descomposiciones de n en primos son iguales.

1.11.1. Grupos resolubles

Definición. Un grupo G es *resoluble* si existe una serie subnormal de G

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

tal que los factores G_{i+1}/G_i son abelianos. Decimos que esta serie es una serie *abeliana*.

Ejemplo 1.11.7.

- Todo grupo abeliano G es resoluble, tomando la serie trivial $\{0\} \lhd G$.
- S_3 es un grupo no abeliano y resoluble, pues $\{1\} \lhd A_3 \lhd S_3$ tiene factores $A_3/\{1\} \simeq \mathbb{Z}_3$ y $S_3/A_3 \simeq \mathbb{Z}_2$.
- S_4 también es resoluble, pues la serie (1.17) es abeliana: $V/\{1\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, $A_4/V \simeq \mathbb{Z}_3$ y $S_4/A_4 \simeq \mathbb{Z}_2$.

  Obtenemos además que A_4 es un grupo resoluble que no es Lagrangiano (recordar la proposición 1.68).
- Recordemos (ejemplo 1.2.4) que $Z(\mathrm{SL_n(k)}) = \mu_n(\mathrm{k})\mathrm{I_n}$. Tenemos entonces la serie

$$\{I_n\} \lhd \mu_n(k)I_n \lhd \mathrm{SL_n(k)} \lhd \mathrm{GL_n(k)}$$

  Si n no es primo, ésta no suele ser una serie de descomposición, pues $\mu_n(k)$ es cíclico de orden n.

  Esta serie no suele ser abeliana, pues (recordar ejemplos 1.2.4 y 1.3.9) mientras que el primer y último cocientes son abelianos, $\mathrm{SL_n(k)}/\mu_n(\mathrm{k})\mathrm{I_n} = \mathrm{PSL_n(k)}$ no suele ser abeliano.
- En el corolario 1.90 demostraremos que los grupos de orden p^n son resolubles.
- **Teorema de Burnside**: Todo grupo de orden $p^a q^b$ es resoluble. La demostración más sencilla de este teorema usa la teoría de caracteres. Como corolarios, todo grupo de orden $p^a q^b$ es simple; además, todo grupo finito no abeliano simple debe tener orden divisible por tres primos diferentes.
- **Teorema de Feit-Thompson, 1963**: Todo grupo finito de orden impar es resoluble. La demostración de este teorema está muy lejos del alcance del humilde redactor de estas notas. Lo enunciamos por completitud y como curiosidad, pero no usaremos el resultado.

La siguiente proposición dice que "ser resoluble" es una propiedad cerrada bajo subgrupos, cocientes, extensiones de grupos, y productos.

Proposición 1.79. *Se cumple:*

1. *Si G es resoluble y $H < G$, entonces H es resoluble.*
2. *Si G es resoluble y $N \lhd G$, entonces G/N es resoluble.*
3. *Si $N \lhd G$ son tal que N y G/N son resolubles, entonces G es resoluble. En particular el producto directo de grupos resolubles es resoluble.*
4. *Si $H, K < G$ son subgrupos resolubles, y $H \lhd G$, entonces HK es resoluble.*

Demostración. 1. Basta aplicar el primer ítem de 1.74 a una serie abeliana de G, y observar que un subgrupo de un grupo abeliano es abeliano.

2. Basta aplicar el segundo ítem de 1.74 a una serie abeliana de G, y observar que un cociente de un abeliano es abeliano.

3. Sea $\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = N$ una serie abeliana de N. Recordando que los subgrupos normales de un cociente K/N son de la forma H/N para $H \lhd K$, una serie abeliana de G/N es de la forma $\{e\} = H_0/N \lhd H_1/N \lhd \cdots \lhd H_s/N = G/N$, donde $N_k = H_0 \lhd H_1 \cdots \lhd H_s = G$. Entonces una serie abeliana de G es

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = H_0 \lhd H_1 \lhd \cdots \lhd H_s = G$$

   En particular, como $H \times K/H \simeq K$, se deduce que $H \times K$ es resoluble.

4. Por el segundo teorema de isomorfismo, $HK/H \simeq K/(H \cap K)$, que es resoluble pues es cociente de K (usando el segundo ítem de esta proposición). Tenemos entonces que HK/H y H son resolubles, luego por el tercer ítem de esta proposición HK también es resoluble. □

Proposición 1.80. *Un grupo finito es simple y resoluble si y sólo si es cíclico de orden primo.*

Demostración. Si un grupo es cíclico de orden primo, entonces es abeliano y no tiene subgrupos propios, luego es simple y resoluble.

Recíprocamente, sea G finito, simple y resoluble. Al ser simple, G admite una única serie subnormal $\{e\} \lhd G$, y al ser G resoluble, $G/\{e\} \simeq G$ debe ser abeliano. Por lo tanto todos sus subgrupos son normales, luego al ser simple no puede tener subgrupos propios. Sea $g \in G$, $g \neq 0$. Entonces $\langle g \rangle \neq \{0\}$, y como G no tiene subgrupos propios debe ser $G = \langle g \rangle$, i.e. G es cíclico. Pero un grupo cíclico finito tiene subgrupos para todos los divisores del orden del grupo (ver ejercicio 10), luego el orden de G debe ser primo. □

Corolario 1.81. *Son equivalentes:*

1. *G es finito y resoluble,*

2. *G tiene una serie normal con factores cíclicos de orden primo,*

3. *G tiene una serie de composición con factores cíclicos de orden primo.*

Demostración. $(1 \Rightarrow 2 \Rightarrow 3)$ G tiene una serie abeliana: sus factores son finitos, abelianos y resolubles por la proposición 1.80: entonces por la proposición anterior, deben ser cíclicos de orden primo. Ésta es además su serie de composición, pues sus factores son no triviales de orden primo (observación 1.11.2).

$(3 \Rightarrow 1)$ Si G tiene una serie de composición con factores cíclicos de orden primo, entonces es una serie abeliana de G. □

Corolario 1.82. *Si $n \geqslant 5$, entonces A_n y S_n no son resolubles.*

Demostración. Ya sabemos que A_n es simple si $n \geqslant 5$ (teorema 1.72), luego al ser finito, para ser resoluble debería ser cíclico de orden primo, y no lo es.

Por el corolario 1.73, la única serie de composición de S_n es $\{1\} \lhd A_n \lhd S_n$. Si S_n fuera resoluble, entonces al ser finito, por el corolario anterior los factores deberían ser cíclicos de orden primo. Pero A_n no es cíclico de orden primo, entonces ya está. □

Para terminar la sección, damos otra caracterización de los grupos resolubles.

Definición. Sea G grupo, $x, y \in G$. El *conmutador* de x e y es

$$[x, y] := x^{-1}y^{-1}xy$$

El nombre se debe a que $xy = yx[x, y]$.

Proposición 1.83. *Los conmutadores cumplen las siguientes propiedades:*

- $xy = yx \iff [x, y] = e$.
- $[x, y]^{-1} = [y, x]$.
- *Si $\varphi : G \to H$ es morfismo de grupos, entonces $\varphi([x, y]) = [\varphi(x), \varphi(y)]$. En particular $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.*

Demostración. El único ítem que no es obvio es el último:

$$\varphi([x, y]) = \varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) = [\varphi(x), \varphi(y)]$$

Se deduce $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$ tomando $H = G$ y φ la conjugación por g. □

Definición. El subgrupo de G generado por todos los conmutadores se llama *subgrupo conmutador* o *subgrupo derivado*, y se nota $[G, G]$ o G'.

Proposición 1.84. *Sea G grupo.*

- *G es abeliano si y sólo si $G' = \{e\}$.*
- *G'* char *G,*[16] *en particular $G' \lhd G$.*
- *Si $G' < H < G$ entonces $H \lhd G$.*
- *G/G' es abeliano.*
- *Si $N \lhd G$, entonces G/N es abeliano si y sólo si $G' < N$.*

Demostración.

- G es abeliano $\iff [x, y] = e \ \ \forall x, y \in G \iff G' = \{e\}$.
- Todo elemento de G' es de la forma $[x_1, y_1] \dots [x_n, y_n]$. Sea $\varphi \in \mathrm{Aut}(G)$. Entonces

$$\begin{aligned}\varphi([x_1, y_1] \dots [x_n, y_n]) &= \varphi([x_1, y_1]) \dots \varphi([x_n, y_n]) \\ &= [\varphi(x_1), \varphi(y_1)] \dots [\varphi(x_n), \varphi(y_n)] \in G'\end{aligned}$$

  luego G' char G.

- Sea H tal que $G' < H < G$ y sean $g \in G, h \in H$. Se tiene

$$(ghg^{-1})^{-1} = g^{-1}hg = (hh^{-1})(g^{-1}hg) = h[h, g] \in H$$

  luego $ghg^{-1} \in H$ y $H \lhd G$.

[16] Más aún, G' es invariante bajo cualquier *endo*morfismo de G. Un tal subgrupo se dice *totalmente característico* ("fully characteristic" en inglés).

- Sean $xG', yG' \in G/G'$. Se tiene

  $$(xG')(yG') = (yG')(xG') \iff xyG' = yxG' \iff x^{-1}y^{-1}xy \in G' \iff [x,y] \in G'$$

  lo cual es cierto, luego G/G' es abeliano.

- Si $G' < N$, entonces por el tercer teorema de isomorfismo $G/N \simeq (G/G')/(N/G')$ que es un cociente de un grupo abeliano por el ítem anterior, luego G/N es abeliano.

  Recíprocamente, si G/N es abeliano entonces $(xN)(yN) = (yN)(xN)$, luego $[x,y] = x^{-1}y^{-1}xy \in N$. Entonces todos los conmutadores están en N, luego el subgrupo que generan también, i.e. $G' < N$. □

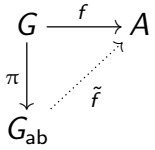
Observación 1.11.8. Las últimas dos propiedades nos dicen que G' es el menor subgrupo normal de G tal que el cociente es abeliano.

De esta manera, el tamaño del subgrupo conmutador nos da una idea de "cuán lejos" está el grupo de ser abeliano: a menor subgrupo conmutador, más "abelianidad". Es un rol "dual" al que cumple el centro: a mayor centro, más "abelianidad".

Más evidencia de esta "dualidad" es que todo subgrupo contenido en el centro es normal, mientras que todo subgrupo que contiene al conmutador es normal.

Definición. Sea G grupo. El grupo abeliano G/G' se llama *abelianización* de G y se denota G_{ab}.

Proposición 1.85 (Propiedad universal de la abelianización)**.** *Sea G grupo. Entonces cualquier homomorfismo de grupos $f : G \to A$ donde A es un grupo abeliano se factoriza a través de G_{ab}. Es decir: existe un único morfismo $\tilde{f}$ tal que el siguiente diagrama conmuta:*



Demostración. Si $g, h \in G$ entonces

$$f([g,h]) = f(g^{-1}h^{-1}gh) = f(g)^{-1}f(h)^{-1}f(g)f(h) = [f(g), f(h)] = e$$

pues A es abeliano. Por lo tanto $G' \subset \ker f$, y la existencia y unicidad de $\tilde{f}$ se siguen de la propiedad universal del cociente. □

Definición. Definimos el *subgrupo derivado n-ésimo* por recursión:

$$G^{(0)} := G \qquad G^{(n+1)} := \left(G^{(n)}\right)'$$

Esto es, el derivado n-ésimo es el conmutador del conmutador del conmutador... n veces. La *serie derivada* de G es

$$G = G^{(0)} \rhd G' = G^{(1)} \rhd \cdots \rhd G^{(n)} \rhd \dots$$

Observación 1.11.9. Como los subgrupos conmutadores son característicos y la propiedad de ser característico es transitiva, la serie derivada es una serie normal.

Teorema 1.86. *Un grupo es resoluble si y sólo si tiene una serie derivada que* estabiliza, *i.e. si existe un* $n \in \mathbb{Z}^+$ *tal que*

$$G = G^{(0)} \rhd G' = G^{(1)} \rhd \cdots \rhd G^{(n)} = \{e\}$$

Además la serie derivada es la menor serie abeliana de un grupo resoluble.

Demostración. Si $n \in \mathbb{Z}^+$ es tal que $G^{(n)} = \{e\}$, entonces su serie derivada es una serie resoluble para G, pues $G^{(i)}/G^{(i+1)}$ es abeliano.

Recíprocamente, sea

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

una serie abeliana de G. Como G/G_1 es abeliano, entonces $G_1 > G'$. Además $G_2 \lhd G_1$, luego $G'G_2 < G_1$. El segundo teorema de isomorfismo nos da $G'/(G' \cap G_2) \simeq G'G_2/G_2 < G_1/G_2$ que es conmutativo, luego $G'/(G' \cap G_2)$ es conmutativo, luego $G'' < G' \cap G_2 < G_2$. Continuando por inducción, se tiene $G^{(i)} < G_i$ para todo i, y por lo tanto $G^{(n)} = \{e\}$. □

1.12. p-grupos y los teoremas de Sylow

Definición. Sea p primo. Un p-grupo es un grupo finito G tal que $|G| = p^n$ para algún $n \in \mathbb{N}$.

Proposición 1.87. *Un grupo finito G es un p-grupo si y sólo si todo elemento tiene orden una potencia de p.*

Demostración. ($\Rightarrow$) Por el teorema de Lagrange.

($\Leftarrow$) Supongamos que existe q primo distinto de p tal que $q \mid |G|$. Entonces por Cauchy G tiene un elemento de orden q, que no es una potencia de p, absurdo. □

Observación 1.12.1. La proposición anterior nos habilita a definir un p-grupo G más generalmente como un grupo donde todo elemento tiene orden una potencia de p, y entonces G no tiene por qué ser finito. Como no trabajaremos con estos p-grupos infinitos, no nos hacemos problema con esta disquisición.

Teorema 1.88. *Todo p-grupo no trivial G tiene centro no trivial. Equivalentemente, si G es un p-grupo no trivial, entonces $p \mid |Z(G)|$.*

Demostración. La equivalencia se sigue del teorema de Lagrange. Probemos la segunda formulación. Sea G un p-grupo no trivial. Entonces $|G : C_G(y)|$ es una potencia de p, para todo y en la ecuación de clases:

$$|G| = |Z(G)| + \sum |G : C_G(y)|$$

Como $|G : C_G(y)| > 1$, entonces $|G : C_G(y)|$ es una potencia de p que no es p^0 para todo y, luego $p \mid \sum |G : C_G(y)|$. Pero además $p \mid |G|$, luego $p \mid |Z(G)|$. □

Corolario 1.89. *Todo p-grupo finito es resoluble.*

Demostración. Por inducción en el orden de G. Como el centro $Z(G)$ es no trivial, la hipótesis de inducción nos da que $G/Z(G)$ es resoluble. Por el tercer ítem de 1.80, como $Z(G)$ y $G/Z(G)$ son resolubles, entonces G es resoluble. □

Teorema 1.90. *Todo p-grupo tiene subgrupos normales de todos los órdenes posibles.*

Demostración. Sea G grupo, $|G| = p^n$. Veamos que G tiene subgrupos normales de orden p^m, para todo $m \leqslant n$, por inducción en n. Para $n = 0$ el resultado es trivial.

Supongamos que el resultado vale para grupos de orden $n - 1$. Si $|G| = p^n$, por el teorema anterior $p \mid |Z(G)|$. El teorema de Cauchy nos dice que existe $g \in Z(G)$ de orden p. Consideremos el subgrupo de orden p, $N = \langle g \rangle \lhd G$, pues $\langle g \rangle < Z(G)$.

Consideremos ahora el cociente G/N: es un grupo de orden $|G|/|N| = p^{n-1}$, luego por hipótesis de inducción G/N tiene subgrupos normales de orden p^m para todo $m \leqslant n - 1$.

La correspondencia entre subgrupos normales del cociente G/N y subgrupos normales $H \lhd G$ que contienen a N nos garantiza la existencia de subgrupos normales de G de orden p^m, para todo $m \leqslant n$. □

Lema 1.91. *Sea G grupo. Si $H < Z(G)$ es tal que G/H es cíclico, entonces G es abeliano.*

Demostración. Supongo $G/H = \langle aH \rangle$. Afirmo que $G = \langle a \rangle H$.

En efecto, si $g \in G$ entonces $gH = a^i H$, luego $a^{-i} g \in H$: existe $h \in H$ tal que $a^{-i} g = h$. Se tiene entonces $g = a^i h$, i.e. $g \in \langle a \rangle H$.

Por lo tanto todo elemento de G es de la forma $a^i h$, $i \in \mathbb{Z}$. Sean entonces $g = a^i h, g' = a^{i'} h' \in G$:

$$gg' = (a^i h)(a^{i'} h') \overset{h \in Z(G)}{=} a^i a^{i'} h h' \overset{h \in Z(G)}{=} a^{i'} a^i h' h \overset{h' \in Z(G)}{=} a^{i'} h' a^i h = g' g \qquad \square$$

Teorema 1.92. *Todo grupo de orden p^2 es conmutativo. Por lo tanto si $|G| = p^2$ entonces $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ o $G \simeq \mathbb{Z}_{p^2}$.*

Demostración. Sea G de orden p^2. Entonces G es un p-grupo no trivial, luego $Z(G) \neq \{e\}$.

Si $|Z(G)| = p$, entonces $|G/Z(G)| = p$, luego $G/Z(G)$ es cíclico: por el lema anterior, esto implica que G es abeliano.

Si $|Z(G)| = p^2$, entonces $Z(G) = G$ y G es abeliano. $\square$

Lema 1.93. *Sea G un p-grupo que actúa en un conjunto finito X. Entonces*

$$|X| \equiv |X_0| \pmod{p}$$

Demostración. Considero la "ecuación de clases general" (1.12):

$$|X| = |X_0| + \sum |G : G_x| \quad \text{con } |G : G_x| > 1 \tag{1.19}$$

Se tiene que $|G : G_x| \mid |G| = p^n$, y además $|G : G_x| > 1$,entonces $p \mid |G : G_x|$.

Se deduce la tesis reduciendo módulo p la ecuación (1.19). $\square$

Corolario 1.94. *Si G es un p-grupo, entonces $|Z(G)| \equiv |G|$ (mód p).*

Demostración. Considerar la acción de G sobre sí mismo por conjugación y aplicar el lema. $\square$

Definición. Sea G grupo, $p \mid |G|$. Un subgrupo de G es un *p-subgrupo de Sylow* si su orden es la mayor potencia de p que divide $|G|$ (i.e. un p-subgrupo de Sylow es un p-subgrupo de orden maximal).

Notamos $\mathrm{Syl}_p(G) = \{p\text{-subgrupos de Sylow de } G\}$.

El siguiente teorema nos garantiza la existencia de p-subgrupos para todas las potencias de p posibles; en particular, nos garantiza la existencia de p-subgrupos de Sylow.

Teorema 1.95 (Sylow I)**.** *Sea G un grupo finito. Si $p^r \mid |G|$ entonces G tiene un subgrupo de orden p^r.*

Demostración. Si probamos que G tiene un p-subgrupo de Sylow ya está, en virtud del teorema 1.91. Sea entonces r maximal: escribimos $|G| = p^r m$, donde $p \nmid m$.

Consideremos $X = \{\text{subconjuntos de } X \text{ de tamaño } p^r\}$ y la acción

$$G \times X \to X, \qquad g \cdot A = gA := \{ga : a \in A\}$$

Observar que efectivamente gA tiene tamaño p^r, $a \mapsto ga$ es una biyección de A en gA, luego la acción está bien definida.

Dado $A \in X$, consideramos $H = \text{Stab}(A) < G$. Afirmo que $|H| \leqslant p^r$. En efecto, dado $a_0 \in A$ se tiene que $H \to A$, $h \mapsto ha_0$ es una inyección de H en A, que tiene tamaño p^r. Por lo tanto

$$|G| = |G : H||H| = |o(A)| \overbrace{|H|}^{\leqslant p^r} \tag{1.20}$$

por el teorema de la órbita y el estabilizador.

Ahora, si podemos probar que existe un A tal que $p \nmid |o(A)|$, entonces H es el subgrupo que estamos buscando. En efecto, si $p \nmid |o(A)|$ entonces como $|G| = p^r m$ con $p \nmid m$, se debe tener $p^r \mid |H| \leqslant p^r$ (por la ecuación 1.20), luego $|H| = p^r$ y ya está.

Probemos que existe un tal A. Consideremos X como unión disjunta de órbitas, $X = \bigsqcup o(A)$. Se tiene entonces

$$|X| = \sum |o(A)|$$

Esta ecuación muestra que si pruebo que $p \nmid |X|$, entonces debe existir un A tal que $p \nmid |o(A)|$, terminando la demostración. Ahora bien,

$$\begin{aligned} |X| = \binom{p^r m}{p^r} &= \frac{(p^r m)!}{(p^r m - p^r)!(p^r)!} = \frac{(p^r m)(p^r m - 1)\dots(p^r m - p^r + 1)(p^r m - p^r)!}{(p^r m - p^r)!(p^r)!} \\ &= \frac{p^r m \dots (p^r m - i)\dots(p^r m - p^r + 1)}{p^r \dots (p^r - i)\dots(p^r - p^r + 1)} \end{aligned}$$

Observar la simetría entre el numerador y el denominador, con $i = 0, \dots, p^r - 1$. Consideremos aquellos i tales que $p \mid (p^r m - i)$. La mayor potencia p^k de p que divide $p^r m - i$ es la misma que la mayor potencia de p que divide a i, pues $i < p^r$ implica $k \leqslant r$ ya que $p \nmid m$.

De la misma manera, para aquellos i tales que $p \mid (p^r - i)$, la mayor potencia de p que divide $p^r - i$ debe ser la mayor potencia de p que divide a i.

Por lo tanto los términos correspondientes en el numerador y el denominador que son divisibles por p, son divisibles por las mismas potencias de p, luego se cancelan todas las potencias de p en el cociente y $p \nmid |X|$, terminando la demostración. □

Lema 1.96. *Sea $P \in \text{Syl}_p(G)$, $H < G$ un p-subgrupo. Si H normaliza a P, i.e. si $H < N_G(P)$, entonces $H < P$. En particular, si $H \in \text{Syl}_p(G)$ y H normaliza a P, se tiene $H = P$.*

Demostración. Para probar $H \subset P$ probaremos $HP = P$. En efecto, si $HP = P$, entonces dado $h \in H$ se tiene que si $p \in P$, entonces $hp = p' \in P$ para algún $p' \in P$, luego $h = p'p^{-1} \in P \Rightarrow h \in P$.

Obviamente $P \lhd N_G(P)$ y $H < N_G(P)$. Por lo tanto $HP < N_G(P)$. Podemos entonces aplicar el segundo teorema de isomorfismo:

$$\frac{H}{H \cap P} \simeq \frac{HP}{P}$$

Entonces como $|H|$ es potencia de p, $|H|/|H \cap P|$ es potencia de p, luego $|HP|/|P|$ es potencia de p, i.e. $|HP : P|$ es potencia de p.

Por otro lado $|HP| = |HP : P||P|$, y $P \in \text{Syl}_p(G)$, luego $|P|$ es la mayor potencia de p que divide $|G|$, y como $HP \subset G$, también $|P|$ es la mayor potencia de p que divide $|HP|$.

Entonces $|HP : P|$ no tiene factores de p, pero recién vimos que $|HP : P|$ es potencia de p, por lo tanto debe ser $|HP : P| = 1$, i.e. $HP = P$ y la demostración está terminada.

Si además H es de Sylow, entonces $H \subset P$ y tienen mismo orden, luego $H = P$. □

Teorema 1.97 (Sylow II)**.** *Sea G grupo finito, $|G| = p^r m$, $p \nmid m$. Entonces:*

a) Todos los p-subgrupos de Sylow son conjugados.

b) Si $s_p = |\mathrm{Syl}_p(G)|$, entonces $s_p \equiv 1$ (mód p) y $s_p \mid m$. Además $s_p = |G : N_G(P)|$ para cualquier $P \in \mathrm{Syl}_p(G)$.

c) Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow.

Demostración. Para toda la prueba consideramos la acción de G en $X = \mathrm{Syl}_p(G)$ por conjugación: $G \times X \to X$, $g \cdot P = gPg^{-1}$. Está bien definida porque conjugar un p-subgrupo de Sylow da un p-subgrupo de Sylow (la condición "ser de Sylow" sólo es una condición en el orden del subgrupo, y conjugar un subgrupo da un subgrupo con el mismo orden).

a) Sea O una G-órbita. Queremos probar que $O = X$, i.e. que la acción es transitiva.

Sabemos que $O \neq \varnothing$ por el teorema de Sylow I que nos garantiza la existencia de p-subgrupos de Sylow. Sea $P \in O$. Entonces la acción se restringe a $P \times O \to O$.

O puede partirse en varias P-órbitas, una de las cuales es $\{P\}$ pues $qPq^{-1} = P$ para todo $q \in P$. Pero esta es la única órbita unitaria, pues $\{Q\}$ es P-órbita $\iff$ P normaliza a Q $\iff$ $Q = P$ pues $P \in \mathrm{Syl}_p(G)$ y el lema 1.97. Entonces aplicando el lema 1.94 se obtiene

$$|O| \equiv 1 \pmod{p} \tag{1.21}$$

Supongamos que existe $R \notin O$. Entonces de nuevo la acción de G se restringe a una acción $R \times O \to O$, y el mismo razonamiento de recién se aplica probando que no hay órbitas unitarias. El lema 1.94 nos da ahora que $|O| \equiv 0$ (mód p), esto contradice la ecuación (1.21). Por lo tanto $O = X$.

b) Recién probamos que $O = \mathrm{Syl}_p(G)$, entonces la ecuación (1.21) nos da $s_p \equiv 1$ (mód p).

Sea $P \in \mathrm{Syl}_p(G)$. Por a), se tiene $s_p = |o(P)| = |G : N_G(P)|$. Entonces:

$$s_p = |G : N_G(P)| = \frac{|G|}{|N_G(P)|} = \frac{|G|}{|N_G(P) : P||P|} = \frac{p^r m}{|N_G(P) : P| p^r} = \frac{m}{|N_G(P) : P|}$$

y por lo tanto $s_p \mid m$.

c) Sea $H < G$ un p-subgrupo. La acción de G en X por conjugación se restringe a $H \times X \to X$. Tenemos:

$$|X_0| \overset{\text{lema } 1,94}{\equiv} |X| \overset{b)}{\equiv} 1 \pmod{p}$$

luego $|X_0| \neq 0$, i.e. $X_0 \neq \varnothing$: existe $P \in X$ tal que $o(P) = \{P\}$, i.e. tal que $hPh^{-1} = P$ para todo $h \in H$. Esto significa que $H \subset N_G(P)$, luego por el lema 1.97 se tiene $H \subset P$. □

Corolario 1.98. *Sea P un p-subgrupo de Sylow de G. Son equivalentes:*

I. *$P \lhd G$,*

II. *P es el único p-subgrupo de Sylow de G (i.e. $s_p = 1$),*

III. *P char G.*

Demostración. ($i. \Rightarrow ii.$) Si $P, Q \in \mathrm{Syl}_p(G)$, $P \lhd G$: entonces por Sylow IIa) existe $g \in G$ tal que $Q = gPg^{-1} \overset{P \lhd G}{=} P$.

($ii. \Rightarrow i.$) Si $\mathrm{Syl}_p(G) = \{P\}$, entonces como $gPg^{-1} \in \mathrm{Syl}_p(G)$ para todo $g \in G$, se tiene $gPg^{-1} = P$ para todo $g \in G$, i.e. $P \lhd G$.

($ii. \Rightarrow iii.$) Si $\alpha \in \mathrm{Aut}(G)$, entonces $|\alpha(P)| = |P|$, luego como $\alpha(P) \in \mathrm{Syl}_p(G)$ se tiene $\alpha(P) = P$.

($iii. \Rightarrow i.$) Siempre. □

Corolario 1.99. *Si p y q son factores primos diferentes de $|G|$ tales que $s_p = 1$ y $s_q = 1$, entonces los elementos del p-subgrupo de Sylow conmutan con los elementos del q-subgrupo de Sylow.*

Demostración. Sea P el p-subgrupo de Sylow, Q el q-subgrupo de Sylow. Como P y Q tienen orden coprimo, se intersectan trivialmente (corolario 1.16). Además, el corolario anterior nos dice que son normales en G. Si $a \in P$ y $b \in Q$, se tiene:

$$aba^{-1}b^{-1} = \overbrace{aba^{-1}}^{\in Q} b^{-1} = a \overbrace{ba^{-1}b^{-1}}^{\in P} \in P \cap Q = \{e\}$$

luego $ab = ba$ y ya está. □

Corolario 1.100. *Sea G grupo con un solo p-subgrupo de Sylow para todo $p \mid |G|$, i.e. $s_p = 1 \quad \forall p \mid |G|$. Entonces G es producto directo de sus p-subgrupos de Sylow.*

Demostración. Descomponiendo el orden de G en factores primos diferentes, tenemos $|G| = p_1^{n_1} \dots p_r^{n_r}$. Sea P_i el p_i-subgrupo de Sylow, para $i = 1, \dots, r$. Consideremos el mapa

$$P_1 \times \cdots \times P_r \to G, \qquad (x_1, \dots, x_m) \mapsto x_1 \dots x_m$$

Es un morfismo de grupos pues los elementos de P_i conmutan con los de P_j si $i \neq j$ por el corolario anterior. Es inyectivo pues el orden de un producto de elementos que conmutan y tienen órdenes coprimos es igual al producto de los órdenes (recordar el ejercicio 18). Entonces como dominio y codominio tienen mismo orden, el mapa es un isomorfismo. □

Ejemplo 1.12.2 (Grupos de orden 99). Veamos que todo grupo G de orden $99 = 11 \times 3^2$ tiene que ser abeliano, de dos maneras diferentes:

1ª manera: Tenemos $s_{11} \mid 9$ y $s_{11} \equiv 1$ (mód 11), luego $s_{11} = 1$. Análogamente $s_3 = 1$. Por lo tanto G tiene sólo un 3-subgrupo de Sylow (que tiene orden 3^2 luego es conmutativo) y sólo un 11-subgrupo de Sylow (que tiene orden primo luego es conmutativo). Entonces G es producto directo de estos dos subgrupos que son conmutativos, luego es abeliano.

2ª manera: Tenemos $s_{11} = 1$, luego G tiene sólo un 11-subgrupo de Sylow $N \lhd G$. Sea Q un 3-subgrupo de Sylow, i.e. $Q < G, |Q| = 9$. Pero $\mathrm{mcd}(|N|, |Q|) = 1$ luego (corolario 1.16) $N \cap Q = \{e\}$, y $|G| = |N||Q|$, por lo tanto $G = NQ$.

Como $N \lhd G$, se tiene que $G = N \rtimes_\theta Q$, para un cierto $\theta : Q \to \mathrm{Aut}(N)$. Ahora, $|\mathrm{Aut}(N)| = 10$ (teorema 1.34), que es coprimo con $|Q| = 9$, luego por el corolario 1.16, θ debe ser el morfismo trivial, i.e. G es producto directo de N y Q que son abelianos, luego G es abeliano.

Teorema 1.101 (Grupos de orden pq, $p < q$)**.** *Sea G de orden pq, con $p < q$. Si $p \nmid q-1$, entonces $G \simeq \mathbb{Z}_{pq}$. Si $p \mid q-1$, entonces hay dos clases de isomorfismo: $\mathbb{Z}_{pq}$ y cierto grupo no abeliano.*

Demostración. Sea $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$, Entonces $|G : Q| = p$ que es el menor primo que divide $|G|$, por lo tanto (proposición 1.55) se tiene $Q \lhd G$.

Como $\mathrm{mcd}(|P|, |Q|) = 1$, entonces $P \cap Q = \{e\}$, y $|G| = |P||Q|$, luego $G = QP$. Como $Q \lhd G$, se tiene que G es un producto semidirecto interno $G = Q \rtimes_\theta P$, para cierto $\theta : P \to \mathrm{Aut}(Q)$.

Ahora, $\mathrm{Aut}(Q) \simeq \mathbb{Z}_{q-1}$ y $|\mathrm{Aut}(Q)| = q-1$, luego si $p \nmid q-1$ se tiene que θ es el morfismo trivial, luego $G \simeq \mathbb{Z}_q \times \mathbb{Z}_p \simeq \mathbb{Z}_{pq}$.

Si $p \mid q-1$, entonces como $\mathrm{Aut}(Q)$ es cíclico tiene un único subgrupo P' de orden p. De hecho, $P' = \{x \mapsto x^i : i \in \mathbb{Z}_q, i^p = 1\} \subset \mathrm{Aut}(Q)$, y necesariamente por Lagrange $\mathrm{Im}\ \theta \subset P'$, i.e. $\theta : P \to P'$.

Como P y Q tienen orden primo, escribo $P = \langle a \rangle$, $Q = \langle b \rangle$. Entonces θ es de la forma

$$\theta(a)(x) = x^{i_0}, \quad i_0 \in \mathbb{Z}_q, i_0^p = 1, i_0 \neq 1$$

Es un morfismo no trivial, luego G es un producto semidirecto no trivial, en particular es un grupo no abeliano (recordar proposición 1.38). La acción de Q en P es por automorfismos internos, i.e. $\theta(a)(b) = aba^{-1} = b^{i_0}$, y elegir un i_0 diferente es equivalente a elegir un generador diferente a para P, luego no resulta en una clase diferente de isomorfismo. □

Teorema 1.102 (Grupos de orden 12)**.** *Las clases de isomorfismo de grupos de orden 12 son:*

$$\mathbb{Z}_{12} \qquad \mathbb{Z}_2 \times \mathbb{Z}_6 \qquad A_4 \qquad D_6 \qquad \mathbb{Z}_3 \rtimes \mathbb{Z}_4$$

Demostración. Sea G grupo de orden $12 = 2^2 3$. Los teoremas de Sylow nos dan:

$$s_2 \mid 3, \quad s_2 \equiv 1 \ (\text{mód } 2), \quad s_3 \mid 4, \quad s_3 \equiv 1 \ (\text{mód } 3).$$

Por lo tanto $s_2 = 1, 3$ y $s_3 = 1, 4$.

Si $s_2 = 1 = s_3$, entonces G es producto directo de un grupo de orden 4 por un grupo de orden 3, i.e. $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12}$ o $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$.

Supongamos $s_3 \neq 1$. Entonces $s_3 = 4$: tenemos 4 3-subgrupos de Sylow diferentes, que se intersectan trivialmente pues tienen orden primo, luego cada uno nos da 2 elementos diferentes, luego G tiene $4 \cdot 2 = 8$ elementos de orden 3. Por lo tanto el resto de los elementos no tiene orden 3; hay $12 - 8 = 4$ de estos. Como G tiene un 2-subgrupo de Sylow que tiene orden 4 (luego se intersecta trivialmente con los 3-subgrupos de Sylow), estos elementos restantes son el 2-subgrupo de Sylow de G, y sólo cabe uno, i.e. necesariamente $s_2 = 1$.

Por lo tanto necesariamente s_3 o s_2 valen 1. Sea P un 2-subgrupo de Sylow, Q un 3-subgrupo de Sylow: uno de ellos es normal en G, luego como $P \cap Q = \{e\}$ y $|G| = |P||Q|$, necesariamente $G = PQ$, entonces G es producto semidirecto de P y Q: es alguno de estos,

$$\mathbb{Z}_4 \rtimes_\theta \mathbb{Z}_3, \quad \mathbf{V} \rtimes_\theta \mathbb{Z}_3, \quad \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_4, \quad \mathbb{Z}_3 \rtimes_\theta \mathbf{V}.$$

En el primer caso, $s_2 = 1$ y $P = \mathbb{Z}_4$. El morfismo es $\theta : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4) \simeq (\mathbb{Z}_4)^* \simeq \mathbb{Z}_2$, luego θ es trivial (proposición 1.16) y $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12}$.

En el segundo caso, $s_2 = 1$ y $P = \mathbf{V}$. El morfismo es $\theta : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbf{V}) \simeq S_3$. El isomorfismo es porque cualquier elemento de orden 2 en $\mathbf{V}$ es intercambiable.

Si θ es trivial, obtenemos $G \simeq \mathbf{V} \times \mathbb{Z}_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$.

Si θ no es trivial, entonces su imagen debe estar contenida en el subgrupo de S_3 de elementos de orden 3, $\{(1), (123), (132)\} < S_3$. Para definir θ basta definir $\theta(1)$, para lo cual tenemos dos posibilidades, $\theta_1 : 1 \mapsto (123)$ o $\theta_2 : 1 \mapsto (132)$. Ahora bien, $(123) = (132)^{-1}$, por lo tanto si $\phi : \mathbb{Z}_3 \to \mathbb{Z}_3$, $\phi(1) = 2$, se tiene $\phi \circ \theta_1 = \theta_2$. Por el ejercicio 29, el producto semidirecto que nos dan θ_1 y θ_2 es el mismo.

Por lo tanto a menos de isomorfismo sólo hay un grupo no abeliano de orden 12 con $s_2 = 1$, y A_4 es un tal grupo pues ya sabemos que tiene un subgrupo normal de orden 4 (recordar la observación 1.10.10).

En el tercer caso, $s_3 = 1$ y $P = \mathbb{Z}_4$. El morfismo es $\theta : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) \simeq (\mathbb{Z}_3)^*$; hay un sólo morfismo no trivial, y es el que está definido por $1 \mapsto 2$. Obtenemos un producto semidirecto no trivial $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

En el cuarto caso, $s_3 = 1$ y $P = \mathbf{V}$. El morfismo es $\theta : \mathbf{V} \to \mathrm{Aut}(Z_3) \simeq (\mathbb{Z}_3)^*$. Hay tres no triviales, pues hay que mandar los generadores $(1, 0)$ y $(0, 1)$ a ± 1 sin mandar ambos a 1. Ahora, precomponiendo cada uno de ellos con algún automorfismo de $\mathrm{Aut}(\mathbf{V}) \simeq S_3$ se obtienen los otros, luego los tres productos semidirectos no triviales son isomorfos.

Por lo tanto a menos de isomorfismo sólo hay un grupo no abeliano de orden 12 con $s_3 = 1$ y un 2-subgrupo de Sylow isomorfo a $\mathbf{V}$, y D_6 es un tal grupo: su 3-subgrupo de Sylow normal es $\langle R^2 \rangle = \{1, R^2, R^4\}$ y su 2-subgrupo de Sylow es $\{1, R^3, S, R^3S\} \simeq \mathbf{V}$. □

Ejercicios

Ej. 40 — Un p-subgrupo normal de un grupo finito G está contenido en la intersección de todos los p-subgrupos de Sylow de G, que es un subgrupo normal.

Ej. 41 — Sea G de orden $p^n q$, donde $p > q$ y $n \in \mathbb{Z}^+$. Entonces alguno de sus subgrupos de Sylow es normal. Por lo tanto un tal grupo no puede ser simple (esto ya nos lo daba el teorema de Burnside que no demostramos).

Ej. 42 — Sea G un grupo de orden 36.

a) Si G es simple, entonces existen dos 3-subgrupos de Sylow diferentes cuya intersección es no trivial.

b) Si G es simple y H es un subgrupo no trivial de un 3-subgrupo de Sylow P, entonces $N_G(H) = P$.

c) Deducir que no hay grupos simples de orden 36.

1.13. Tabla de grupos de orden pequeño

Orden	N° de clases de iso.	Grupos
1	1	Trivial
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4$ y $\mathbf{V}$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6$ y S_3
7	1	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q
9	2	$\mathbb{Z}_3 \times \mathbb{Z}_3$ y $\mathbb{Z}_9$
10	2	$\mathbb{Z}_{10}$ y D_5
11	1	$\mathbb{Z}_{11}$
12	5	$\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, D_6, A_4, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$
13	1	$\mathbb{Z}_{13}$
14	2	$\mathbb{Z}_{14}$, D_7
15	1	$\mathbb{Z}_{15}$

Esta tabla es el resultado de juntar la clasificación que hicimos en el texto de los grupos de orden p, p^2, $2p$, pq, 8 y 12.

Para una discusión de los grupos de orden 16 (de los cuales hay 14 clases de isomorfismo), ver [Wi].

Capítulo 2

Teoría de cuerpos y teoría de Galois

2.0. Preliminares sobre polinomios

Antes de empezar recordamos algunas definiciones y resultados de polinomios.

Recordemos que si R es un anillo, $R[X]$ es el anillo de polinomios de R en una indeterminada. $R[X_1, \ldots, X_n]$ es el anillo de polinomios en n indeterminadas que conmutan.

Si R es un dominio de factorización única, entonces $R[X]$ también lo es. Si $R = k$ es un cuerpo, entonces $k[X]$ es un dominio de ideales principales.

Si $I \lhd R$ es un ideal de un anillo conmutativo, entonces I es un ideal maximal si y sólo si el cociente R/I es un cuerpo.

Definición. El *máximo común divisor* de dos polinomios p y q no ambos nulos es el único polinomio mónico d de grado mayor tal que $d \mid p$, $d \mid q$.

Observación 2.0.1. $\text{mcd}(p,q) = 1 \iff p, q$ no tienen raíces en común. Por lo tanto, si $\text{mcd}(p, q) \neq 1$ y $\text{gr mcd}(p, q) < 1$ entonces $p = 0$ o $q = 0$.

Proposición 2.1 (Criterio de la raíz racional)**.** *Sea $r \in \mathbb{Q}$ raíz del polinomio $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Entonces si $r = c/d$ con $\text{mcd}(c, d) = 1$, se tiene $c \mid a_0$ y $d \mid a_n$.*

Proposición 2.2 (Criterio de Eisenstein)**.** *Sea $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Si existe un primo p tal que:*

- $p \mid a_0, \ldots, p \mid a_{n-1}$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

entonces f es irreducible en $\mathbb{Q}[X]$.

Recordemos que un ideal $\mathfrak{p} \subset R$ de un anillo conmutativo es *primo* si $\mathfrak{p} \neq R$ y $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

Proposición 2.3 (Criterio de Eisenstein general)**.** *Sea D un dominio de factorización única, $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in D[X]$. Supongamos que existe un ideal primo $\mathfrak{p} \subset D$ tal que:*

- $a_i \in \mathfrak{p}$ *para cada* $i = 0, \ldots, n-1$
- $a_n \notin \mathfrak{p}$,
- $a_0 \notin \mathfrak{p}^2$,

entonces f *es irreducible sobre* $\mathrm{Frac}(D)[X]$.

Observación 2.0.2. Sea $\varphi : R \to S$ un homomorfismo de anillos; lo extendemos a $\varphi : R[X] \to S[X]$. Si $f \in R[X]$ es tal que $\varphi(f)$ es irreducible en $S[X]$, entonces f es irreducible en $R[X]$ (pues una factorización de f en R es enviada a una factorización de $\varphi(f)$ en S).

Esto nos da otra manera de verificar que un polinomio es irreducible. Es usual tomar $R = \mathbb{Z}$ y $S = \mathbb{Z}_p$ para algún primo p. Para probar que un polinomio es irreducible en $\mathbb{Z}_p$ se puede utilizar el criterio de Eisenstein general.

Existen sin embargo polinomios en $\mathbb{Z}[X]$ irreducibles que son reducibles módulo p para cualquier primo p, por ejemplo $f(X) = X^4 - 10X^2 + 1$.

Una prueba sencilla de este hecho es la siguiente ([M2], pp. 6-7). Sea p primo. Si 2 fuera un cuadrado en $(\mathbb{F}_p)^*$, entonces:

$$X^4 - 10X^2 + 1 = (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1)$$

y $X^4 - 10X^2 + 1$ es reducible módulo p. Si 3 fuera un cuadrado en $(\mathbb{F}_p)^*$, entonces:

$$X^4 - 10X^2 + 1 = (X^2 - 2\sqrt{3}X + 1)(X^2 + 2\sqrt{3}X + 1)$$

y $X^4 - 10X^2 + 1$ es reducible módulo p. Si ni 2 ni 3 son cuadrados, entonces por el ejercicio 16, 6 debe ser un cuadrado en $(\mathbb{F}_p)^*$, y entonces:

$$X^4 - 10X^2 + 1 = (X^2 - (5 + 2\sqrt{6}))(X^2 - (5 - 2\sqrt{6}))$$

y $X^4 - 10X^2 + 1$ es reducible módulo p.

2.1. Definiciones y propiedades básicas

Definición. Un *cuerpo* es una quíntupla $(K, +, \cdot, 0, 1)$, donde K es un conjunto, $+, \cdot$ son operaciones binarias en K, $0, 1 \in K$ y se verifica:

- $1 \neq 0$,
- $(K, +, 0)$ es un grupo abeliano,
- $(K\backslash\{0\}, \cdot, 1)$ es un grupo abeliano,
- Propiedad distributiva: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ para todo $a, b, c \in K$.

Equivalentemente, un cuerpo es un anillo con división conmutativo.

Cuando no haya riesgo de confusión, sobreentenderemos las operaciones y diremos simplemente que K es un cuerpo.

Definición. Sea K un cuerpo. Si $F \subset K$ es un subconjunto que es un cuerpo con las operaciones de K restringidas a F, decimos que F es un *subcuerpo* de K, que K es una extensión de F y que $F \subset K$ es una *extensión de cuerpos*.

Observación 2.1.1. $F \subset K$, $F \neq \varnothing$ es un subcuerpo si y sólo si:

- $a - b \in F$ para todo $a, b \in F$,
- $ab^{-1} \in F$ para todo $a, b \in F$, $b \neq 0$,
- $1 \in F$.

Observación 2.1.2. La intersección de una familia no vacía de subcuerpos es un subcuerpo.

Definición. La *característica* de un cuerpo K es el menor natural $n \geqslant 2$ tal que $n \cdot 1_F = \overbrace{1_F + \cdot + 1_F}^{n \text{ veces}} = 0_F$. Si no existe un tal n, diremos que la característica del cuerpo es 0.

Notamos car $k = n$ o car $k = 0$.

Observación 2.1.3. Si la característica es positiva, entonces es prima. En efecto, si $n = ab$, entonces $n \cdot 1_F = (ab) \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F) = 0$. Como F es un dominio de integridad, entonces $a \cdot 1_F = 0$ o $b \cdot 1_F = 0$, contradiciendo la minimalidad de n.

Ejemplo 2.1.4. Recordemos que $\mathbb{Z}_n$ es un cuerpo si y sólo si n es primo.

$\mathbb{Z}_p(X)$ es un cuerpo infinito de característica finita.

Definición. Sean F, K cuerpos. Un *homomorfismo de cuerpos* o simplemente *morfismo* entre F y K es una función $\varphi : F \to K$ que satisface:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ para todo $a, b \in F$,
- $\varphi(ab) = \varphi(a)\varphi(b)$ para todo $a, b \in F$,
- $\varphi(1) = 1$.

Análogamente a la situación con grupos, se define monomorfismo, epimorfismo, isomorfismo, endomorfismo y automorfismo de cuerpos.

Observación 2.1.5. Una función entre dos cuerpos es un homomorfismo de cuerpos si y sólo si es un homomorfismo de anillos. Por lo tanto, dados dos cuerpos, los homomorfismos de cuerpos entre ellos son todos los homomorfismos de anillos.[1] Tenemos entonces a nuestra disposición los teoremas de isomorfismo y más propiedades que conocemos para morfismos de anillos.

Proposición 2.4. *Sea F un cuerpo y A un anillo no trivial. Entonces todo morfismo de anillos $F \to A$ es un monomorfismo.*

Demostración. Sea $\varphi : F \to A$ homomorfismo de anillos. Entonces $\ker \varphi$ es un ideal de F. Pero en un cuerpo los ideales son triviales: si $\ker \varphi = \{0\}$, entonces φ es un monomorfismo y terminamos. El caso $\ker \varphi = F$ es absurdo, pues implicaría que $1 = \varphi(1) = 0$ que no puede suceder pues $A \neq \{0\}$. □

Como corolario, la siguiente sorprendente propiedad de la categoría de cuerpos: todo morfismo es inyectivo.

Corolario 2.5. *Todo morfismo de cuerpos es un monomorfismo.*

Definición. Sea K cuerpo. El *cuerpo primo* de K es el menor subcuerpo de K.

Observación 2.1.6. $F \subset K$ es el cuerpo primo de K si y sólo si $F = \langle 1 \rangle$.

Todo cuerpo es una extensión de su cuerpo primo.

Proposición 2.6. *Todo cuerpo tiene una copia de $\mathbb{Q}$ o de $\mathbb{Z}_p$ para un único primo p (y sólo de uno de ellos).*

Demostración. Para cualquier cuerpo F tenemos un morfismo de anillos $\varphi : \mathbb{Z} \to F$, $n \mapsto n \cdot 1_F$. Tenemos entonces $\ker \varphi = \langle \operatorname{car} F \rangle$, y el primer teorema de isomorfismo nos da:

$$\frac{\mathbb{Z}}{\langle \operatorname{car} F \rangle} \simeq \operatorname{Im} \varphi \subset F$$

Ahora bien, como la característica de un cuerpo es prima o nula, se tiene $\langle \operatorname{car} F \rangle = \{0\}$ o $\langle \operatorname{car} F \rangle = p\mathbb{Z}$. Por lo tanto F tiene una copia de $\mathbb{Z}$ o de $\mathbb{Z}_p$. Si F tiene una copia de $\mathbb{Z}$, entonces tiene una copia de $\mathbb{Q}$, pues por definición $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$ es el menor cuerpo que contiene a $\mathbb{Z}$.

Si tiene una copia de $\mathbb{Z}_p$, entonces no tiene una copia de $\mathbb{Z}_q$ para ningún otro primo q, pues la característica es única. Además, tiene una copia de $\mathbb{Z}_p$ si y sólo si no tiene una copia de $\mathbb{Q}$, pues tiene característica prima si y sólo si no tiene característica 0. □

Observación 2.1.7. Como $\mathbb{Q}$ y $\mathbb{Z}_p$ no tienen subcuerpos, deducimos que el cuerpo primo de un cuerpo siempre es isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}_p$.

Definición. Sea $F \subset K$ una extensión de cuerpos. En esta situación K es un F-espacio vectorial. La dimensión $\dim_F K$ de K como F-espacio vectorial se llama el *grado* de la extensión.

Notamos $|K : F| := \dim_F K$. Si $|K : F| < \infty$, la extensión se dice *finita*. En caso contrario se dice *infinita*.

[1] Esto nos dice que la categoría de cuerpos es una *subcategoría plena* de la categoría de anillos.

Ejemplo 2.1.8. $|\mathbb{R} : \mathbb{Q}| = \infty$: en efecto, todo espacio vectorial de dimensión finita sobre $\mathbb{Q}$ es isomorfo a $\mathbb{Q}^n$ para algún n, y por lo tanto es numerable (pues $\mathbb{Q}$ lo es y el producto cartesiano finito de numerables es numerable), pero $\mathbb{R}$ no es numerable.

A continuación empezamos una de las construcciones más importantes que haremos con cuerpos: la de ir agregando raíces de polinomios al cuerpo que previamente no estaban.

Teorema 2.7. *Sea F cuerpo, $p \in F[X]$ un polinomio no constante. Existe una extensión de F en la que p tiene una raíz.*

Demostración. Como $F[X]$ es un dominio de factorización única, dado $p \in F[X]$ lo podemos descomponer como producto de polinomios irreducibles, $p = p_1 \dots p_n$.

Basta ver que existe una extensión de F en la que p_1 tiene una raíz.

Identifiquemos a F con su copia en $K = F[X]/\langle p_1 \rangle$. Como p_1 es irreducible y $F[X]$ es un dominio de ideales principales, $\langle p_1 \rangle$ es un ideal maximal, luego K es un cuerpo que tiene una copia de F.

Además p_1 tiene a $\overline{X}$ como raíz en K: $p_1(\overline{X}) = \overline{p_1(X)} = \overline{0}$. □

Corolario 2.8. *Sean $p, q \in F[X]$ no constantes. Entonces son coprimos si y sólo si no tienen raíces en común en ninguna extensión de F.*

Demostración. Si p, q son coprimos, entonces existen $u, v \in F[X]$ tales que $pu + qv = 1$. Si hubiera una raíz común a p y q en alguna extensión de F, evaluando obtendríamos $0 = 1$, absurdo.

Recíprocamente, supongamos que p, q tienen un factor común $h \in F[X]$. Sea $F \subset K$ una extensión en la que h tiene una raíz. Este elemento es también raíz de p y q en K, absurdo. □

Teorema 2.9. *Sea $p \in F[X]$ irreducible de grado n, y sea $K = F[X]/\langle p \rangle$. Entonces $\mathcal{B} = \{1, \overline{X}, \dots, \overline{X}^{n-1}\}$ es una base de K como F-espacio vectorial. En particular $|K : F| = n$, y*

$$F[X]/\langle p \rangle = \{a_0 + a_1\overline{X} + \cdots + a_{n-1}\overline{X}^{n-1} : a_0, a_1, \dots, a_{n-1} \in F\}$$

Demostración. $\mathcal{B}$ es generador de K: Sea $a \in F[X]$. Lo divido por p: $a = pq + r$ donde $q, r \in F[X]$, y $r = 0$ o $\operatorname{gr}(r) < n$.

$pq \in \langle p \rangle$, luego en K se tiene $\overline{a} = \overline{pq + r} = \overline{pq} + \overline{r} = \overline{r}$, que es nulo o tiene grado menor que n, luego $\overline{a}$ es combinación lineal de $\{1, \overline{X}, \dots, \overline{X}^{n-1}\}$.

$\mathcal{B}$ es linealmente independiente: si $b_0 + b_1\overline{X} + \cdots + b_{n-1}\overline{X}^{n-1} = \overline{0}$, entonces $p \mid b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$, pero p tiene grado $n > n-1$, luego $b_0 = \cdots = b_{n-1} = 0$. □

Ejemplo 2.1.9.

- Consideremos $X^2 + 1 \in \mathbb{R}[X]$. Es irreducible de grado 2, luego $\mathbb{R}[X]/\langle X^2 + 1 \rangle$ es una extensión de $\mathbb{R}$ de grado 2, y

  $$\mathbb{R}[X]/\langle X^2 + 1 \rangle = \{a + bi : a, b \in \mathbb{R}\}, \quad i := \overline{X}$$

  es un cuerpo isomorfo a $\mathbb{C}$.

- Consideremos $X^2 - 2 \in \mathbb{Q}[X]$. Es irreducible de grado 2, luego $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$ es una extensión de $\mathbb{Q}$ de grado 2, y

  $$\mathbb{Q}[X]/\langle X^2 - 2 \rangle = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}, \quad \sqrt{2} := \overline{X}$$

  En esta construcción, $\sqrt{2}$ es alguna raíz de $X^2 - 2$. Si queremos ser coherentes con la definición usual de $\sqrt{2}$, podemos decir que tomamos la raíz positiva.

Definición. Sea $F \subset K$ una extensión de cuerpos, $S \subset K$ un subconjunto. El menor subcuerpo de K que contiene a F y a S se denota $F(S)$ y decimos que es el *cuerpo de adjunción* a F de los elementos de S.

Si $S = \{a_1, \ldots, a_n\}$ es finito, decimos que la extensión es *finitamente generada*, y notamos $F(S) = F(a_1, \ldots, a_n)$. En el caso particular en que $S = \{\alpha\}$, decimos que $F(\alpha)$ es una *extensión simple* de F, y α se llama *elemento primitivo* de la extensión.

Definición. Sea $F \subset K$ extensión de cuerpos. Si $\alpha \in K$ es raíz de un polinomio en $F[X]$, entonces α se dice *algebraico* sobre F. En caso contrario, se dice *trascendente* sobre F.

Observación 2.1.10. Es equivalente ser algebraico con ser raíz de un polinomio *irreducible* en $F[X]$, pues $F[X]$ es dominio de factorización única.

Proposición 2.10. *Sea $F \subset K$ extensión de cuerpos.*

1. *Si $\alpha \in K$ es algebraico sobre F, raíz de un polinomio $p \in F[X]$ irreducible, entonces $F(\alpha) \simeq F[X]/\langle p \rangle$.*
2. *Si $\alpha \in K$ es trascendente sobre F entonces $F(\alpha) \simeq F(X)$.*

Demostración. 1. Sea $\varphi : F[X] \to F(\alpha)$, $f \mapsto f(\alpha)$. Es un morfismo de anillos. Como $p(\alpha) = 0$, entonces $\langle p \rangle \subset \ker \varphi$, luego la propiedad universal del cociente nos da un mapa $\tilde{\varphi} : F[X]/\langle p \rangle \to F(\alpha)$.

Como p es irreducible, $F[X]/\langle p \rangle$ es un cuerpo, y el morfismo no es nulo pues por ejemplo $\tilde{\varphi}|_F = \mathrm{id}_F$, luego $\tilde{\varphi}$ es inyectiva. La imagen es un subcuerpo de $F(\alpha)$ que contiene a $F = \tilde{\varphi}(F)$ y a $\alpha = \tilde{\varphi}(\overline{X})$, por lo tanto es igual a $F(\alpha)$.

2. Definimos $\varphi : F(X) \to F(\alpha)$, $f/g \mapsto f(\alpha)/g(\alpha)$ morfismo de cuerpos. Es inyectiva: si existiera $f/g \in F(X)$ tal que $f(\alpha)/g(\alpha) = 0$, entonces $f(\alpha) = 0$ y α sería raíz de $f \in F[X]$. La imagen es un subcuerpo de $F(\alpha)$ que contiene a $F = \varphi(F)$ y a $\alpha = \varphi(X)$, luego es igual a $F(\alpha)$. Por lo tanto φ es el isomorfismo deseado. □

Corolario 2.11. *Sea $F \subset K$ extensión de cuerpos y $\alpha \in K$ algebraico sobre F. Si α es raíz de un polinomio $p \in F[X]$ irreducible, entonces si $n = \mathrm{gr}\ p$:*

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in F\}$$

Demostración. En efecto, la base $\{1, \overline{X}, \ldots, \overline{X}^{n-1}\}$ de $F[X]/\langle p \rangle$ se envía a $\{1, \alpha, \ldots, \alpha^{n-1}\} \subset F(\alpha)$ por el isomorfismo, por lo tanto es una base de $F(\alpha)$. □

Ejemplo 2.1.11. El ejemplo anterior nos dice que $\mathbb{C} \simeq \mathbb{R}(i)$: el cuerpo de los números complejos es el resultado de adjuntar la unidad imaginaria i a $\mathbb{R}$.

Teorema 2.12 (de extensión)**.** *Sea $\varphi : F \to F'$ isomorfismo de cuerpos.*

1. *Sea $p \in F[X]$ irreducible y p' el polinomio en $F'[X]$ obtenido al aplicarle φ a los coeficientes de p. Sea $\alpha \in F$ raíz de p, $\beta \in F'$ raíz de p'. Entonces existe $\sigma : F(\alpha) \to F'(\beta)$ isomorfismo de cuerpos tal que $\alpha \mapsto \beta$ y $\sigma|_F = \varphi$.*

2. *Si $F \subset K$, $F' \subset K'$ son extensiones de cuerpos, y $\alpha \in K$, $\beta \in K'$ no son raíces de ningún polinomio en $F[X]$ y $F'[X]$ respectivamente, entonces existe $\sigma : F(\alpha) \to F'(\beta)$ isomorfismo de cuerpos tal que $\alpha \mapsto \beta$ y $\sigma|_F = \varphi$.*

Demostración. 1. Veamos que p' es irreducible en $F'[X]$: φ se extiende a $\varphi : F[X] \to F'[X]$ isomorfismo de anillos, que manda el ideal maximal $\langle p \rangle$ en $\langle p' \rangle$, luego $\langle p' \rangle$ también es maximal y por lo tanto p' es irreducible.

Bajamos el isomorfismo al cociente:

$$\begin{array}{ccccc} F[X] & & \xrightarrow[\simeq]{\varphi} & & F'[X] \\ \downarrow{\scriptstyle \pi_p} & & & & \downarrow{\scriptstyle \pi_{p'}} \\ F(\alpha) & \xrightarrow{\simeq} \dfrac{F[X]}{\langle p \rangle} & \xrightarrow{\simeq} & \dfrac{F'[X]}{\langle p' \rangle} & \xrightarrow{\simeq} F'(\beta) \end{array}$$

y obtenemos el isomorfismo deseado.

2. El isomorfismo $\varphi : F \to F'$ se extiende a un isomorfismo de cuerpos $\varphi : F(X) \to F'(X)$. La proposición 2.10 nos da la siguiente cadena de isomorfismos:

$$F(\alpha) \xrightarrow{\psi^{-1}} F(X) \xrightarrow{\varphi} F'(X) \xrightarrow{\eta} F'(\beta)$$

La composición es el isomorfismo buscado. □

Corolario 2.13. *Sean $F \subset K$, $F \subset E$ extensiones de cuerpos, y sean $\alpha \in K$, $\beta \in E$ algebraicos sobre F. Entonces α y β son raíz del mismo polinomio irreducible $f \in F[X]$ si y sólo si existe un isomorfismo de cuerpos $\sigma : F(\alpha) \to F(\beta)$ tal que $\sigma : \alpha \mapsto \beta$, $\sigma|_F = \mathrm{id}$.*

Demostración. ($\Rightarrow$) Es el teorema de extensión aplicado a $\varphi = \mathrm{id} : F \to F$.

($\Leftarrow$) Sea $f \in F[X]$ un polinomio irreducible con α como raíz. Si $f = \sum_{i=0}^{n} a_i X^i$, entonces $0 = f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$. Pero entonces

$$\begin{aligned} 0 = \sigma(0) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) &= \sum_{i=0}^{n} \sigma(a_i \alpha^i) = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha)^i \\ &\overset{\sigma|_F = \mathrm{id}}{=} \sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} a_i \beta^i = f(\beta) \end{aligned}$$

□

Ejercicios

Ej. 43 — (Invariancia del mcd bajo extensiones de cuerpos) Sea $F \subset K$ extensión de cuerpos, y sean $f, g \in F[X]$ polinomios no nulos. Entonces el mcd de f y g como polinomios en $K[X]$ es igual al mcd de f y g como polinomios en $F[X]$.
En particular, $f \mid g$ en $F[X]$ sii $f \mid g$ en $K[X]$, y f, g son coprimos en $F[X]$ sii son coprimos en $K[X]$.

Ej. 44 — $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{2})$ son isomorfos como $\mathbb{Q}$-espacios vectoriales pero no como cuerpos.

2.2. Extensiones algebraicas

Definición. Sea $F \subset K$ extensión de cuerpos. Decimos que es *algebraica* si todo $\alpha \in K$ es algebraico sobre F. En caso contrario, i.e. si existe $\alpha \in K$ trascendente sobre F, decimos que es una extensión *trascendente*.

Proposición 2.14. *Sea $F \subset K$ extensión de cuerpos, $\alpha \in K$ algebraico sobre F. Entonces:*

1. *Existe un único polinomio $m_{\alpha,F}$ en $F[X]$ mónico e irreducible tal que $m_{\alpha,F}(\alpha) = 0$.*
2. *Si $f \in F[X]$ es tal que $f(\alpha) = 0$, entonces $m_{\alpha,F} \mid f$.*

Demostración. Como α es algebraico sobre F, el conjunto $\{f \in F[X] : f(\alpha) = 0\}$ es no vacío. Elijo g en ese conjunto de grado mínimo. Como F es cuerpo, puedo suponer g mónico (dividiendo por el coeficiente líder si no lo fuera).

Supongo $g = ab$, $a, b \in F[X]$ de grado $\geqslant 1$. Pero entonces $g(\alpha) = a(\alpha)b(\alpha)$, y como F es dominio de integridad se tiene $a(\alpha) = 0$ o $b(\alpha) = 0$, lo cual contradice la minimalidad del grado de g. Por lo tanto g prueba la existencia del polinomio buscado.

Si $m_{\alpha,F} \mid f$ entonces todas las raíces de $m_{\alpha,F}$ lo son de f, en particular $f(\alpha) = 0$.

Sea f tal que $f(\alpha) = 0$. Tiene grado mayor o igual que g. Entonces $f = gq + r$, donde $q, r \in F[X]$ y gr $r <$ gr g o $r = 0$.

Por lo tanto $0 = f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, luego por minimalidad del grado de g debe ser $r = 0$. Entonces $f = gq$ y $g \mid f$.

Por lo tanto g es el único polinomio en $F[X]$ mónico, irreducible de grado mínimo que anula a α, pues cualquier otro de grado mínimo que anule a α debe ser múltiplo escalar de g, que es mónico; luego g es único. □

Definición. Sea $F \subset K$ extensión de cuerpos, $\alpha \in K$ algebraico sobre F. Llamaremos *polinomio mínimo* de α sobre F al único polinomio en $F[X]$ mónico e irreducible que anula a α, y lo notaremos $m_{\alpha,F}$. El *grado* de α sobre F, notado $\mathrm{gr}_F(\alpha)$ es el grado de $m_{\alpha,F}$.

Corolario 2.15. *Sean $p, q \in F[X]$, $p \neq q$ irreducibles y mónicos. Entonces no tienen raíces en común.*

Demostración. Supongamos que existe $\alpha \in F$ raíz de p y q. Entonces $m_{\alpha,F} \mid p$ y $m_{\alpha,F} \mid q$, i.e. existen $p_1, q_1 \in F[X]$ tales que $p = m_{\alpha,F}p_1$, $q = m_{\alpha,F}q_1$. Como $p \neq q$ se debe tener $p_1 \neq q_1$. Pero p y q son mónicos, entonces como $m_{\alpha,F}$ también lo es, necesariamente p_1 o q_1 es de grado $\geqslant 1$, y entonces p o q no es irreducible, absurdo. □

Definición. Una sucesión de cuerpos encajados $F_1 \subset F_2 \subset \cdots$ se dice una *torre de cuerpos*.

Observación 2.2.1. Si $F \subset K \subset L$ es una torre de cuerpos donde L es algebraico sobre F, entonces obviamente L es algebraico sobre K.

Corolario 2.16. *Sea $F \subset K \subset L$ una torre de cuerpos, $\alpha \in L$ algebraico sobre F. Entonces $m_{\alpha,K} \mid m_{\alpha,F}$.*

Demostración. $m_{\alpha,F} \in F[X] \subset K[X]$, luego $m_{\alpha,F}$ es un polinomio con coeficientes en K que anula a α. Por definición de $m_{\alpha,K}$ se debe tener $m_{\alpha,K} \mid m_{\alpha,F}$. □

Proposición 2.17. *Sea $F \subset K$ extensión de cuerpos, $\alpha \in K$ algebraico sobre F. Entonces $F(\alpha) \simeq F[X]/\langle m_{\alpha,F} \rangle$. En particular $|F(\alpha) : F| = \text{gr } m_{\alpha,F} = \text{gr}_F(\alpha)$.*

Demostración. Se deduce de la proposición 2.10, con $p = m_{\alpha,F}$, y del teorema 2.9. □

Proposición 2.18. *Sea $F \subset K$ extensión de cuerpos. Entonces α es algebraico sobre F si y sólo si la extensión $F \subset F(\alpha)$ es finita.*

Demostración. ($\Rightarrow$) Si α es algebraico sobre F, entonces $|F(\alpha) : F| = \text{gr } m_{\alpha,F} < \infty$.

($\Leftarrow$) Sea $n = |F(\alpha) : F|$. El F-espacio vectorial $F(\alpha)$ tiene como F-base a $\{1, \alpha, \ldots, \alpha^{n-1}\}$, entonces existen $a_0, \ldots, a_n \in F$ no todos nulos tales que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Por lo tanto el polinomio $f = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ anula a α, i.e. α es algebraico sobre F. □

Corolario 2.19. *Toda extensión de cuerpos finita es algebraica.*

Demostración. Sea $F \subset K$ extensión de cuerpos finita. Sea $\alpha \in K$. Se tiene que $F(\alpha) \subset K$ es un F-subespacio vectorial, por lo tanto $|F(\alpha) : F| \leqslant |K : F| < \infty$, luego $|F(\alpha) : F| < \infty$ para todo $\alpha \in K$. Por la proposición anterior, esto implica que todo $\alpha \in K$ es algebraico sobre F, i.e. $F \subset K$ es algebraica. □

Teorema 2.20 (Transitividad de grados)**.** *Sea $F \subset K \subset L$ una torre de cuerpos. Entonces*

$$|L : F| = |L : K||K : F|$$

Demostración. Supongamos primero que $F \subset K$, $K \subset L$ son extensiones finitas. Sean entonces $\{\alpha_1, \ldots, \alpha_m\}$ una K-base de L, y $\{\beta_1, \ldots, \beta_n\}$ una F-base de K.

Dado $\gamma \in L$, existen únicos $a_i \in K$ tales que $\gamma = a_1\alpha_1 + \cdots + a_m\alpha_m$.

A su vez $a_i \in K$, luego existen $b_{ij} \in F$ tales que $a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n$. Por lo tanto

$$\gamma = \sum_{i=1,j=1}^{m,n} b_{ij}\beta_j\alpha_i$$

Entonces $\{\beta_j\alpha_i\}_{i,j=1}^{m,n}$ es un generador de F sobre L.

Es linealmente independiente: supongamos que $\sum_{i,j} b_{ij}\beta_j\alpha_i = 0$, i.e. $\sum_i a_i\alpha_i = 0$. Como $\{\alpha_i\}_{i=1}^m$ es l.i., entonces $a_i = 0$ para todo $i = 1, \ldots, m$. Entonces $b_{i1}\beta_1 + \cdots + b_{in}\beta_n = 0$. Como $\{\beta_j\}_{j=1}^n$ es l.i., entonces $b_{ij} = 0$ para todo i, j.

Tenemos entonces que $\{\beta_j\alpha_i\}_{i,j=1}^{m,n}$ es una F-base de L. Como tiene cardinal mn, se deduce lo deseado.

En el caso en que $F \subset K$, $K \subset L$ son extensiones infinitas, entonces $F \subset L$ es infinita, pues L como F-espacio vectorial contiene al subespacio K de dimensión infinita. □

Corolario 2.21. *Si $F \subset K \subset L$ es una torre de cuerpos, entonces $|K : F| \mid |L : F|$ y $|L : K| \mid |L : F|$.*

Proposición 2.22. *Sea $F \subset K$, $\alpha, \beta \in K$. Entonces $F(\alpha, \beta) = F(\alpha)(\beta)$.*

Demostración. ($\subset$) $F(\alpha,\beta)$ es el menor subcuerpo de K que contiene a F, α y β. Pero $F(\alpha)(\beta)$ es un subcuerpo de K que contiene a F, α y β, luego $F(\alpha,\beta)\subset F(\alpha)(\beta)$.

($\supset$) $F(\alpha)(\beta)$ es el menor subcuerpo de K que contiene a $F(\alpha)$ y a β. Pero $F(\alpha,\beta)$ es un subcuerpo de K que contiene a $F(\alpha)$ y a β, luego $F(\alpha)(\beta)\subset F(\alpha,\beta)$. □

Corolario 2.23. *Sea $F\subset K$ extensión de cuerpos. Si $\alpha_1,\dots,\alpha_k\in K$ son algebraicos sobre F, y $\mathrm{gr}_F\alpha_i=n_i$ para todo i, entonces*

$$|F(\alpha_1,\dots,\alpha_k):F|\leqslant n_1\dots n_k$$

Demostración. Consideremos la torre

$$F\subset F(\alpha_1)\subset F(\alpha_1,\alpha_2)\subset\cdots\subset F(\alpha_1,\dots,\alpha_k)$$

La primera extensión tiene grado n_1. La segunda extensión tiene grado

$$|F(\alpha_1,\alpha_2):F(\alpha_1)|=|F(\alpha_1)(\alpha_2):F(\alpha_1)|=\mathrm{gr}\ m_{\alpha_2,F(\alpha_1)}\leqslant\mathrm{gr}\ m_{\alpha_2,F}=|F(\alpha_2):F|=n_2$$

Por inducción, cada cuerpo en la torre tiene grado sobre el cuerpo anterior menor o igual que el grado del nuevo elemento que se adjunta. Por lo tanto, aplicando transitividad de grados k veces, se obtiene lo deseado. □

Ejemplo 2.2.2.

- $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt[6]{2})=\mathbb{Q}(\sqrt[6]{2})$ (pues $(\sqrt[6]{2})^3=\sqrt{2}$) es un ejemplo de desigualdad estricta. En efecto, $|\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}|=6$ pues por el criterio de la raíz racional (proposición 2.1) X^6-2 es irreducible sobre $\mathbb{Q}$. Entonces:

$$|\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}|=6<\mathrm{gr}_{\mathbb{Q}}\sqrt{2}\ \mathrm{gr}_{\mathbb{Q}}\sqrt[6]{2}=12$$

- $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Es trivial que $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$. Veamos la desigualdad inversa.

  Sea $u=\sqrt{2}+\sqrt{3}$. Entonces

$$u-\sqrt{2}=\sqrt{3}\Rightarrow(u-\sqrt{2})^2=3\Rightarrow u^2-2\sqrt{2}u+2=3\Rightarrow\sqrt{2}=\frac{u^2-1}{2u}$$

  Por lo tanto $\sqrt{2}\in\mathbb{Q}(u)$. Además $\sqrt{3}=u-\sqrt{2}$ luego $\sqrt{3}\in\mathbb{Q}(u)$. Por lo tanto $\sqrt{2},\sqrt{3}\in\mathbb{Q}(u)\Rightarrow\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(u)$.

  Observar además que este método también nos da el polinomio mínimo de u sobre $\mathbb{Q}$:

$$\sqrt{2}=\frac{u^2-1}{2u}\Rightarrow 2=\frac{u^4-2u^2+1}{4u^2}\Rightarrow 8u^2=u^4-2u^2+1\Rightarrow u^4-10u^2+1=0$$

  Por lo tanto $X^4-10X^2+1\in\mathbb{Q}[X]$ es un polinomio mónico de grado 4 que anula a u. Probemos que es el polinomio mínimo de u sobre $\mathbb{Q}$.

  Basta probar que $|\mathbb{Q}(u):\mathbb{Q}|=|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}|=4$ para haber probado que es el polinomio mínimo de u sobre $\mathbb{Q}$. Para ver esto, consideremos la torre $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$. Por transitividad de grados se tiene:

$$|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}|=|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}):\mathbb{Q}|$$

  Tenemos que X^2-2 es un polinomio de grado 2 irreducible sobre $\mathbb{Q}$ que anula a $\sqrt{2}$, luego $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}|=2$. Además $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})|=2$ pues $\sqrt{3}$ es raíz de X^2-3 que es irreducible en $\mathbb{Q}(\sqrt{2})$.

Teorema 2.24. *Una extensión de cuerpos $F \subset K$ es finita si y sólo si es finitamente generada por elementos algebraicos, si y sólo si es finitamente generada y algebraica.*

Demostración. Si una extensión es finitamente generada y algebraica, obviamente es finitamente generada por elementos algebraicos. Recíprocamente, si es finitamente generada por elementos algebraicos $\alpha_1, \ldots, \alpha_k \in K$, entonces es algebraica, pues en virtud del corolario anterior, si $n_i = \text{gr } \alpha_i$ para todo i,

$$|F(\alpha_1, \ldots, \alpha_k) : F| \leqslant n_1 \ldots n_k < \infty$$

entonces $F \subset F(\alpha_1, \ldots, \alpha_k)$ es finita, luego algebraica.

Veamos que si $F \subset K$ es finita entonces es finitamente generada por elementos algebraicos. Ya sabemos que es algebraica, por lo tanto basta ver que es finitamente generada. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una F-base de K. Entonces $K = F(\alpha_1, \ldots, \alpha_n)$, y K es finitamente generado sobre F.

Recíprocamente, supongamos que K es finitamente generada sobre F por elementos algebraicos. Trabajemos por inducción en la menor cantidad de elementos algebraicos de K que generan K sobre F. Por simplicidad supongamos que es 2, i.e. $K = F(\alpha, \beta)$ con $\alpha, \beta \in K$ algebraicos sobre F. Se tiene $|F(\alpha, \beta) : F(\alpha)| < \infty$ pues al ser $F(\alpha, \beta)$ algebraica sobre F también es algebraica sobre $F(\alpha)$. Entonces como $|F(\alpha, \beta) : F| = |F(\alpha, \beta) : F(\alpha)||F(\alpha) : F|$ y también $|F(\alpha) : F| < \infty$, se tiene $|F(\alpha, \beta) : F| < \infty$. □

Corolario 2.25. *Sea $F \subset K$ una extensión de cuerpos. Los elementos de K algebraicos sobre F forman un subcuerpo de K.*

Demostración. Sean $\alpha, \beta \in K$ algebraicos sobre F. Entonces $F \subset F(\alpha, \beta)$ es algebraica, y $\alpha - \beta, \alpha\beta^{-1} \in F(\alpha, \beta)$. Por lo tanto $\alpha - \beta, \alpha\beta^{-1}$ son algebraicos sobre F, para todo $\alpha, \beta \in K$ algebraicos sobre F, de donde se deduce la tesis. □

Ejemplo 2.2.3. Sea $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ es algebraico sobre } \mathbb{Q}\}$. Por el corolario anterior es un subcuerpo de $\mathbb{C}$, que llamamos cuerpo de los *números algebraicos*.

$\mathbb{Q} \subset \overline{\mathbb{Q}}$ es una extensión algebraica. Es infinita: en efecto, $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ para todo $n \in \mathbb{Z}^+$. Por lo tanto $|\overline{\mathbb{Q}} : \mathbb{Q}| \geqslant n$ para todo $n \in \mathbb{Z}^+$, luego $|\overline{\mathbb{Q}} : \mathbb{Q}| = \infty$.

En particular $\mathbb{Q} \subset \overline{\mathbb{Q}}$ no puede ser una extensión finitamente generada.

Se puede probar que $\overline{\mathbb{Q}} \neq \mathbb{R}$, probando por ejemplo que $\pi \in \mathbb{R} \backslash \overline{\mathbb{Q}}$. Los elementos de $\mathbb{R} \backslash \overline{\mathbb{Q}}$ se llaman *números trascendentes*.

Proposición 2.26. *Sea $F \subset K \subset L$ torre de cuerpos. Si $F \subset K$ y $K \subset L$ son extensiones algebraicas, entonces $F \subset L$ es una extensión algebraica.*

Demostración. Sea $\alpha \in L$. Como L es algebraico sobre K, existen $a_0, \ldots, a_n \in K$ tales que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0 \tag{2.1}$$

Se tiene entonces por transitividad de grados:

$$|F(\alpha, a_0, \ldots, a_n) : F| = |F(a_0, \ldots, a_n)(\alpha) : F(a_0, \ldots, a_n)||F(a_0, \ldots, a_n) : F| \tag{2.2}$$

$|F(a_0,\dots,a_n):F|<\infty$ pues $a_0,\dots,a_n\in K$ que es algebraica sobre F, luego $F(a_0,\dots,a_n)$ es algebraica sobre F y finitamente generada, entonces finita.

$|F(a_0,\dots,a_n)(\alpha):F(a_0,\dots,a_n)|<\infty$, pues por el polinomio (2.1) se tiene que α es una raíz de un polinomio con coeficientes en $F(a_0,\dots,a_n)$, i.e. $F(a_0,\dots,a_n)\subset F(a_0,\dots,a_n)(\alpha)$ es una extensión algebraica, y es finitamente generada, entonces es finita.

La ecuación (2.2) nos da entonces que $|F(\alpha,a_0,\dots,a_n):F|<\infty$ para todo $\alpha\in L$. Pero usando transitividad de grados en la torre $F\subset F(\alpha)\subset F(\alpha,a_0,\dots,a_n)$ se ve que esto implica que $|F(\alpha):F|<\infty$ para todo $\alpha\in L$, i.e. $F\subset L$ es algebraica. □

Ejercicios

Ej. 45 — Se tiene que $\sqrt{2}+\sqrt[3]{5}$ es algebraico sobre $\mathbb{Q}$ de grado 6. ¿Cuál es el grado de $\sqrt{2}+\sqrt[3]{5}$ sobre $\mathbb{Q}(\sqrt{2})$ y sobre $\mathbb{Q}(\sqrt[3]{5})$?

Ej. 46 — Sea $F\subset K$ extensión de cuerpos y $\alpha,\beta\in K$. Si β es algebraico sobre $F(\alpha)$ y β es trascendente sobre F, entonces α es algebraico sobre $F(\beta)$.

Ej. 47 — Hallar una base de $\mathbb{Q}(i,\sqrt{3},\omega)$ donde ω es una raíz cúbica primitiva de la unidad.

Ej. 48 — Un natural $n\in\mathbb{N}$ es *libre de cuadrados* si no existe $m\geqslant 2$ tal que $m^2\mid n$. El conjunto $\{\sqrt{n}:n\in\mathbb{N}\}$ es linealmente independiente sobre $\mathbb{Q}$.[2] Se deduce entonces que $\mathbb{Q}(\sqrt{p}:p \text{ es primo})$ es una extensión algebraica de $\mathbb{Q}$ que no es finita ni finitamente generada.

[2]Sugerencia: proceder por inducción. Ver http://www.thehcmr.org/issue2_1/mfp.pdf para una discusión sobre este problema.

2.3. Construcciones con regla y compás

Nuestro objetivo en esta sección es demostrar o refutar la posibilidad de las siguientes construcciones clásicas griegas con regla (sin graduar) y compás:

1. Duplicar el cubo: construir un cubo con el doble de volumen de uno dado.
2. Trisectar el ángulo: construir un ángulo que sea el tercio de uno dado.
3. Cuadrar el círculo: construir un cuadrado con la misma área que uno dado.

Empezamos con el plano $\mathbb{R}^2$ donde tenemos los ejes graduados por una distancia prefijada que denotamos 1, y que se cruzan en el origen. A partir de esto, diremos que un punto $(x, y) \in \mathbb{R}^2$ es *constructible* a partir de 1 (o sencillamente *constructible*) si utilizamos las siguientes construcciones:

1. Unir dos puntos con una recta,
2. Encontrar el punto de intersección de dos rectas,
3. Construir una circunferencia con centro y radio dados,
4. Hallar la intersección entre dos circunferencias o una circunferencia y una recta.

Un número $x \in \mathbb{R}$ es *constructible* si es la coordenada de un punto $(x, y) \in \mathbb{R}^2$ constructible.

El conjunto de los números constructibles es un subcuerpo de $\mathbb{R}$. En efecto, dados a, b constructibles, podemos construir con regla y compás $a \pm b$, ab, a/b. Está claro cómo construir $a \pm b$; las figuras 2.1 y 2.2 muestran cómo construir ab y a/b a partir de a y b. Por lo tanto $\mathbb{Q}$, el menor subcuerpo de $\mathbb{R}$, consiste de números constructibles.

La raíz cuadrada de un número constructible es constructible: la figura 2.3 muestra cómo construir $\sqrt{a}$ a partir de a.

Veamos que éstas son esencialmente las únicas construcciones que podemos hacer para conseguir nuevos números constructibles. En efecto, si $F \subset \mathbb{R}$ consiste de números constructibles (ya sabemos que $\mathbb{Q} \subset F$), entonces tenemos cuatro maneras de conseguir nuevos números.

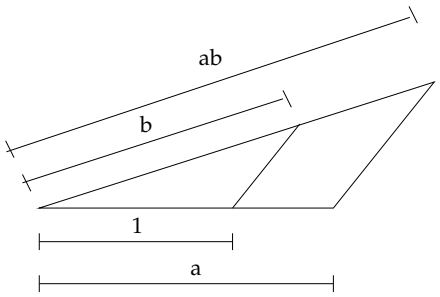


Figura 2.1: Cómo construir ab a partir de a y b constructibles

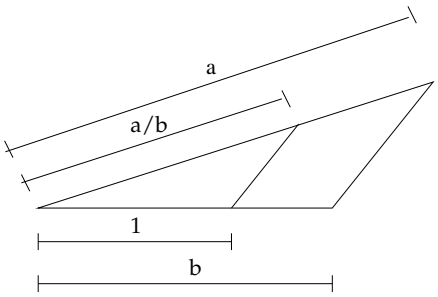


Figura 2.2: Cómo construir a/b a partir de a y b constructibles

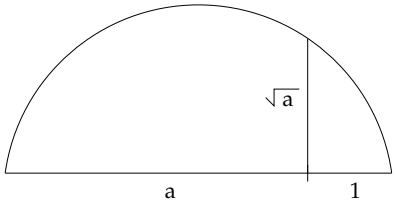


Figura 2.3: Cómo construir $\sqrt{a}$ a partir de a constructible

Intersectar dos rectas es resolver el sistema $\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$ donde $a, a', b, b', c, c' \in F$. Es un sistema de dos ecuaciones lineales en F; si tiene solución, será en F, luego no conseguimos elementos adicionales.

Intersectar una circunferencia y una recta es resolver el sistema $\begin{cases} (x-h)^2 + (y-k)^2 = r^2 \\ ax + by = c \end{cases}$ donde $h, k, r, a, b, c \in F$. De la última ecuación se deduce $y = \frac{c-ax}{b}$, sustituyendo en la primera vemos que x se obtiene con a lo sumo una extracción de raíz de un elemento de F, e y se consigue linealmente a partir de x.

Intersectar dos circunferencias C_1 y C_2 es resolver el sistema

$$\begin{cases} (x-h)^2 + (y-k)^2 = r^2 & C_1 \\ (x-h')^2 + (y-k')^2 = r'^2 & C_2 \end{cases}$$

donde $h, k, r, h', k', r' \in F$. Esto es lo mismo que intersectar C_1 con la resta $C_1 - C_2$ que es una recta, entonces como antes, agregando la intersección se obtiene a lo sumo un elemento que es extracción de raíz de un elemento de F.

Por lo tanto, un elemento constructible a partir de F es resultado de finitas extracciones sucesivas de raíces cuadradas empezando con un elemento de F. Recíprocamente, si un elemento es resultado de finitas extracciones sucesivas de raíces cuadradas a partir de un elemento de F, entonces es constructible. En particular los elementos de F al ser constructibles son resultado de finitas extracciones sucesivas de raíces cuadradas a partir de un elemento de $\mathbb{Q}$. En conclusión,

Teorema 2.27. *$\alpha \in \mathbb{R}$ es constructible con regla y compás si y sólo si existe una torre de cuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$$

donde $|F_i : F_{i-1}| = 2$ para todo $i = 1, \ldots, n$ y $\alpha \in F_n$.

En particular, si $\alpha \in \mathbb{R}$ se construye a partir de $F \subset \mathbb{R}$ con regla y compás, entonces $|F(\alpha) : F| = 2^k$ para cierto $k \in \mathbb{N}$.

Teorema 2.28. *Ninguna de las tres construcciones clásicas es posible.*

Demostración. 1. Duplicar el cubo: para duplicar el cubo unitario tendríamos que construir $\sqrt[3]{2}$ a partir de $\mathbb{Q}$, pero $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ que no es potencia de 2.

2. Trisectar el ángulo: trisectar un ángulo dado θ es equivalente a: dado $\cos\theta$, construir $\cos\theta/3$. En efecto, tener un ángulo θ es equivalente a tener el punto en la circunferencia unidad con ángulo θ, i.e. a tener $(\cos\theta, \sin\theta)$, que es equivalente a tener sólo $\cos\theta$.

   Consideremos $\theta = 60^\circ$. Entonces $\cos\theta = 1/2$. Tenemos la identidad:

   $$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3$$

   En este caso, si $\beta = \cos 20^\circ$, la fórmula queda

   $$4\beta^3 - 3\beta - 1/2 = 0 \Rightarrow 8\beta^3 - 6\beta - 1 = 0 \Rightarrow (2\beta)^3 - 3(2\beta) - 1 = 0$$

   Si $\alpha = 2\beta$, nos queda $\alpha^3 - 3\alpha - 1 = 0$. Construir β es equivalente a construir α, pero α es raíz del polinomio $f = X^3 - 3X - 1$ de grado 3 que es irreducible sobre $\mathbb{Q}$ pues ± 1 no son raíces (proposición 2.1). Tenemos entonces $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$, luego α no es constructible.

3. Cuadrar el círculo: para construir un cuadrado con misma área que un círculo de diámetro 1, tendríamos que construir $\sqrt{\pi}$. Pero si $\sqrt{\pi}$ fuera algebraico, también π sería algebraico. En efecto, si consideramos $\mathbb{Q} \subset \mathbb{Q}(\pi) \subset \mathbb{Q}(\sqrt{\pi})$, entonces la transitividad de grados nos dice $|\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)||\mathbb{Q}(\pi) : \mathbb{Q}|$. Suponiendo el lado izquierdo finito, se tendría $|\mathbb{Q}(\pi) : \mathbb{Q}| < \infty$, absurdo. □

Más adelante, en el teorema 2.84 daremos un criterio necesario y suficiente para construir un n-ágono regular.

2.4. Cuerpos de descomposición y clausuras algebraicas

Definición. Sea $f \in F[X]$. Decimos que f *se escinde* sobre F, o que *se factoriza completamente* sobre F, si f se escribe como producto de factores lineales en F.

Ejemplo 2.4.1. $X^2 + 1$ no se escinde sobre $\mathbb{R}$; se escinde sobre $\mathbb{C}$.

Definición. Sea $F \subset K$ extensión de cuerpos. Decimos que K es un *cuerpo de descomposición* de un polinomio $f \in F[X]$ sobre F si f se factoriza completamente en K, y K es el menor tal que esto ocurre. Notamos $K = \text{Desc}_F(f)$.[3]

Ejemplo 2.4.2.

- $\text{Desc}_{\mathbb{Q}}(X^2 + 1) = \mathbb{Q}(i)$, y $\text{Desc}_{\mathbb{R}}(X^2 + 1) = \mathbb{C}$.
- $\mathbb{Q}(\sqrt[3]{2})$ no es el cuerpo de descomposición de $f = X^3 - 2$ sobre $\mathbb{Q}$: en efecto, $\mathbb{Q}(\sqrt[3]{2})$ tiene sólo una de las tres raíces de f. De hecho el cuerpo de descomposición de f sobre $\mathbb{Q}$ tiene grado 6.
- El cuerpo de descomposición de $f = X^4 + 4$ sobre $\mathbb{Q}$ tiene grado 2, pues $f = (X^2 + 2X + 2)(X^2 - 2X + 2) \in \mathbb{Q}[X]$ tiene raíces $\pm 1 \pm i$, luego $\text{Desc}_{\mathbb{Q}}(f) = \mathbb{Q}(i)$.

Los ejemplos anteriores muestran que el grado del cuerpo de descomposición sobre el cuerpo base puede ser igual, mayor o menor que el grado del polinomio.

Teorema 2.29. *Dado $f \in F[X]$, existe un cuerpo de descomposición para f sobre F.*

Demostración. La idea de la prueba es la siguiente. Sabemos que existe una extensión de F donde f tiene una raíz. Miramos f sobre esta extensión, y aplicando el mismo teorema vamos agregando raíces hasta agotarlas todas.

Más formalmente, es por inducción en el grado de f. Si $\text{gr } f = 1$, el cuerpo de descomposición es $E = F$. Si $\text{gr } f = n$: si f se factoriza en factores lineales en F, tomo $E = F$. Si no, considero $F(\alpha)$ con α raíz de un factor irreducible de f en F. El polinomio que queda al quitarle este factor irreducible a f tiene grado menor que n: por hipótesis de inducción tiene un cuerpo de descomposición E sobre F.

Considero $E(\alpha)$: f se factoriza en factores lineales en $E(\alpha)$. Entonces $\bigcap\{K \text{ cuerpo } : F \subset K \subset E(\alpha), f \text{ se factoriza completamente en } K\}$ es el cuerpo buscado. □

Observación 2.4.3. Se desprende de la prueba que si $F \subset K$, $K = \text{Desc}_F(f)$ y $\alpha_1, \ldots, \alpha_r \in K$ son las raíces de f, entonces $K = F(\alpha_1, \ldots, \alpha_r)$.

Proposición 2.30. *Sea $f \in F[X]$ de grado n. Entonces $|\text{Desc}_F(f) : F| \leqslant n!$.*

Demostración. Sea $\alpha_1 \in \text{Desc}_F(f)$ raíz de f. Entonces como $m_{\alpha_1,F} \mid f$, se tiene

$$|F(\alpha_1) : F| = \text{gr } m_{\alpha_1,F} \leqslant \text{gr } f = n$$

Sea $\alpha_2 \in \text{Desc}_F(f)$ raíz del polinomio g_1 que queda al sacarle todos los factores $(X - \alpha_1)$ a f: se tiene $\text{gr } g_1 \leqslant n - 1$. Entonces $|F(\alpha_1)(\alpha_2) : F(\alpha_1)| \leqslant n - 1$.

Continuando hasta agotar todas las raíces $\alpha_1, \ldots, \alpha_r$ de f, se tiene $|\text{Desc}_F(f) : F| = |F(\alpha_1, \ldots, \alpha_r) : F| \leqslant n(n-1)\ldots 1 = n!$. □

[3] Esta notación se ve justificada por el hecho que dos cuerpos de descomposición de un polinomio sobre un cuerpo son isomorfos, como veremos más tarde.

Teorema 2.31. *Sea $\varphi : F \to F'$ isomorfismo de cuerpos, $f \in F[X]$ y $f' \in F'[X]$ el resultado de aplicarle φ a los coeficientes de f. Sea E un cuerpo de descomposición para f sobre F; E' un cuerpo de descomposición para f' sobre F'. Entonces φ se extiende a $\varphi : E \to E'$ isomorfismo de cuerpos.*

Demostración. Es extender φ de a una raíz de f, usando el teorema de extensión 2.12. □

El siguiente corolario nos permite hablar de *el* cuerpo de descomposición de un polinomio sobre un cuerpo, y escribir $\mathrm{Desc}_F(f)$.

Corolario 2.32. *Dos cuerpos de descomposición de un mismo polinomio son isomorfos.*

Demostración. La identidad id: $F \to F$ se extiende a un isomorfismo entre dos cuerpos de descomposición dados del mismo polinomio $f \in F[X]$. □

Proposición 2.33. *Sea K cuerpo. Son equivalentes:*

1. *K no tiene extensiones algebraicas distintas de sí mismo.*
2. *Los polinomios irreducibles en $K[X]$ son los polinomios de grado 1.*
3. *Todo polinomio en $K[X]$ no constante tiene una raíz en K.*
4. *Todo polinomio en $K[X]$ se escinde sobre K.*
5. *K contiene un subcuerpo F tal que la extensión $F \subset K$ es algebraica y todo polinomio en $F[X]$ se escinde sobre K.*

Demostración. (1 $\Rightarrow$ 2) Si existiera un polinomio irreducible $p \in K[X]$ de grado mayor que 1, entonces existiría una extensión $K(\alpha)$ de K donde p tendría una raíz α que no está en K. Entonces $K \subset K(\alpha)$ sería una extensión algebraica propia, absurdo.

(2 $\Rightarrow$ 3) Un polinomio no constante debe tener un factor irreducible, que por hipótesis será de la forma $ax + b \in K[X]$ con $a \neq 0$. Pero entonces tiene como raíz a $-b/a$.

(3 $\Rightarrow$ 4) Si $f \in K[X]$ es constante, entonces se escinde sobre K. Si no es constante, entonces tiene una raíz $\alpha_1 \in K$, luego $f = (X - \alpha_1)f_1$ para cierto $f_1 \in K[X]$. Si f_1 es constante ya está. Si no lo es, entonces tiene una raíz $a_2 \in K$, y $f = (X - \alpha_1)(X - \alpha_2)f_2$, para cierto $f_2 \in K[X]$. Iterando la construcción, eventualmente llegamos a un $f_n = \alpha_0 \in K$ constante (pues a cada paso el polinomio f_i baja de grado), y se tiene $f = \alpha_0(X - \alpha_1)\dots(X - \alpha_{n-1})$.

(4 $\Rightarrow$ 5) Basta tomar $F = K$.

(5 $\Rightarrow$ 1) Sea $K \subset L$ extensión algebraica, $\alpha \in L$. Entonces α es algebraico sobre F, luego tiene un polinomio mínimo $m_{\alpha,F}$ que por hipótesis se escinde sobre K. Luego $m_{\alpha,F} = \alpha_0(X - \alpha_1)\dots(X - \alpha_n)$ para ciertos $\alpha_0, \dots, \alpha_n \in K$.

Como $m_{\alpha,F}$ anula a α, necesariamente $\alpha = \alpha_i$ para algún $i = 1, \dots, n$, pero entonces $\alpha \in K$ para todo $\alpha \in L$, i.e. $L = K$. □

Definición. Un cuerpo K es *algebraicamente cerrado* si cumple cualquiera de las condiciones equivalentes del teorema anterior.

Un cuerpo K es una *clausura algebraica* de un cuerpo F si $F \subset K$ es una extensión algebraica y todo polinomio $f \in F[X]$ se escinde sobre K.

Observación 2.4.4. La condición 5 de la proposición anterior nos dice que es equivalente ser algebraicamente cerrado a ser la clausura algebraica de un subcuerpo.

Observación 2.4.5. Supongamos que no conocemos la proposición anterior. Digamos que un cuerpo K es algebraicamente cerrado si todo polinomio en $K[X]$ se escinde sobre K. Entonces la equivalencia con el ítem 3 de la proposición nos dice que para verificar que un cuerpo K es algebraicamente cerrado, basta verificar sencillamente que todo polinomio (no constante) en $K[X]$ tiene *una* raíz en K.

Por otro lado, la condición 5 nos dice que basta verificar que todos los polinomios de un subcuerpo F del cual K es una extensión algebraica se escinden sobre K.

Es natural preguntarse si podemos juntar estas dos aparentes debilitaciones de ser algebraicamente cerrado, en una debilitación mayor: ¿será cierto que si todos los polinomios de un subcuerpo F del cual K es una extensión algebraica tienen *una* raíz en K, entonces K es algebraicamente cerrado?

Esto es cierto pero considerablemente más difícil de probar: es el teorema 2.94.

Teorema 2.34. *Todo cuerpo tiene una clausura algebraica.*

Demostración. Sea K cuerpo, y P el conjunto de todos los polinomios no constantes de $K[X]$. La idea de la demostración es formalizar lo que uno haría intuitivamente, que es adjuntar a K todas las raíces de todos los polinomios no constantes de $K[X]$. Para hacer esto, tenemos que usar el axioma de elección. Éste nos garantiza que existe $\leqslant$ un buen orden en P.[4]

Vamos a construir por recursión en el buen orden $(P, \leqslant)$ una cadena $\{K_q\}_{q \in P}$ de K tales que para todo $q, q' \in P$:

I. $K \subset K_q$ es una extensión algebraica,

II. Si $q \leqslant q'$ entonces $K_q \subset K_{q'}$,

III. q se escinde sobre K_q.

Definimos $K_{p_0} = \mathrm{Desc}_K(p_0)$, es una extensión algebraica de K. Definamos $K_{q'}$ supuestos definidos $\{K_q\}_{q<q'}$: sea

$$K_{q'}^* = \bigcup_{q<q'} K_q$$

Es un cuerpo por la condición *ii*. de los K_q para $q < q'$, y es una extensión algebraica de K por la condición *i* para $q < q'$. Podemos definir entonces $K_{q'} = \mathrm{Desc}_{K_{q'}^*}(q')$. Esto completa la definición por recursión.

Sea ahora $\overline{K} = \bigcup_{q \in P} K_q$. Es un cuerpo por la condición *ii*. de todos los K_q, y es una extensión algebraica por la condición *i*. de todos los K_q. Ahora, todo polinomio no constante

[4] Recordemos que un buen orden es un orden total tal que todo subconjunto tiene un mínimo. Los buenos órdenes permiten, como los naturales, hacer definiciones por recursión. Si el lector no se siente cómodo con esta demostración porque la instancia del axioma de elección que utilizamos (el principio de buena ordenación) le resulta incómoda, lo remitimos a [M2] para otras demostraciones que usan, por ejemplo, el lema de Zorn.

$p \in K[X]$ se escinde sobre $K_p \subset \overline{K}$, luego se escinde sobre $\overline{K}$, y $\overline{K}$ es la clausura algebraica de K buscada. □

Ejemplo 2.4.6. El teorema fundamental del álgebra (que probaremos más adelante) afirma que $\mathbb{C}$ es una clausura algebraica de $\mathbb{R}$.

Una clausura algebraica de $\mathbb{Q}$ es el cuerpo de los números algebraicos $\overline{\mathbb{Q}}$ discutido en el ejemplo 2.2.3.

Teorema 2.35. *Sea $F \subset K$ una extensión algebraica, L un cuerpo algebraicamente cerrado. Entonces cualquier morfismo $\sigma : F \to L$ se extiende a un morfismo $\sigma^* : K \to L$.*

Demostración. Consideraremos el conjunto de cuerpos intermedios entre F y K junto con sus extensiones de σ. El lema de Zorn nos garantizará un elemento maximal que mostraremos que debe ser K, y esto terminará la prueba.

Sea $M = \{(A, \tau) : A \text{ cuerpo }, F \subset A \subset K, \tau : A \to L \text{ morfismo que extiende a } \sigma\}$.

Consideremos el orden parcial $\leqslant$ en M dado por

$$(A, \tau) \leqslant (A', \tau') \iff A \subset A' \text{ y } \tau'|_A = \tau$$

Toda cadena $\{(A_\alpha, \tau_\alpha)\}_{\alpha \in I}$ tiene cota superior: es (A, τ), con $A = \bigcup_{\alpha \in I} A_\alpha$ y $\tau : A \to L$ definida como $\tau(a) = \tau_\alpha(a)$ para cierto $\alpha \in I$ tal que $a \in A_\alpha$.

Por el lema de Zorn, M tiene un elemento maximal (A, τ): esto es, σ no se extiende a ningún otro cuerpo más grande que A. Basta probar que $A = K$.

Supongamos que $A \subsetneq K$. Sea $\alpha \in K \backslash A$.

Afirmación: τ se extiende a un morfismo $A(\alpha) \to L$.

Demostración: $A(\alpha) = A[X]/\langle m_{\alpha,A} \rangle$. Si le aplico τ a los coeficientes de $m_{\alpha,A}$ me da un polinomio $\tau m_{\alpha,A} \in L[X]$ que tiene una raíz $r \in L$ pues L es algebraicamente cerrado.

Sea $\varphi : A[X] \to L$ definido por $\varphi|_A = \tau$, $\varphi(X) = r$. Es un morfismo de anillos tal que $\varphi : m_{\alpha,A}(X) \mapsto \tau m_{\alpha,A}(r) = 0$, entonces por la propiedad universal del cociente, obtenemos $A(\alpha) \simeq A[x]/\langle m_{\alpha,A} \rangle \xrightarrow{\tilde{\varphi}} L$ morfismo. Esto demuestra la afirmación.

La afirmación demostrada contradice la maximalidad de (A, τ). □

Corolario 2.36. *Sean $F \subset K$, $F' \subset K'$ clausuras algebraicas de F y de F'. Entonces un isomorfismo $\sigma : F \to F'$ se extiende a un isomorfismo $K \to K'$. En particular dos clausuras algebraicas de un cuerpo F son isomorfas.*

Demostración. El isomorfismo $\sigma : F \to F'$ puede ser visto como un (mono)morfismo $\sigma : F \to K'$. Por el teorema anterior se extiende a un (mono)morfismo $\sigma^* : K \to K'$. Como K es algebraicamente cerrado, entonces $\sigma^*(K)$ también lo es. Además $K \subset K'$ es algebraica, entonces $\sigma^*(K) \subset K'$ también es una extensión algebraica, por lo tanto $\sigma^*(K) = K'$. Entonces σ^* es sobreyectiva, luego es un isomorfismo.

En particular, tomando $F = F'$ y $\sigma = \mathrm{id}$, se obtiene que dos clausuras algebraicas de un cuerpo F son isomorfas. □

Ejemplo 2.4.7. La clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ que discutimos en el ejemplo 2.2.3 descansa sobre el teorema fundamental del álgebra, que aún no demostramos. Podemos afirmar ahora la existencia de una clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, sin pasar por los complejos. El corolario anterior nos dice que de todas maneras el resultado es el mismo.

2.5. Separabilidad y perfección

Definición. Un polinomio $f \in F[X]$ es *separable* si no tiene raíces múltiples en su cuerpo de descomposición sobre F.[5]

Una extensión de cuerpos $F \subset E$ es *separable* (o *algebraicamente separable*) si todo elemento de E es raíz de un polinomio $f \in F[X]$ separable.

Un polinomio o una extensión que no es separable se dice *inseparable*.

Observación 2.5.1. Si $F \subset K$ y $\alpha \in K$ es raíz de un polinomio separable $f \in F[X]$, entonces como $m_{\alpha,F} \mid f$, se tiene que $m_{\alpha,F}$ también es separable. Por lo tanto es lo mismo que α sea raíz de un polinomio separable que $m_{\alpha,F}$ sea separable. De esta manera, una extensión es separable si y sólo si es algebraica y todos los polinomios mínimos son separables.

Observación 2.5.2. Si $F \subset E \subset K$ es torre de cuerpos con $F \subset K$ separable, entonces $F \subset E$ es separable.

Definición. Sea $f \in F[X]$, $f = \sum_{i=0}^{n} a_i X^i$. La *derivada formal* del polinomio f es el polinomio

$$Df = f' := \sum_{i=1}^{n} i a_i X^{i-1} \in F[X]$$

Proposición 2.37. *Sean $f, g \in F[X]$. Se cumplen las siguientes propiedades:*

- *Si $f \in F$ entonces $f' = 0$.*
- *Si $c \in F$ entonces $(cf)' = cf'$.*
- $(f+g)' = f' + g'$.
- $(fg)' = f'g + fg'$.
- $(f/g)' = (f'g - fg')/g^2$.

Demostración. Ejercicio. □

Proposición 2.38. *Sea $f \in F[X]$. Entonces f tiene una raíz múltiple α si y sólo si α es también raíz de la derivada Df.*

En particular f es separable si y sólo si mcd(f,Df)=1 sobre el cuerpo de descomposición de f sobre F.

Demostración. ($\Rightarrow$) Sea α raíz múltiple de f. Entonces sobre $\mathrm{Desc}_F(f)$ se tiene $f = (X-\alpha)^n g(x)$ para cierto $n \geqslant 2$. Derivando obtenemos $Df = n(X-\alpha)^{n-1} + (X-\alpha)^n Dg$, con $n-1 \geqslant 1$. Por lo tanto Df tiene a α como raíz.

($\Leftarrow$) Si α es raíz de f, entonces $f = (X-\alpha)h$ para cierto $h \in F[X]$. Derivando obtenemos $Df = h + (X-\alpha)Dh$. Como α también es raíz de Df, α debe ser entonces raíz de h, luego $f = (X-\alpha)^2 h_1$ para cierto $h_1 \in F[X]$.

Por lo tanto α es raíz múltiple de f si y sólo si f y Df son ambos divisibles por $m_{\alpha,F}$. En particular f no tiene raíces múltiples (i.e. es separable) si y sólo si mcd(f,Df)=1. □

[5] Algunos autores como [M2] dan una definición no equivalente de un polinomio separable: un polinomio es separable si todos sus factores irreducibles no tienen raíces múltiples en sus cuerpos de descomposición respectivos.

Corolario 2.39.

- *Todo polinomio irreducible sobre un cuerpo de característica cero es separable. Por lo tanto toda extensión algebraica de un cuerpo de característica cero es separable.*
- *Un polinomio sobre un cuerpo de característica cero es separable si y sólo si es producto de irreducibles diferentes.*

Demostración. ▪ Sea F cuerpo de característica cero, $f \in F[X]$ irreducible de grado n. Sus factores irreducibles son de grado 0 y n, pero su derivada Df tiene grado $n-1$ porque al tener car $F = 0$, se tiene $n - 1 \neq 0$. Entonces necesariamente mcd(f,Df)=1, luego f es separable.

- ($\Rightarrow$) Siempre p es producto de irreducibles: éstos deben ser distintos pues p es separable.

  ($\Leftarrow$) Sea p producto de irreducibles diferentes. Sin pérdida de generalidad podemos suponer p mónico. Entonces p es producto de *separables* diferentes (por el primer ítem), luego producto de irreducibles que no tienen raíces en común. Aplicando el corolario 2.15 se tiene que p debe ser separable. □

Ejemplo 2.5.3. El corolario anterior nos dice que en característica cero, los polinomios inseparables son aquéllos donde un factor irreducible se repite, por ejemplo $(X^2+1)^2 \in \mathbb{Q}[X]$.

Un ejemplo menos trivial es $X^2 - t \in \mathbb{Z}_2(t)[X]$. Es irreducible por el criterio de Eisenstein general (el ideal $\langle t \rangle \subset \mathbb{Z}_2[t]$ es primo), pero no es separable: sea $\sqrt{t}$ una raíz en algún cuerpo de descomposición. Entonces $(X - \sqrt{t})^2 = X^2 - 2X\sqrt{t} + t = X^2 + t = X^2 - t$ usando reiteradamente que la característica de $\mathbb{Z}_2$ es dos. Entonces $\sqrt{t}$ es una raíz doble de $X^2 - t$, luego $X^2 - t$ no es separable.

Análogamente $X^p - t \in \mathbb{Z}_p(t)[X]$ es irreducible y no es separable.

Proposición 2.40. *Sea $f \in F[X]$ irreducible no constante. Son equivalentes:*

a) f *es inseparable.*

b) $\text{mcd}(f, Df) \neq 1$.

c) $Df = 0$.

d) car $F = p > 0$ *y* f *es un polinomio en* X^p.

e) Todas las raíces de f *son múltiples.*

Demostración. (a $\Leftrightarrow$ b) Ya lo sabemos.

(b $\Rightarrow$ c) f es irreducible, y gr $Df <$ gr f, entonces $\text{mcd}(f, Df) \neq 1 \Rightarrow Df = 0$ (recordar observación 2.0.1).

(c $\Rightarrow$ d) Como f no es constante, Df puede ser el polinomio nulo sólo si f es un polinomio en X^p y car $F = p$, pues todos los factores de la derivada se tienen que anular.

(d $\Rightarrow$ e) Sea $f(X) = g(X^p)$. Escribo $g(X) = \prod (X - a_i)^{m_i}$ en el cuerpo de descomposición para f sobre F. Entonces en ese cuerpo, usando el lema 2.71,

$$f(X) = g(X^p) = \prod (X^p - a_i)^{m_i} = \prod (X - \sqrt[p]{a_i})^{pm_i}$$

donde $\sqrt[p]{a_i}$ es alguna raíz de $X^p - a_i$. Entonces todas las raíces de f tienen multiplicidad al menos p.

(e $\Rightarrow$ a) Obvio. □

Definición. Un cuerpo F es *perfecto* si todo polinomio $f \in F[X]$ irreducible es separable.

Ejemplo 2.5.4. Todo cuerpo algebraicamente cerrado es perfecto.

Definición. Sea F un cuerpo de característica $p > 0$. El *endomorfismo de Frobenius* es el morfismo $F \to F$, $x \mapsto x^p$.

Observación 2.5.5. El endomorfismo de Frobenius σ es efectivamente un endomorfismo: si $a, b \in F$, $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$, obviamente $\sigma(1) = 1$ y por el lema 2.71 se tiene $\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$.

La siguiente propiedad nos dice que "casi todos los cuerpos son perfectos".

Proposición 2.41.

1. *Todo cuerpo de característica cero es perfecto.*
2. *Si F es un cuerpo de característica $p > 0$, entonces F es perfecto si y sólo si $F = F^p := \{a^p : a \in F\}$ (i.e. si y sólo si el endomorfismo de Frobenius es un automorfismo).*
3. *Todo cuerpo finito es perfecto.*

Demostración. 1. Ya lo sabemos.

2. ($\Rightarrow$) Si $a \in F \backslash F^p$, entonces $X^p - a \in F[X]$ es irreducible (pues a no es raíz) , y no es separable, pues por el lema 2.71, si $\sqrt[p]{a}$ es una raíz de $X^p - a$ en el cuerpo de descomposición, se tiene $X^p - a = (X - \sqrt[p]{a})^p$.

   ($\Leftarrow$) Supongamos que $f \in F[X]$ es irreducible pero no separable. Entonces f es un polinomio en X^p:

   $$f(X) = \sum a_i X^{pi} = \sum b_i^p X^{pi} = \left(\sum b_i X^i\right)^p$$

   para ciertos $a_i \in F$, $b_i \in F$ tales que $a_i = b_i^p$ (existen pues $F = F^p$); en el último paso usamos el lema 2.71. Pero entonces f no sería irreducible, absurdo.

3. Sea F un cuerpo finito, entonces tiene característica $p > 0$. Sea $\phi : F \to F^p$, $a \mapsto a^p$ el endomorfismo de Frobenius. Es inyectivo: $a^p = b^p \Rightarrow (a-b)^p = 0 \Rightarrow a = b$, y es obviamente sobreyectivo, luego $F = F^p$. □

Por lo tanto para que un cuerpo no sea perfecto, debe tener característica p y ser infinito. En el ejemplo 2.5.3 vimos que $\mathbb{Z}_p(t)$ no es perfecto.

Proposición 2.42. *Sea F cuerpo. Son equivalentes:*

1. *F es perfecto,*
2. *Toda extensión finita de F es separable,*
3. *Toda extensión algebraica de F es separable.*

Demostración. $(1 \Rightarrow 2)$ Si $F \subset K$ es finita, entonces como F es perfecto para todo $\alpha \in K$ se tiene que $m_{\alpha,F}$ es separable, i.e. $F \subset K$ es separable.

$(2 \Rightarrow 1)$ Supongamos que toda extensión finita de F es separable. Sea $p \in F[X]$ irreducible. Consideremos $K = F(\alpha)$ donde α es alguna raíz de p. La extensión $F \subset K$ es finita, por lo tanto separable. Como $p = m_{\alpha,F}$ entonces p es separable.

$(2 \Rightarrow 3)$ Sea $F \subset K$ algebraica. Entonces dado $\alpha \in K$ tenemos que $F \subset F(\alpha)$ es finita, luego separable, de donde α es raíz de un polinomio en $F[X]$ separable.

$(3 \Rightarrow 2)$ Toda extensión finita es algebraica. □

2.6. Fundamentos de la teoría de Galois

Citamos el primer párrafo de la introducción de [KM] como motivación para la definición siguiente.

> ¿Por qué un cuadrado nos parece una figura simétrica, un círculo aún más simétrico, pero el dígito "4" completamente asimétrico? Para responder a esta pregunta, consideremos los movimientos del plano que dejan cada una de estas figuras en el mismo lugar que antes. Es fácil ver que para el cuadrado hay ocho de estos movimientos, para el círculo hay infinitos, pero para el dígito "4" sólo uno, la identidad, que deja cada punto del dígito fijo. El conjunto G de movimientos diferentes que dejan una figura ocupando el mismo lugar que antes sirve como una medida para su grado de simetría: a mayor cantidad de elementos de G, i.e., los movimientos, a mayor simetría de la figura. [Este conjunto G es un grupo con la composición.]
>
> M.I. Kargapolov, Ju.I. Merzljakov

Definición. Sea $F \subset K$ extensión de cuerpos. El *grupo de Galois* de la extensión es

$$\mathrm{Gal}_F^K := \{\sigma \in \mathrm{Aut}(K) : \sigma(\alpha) = \alpha \quad \forall \alpha \in F\}$$

Consiste de los elementos de $\mathrm{Aut}(K)$ que dejan fijo F.

Definición. Sea $k \subset F \subset L$ torre de cuerpos. Si $\sigma : F \to L$ es tal que $\sigma|_k = \mathrm{id}$, decimos que σ es un *k-monomorfismo* de cuerpos.

De esta manera, los elementos del grupo de Galois Gal_F^K son los F-automorfismos de K.

Proposición 2.43. *Sea $F \subset K$ extensión de cuerpos. Entonces Gal_F^K permuta las raíces de los polinomios en $F[X]$.*

Demostración. Sea $\sigma \in \mathrm{Gal}_F^K$ y α raíz de un polinomio $f = a_n X^n + \cdots + a_1 X + a_0 \in F[X]$. Se tiene entonces $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Apliquémosle σ:

$$\begin{aligned} 0 = \sigma(0) = \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) &= \sigma(a_n)\sigma(\alpha)^n + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &\overset{\sigma|_F = \mathrm{id}}{=} a_n\sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 \end{aligned}$$

Tenemos entonces que $\sigma(\alpha)$ es también raíz de f, i.e., todo $\sigma \in \mathrm{Gal}_F^K$ permuta las raíces de los polinomios en $F[X]$. □

Observación 2.6.1. Si descomponemos un polinomio como producto de irreducibles, entonces el grupo de Galois permuta sus raíces permutando las de cada factor irreducible.

Definición. Sea K cuerpo, $H < \mathrm{Aut}(K)$. Definimos el *cuerpo fijo* de H como

$$\mathrm{Fix}(H) := \{\alpha \in K : \sigma(\alpha) = \alpha \quad \forall \sigma \in H\}$$

Consiste de los elementos de K que quedan fijos por H.

Observación 2.6.2. "Grupo de Galois" y "cuerpo fijo" es considerar la ecuación $\sigma(\alpha) = \alpha$ desde los dos puntos de vista posibles.

Observación 2.6.3. Es sencillo verificar que el cuerpo fijo de H es un subcuerpo de K.

Proposición 2.44. *Las asociaciones $F \subset K \mapsto \mathrm{Gal}_F^K$ y $H < \mathrm{Aut}(K) \mapsto \mathrm{Fix}(H)$ revierten inclusiones:*

- *Si $F_1 \subset F_2 \subset K$ es torre de cuerpos, entonces $\mathrm{Gal}_{F_2}^K < \mathrm{Gal}_{F_1}^K$*
- *Si $H_1 \subset H_2 \subset \mathrm{Aut}(K)$ es una cadena de subgrupos, entonces $\mathrm{Fix}(H_2) \subset \mathrm{Fix}(H_1)$.*

Demostración. Todo automorfismo de K que deja fijo F_2 es un automorfismo de K que deja fijo F_1.

Si un elemento de K queda fijo por H_2, entonces queda fijo por H_1. □

Definición. Una extensión de cuerpos finita $F \subset K$ es *de Galois* si $\mathrm{Fix}(\mathrm{Gal}_F^K) = F$. Equivalentemente, si para todo $u \in K \backslash F$ existe $\sigma \in \mathrm{Gal}_F^K$ tal que $\sigma(u) \neq u$.

Observación 2.6.4. Una extensión es de Galois cuando el grupo de Galois es lo más grande posible, i.e. cuando hay la mayor cantidad posible de automorfismos que dejan fijo F. En virtud de la cita del comienzo de la sección, una extensión es de Galois cuando "exhibe la mayor simetría posible".

Observación 2.6.5. Sea $F \subset K$ extensión de cuerpos finita. La extensión $\mathrm{Fix}(\mathrm{Gal}_F^K) \subset K$ siempre es de Galois. Esto no es más que un juego de palabras: en efecto, estamos diciendo que para todo elemento u en K que no queda fijo por los automorfismos de K que dejan fijo F hay un automorfismo de K que deja fijo lo que queda fijo por los automorfismos de K que dejan fijo F que mueve u (¡!).

Definición. Un *carácter* de un grupo G sobre un cuerpo L es un morfismo de grupos $G \to L^*$.

Definición. Sean $\chi_1, \ldots, \chi_n$ caracteres de un grupo G sobre un cuerpo L. Decimos que son *linealmente independientes* si lo son como elementos del L-espacio vectorial $\mathrm{Hom}(G, L^*)$, i.e. si para todo $a_1, \ldots, a_n \in L$ se tiene

$$a_1\chi_1 + \cdots + a_n\chi_n = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Si no son linealmente independientes, se dicen *linealmente dependientes*.

Teorema 2.45 (de independencia lineal de caracteres de Dedekind)**.** *Si $\chi_1, \ldots, \chi_n$ son caracteres diferentes de un grupo G sobre un cuerpo L, entonces son linealmente independientes.*

Demostración. Supongamos por absurdo que son linealmente dependientes. Sea m el menor número de escalares no nulos tal que hay una relación de dependencia lineal entre m caracteres de los n. A menos de reordenación podemos suponer que son los m primeros. Se tiene entonces para ciertos $a_1, \ldots, a_m \in L$:

$$a_1\chi_1 + \cdots + a_m\chi_m = 0, \quad a_i \neq 0 \quad \forall i = 1, \ldots, m$$

Evaluando en $g \in G$ se tiene

$$a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0 \quad \forall g \in G \tag{2.3}$$

Como $\chi_1 \neq \chi_m$, existe $g_0 \in G$ tal que $\chi_1(g_0) \neq \chi_m(g_0)$. Evaluando en $g_0 g$ y usando que los χ_i son morfismos de grupos, se obtiene

$$a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0 \quad \forall g \in G \tag{2.4}$$

Restándole a la ecuación (2.4) la ecuación (2.3) multiplicada por $\chi_m(g_0)$, se obtiene

$$\begin{aligned} 0 &= a_1\chi_1(g_0)\chi_1(g) + \cdots + \cancel{a_m\chi_m(g_0)\chi_m(g)} - a_1\chi_1(g)\chi_m(g_0) - \cdots - \cancel{a_m\chi_m(g)\chi_m(g_0)} \\ &= \underbrace{a_1(\chi_1(g_0) - \chi_m(g_0))}_{\neq 0}\chi_1(g) + \ldots a_{m-1}(\chi_{m-1}(g_0) - \chi_m(g_0))\chi_{m-1}(g) \quad \forall g \in G \end{aligned}$$

Ésta es una relación de dependencia lineal no trivial de $m-1$ caracteres: contradice la minimalidad de m, llegando a un absurdo. □

Corolario 2.46. *Sean $\sigma_1, \ldots, \sigma_n : K \to L$ morfismos de cuerpos diferentes. Entonces son linealmente independientes como funciones $K \to L$.*

Demostración. Como un morfismo de cuerpos envía el cero en el cero, cada σ_i induce un morfismo de grupos $\sigma_i^* : K^* \to L^*$. Estos σ_i^* son caracteres del grupo K^* sobre L. Por el teorema anterior, $\sigma_1^*, \ldots, \sigma_n^*$ son linealmente independientes, luego $\sigma_1, \ldots, \sigma_n$ son linealmente independientes, pues difieren con los σ_i^* sólo en el cero, lo cual no afecta a la independencia lineal. □

Sobre el siguiente teorema (cuya prueba es esencialmente álgebra lineal) descansa gran parte de los teoremas posteriores de teoría de Galois.

Teorema 2.47. *Sea K cuerpo, $H = \{\sigma_1, \ldots, \sigma_n\} < \mathrm{Aut}(K)$. Entonces*

$$|K : \mathrm{Fix}(H)| = |H : 1| = |H| = n$$

Gráficamente,[6]

$$\begin{array}{cc} K & 1 \\ | & | \\ \mathrm{Fix}(H) & H \end{array}$$

Demostración. Notemos $F := \mathrm{Fix}(H)$. Supongamos por absurdo que $n \neq |K : F|$.

Caso 1: $n > |K : F| =: m$.

Sea $\omega_1, \ldots, \omega_m$ una F-base de K. El sistema

$$\begin{cases} \sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n = 0 \\ \vdots \\ \sigma_1(\omega_m)x_1 + \cdots + \sigma_n(\omega_m)x_n = 0 \end{cases}$$

es un sistema lineal homogéneo de m ecuaciones con n incógnitas, $m < n$: tiene una solución no trivial $\beta_1, \ldots, \beta_n$.

[6] El diagrama tendrá más sentido cuando enunciemos el teorema fundamental de la teoría de Galois.

Sean $a_1, \ldots, a_m$ elementos arbitrarios de F. Como $F = \text{Fix}(H)$, entonces $\sigma_i(a_j) = a_j$ para todo $i = 1, \ldots, n$, $j = 1, \ldots, m$. Por lo tanto, multiplicando la i-ésima ecuación por a_i y remplazando las incógnitas por la solución no trivial, se obtiene:

$$\begin{cases} \sigma_1(a_1\omega_1)\beta_1 + \cdots + \sigma_n(a_1\omega_1)\beta_n = 0 \\ \vdots \\ \sigma_1(a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_m\omega_m)\beta_n = 0 \end{cases}$$

Sumando las m ecuaciones, se obtiene:

$$\sigma_1(a_1\omega_1 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + \cdots + a_m\omega_m)\beta_n = 0$$

para cualquier $a_1, \ldots, a_m \in F$. Pero $\omega_1, \ldots, \omega_m$ es una F-base, luego $a_1\omega_1 + \cdots + a_m\omega_m$ representa un elemento arbitrario $\alpha \in K$. La ecuación queda entonces

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0 \quad \forall \alpha \in K$$

Como los β_i no son todos cero, entonces la ecuación anterior nos dice que $\sigma_1, \ldots \sigma_n$ son morfismos de cuerpos linealmente dependientes. Esto contradice el corolario anterior.

Caso 2: $n < |K : F|$.

Existen entonces $n + 1$ elementos $\alpha_1, \ldots, \alpha_{n+1} \in K$ linealmente independientes sobre F. El sistema

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{cases} \tag{2.5}$$

es un sistema lineal homogéneo de n ecuaciones con $n+1$ incógnitas, luego tiene una solución no trivial $\beta_1, \ldots, \beta_n \in K$.

Afirmación: existe j tal que $\beta_j \notin F$.

Demostración: Supongamos por absurdo que los β_i están todos en F. Existe un i tal que $\sigma_i = \text{id}$ (pues H es un grupo). La ecuación i-ésima queda entonces $\alpha_1\beta_1 + \cdots + \alpha_{n+1}\beta_{n+1} = 0$: es una relación de dependencia de los α_i, absurdo pues estos son linealmente independientes sobre F.

Elegimos una solución del sistema con número mínimo r de β_i no nulos. A menos de reordenación podemos suponer que son los r primeros: $\beta_1, \ldots, \beta_r$, y podemos suponer $\beta_r = 1$ por estar trabajando en un cuerpo y ser el sistema homogéneo. Como no pueden estar todos en F, debe ser $r > 1$ (pues $1 \in F$). A menos de reordenación podemos suponer $\beta_1 \notin F$.

El sistema queda

$$\begin{cases} \sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0 \\ \vdots \\ \sigma_n(\alpha_1)\beta_1 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0 \end{cases} \tag{2.6}$$

Como $F = \text{Fix}(H)$ y $\beta_1 \notin F$, entonces existe $k_0 \in \{1, \ldots, n\}$ tal que $\sigma_{k_0}(\beta_1) \neq \beta_1$. Apliquemos σ_{k_0} al sistema: para todo $j = 1, \ldots, n$ se tiene

$$(\sigma_{k_0}\sigma_j)(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + (\sigma_{k_0}\sigma_j)(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}\sigma_j(\alpha_r) = 0$$

Pero $\{\sigma_{k_0}\sigma_1, \ldots, \sigma_{k_0}\sigma_n\} = \{\sigma_1, \ldots, \sigma_n\}$ pues H es un grupo. El sistema queda, para todo $i = 1, \ldots, n$:

$$\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0$$

Restándoselo al sistema (2.6), nos queda, para todo $i = 1, \ldots, n$:

$$\sigma_i(\alpha_1)\overbrace{[\beta_1 - \sigma_{k_0}(\beta_1)]}^{\neq 0} + \cdots + \sigma_i(\alpha_{r-1})[\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})] = 0$$

Esta es una solución no trivial del sistema (2.5) con a lo sumo $r-1$ elementos no nulos: contradice la minimalidad de r. □

Corolario 2.48. *Sea $F \subset K$ extensión de cuerpos finita. Entonces $|\mathrm{Gal}_F^K| \leqslant |K : F|$, y*

$$|\mathrm{Gal}_F^K| = |K : F| \iff F \subset K \text{ es de Galois.}$$

Demostración. Aplicando el teorema anterior a $H = \mathrm{Gal}_F^K$ obtenemos $|K : \mathrm{Fix}(H)| = |\mathrm{Gal}_F^K|$. Por otro lado tenemos la torre de cuerpos $F \subset \mathrm{Fix}(H) \subset K$: la transitividad de grados nos da $|K : F| = |K : \mathrm{Fix}(H)||\mathrm{Fix}(H) : F|$, i.e.

$$|K : F| = |\mathrm{Gal}_F^K||\mathrm{Fix}(H) : F|$$

Luego $|\mathrm{Gal}_F^K| \leqslant |K : F|$, y

$$|\mathrm{Gal}_F^K| = |K : F| \iff |\mathrm{Fix}(H) : F| = 1 \iff \mathrm{Fix}(H) = F \overset{\text{def.}}{\iff} F \subset K \text{ es de Galois.}$$ □

Corolario 2.49. *Sea K cuerpo, $H < \mathrm{Aut}(K)$. Entonces $\mathrm{Gal}_{\mathrm{Fix}(H)}^K = H$, luego si $\mathrm{Fix}(H) \subset K$ es finita, es de Galois.*

Demostración. ($\supset$) Por definición de Fix.

($\subset$) Como tenemos la inclusión $\supset$, basta ver que $|\mathrm{Gal}_{\mathrm{Fix}(H)}^K| = |H|$. Pero tenemos

$$|K : \mathrm{Fix}(H)| \overset{\text{teo.}}{=} |H| \overset{\supset}{\leqslant} |\mathrm{Gal}_{\mathrm{Fix}(H)}^K| \overset{\text{corolario}}{\leqslant} |K : \mathrm{Fix}(H)|$$

Por lo tanto la cadena de desigualdades es de igualdades, y $\mathrm{Gal}_{\mathrm{Fix}(H)}^K = H$. □

Corolario 2.50. *Sea K cuerpo. La función* Fix *que a cada subgrupo de $\mathrm{Aut}(K)$ le asocia su cuerpo fijo es inyectiva.*

Demostración. En efecto, lo que nos dice el corolario anterior es que dado un subgrupo de $\mathrm{Aut}(K)$, aplicar Fix y luego la función Gal_-^K que a un subcuerpo de K le asocia su grupo de Galois es la identidad, i.e. Fix tiene inversa por izquierda, i.e. es inyectiva. □

Teorema 2.51. *Sea F cuerpo. Si $f \in F[X]$ es separable, entonces*

$$|\mathrm{Gal}_F^{\mathrm{Desc}_F(f)}| = |\mathrm{Desc}_F(f) : F|$$

y por lo tanto si una extensión de F es el cuerpo de descomposición de un polinomio separable, entonces es de Galois.

Demostración. Sean $\alpha_1, \ldots, \alpha_m$ las raíces diferentes de f en su cuerpo de descomposición sobre F. La prueba es por inducción en m; lo haremos para $m = 2$ por simplicidad.

Considero $m_{\alpha_1,F}$: es irreducible sobre F. Con el teorema de extensión extiendo la identidad id: $F \to F$ a un isomorfismo $\varphi_1 : F(\alpha_1) \to F(\alpha_1')$ donde α_1' es otra raíz de $m_{\alpha_1,F}$. El número de φ_1's posibles es en general $\leqslant$ gr $m_{\alpha_1,F} = |F(\alpha_1) : F|$, pero se da la igualdad pues $m_{\alpha_1,F}$ es separable (pues divide a f que es separable).

Considero $m_{\alpha_2,F(\alpha_1)}$: es irreducible sobre $F(\alpha_1)$. Con el teorema de extensión extiendo el isomorfismo $\varphi_1 : F(\alpha_1) \to F(\alpha_1')$ a un isomorfismo $\varphi_2 : F(\alpha_1, \alpha_2) \to F(\alpha_1', \alpha_2')$ donde α_2' es otra raíz de $m_{\alpha_2,F(\alpha_1)}$. Observar que $F(\alpha_1', \alpha_2') = F(\alpha_1, \alpha_2)$ pues sólo hay dos raíces posibles para $m_{\alpha_2,F(\alpha_1)}$ ya que divide a f. El número de φ_2's posibles es en general $\leqslant$ gr $m_{\alpha_2,F(\alpha_1)} = |F(\alpha_1, \alpha_2) : F(\alpha_1)|$, pero se da la igualdad pues $m_{\alpha_2,F(\alpha_1)}$ es separable (pues divide a f que es separable).

Considero la torre de cuerpos $F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2)$:

$$\begin{aligned}
|\mathrm{Desc}_F(f) : F| &= |F(\alpha_1, \alpha_2) : F| \\
&= |F(\alpha_1) : F||F(\alpha_1, \alpha_2) : F(\alpha_1)| \\
&= \text{n}^\circ \text{ de } \varphi_1\text{'s } \cdot \text{n}^\circ \text{ de } \varphi_2\text{'s} \\
&= \text{n}^\circ \text{ de extensiones de id} : F \to F \text{ a un iso. } \varphi : F(\alpha_1, \alpha_2) \to F(\alpha_1, \alpha_2) \\
&= |\mathrm{Gal}_F^{\mathrm{Desc}_F(f)}| \qquad \square
\end{aligned}$$

Definición. Una extensión finita $F \subset K$ es *normal* si todo polinomio $f \in F[X]$ irreducible que tiene una raíz en K se escinde sobre K.

Ejemplo 2.6.6. La extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ no es normal: el polinomio $X^3 - 2 \in \mathbb{Q}[X]$ tiene una raíz $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$, pero no tiene a las dos otras.

Teorema 2.52. *Si $F \subset K$ es de Galois entonces es normal y separable.*

Demostración. Sea $p \in F[X]$ irreducible tal que existe $\alpha \in K$ raíz de p. Sin pérdida de generalidad podemos suponer p mónico. Veamos que p se escinde sobre K.

Sea $\mathrm{Gal}_F^K = \{\mathrm{id}, \sigma_2, \ldots, \sigma_n\}$. Considero entre $\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha) \in K$ los elementos diferentes, que llamo $\alpha, \alpha_2, \ldots, \alpha_r$, $0 \leqslant r \leqslant n$.

Sea $f = (X - \alpha)(X - \alpha_2)\ldots(X - \alpha_r) \in K[X]$.

Afirmación: $p = f$.

Demostración: Como todas las raíces de f lo son de p, entonces $f \mid p$.

Si pruebo que $f \in F[X]$ y anula a α, entonces como $p = m_{\alpha,F}$ se tiene $p \mid f$. Obviamente $f(\alpha) = 0$: veamos que $f \in F[X]$.

Usemos que $F = \mathrm{Fix}(\mathrm{Gal}_F^K)$ para demostrar esto. Sea $\tau \in \mathrm{Gal}_F^K$, entonces como $\{\tau, \tau\sigma_2, \ldots, \tau\sigma_n\} = \{\mathrm{id}, \sigma_2, \ldots, \sigma_n\}$, aplicarle τ a $\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ los permuta. A su vez $\{\mathrm{id}, \sigma_2, \ldots, \sigma_n\}$ permutan $\alpha, \alpha_2, \ldots, \alpha_r$ (pues son raíces de p) luego τ permuta $\alpha, \alpha_2, \ldots, \alpha_r$.

Por lo tanto f queda invariante por Gal_F^K , i.e. los coeficientes de f (no estamos diciendo los α_i, atención) están en $\mathrm{Fix}(\mathrm{Gal}_F^K) = F$, i.e. $f \in F[X]$.

Entonces $f \mid p$, $p \mid f$ y son ambos mónicos: se tiene $p = f$.

Por lo tanto p se escinde sobre K, y más aún, es separable. Entonces la extensión es normal, y es separable, pues dado $\alpha \in K$ obtuvimos que $m_{\alpha,F}$ es separable. $\square$

Teorema 2.53. *Una extensión $F \subset K$ es finita, normal y separable si y sólo si K es el cuerpo de descomposición sobre F de un polinomio en $F[X]$ separable.*

Demostración. ($\Leftarrow$) Es el teorema 2.51 junto con el teorema anterior 2.52.

($\Rightarrow$): Como $F \subset K$ es finita, sea $\{\omega_1, \ldots, \omega_n\}$ una F-base de K. Sea $p_i = m_{\omega_i, F}$: son irreducibles y tienen una raíz en K, luego como $F \subset K$ es normal y separable, los p_i se escinden sobre K y son separables. Sea f el producto $p_1 \ldots p_n$ sacando los factores repetidos.

Afirmación: $K = \mathrm{Desc}_F(f)$.

Demostración: ($\supset$) Es obvio pues $\mathrm{Desc}_F(f)$ está generado por las raíces de f que son elementos de K.

($\subset$) Se tiene $\omega_1, \ldots, \omega_n \in \mathrm{Desc}_F(f)$ por construcción, y $\mathrm{Desc}_F(f) \subset K$ es un F-subespacio vectorial, luego como los ω_i son una F-base de K, necesariamente $\mathrm{Desc}_F(f) = K$. □

Resumamos la situación:

Teorema 2.54. *Sea $F \subset K$ extensión de cuerpos. Son equivalentes:*

1. *La extensión es de Galois.*
2. $|K : F| = |\mathrm{Gal}_F^K|$.
3. $K = \mathrm{Desc}_F(f)$ *para algún $f \in F[X]$ separable.*
4. *La extensión es finita, normal y separable.*

Demostración. ($1 \Leftrightarrow 2$) es el corolario 2.48. Los teoremas anteriores son $1 \Rightarrow 4 \Rightarrow 3 \Rightarrow 2$. □

A continuación, un lema técnico que nos será de utilidad a posteriori.

Lema 2.55. *Sea $k \subset F \subset K \subset L$ una torre de extensiones algebraicas, con $K = \mathrm{Desc}_k(f)$ para algún $f \in k[X]$. Entonces si $\sigma : F \to L$ es un k-monomorfismo de cuerpos, se tiene que $\sigma(F) \subset K$, y σ se extiende a un k-automorfismo de K (i.e. un elemento de Gal_k^K.)*

Demostración. Sea L' una clausura algebraica de L (lo es entonces de F y de $\sigma(F)$). Entonces como $\sigma : F \to \sigma(F)$ es un k-automorfismo, por el corolario 2.36, se extiende a un k-automorfismo $\sigma^* : L' \to L'$. Basta ver que $\sigma^*(K) = K$, porque entonces $\sigma(F) = \sigma^*(F) \subset K$, y además la restricción $\sigma^*|_K$ es el automorfismo buscado.

Tenemos que $K = \mathrm{Desc}_k(f)$. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de f en K: se tiene entonces $K = k(\alpha_1, \ldots, \alpha_n)$. Entonces $\sigma^*(K) = k(\sigma^*(a_1), \ldots, \sigma^*(a_n)$ pues $\sigma^*|_k = \mathrm{id}$.

Pero $\sigma^* \in \mathrm{Gal}_k^{L'}$, luego lleva raíces de f en raíces de f. Al ser un automorfismo es biyectivo, luego $\{\sigma^*(a_1), \ldots, \sigma^*(a_n)\} = \{a_1, \ldots, a_n\}$.

Por lo tanto $\sigma^*(K) = k(a_1, \ldots, a_n) = K$ y el lema queda demostrado. □

2.6.1. Un poco más de extensiones normales

Una extensión es finita, normal y separable si y sólo si es el cuerpo de descomposición de un polinomio separable. Esto sigue siendo válido si quitamos la separabilidad de ambos lados. Para demostrar esto, usamos el lema técnico recién demostrado.

Proposición 2.56. *Una extensión finita $F \subset K$ es normal si y sólo si K es el cuerpo de descomposición sobre F de un polinomio en $F[X]$.*

Demostración. ($\Rightarrow$) La extensión $F \subset K$ es finita, luego finitamente generada por elementos algebraicos: $K = F(\alpha_1, \ldots, \alpha_n)$. Como la extensión es normal, los polinomios $p_i = m_{\alpha_i,F}$ se escinden sobre K, luego $f = p_1 \ldots p_n$ también se escinde sobre K. Entonces $K = F(\alpha_1, \ldots, \alpha_n) = \mathrm{Desc}_F(f)$.

($\Leftarrow$) Sea $p \in F[X]$ un polinomio irreducible con una raíz $\alpha \in K$. Sea L una clausura algebraica de K, y $\beta \in L$ otra raíz de p. Entonces extendiendo la identidad id: $F \to F$ con el teorema de extensión, existe un F-isomorfismo $\sigma : F(\alpha) \to F(\beta)$. Por el lema anterior (con $F = k(\alpha)$) resulta que $k(\beta) \subset K$, para cualquier otra raíz $\beta \in L$ de f. Pero f se escinde sobre L pues L es algebraicamente cerrado, luego en realidad se escinde sobre K. □

De esta manera, el lema 2.55 nos dice que un k-monomorfismo que parte de un subcuerpo de una extensión normal a un cuerpo mayor, en realidad no se sale de la extensión normal, y además se extiende a un k-automorfismo de la extensión normal.

Definición. Sea $F \subset E$ extensión de cuerpos finita. Decimos que un cuerpo K es una *clausura normal* de la extensión si $F \subset K$ es normal, $K \supset E$, y K es la menor extensión normal de F tal que $K \supset E$.

Proposición 2.57. *Toda extensión finita $F \subset E$ tiene una clausura normal K, y dos clausuras normales son isomorfas.*

Demostración. Tenemos $E = F(\alpha_1, \ldots, \alpha_n)$ para ciertos $\alpha_1, \ldots, \alpha_n \in E$. Consideremos $f = m_{\alpha_1,F} \ldots m_{\alpha_n,F}$ y $K = \mathrm{Desc}_F(f)$. Entonces $F \subset K$ es normal, $K \supset E$ y por definición de cuerpo de descomposición f no se escinde en ningún subcuerpo propio de K que contiene a E, luego K es una clausura normal de $F \subset E$. Además K es único a menos de isomorfismo porque dos cuerpos de descomposición para f sobre F son isomorfos. □

Definición. Sea $F \subset E$ extensión de cuerpos finita. Decimos que un cuerpo K es una *clausura de Galois* de la extensión si $F \subset K$ es de Galois, $K \supset E$, y K es la menor extensión de Galois de F tal que $K \supset E$.

Corolario 2.58. *Toda extensión finita y separable $F \subset E$ tiene una clausura de Galois, que es la clausura normal.*

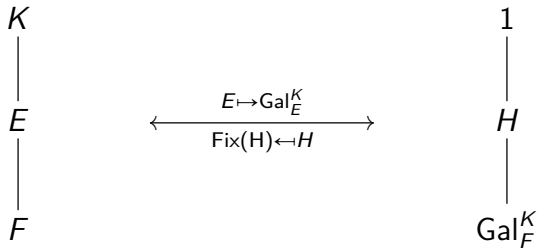
Demostración. Sea K la clausura normal de $F \subset E$. Como en la demostración de la proposición anterior, K es el cuerpo de descomposición sobre F de $f = m_{\alpha_1,F} \ldots m_{\alpha_n,F}$. En este caso los $m_{\alpha_i,F}$ son separables. Entonces si a f le quitamos los factores repetidos, nos queda un polinomio separable $g \in F[X]$ tal que $\mathrm{Desc}_F(f) = \mathrm{Desc}_F(g)$, por lo tanto $F \subset K$ es de Galois. □

2.6.2. Teorema fundamental de la teoría de Galois

Teorema 2.59 (Teorema fundamental de la teoría de Galois)**.** *Sea $F \subset K$ extensión de cuerpos de Galois. Hay una biyección entre los* subcuerpos intermedios *de la extensión (los subcuerpos $E \subset K$ que contienen a F) y los subgrupos $H \subset \mathrm{Gal}_F^K$ dada por las correspondencias inversas*

una de la otra $E \overset{\mathrm{Gal}_{-}^{K}}{\mapsto} \mathrm{Gal}_{E}^{K}$ *y* $\mathrm{Fix}(H) \overset{\mathrm{Fix}}{\mapsto} H$*:*

$$\{\text{subcuerpos } E \subset K \text{ que contienen a } F\} \underset{\mathrm{Fix}}{\overset{\mathrm{Gal}_{-}^{K}}{\longleftrightarrow}} \{\text{subgrupos } H \subset \mathrm{Gal}_{F}^{K}\}$$



Esta correspondencia, llamada correspondencia de Galois*, cumple las siguientes propiedades:*

1. *Revierte inclusiones: si subcuerpos intermedios* E_1, E_2 *se corresponden con subgrupos* H_1*,* H_2*, entonces* $E_1 \subset E_2 \iff H_2 < H_1$*.*

2. $E \subset K$ *es de Galois para cualquier subcuerpo* E *de* K *que contiene a* F*.*

3. *Para cualquier subcuerpo intermedio* E *se tiene*

$$|K : E| = |\mathrm{Gal}_{E}^{K}| \quad \text{y} \quad |E : F| = |\mathrm{Gal}_{F}^{K} : \mathrm{Gal}_{E}^{K}|$$

4. *Para cualquier subcuerpo intermedio* E *se tiene que* $F \subset E$ *es Galois* $\iff \mathrm{Gal}_{E}^{K} \lhd \mathrm{Gal}_{F}^{K}$*. Si este es el caso, entonces* $\mathrm{Gal}_{F}^{E} \simeq \frac{\mathrm{Gal}_{F}^{K}}{\mathrm{Gal}_{E}^{K}}$*.*

Demostración. Ya sabemos que Fix es inyectivo con inversa por izquierda Gal_{-}^{K}.

Para probar que Fix es sobreyectivo probemos primero 2. Sea E un subcuerpo intermedio. Como $F \subset K$ es de Galois, entonces $K = \mathrm{Desc}_{F}(f)$ para cierto $f \in F[X]$ separable. Pero entonces $f \in E[X]$ y $E \subset K = \mathrm{Desc}_{E}(f)$, luego $E \subset K$ es de Galois.

Por definición de extensión de Galois se tiene $E = \mathrm{Fix}(\mathrm{Gal}_{E}^{K})$. Esto nos dice que Fix tiene inversa por derecha Gal_{-}^{K}. Por lo tanto Fix y Gal_{-}^{K} son biyectivos, uno inverso del otro.

1. Es la proposición 2.44.

3. Como $E \subset K$ es de Galois, entonces $|K : E| = |\mathrm{Gal}_{E}^{K}|$.

   Como $F \subset K$ es de Galois, entonces $|K : F| = |\mathrm{Gal}_{F}^{K}|$. Por otro lado la torre $F \subset E \subset K$ nos da $|K : F| = |K : E||E : F|$. Tenemos entonces

$$|\mathrm{Gal}_{F}^{K} : \mathrm{Gal}_{E}^{K}| = \frac{|\mathrm{Gal}_{F}^{K}|}{|\mathrm{Gal}_{E}^{K}|} = \frac{|K : F|}{|K : E|} = |E : F|$$

4. ($\Rightarrow$) Sea $F \subset E$ de Galois, en particular es normal. Sea $\sigma \in \mathrm{Gal}_{E}^{K}$, $\tau \in \mathrm{Gal}_{F}^{K}$. Sabemos que $\tau\sigma\tau^{-1} \in \mathrm{Gal}_{F}^{K}$, pero queremos que ver que $\tau\sigma\tau^{-1} \in \mathrm{Gal}_{E}^{K}$.

Tenemos la torre $F \subset E \subset E \subset K$, donde $F \subset E$ es normal y $\tau^{-1}|_E : E \to K$ es un F-monomorfismo. Entonces por el lema 2.55, se tiene que $\tau^{-1}|_E(E) \subset E$, i.e. $\tau^{-1}(E) \subset E$.

Entonces dado $a \in E$, se tiene $\tau^{-1} \in E$. Por lo tanto como σ es un E-automorfismo, $\sigma\tau^{-1}(a) = \tau^{-1}(a)$. Aplicando τ se obtiene $\tau\sigma\tau^{-1}(a) = \tau\tau^{-1}(a) = a$, luego $\tau\sigma\tau^{-1}|_E = \mathrm{id}$ y $\tau\sigma\tau^{-1} \in \mathrm{Gal}_E^K$.

($\Leftarrow$) Supongamos $\mathrm{Gal}_E^K \lhd \mathrm{Gal}_F^K$. Tenemos que $F \subset E$ es separable pues $F \subset K$ lo es. Veamos que $F \subset E$ es normal: sea $p \in F[X]$ irreducible con una raíz $a \in E$.

Como $F \subset K$ es normal (por ser de Galois), p se escinde sobre K. Basta ver que las raíces de p en K están en E.

Sea b otra raíz de p en K. Entonces por el teorema de extensión, existe $\tau \in \mathrm{Gal}_F^K$ tal que $\tau(b) = a$. Para ver que $b \in E$ veamos que $b \in \mathrm{Fix}(\mathrm{Gal}_E^K)$, aprovechando que $E \subset K$ es de Galois.

Sea $\sigma \in \mathrm{Gal}_E^K$. Entonces $\tau\sigma\tau^{-1} \in \mathrm{Gal}_E^K$ por normalidad, luego

$$\tau\sigma\tau^{-1}(a) = a \Rightarrow \tau\sigma(b) = a \Rightarrow \sigma(b) = \tau^{-1}(a) = b$$

Entonces $\sigma(b) = b$, i.e. $b \in \mathrm{Fix}(\mathrm{Gal}_E^K)$. □

Observación 2.6.7. En la prueba del recíproco del cuarto ítem hemos probado que $F \subset E$ es normal $\iff$ Gal_E^K es normal en Gal_F^K, lo cual explica por qué la misma nomeclatura.

En la proposición 2.64 detallamos otro aspecto de la correspondencia de Galois.

2.6.3. Aplicación: teorema fundamental del álgebra

El teorema fundamental del álgebra no tiene una demostración que se base únicamente en el álgebra. Esto es lógico pues en el fondo nos dice algo sobre números reales, y los números reales no son una construcción algebraica.

La demostración que daremos usa una cantidad mínima de análisis que se concentra en el siguiente lema.

Lema 2.60. *a) Todo polinomio en $\mathbb{R}[X]$ de grado impar tiene una raíz real. Por lo tanto $\mathbb{R}$ no admite extensiones propias de grado impar.*

b) $\mathbb{C}$ no admite extensiones cuadráticas (de grado 2), i.e. todo $f \in \mathbb{C}[X]$ de grado 2 se escinde sobre $\mathbb{C}$.

Demostración. a) Los polinomios de grado impar tienden a $\pm\infty$ en $-\infty$, y a $\mp\infty$ en $+\infty$, luego por el teorema de Bolzano, tienen una raíz real.

Si $\mathbb{R}$ tuviera una extensión de grado impar, existiría un polinomio de grado impar sobre $\mathbb{R}$ irreducible, absurdo.

b) Por la fórmula de las raíces de los polinomios de grado 2, basta ver que todo $\alpha \in \mathbb{C}$ tiene una raíz cuadrada en $\mathbb{C}$. Escribiendo $\alpha = re^{i\theta}$, $r \geqslant 0$, $\theta \in [0, 2\pi)$, se tiene que $\sqrt{r}e^{i\frac{\theta}{2}}$ es una raíz cuadrada de α en $\mathbb{C}$. □

Teorema 2.61 (fundamental del álgebra)**.** *Todo polinomio no constante en* $\mathbb{R}[X]$ *tiene una raíz en* $\mathbb{C}$*. En otras palabras,* $\mathbb{C}$ *es algebraicamente cerrado.*

Demostración. Sea $f \in R[X]$, gr $f = n \geqslant 1$, y sea $K = \mathrm{Desc}_{\mathbb{R}}(f)$.

Adjuntarle i a K es lo mismo que tomar el cuerpo de descomposición sobre $\mathbb{R}$ del producto $f \cdot (X^2+1)$, i.e. $K(i) = \mathrm{Desc}_{\mathbb{R}}(f \cdot (X^2+1))$, entonces $\mathbb{R} \subset K(i)$ es de Galois.

Consideremos $\mathrm{Gal}_{\mathbb{C}}^{K(i)} < \mathrm{Gal}_{\mathbb{R}}^{K(i)}$. Queremos probar que $\mathrm{Gal}_{\mathbb{C}}^{K(i)} = \{\mathrm{id}\}$, en cuyo caso por la correspondencia de Galois $\mathbb{C} = K(i)$, luego como $K(i) = \mathrm{Desc}_{\mathbb{R}}(f \cdot (X^2+1))$, se tendría que f tiene una raíz en $\mathbb{C}$ y el teorema estaría demostrado.

Supongamos por absurdo que $\mathrm{Gal}_{\mathbb{C}}^{K(i)} \neq \{\mathrm{id}\}$.

Sea P_2 un 2-subgrupo de Sylow de $\mathrm{Gal}_{\mathbb{R}}^{K(i)}$. Entonces $|P_2|$ es par, luego $|\mathrm{Gal}_{\mathbb{R}}^{K(i)} : P_2|$ es impar. Por la correspondencia de Galois, $|\mathrm{Fix}(P_2) : \mathbb{R}|$ es impar, luego por la parte a) del lema 2.60, $\mathrm{Fix}(P_2) = \mathbb{R}$.

Entonces $\mathrm{Gal}_{\mathbb{R}}^{K(i)} = \mathrm{Gal}_{\mathrm{Fix}(P_2)}^{K(i)} = P_2$, luego como $\{\mathrm{id}\} \neq \mathrm{Gal}_{\mathbb{C}}^{K(i)} < \mathrm{Gal}_{\mathbb{R}}^{K(i)} = P_2$, se tiene que $\mathrm{Gal}_{\mathbb{C}}^{K(i)}$ es un 2-grupo. Por ser un p-grupo tiene subgrupos de todos los órdenes posibles, en particular uno de índice 2, que por la correspondencia de Galois se corresponde con una extensión cuadrática de $\mathbb{C}$, absurdo por la parte b) del lema 2.60. □

Observación 2.6.8. De los números reales tuvimos que usar la completitud, necesariamente, pues esto está en la base de su definición. Sin embargo no usamos la completitud en toda su potencia, la usamos sólo en la expresión del lema 2.60. Esto nos dice que la demostración que hemos dado del teorema fundamental del álgebra no nos dice sólo que $R(\sqrt{-1})$ es algebraicamente cerrado, donde R es el único cuerpo ordenado y completo, sino que $R(\sqrt{-1})$ es algebraicamente cerrado cuando R es un cuerpo ordenado que satisface las condiciones del lema 2.60 (observar que la condición b) es una consecuencia de que todo número real positivo tiene una raíz cuadrada real).

Más explícitamente, un *cuerpo ordenado* es un cuerpo F junto con un orden total $\leqslant$ en F que es compatible con las operaciones de F, de esta manera:

- $a \leqslant b \Rightarrow a + c \leqslant b + c$ para todo $a, b, c \in F$,
- $a, b \leqslant 0 \Rightarrow ab \leqslant 0$ para todo $a, b \in F$.

Un *cuerpo real cerrado* es un cuerpo ordenado R tal que todo elemento positivo tiene raíz cuadrada en R, y todo polinomio de grado impar en $R[X]$ tiene una raíz en R..

Un ejemplo de cuerpo real cerrado, aparte de $\mathbb{R}$, es el de los números algebraicos reales, i.e. $\overline{\mathbb{Q}} \cap \mathbb{R}$.

Con esta definición capturamos exactamente lo que utilizamos de los números reales para probar el teorema fundamental del álgebra. Podemos entonces enunciar lo que hemos probado en realidad:

Teorema (fundamental del álgebra generalizado). Sea R un cuerpo real cerrado. Entonces $R(\sqrt{-1})$ es algebraicamente cerrado.

Como última observación, destacamos que la noción de cuerpo real cerrado captura *exactamente* las propiedades de los números reales necesarias para que valga el teorema fundamental del álgebra. Es decir, vale el recíproco: si R es un cuerpo no algebraicamente cerrado tal que $R(\sqrt{-1})$ es algebraicamente cerrado, entonces R es un cuerpo real cerrado.

Además, captura otras propiedades equivalentes, por ejemplo: si R es un cuerpo ordenado, es real cerrado si y sólo si hay un orden en R que no se extiende a ningún orden en cualquier extensión algebraica propia de R, si y sólo si hay un orden en R que hace que R sea un cuerpo ordenado tal que, con este orden, vale el teorema del valor intermedio para todos los polinomios sobre R.

Recomendamos [J], capítulo 5, para profundizar en este tema.

Ejercicios

Ej. 49 — Toda extensión de grado 2 es normal.

Ej. 50 — $\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{R}} = \{\mathrm{id}\}$ (Sugerencia: un automorfismo de $\mathbb{R}$ es una función monótona. Además, por Dedekind-completitud de $\mathbb{R}$, para todo $x \in \mathbb{R}\backslash\mathbb{Q}$, $A = \{a \in \mathbb{Q} : a < x\}$ y $B = \{b \in \mathbb{Q} : b > x\}$ conforman una partición de $\mathbb{Q}$ tal que $a < b$ para todo $a \in A$, $b \in B$ y $x = \sup A = \text{ínf } B$.)

Ej. 51 — Hallar los grupos de Galois sobre $\mathbb{Q}$ de $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ y de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

2.7. Extensiones compuestas y extensiones simples

Definición. Sean $K_1, K_2 \subset K$ subcuerpos. El *cuerpo compuesto* de K_1 y K_2, notado K_1K_2, es el menor subcuerpo de K que contiene K_1 y K_2.

Tomar el cuerpo compuesto de dos subcuerpos es la idea recíproca de tomar su intersección.

Proposición 2.62. *Sean K_1, K_2 extensiones finitas de F contenidas en K. Entonces*

$$|K_1K_2 : F| \leqslant |K_1 : F||K_2 : F|$$

y se da la igualdad si y sólo si una F-base de K_1 es linealmente independiente en K_2 o viceversa.

Demostración. Consideremos la torre $F \subset K_1 \subset K_1K_2$. La transitividad de grados nos da

$$|K_1K_2 : F| = |K_1 : F||K_1K_2 : K_1| \leqslant |K_1 : F||K_2 : F|$$

Se tiene $|K_1K_2 : K_1| \leqslant |K_2 : F|$ pues si tomo una F-base de K_2, es un K_1-generador de K_1K_2. Se da la igualdad si y sólo si es l.i. en K_1. □

Corolario 2.63. *Si K_1, K_2 son extensiones finitas de F contenidas en K tales que $|K_1 : F| = n$ y $|K_2 : F| = m$, con $mcd(m, n) = 1$, entonces $|K_1K_2 : F| = mn$.*

Demostración. Las torres $F \subset K_1 \subset K_1K_2$ y $F \subset K_2 \subset K_1K_2$ nos dan respectivamente

$$n = |K_1 : F| \mid |K_1K_2 : F| \quad \text{y} \quad m = |K_2 : F| \mid |K_1K_2 : F|$$

Por lo tanto $\text{mcm}(n, m) = nm \mid |K_1K_2 : F|$, y por la proposición $|K_1K_2 : F| \leqslant nm$, por lo tanto se da la igualdad. □

Ejemplo 2.7.1. Sea $F \subset K$ extensión de cuerpos, $\alpha, \beta \in K$ algebraicos de grados n, m respectivamente. Se tiene $F(\alpha)F(\beta) = F(\alpha, \beta)$. Entonces $|F(\alpha, \beta) : F| \leqslant nm$, y se da la igualdad si m y n son coprimos.

La siguiente proposición nos da más información sobre la correspondencia de Galois, y nos dice que "tomar cuerpo compuesto" se corresponde con "tomar subgrupo generado por la unión". No podemos simplemente tomar la unión de dos subgrupos puesto que no tendría por qué ser un subgrupo.

Proposición 2.64. *En la correspondencia de Galois, si subcuerpos intermedios E_1 y E_2 se corresponden con subgrupos H_1 y H_2, entonces $E_1 \cap E_2 \mapsto \langle H_1 \cup H_2 \rangle$ y $E_1E_2 \mapsto H_1 \cap H_2$.*

Demostración. $E_1E_2 \mapsto H_1 \cap H_2 \iff \text{Gal}^K_{E_1E_2} = H_1 \cap H_2$, con $H_1 = \text{Gal}^K_{E_1}$ y $H_2 = \text{Gal}^K_{E_2}$.

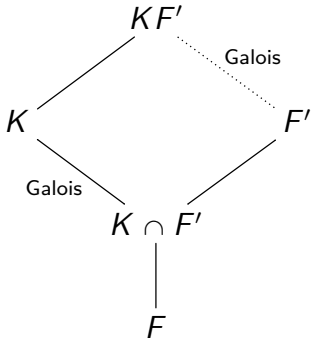
($\subset$) Si $\sigma \in \text{Gal}^K_{E_1E_2}$ entonces claramente $\sigma \in \text{Gal}^K_{E_1}$ y $\sigma \in \text{Gal}^K_{E_2}$, luego $\sigma \in H_1 \cap H_2$.

($\supset$) Si $\sigma \in H_1 \cap H_2$, entonces $\sigma|_{E_1} = \text{id}$ y $\sigma|_{E_2} = \text{id}$, luego $\sigma|_{E_1E_2} = \text{id}$, por lo tanto $\sigma \in \text{Gal}^K_{E_1E_2}$. □

La proposición anterior nos dice que el retículo de subcuerpos de K que contienen F y el retículo de subgrupos de Gal^K_F son "duales".

Es fácil recordar la proposición que sigue pensando que "deslizamos" hacia arriba a la derecha una extensión de Galois a una de Galois.

Proposición 2.65. *Sea $F \subset K$ extensión de Galois, $F \subset F'$ extensión. Supongamos que K, F' están contenidas en alguna extensión de F. Entonces $F' \subset KF'$ es de Galois, y $\mathrm{Gal}_{F'}^{KF'} \simeq \mathrm{Gal}_{K\cap F'}^{K}$. Gráficamente,*



Demostración. Como $F \subset K$ es de Galois, entonces $K = \mathrm{Desc}_F(f)$ para cierto $f \in F[X]$ separable. Entonces $K = F(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son las raíces de f. Luego como $F \subset F'$, se tiene $KF' = F'(\alpha_1, \ldots, \alpha_n)$, i.e. $KF' = \mathrm{Desc}_{F'}(f)$ y f es separable, luego $F' \subset KF'$ es de Galois.

Sea $\varphi : \mathrm{Gal}_{F'}^{KF'} \to \mathrm{Gal}_F^K$, $\sigma \mapsto \sigma|_K$. Está bien definida: $\sigma : KF' \to KF'$, y como $\sigma|_{F'} = \mathrm{id}$, entonces $\sigma|_K : K \to K$ y es inyectiva. Como $F \subset K$ es finita, entonces $\sigma|_K$ es un automorfismo de K, y deja fijo F pues deja fijo $F' \supset F$.

Obviamente φ es un morfismo de grupos. Se tiene $\ker \varphi = \{\sigma \in \mathrm{Gal}_{F'}^{KF'} : \sigma|_K = \mathrm{id}\} = \{\mathrm{id}\}$, pues un elemento de $\ker \varphi$ es la identidad en K y en F', luego en KF'. Por lo tanto φ es inyectiva.

Afirmación: $\mathrm{Im}\ \varphi = \mathrm{Gal}_{K\cap F'}^{K}$

Demostración: Para ver esto, por la correspondencia de Galois basta probar que $\mathrm{Fix}(\mathrm{Im}\ \varphi) = K \cap F'$, pues $F \subset K$ es de Galois.

($\subset$): $\mathrm{Fix}(\mathrm{Im}\ \varphi) = \mathrm{Fix}(\mathrm{Gal}_{F'}^{KF'} \cap \mathrm{Aut}(K)) = F' \cap K$.

($\supset$): Si $x \in K \cap F'$, entonces $\sigma|_K(x) = x$ pues $x \in F'$, para todo $\sigma|_K \in \mathrm{Im}\ \varphi$.

Entonces φ es un isomorfismo sobre su imagen, y ya está. □

El siguiente corolario debe ser leído sobre el mismo diagrama que la proposición anterior.

Corolario 2.66. *Si $F \subset K$ es de Galois y $F \subset F'$ es finita, con K, F' contenidas en alguna extensión de F, entonces*

$$|KF' : F| = \frac{|K : F||F' : F|}{|K \cap F' : F|}$$

Demostración. Por la proposición anterior, $|KF' : F'| = |K : K \cap F'|$.

Por otro lado las torres $F \subset F' \subset KF'$ y $F \subset K \cap F' \subset K$ nos dan respectivamente

$$|KF' : F| = |KF' : F'||F' : F| \quad \text{y} \quad |K : K \cap F'| = \frac{|K : F|}{|K \cap F' : F|}$$

Juntando las tres igualdades se deduce la tesis. □

Proposición 2.67. *Sean $F \subset K_1$, $F \subset K_2$ extensiones de Galois con K_1, K_2 contenidas en alguna extensión de F. Entonces:*

1. *$F \subset K_1 \cap K_2$ es de Galois.*

2. *$F \subset K_1K_2$ es de Galois, y* $\mathrm{Gal}_F^{K_1K_2} \simeq \{(\sigma,\tau) \in \mathrm{Gal}_F^{K_1} \times \mathrm{Gal}_F^{K_2} : \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\} =: H$.

Demostración. 1. Basta ver que la extensión es normal. Si $p \in F[X]$ es irreducible con una raíz $\alpha \in K_1 \cap K_2$, entonces para $i = 1, 2$, $\alpha \in K_i$ que es de Galois sobre F, luego todas las raíces de p están en K_i, i.e. están todas en $K_1 \cap K_2$.

2. Tenemos $K_1 = \mathrm{Desc}_F(f_1)$ y $K_2 = \mathrm{Desc}_F(f_2)$ para sendos $f_1, f_2 \in F[X]$ separables.

   Entonces $K_1K_2 = \mathrm{Desc}_F(g)$, donde g es el producto f_1f_2 a menos de factores repetidos, de donde g es separable. Por lo tanto $F \subset K_1K_2$ es de Galois.

   Sea $\varphi : \mathrm{Gal}_F^{K_1K_2} \to \mathrm{Gal}_F^{K_1} \times \mathrm{Gal}_F^{K_2}$, $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$. Está bien definida: para $i = 1, 2$ se tiene $\mathrm{Im}\ \sigma|_{K_i} \subset K_i$ pues las raíces de f_i van a parar a raíces de f_i por σ.

   Claramente φ es un morfismo de grupos. Es inyectivo:

$$\ker \varphi = \{\sigma \in \mathrm{Gal}_F^{K_1K_2} : \sigma|_{K_1} = \sigma|_{K_2} = \mathrm{id}\} = \{\sigma \in \mathrm{Gal}_F^{K_1K_2} : \sigma|_{K_1K_2} = \mathrm{id}\} = \{\mathrm{id}\}$$

   Veamos que $\mathrm{Im}\ \varphi = H$. Se tiene $\mathrm{Im}\ \varphi \subset H$ pues $(\sigma|_{K_1})|_{K_1\cap K_2} = \sigma|_{K_1\cap K_2} = (\sigma|_{K_2})|_{K_1\cap K_2}$. Para ver la igualdad, veamos que tienen el mismo orden. Sea $\sigma \in \mathrm{Gal}_F^{K_1}$.

   Considero $\sigma|_{K_1\cap K_2}$: hay $|\mathrm{Gal}_{K_1\cap K_2}^{K_2}|$ maneras de extender $\sigma|_{K_1\cap K_2}$ a K_2. Luego considerando la torre de extensiones de Galois $F \subset K_1 \cap K_2 \subset K_2$,

$$|H| = |\mathrm{Gal}_F^{K_1}||\mathrm{Gal}_{K_1\cap K_2}^{K_2}| = |\mathrm{Gal}_F^{K_1}|\frac{|\mathrm{Gal}_F^{K_2}|}{|\mathrm{Gal}_F^{K_1\cap K_2}|} \overset{\text{corolario}}{=} |K_1K_2 : F| = |\mathrm{Gal}_F^{K_1K_2}| = |\mathrm{Im}\ \varphi|$$

   donde la última igualdad se deduce de que φ es inyectiva. Esto termina la demostración. □

Corolario 2.68. *Sean $F \subset K_1$, $F \subset K_2$ extensiones de Galois, con $K_1 \cap K_2 = F$ y K_1, K_2 contenidas en alguna extensión de F. Entonces* $\mathrm{Gal}_F^{K_1K_2} \simeq \mathrm{Gal}_F^{K_1} \times \mathrm{Gal}_F^{K_2}$.

Recíprocamente, si $F \subset K$ es de Galois y $\mathrm{Gal}_F^K = G_1 \times G_2$, *entonces $K = K_1K_2$ con $K_1 \cap K_2 = F$, para ciertas extensiones de Galois $F \subset K_1$, $F \subset K_2$ tales que $K_1 \cap K_2 = F$.*

Demostración. ($\Rightarrow$) Se deduce de la proposición anterior, observando que

$$\mathrm{Im}\ \varphi = \{(\sigma,\tau) : \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\} = \mathrm{Gal}_F^{K_1} \times \mathrm{Gal}_F^{K_2}$$

pues $\sigma|_{K_1\cap K_2} = \sigma|_F = \mathrm{id} = \tau|_F = \tau|_{K_1\cap K_2}$ para cualquier (σ,τ).

($\Leftarrow$) Tomemos $K_1 = \mathrm{Fix}(G_1)$ y $K_2 = \mathrm{Fix}(G_2)$.

Por la correspondencia de Galois, $K_1 \cap K_2 \mapsto G_1G_2 = \mathrm{Gal}_F^K$ pues Gal_F^K es el producto directo, y $\mathrm{Gal}_F^K \mapsto F$. Por lo tanto $K_1 \cap K_2 = F$.

$K_1K_2 \mapsto G_1 \cap G_2 = \{e\}$, y $\{e\} \mapsto K$, luego $K_1K_2 = K$. □

Teorema 2.69. *Sea $F \subset K$ extensión de cuerpos finita. Entonces $F \subset K$ es simple si y sólo si hay finitos subcuerpos intermedios entre F y K.*

Demostración. ($\Rightarrow$) Como $F \subset K$ es simple, existe $\theta \in K$ tal que $K = F(\theta)$.

Sea E cuerpo tal que $F \subset E \subset K$. Sea $f := m_{\theta,F}$. Como $m_{\theta,F} \in E[X]$ y anula a θ, $m_{\theta,E} \mid f$.

Si $m_{\theta,E} = a_0 + a_1X + \cdots + a_nX^n \in E[X]$, considero $E' := F(a_0, \ldots, a_n)$. Se tiene $E' \subset E$.

Como $F \subset E' \subset E \subset K = F(\theta)$, entonces también $K = E(\theta) = E'(\theta)$.

Además $m_{\theta,E} = m_{\theta,E'}$. En efecto, $E' \subset E \Rightarrow m_{\theta,E} \mid m_{\theta,E'}$, y $m_{\theta,E} \in E'[X]$ por definición de E' luego $m_{\theta,E'} \mid m_{\theta,E}$. Por lo tanto

$$|K : E| = |E(\theta) : E| = \text{gr } m_{\theta,E} = \text{gr } m_{\theta,E'} = |E'(\theta) : E'| = |K : E'|$$

Entonces E' y E tienen el mismo grado sobre K y $E' \subset E$, luego $E' = E$.

Obtenemos que $\{$subcuerpos de K que contienen F$\} \subset \{$subcuerpos de K que contienen F y son generados sobre F por los coeficientes de un polinomio mónico irreducible que divide a $f\}$, y este último conjunto es obviamente finito.

($\Leftarrow$) Caso 1: F es finito. Tomemos $\{e_1, \ldots, e_n\}$ una F-base de E. Se tiene que $E = \{\sum_{i=1}^n f_i e_i, f_i \in F\}$ es finito ya que F lo es. Entonces por el teorema 1.7, E^* es cíclico: existe $\theta \in E$ tal que $E^* = \langle\theta\rangle$ y por lo tanto como $0 \in F$, se tiene $E = F(\theta)$.

Caso 2: F es infinito. Como $F \subset K$ es finita, es finitamente generada. La prueba es por inducción en el tamaño de un generador de K sobre F. Por simplicidad supongamos que K está generado sobre F por dos elementos $\alpha, \beta \in K$, i.e. $K = F(\alpha, \beta)$.

Consideremos los subcuerpos de K de la forma $F(\alpha + c\beta)$, donde $c \in F$. Pero F es infinito, y estos son subcuerpos de K que contienen a F, por lo tanto debe haber finitos de ellos. Luego existen $c, c' \in F$, $c \neq c'$ tales que $F(\alpha + c\beta) = F(\alpha + c'\beta)$.

Entonces $\alpha + c\beta, \alpha + c'\beta \in F(\alpha + c\beta)$, luego su diferencia también: $(c - c')\beta \in F(\alpha + c\beta)$. Pero $c - c' \in F$, luego necesariamente $\beta \in F(\alpha + c\beta)$. Entonces $\alpha = (\alpha + c\beta) - c\beta \in F(\alpha + c\beta)$. Tenemos entonces $F(\alpha, \beta) \subset F(\alpha + c\beta)$, y la inclusión inversa es obvia, por lo tanto $K = F(\alpha, \beta) = F(\alpha + c\beta)$ y $F \subset K$ es simple. □

Corolario 2.70 (Teorema del elemento primitivo)**.** *Toda extensión finita y separable es simple. En particular toda extensión finita de un cuerpo de característica cero es simple.*

Demostración. Sea $F \subset K$ extensión finita y separable. Sea L la clausura de Galois de K sobre F. Entonces cualquier subcuerpo de K que contenga a F se corresponde con un subgrupo del grupo de Galois Gal_F^L que es finito porque $F \subset L$ es de Galois. Luego hay finitos subgrupos en Gal_F^L: la correspondencia de Galois nos da que hay finitos cuerpos entre F y L, en particular entre F y K. La proposición anterior implica entonces que $F \subset K$ es una extensión simple.

En característica cero, toda extensión finita es separable, luego por lo recién probado es simple. □

Veamos un ejemplo de una extensión que *no* es simple.

Ejemplo 2.7.2. Sea $F = \mathbb{F}_p(s, t)$ y E el cuerpo de descomposición sobre F de $(X^p - s)(X^p - t)$. En otras palabras, $E = F(\alpha, \beta)$ donde $\alpha^p = s$ y $\beta^p = t$. Entonces $|E : F| = p^2$. Por otro lado es fácil verificar que para todo $\alpha \in E$ se tiene que $\alpha^p \in F$, luego $|F(\alpha) : F| \in \{1, p\}$, y en particular $F(\alpha) \subset E$ para cualquier $\alpha \in E$, mostrando que E no puede ser una extensión simple.

Ejercicios

Ej. 52 — Sean $F \subset E_1 \subset K$, $F \subset E_2 \subset K$ extensiones de cuerpos, con $F \subset E_1, F \subset E_2$ de Galois.

a) Todo $\sigma \in \mathrm{Gal}_F^{E_1}$ se extiende a un automorfismo $\tilde{\sigma} \in \mathrm{Gal}_F^{E_1E_2}$, no necesariamente único.

b) $E_1 \cap E_2 = F$ si y sólo si todo $\sigma \in \mathrm{Gal}_F^{E_1}$ se extiende a un automorfismo $\tilde{\sigma} \in \mathrm{Gal}_F^{E_1E_2}$ tal que $\tilde{\sigma}|_{E_2} = \mathrm{id}$.

2.8. Cuerpos finitos

Empecemos demostrando un lema que ya hemos utilizado.

Lema 2.71. *Sea F cuerpo de característica $p > 0$. Entonces para todo $a, b \in F$ y $n \in \mathbb{N}$ se tiene $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$.*

Demostración. Por inducción en n. Probémoslo para $n = 1$. El teorema del binomio nos da

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

Pero sabemos que $p \mid \binom{p}{k}$ si $0 < k < p$, luego al estar en característica p, concluimos $(a+b)^p = a^p + b^p$.

Además $(a-b)^p = (a+(-b))^p = a^p + (-b)^p$. Pero $(-b)^p = -b^p$: si p es impar, $(-b)^p = (-1)^p b^p = -b^p$, y si $p = 2$ entonces $b^2 + b^2 = 2b^2 = 0 \Rightarrow b^2 = -b^2$.

Supongamos que vale para $n-1$. Entonces:

$$(a \pm b)^{p^n} = \left((a \pm b)^{p^{n-1}}\right)^p = \left(a^{p^{n-1}} \pm b^{p^{n-1}}\right)^p = \left(a^{p^{n-1}}\right)^p \pm \left(b^{p^{n-1}}\right)^p = a^{p^n} \pm b^{p^n} \qquad \square$$

Veamos que los cuerpos finitos no pueden tener cualquier tamaño.

Proposición 2.72. *Si F es un cuerpo finito de característica p, entonces $|F| = p^n$ para algún $n \in \mathbb{N}$.*

Demostración. Sea F un cuerpo finito. Entonces su característica p es prima. Entonces debe ser una extensión finita de su cuerpo primo $\mathbb{Z}_p$ pues de lo contrario contendría una base infinita y entonces sería infinito. Luego $|F : \mathbb{Z}_p| = n$ para algún $n \in \mathbb{N}$. Entonces F es un $\mathbb{Z}_p$-espacio vectorial de dimensión n, luego es linealmente isomorfo a $\overbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}^{n \text{ veces}}$, luego $|F| = p^n$. $\square$

Observación 2.8.1. El isomorfismo de la demostración anterior es un isomorfismo de $\mathbb{Z}_p$-espacios vectoriales, en particular de grupos abelianos. No estamos diciendo que $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ tenga estructura de cuerpo. De hecho aún no sabemos que exista un cuerpo de cardinal p^n. Pero sabemos que si existe, entonces su grupo aditivo es isomorfo a $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

Teorema 2.73. *Sea p primo, $n \in \mathbb{N}$. Entonces $\mathrm{Desc}_{\mathbb{Z}_p}(X^{p^n} - X)$ es un cuerpo con p^n elementos, que notaremos $\mathbb{F}_{p^n}$. Además es el único cuerpo de p^n elementos, a menos de isomorfismo.*

Demostración. Existencia: Probemos que $\mathrm{Desc}_{\mathbb{Z}_p}(X^{p^n} - X) = \{\text{raíces de } X^{p^n} - X \in \mathbb{Z}_p[X]\}$.

Basta probar que los elementos del conjunto de la derecha son un cuerpo, porque entonces es necesariamente el menor que tiene todas las raíces de $X^{p^n} - X$, i.e. es igual a $\mathrm{Desc}_{\mathbb{Z}_p}(X^{p^n} - X)$. Veamos esto. Si u, v son raíces de $X^{p^n} - X$, entonces:

$(uv)^{p^n} - uv = u^{p^n} v^{p^n} - uv = (u^{p^n} - u)(v^{p^n} - v) = 0$.

$u^{p^n} = u \Rightarrow u^{-p^n} = u^{-1} \Rightarrow (u^{-1})^{p^n} - u^{-1} = 0$.

$(u-v)^{p^n} = u^{p^n} - v^{p^n} = u - v \Rightarrow (u-v)^{p^n} - (u-v) = 0$.

Para ver que tiene p^n elementos, hay que ver que las raíces de $X^{p^n} - X$ son todas diferentes, i.e. que $f := X^{p^n} - X$ es separable. Pero su derivada es $Df = p^n X^{p^n - 1} - 1 = -1$, luego

$\mathrm{mcd}(f, Df) = 1$, entonces es separable.

Unicidad: Sea F un cuerpo con p^n elementos. Entonces si probamos que todo elemento de F es raíz de $X^{p^n} - X$, como recién vimos que $X^{p^n} - X$ tiene p^n raíces diferentes, se tiene que F es el menor cuerpo que contiene todas las raíces de $X^{p^n} - X$, i.e. F es un cuerpo de descomposición de $X^{p^n} - X$ sobre $\mathbb{Z}_p$, y son todos isomorfos, concluyendo el teorema.

Tenemos que F^* es cíclico de orden $p^n - 1$, luego para todo $u \in F^*$ se tiene $u^{p^n-1} = 1$, i.e. $u^{p^n} - u = 0$ para todo $u \in F^*$. Esta ecuación vale trivialmente para $u = 0$, entonces todo elemento de F es raíz de $X^{p^n} - X$. □

Observación 2.8.2. $\mathbb{F}_p \simeq \mathbb{Z}_p$, pero como dijimos en la observación anterior, $\mathbb{F}_{p^n}$ es un cuerpo con p^n elementos mientras que ni $\mathbb{Z}_{p^n}$ ni $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ tienen estructura de cuerpo si $n \geqslant 2$ (pues el grupo multiplicativo de un cuerpo finito debe ser cíclico).

Proposición 2.74. *La extensión $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ es de Galois, y $\mathrm{Gal}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} = \langle \sigma \rangle$, donde $\sigma : a \mapsto a^p$ es el endomorfismo de Frobenius.*

Demostración. $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ es de Galois pues por el teorema anterior es el cuerpo de descomposición de un polinomio separable.

σ es un automorfismo de $\mathbb{F}_{p^n}$, pues es un morfismo inyectivo y $\mathbb{F}_{p^n}$ es finito.

$\sigma|_{\mathbb{F}_p} = \mathrm{id}$ pues $a^{p-1} = 1 \Rightarrow a^p a^{-1} = 1 \Rightarrow a^p = a$ para todo $a \in \mathbb{F}_p$.

Ahora, $a \in \mathrm{Fix}(\langle \sigma \rangle) \iff a^p = a \iff a \in \mathbb{F}_p$, luego $\mathrm{Fix}(\langle \sigma \rangle) = \mathbb{F}_p$ y como $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ es Galois, se tiene $\mathbb{F}_p = \mathrm{Fix}(\mathrm{Gal}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}})$. La inyectividad de Fix nos da $\langle \sigma \rangle = \mathrm{Gal}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}}$. □

Observación 2.8.3. La proposición anterior nos da una manera de construir grupos de Galois cíclicos.

Corolario 2.75. *$\mathbb{F}_{p^n}$ contiene exactamente un subcuerpo con p^m elementos, para todo $m \mid n$, $m \geqslant 0$.*

Demostración. $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ es de Galois, y $\mathrm{Gal}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} = \langle \sigma \rangle$, pero $\langle \sigma \rangle$ tiene exactamente un subgrupo de orden n/m para todo $m \mid n$, i.e. $\langle \sigma^m \rangle$.

Por la correspondencia de Galois $\mathbb{F}_{p^n}$ tiene exactamente un subcuerpo de grado m sobre $\mathbb{F}_p$ para todo $m \mid n$, i.e. $\mathrm{Fix}(\langle \sigma^m \rangle)$. Pero $|\mathrm{Fix}(\langle \sigma^m \rangle) : \mathbb{F}_p| = m \Rightarrow |\mathrm{Fix}(\langle \sigma^m \rangle)| = p^m$. □

Corolario 2.76. *Sea $n \in \mathbb{N}$ y $d \mid n$. Todo polinomio $f \in \mathbb{Z}_p[X]$ irreducible de grado d aparece exactamente una vez como factor de $X^{p^n} - X$. En particular $|\mathrm{Desc}_{\mathbb{Z}_p}(f) : \mathbb{Z}_p| \leqslant d$.*

Demostración. Ya vimos que $X^{p^n} - X$ es separable, luego todos sus factores en un cuerpo de descomposición son distintos. Entonces si f es de grado $d \mid n$, basta ver que $f \mid X^{p^n} - X$.

Como f es irreducible de grado d, f tiene una raíz α en un cuerpo L de grado d sobre $\mathbb{Z}_p$. Pero $\mathrm{Desc}_{\mathbb{Z}_p}(X^{p^n} - X) = \mathbb{F}_{p^n}$, que por el corolario anterior tiene una copia de todo cuerpo de grado d sobre $\mathbb{F}_p$, para todo $d \mid n$. Por lo tanto $L \subset \mathbb{F}_{p^n} = \{\text{raíces de } X^{p^n} - X \text{ sobre } \mathbb{Z}_p\}$, luego α es raíz de $X^{p^n} - X$, en particular $f \mid X^{p^n} - X$.

En particular, tomando $n = d$ se obtiene $f \mid X^{p^d} - X \Rightarrow f$ se escinde en $\mathrm{Desc}_{\mathbb{Z}_p}(X^{p^d} - X)$ que tiene grado d sobre $\mathbb{Z}_p$, luego $|\mathrm{Desc}_{\mathbb{Z}_p}(f) : \mathbb{Z}_p| \leqslant d$. □

Corolario 2.77. *Sea F una clausura algebraica de $\mathbb{F}_p$. Entonces F contiene exactamente una copia de $\mathbb{F}_{p^n}$ para todo $n \in \mathbb{Z}^+$, que consiste de las raíces de $X^{p^n} - X$. Más aún, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$.*

En particular, una clausura algebraica de $\mathbb{F}_p$ es $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

2.9. Grupos de Galois de polinomios

Definición. Sea F cuerpo, $f \in F[X]$. El *grupo de Galois* de f sobre F es el grupo de Galois de $\mathrm{Desc}_F(f)$ sobre F.

Observación 2.9.1. Si f tiene raíces $\alpha_1, \ldots, \alpha_n$, entonces como los elementos de $\mathrm{Gal}_F(f)$ las permutan (y son biyecciones), se tiene que $\mathrm{Gal}_F(f) \subset \mathrm{Sym}(\alpha_1, \ldots, \alpha_n) \simeq S_n$. De esta manera podemos pensar $\mathrm{Gal}_F(f) \subset S_n$.

Si f se factoriza en irreducibles $f = f_1 \ldots f_k$, y $n_i := \mathrm{gr}\, f_i$, entonces como $\mathrm{Gal}_F(f)$ actúa en las raíces de f permutando las de los factores irreducibles, podemos pensar $\mathrm{Gal}_F(f) \subset S_{n_1} \times \cdots \times S_{n_k}$.

Más aún: si f es irreducible, entonces dadas dos raíces de f, por el teorema de extensión existe un elemento de $\mathrm{Gal}_F(f)$ que manda una en la otra. Esto nos dice que la acción $\mathrm{Gal}_F(f) \times \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}$ es transitiva. Por lo tanto si $n := \mathrm{gr}\, f$, entonces $\mathrm{Gal}_F(f)$ se identifica con un subgrupo transitivo de S_n.

Definición. Sea $f \in F[X]$ un polinomio que se factoriza en su cuerpo de descomposición como $f = c(X - r_1) \ldots (X - r_n)$. Se define su *discriminante*, $\Delta(f)$ como

$$\Delta(f) := \prod_{i<j} (r_j - r_i)^2$$

Cuando no haya riesgo de confusión notaremos simplemente Δ.

Observación 2.9.2. Para un polinomio de grado 2, $f = aX^2 + bX + c$, su discriminante es $\Delta = \frac{b^2 - 4ac}{a^2}$.

Enunciaremos ahora la clasificación de los grupos de Galois de polinomios de grados 2, 3 y 4 (para cuerpos de característica $\neq 2$). Las demostraciones son cálculos no muy ilustrativos; remitimos al lector al artículo [KC] para los detalles.

Polinomios de grado 2: Sea $f = aX^2 + bX + c \in F[X]$ polinomio de grado 2.

Si es reducible sobre F, entonces se escribe como producto de dos factores lineales sobre F, luego su grupo de Galois es trivial.

Si es irreducible, sus raíces son $\frac{-b \pm \sqrt{\Delta}}{2}$. El grupo de Galois es trivial si Δ es un cuadrado en F. Notaremos $\Delta = \square$ en F.

Si $\Delta \neq \square$ en F, entonces su grupo de Galois es isomorfo a $\mathbb{Z}_2$, pues $\mathrm{Desc}_F(f) = F(\sqrt{\Delta})$.

Polinomios de grado 3: Sea $f \in F[X]$ polinomio de grado 3, irreducible y separable[7]. Entonces:

Si $\Delta = \square$ en F, $\mathrm{Gal}_F(f) \simeq \mathbb{Z}_3$.

Si $\Delta \neq \square$ en F, $\mathrm{Gal}_F(f) \simeq S_3$.

Por lo tanto, los grupos de Galois de polinomios de grado 3 se determinan completamente a partir del discriminante.

El discriminante de un polinomio de grado 3 mónico es $\Delta(X^3 + aX + b) = -4a^3 - 27b^2$.

[7] Si car $F \neq 3$, los polinomios de grado 3 irreducibles son separables.

Polinomios de grado 4: sea $f \in F[X]$ de grado 4. En este caso la clasificación es un poco más complicada.

Definición. Si $f \in F[X]$ es un polinomio mónico irreducible de grado 4, $f = X^4 + aX^3 + bX^2 + cX + d$, su *resolvente cúbica* es el polinomio de grado 3

$$R_3(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd) \in F[X]$$

La siguiente tabla determina casi todas las posibilidades:

$\Delta(f)$ en F	$R_3(X)$ en F	$\mathrm{Gal}_F(f)$
$\neq \square$	irreducible	S_4
$= \square$	irreducible	A_4
$= \square$	reducible	$\mathbf{V}$
$\neq \square, < 0$	reducible	D_4
$\neq \square, > 0$	reducible	D_4 o $\mathbb{Z}_4$

En el último caso, el criterio debido a Kappe-Warren es el siguiente:
Si $f = X^4 + aX^3 + bX^2 + cX + d$, y $r' \in F$ es la única raíz de R_3 en F, considero:

$$\xi_1 = (a^2 - 4(b - r'))\Delta, \quad \xi_2 = (r'^2 - 4d)\Delta$$

Si al menos uno $\neq \square$ en F, entonces $\mathrm{Gal}_F(f) \simeq D_4$.
Si ambos $= \square$ en F, entonces $\mathrm{Gal}_F(f) \simeq \mathbb{Z}_4$.

Ejercicios

Ej. 53 — Sea $f = X^4 - 3 \in \mathbb{Q}[X]$. Determinar $\mathrm{Gal}_{\mathbb{Q}}(f)$ como subgrupo de S_4.

Ej. 54 — Determinar el grupo de Galois de los siguientes polinomios sobre los cuerpos indicados:

a) $X^3 - 2$ sobre $\mathbb{Q}$,

b) $(X^3 - 2)(X^2 - 5)$ sobre $\mathbb{Q}$,

c) $X^4 - 5$ sobre $\mathbb{Q}$, sobre $\mathbb{Q}(\sqrt{5})$ y sobre $\mathbb{Q}(i\sqrt{5})$,

d) $X^3 - 10$ sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(\sqrt{2})$.

Ej. 55 — Determinar todos los subgrupos del grupo de Galois y todas las extensiones intermedias del cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $X^3 - 2 \in \mathbb{Q}[X]$.

2.10. Polinomios simétricos

La siguiente definición involucra algunas verificaciones de rutina que dejamos como ejercicio sencillo para el lector. Intuitivamente lo único que haremos será ver S_n como subgrupo de $\mathrm{Aut}(F(X_1,\dots,X_n))$, de manera obvia, i.e. una permutación de $\{1,\dots,n\}$ se corresponde con el automorfismo que permuta las n indeterminadas de una función racional.

Definición. Sea F cuerpo, $\sigma \in S_n$. σ induce un mapa $\overline{\sigma} : F[X_1,\dots X_n] \to F[X_1,\dots,X_n]$ permutando las indeterminadas, i.e. definido mediante

$$\overline{\sigma}(p(X_1,\dots,X_n)) = p(X_{\sigma_1},\dots,X_{\sigma(n)})$$

Es un endomorfismo de anillos; claramente es un automorfismo que se extiende a un automorfismo de cuerpos (que seguiremos llamando $\overline{\sigma}$) de $F(X_1,\dots,X_n)$.

El mapa $S_n \to \mathrm{Aut}(F(X_1,\dots,X_n))$, $\sigma \mapsto \overline{\sigma}$ es un monomorfismo de grupos; podemos identificar entonces S_n con un subgrupo de $\mathrm{Aut}(F(X_1,\dots,X_n))$. Escribiremos $\sigma(p)$ en vez de $\overline{\sigma}(p)$ si no hay riesgo de confusión.

Una función racional p (en particular un polinomio) se dice *simétrico* si $\sigma(p) = p$ para toda $\sigma \in S_n$, i.e. si $p(X_1,\dots,X_n) = p(X_{\sigma(1)},\dots,X_{\sigma(n)})$ para toda $\sigma \in S_n$.

Observación 2.10.1. Como $\overline{\sigma}$ son isomorfismos, los polinomios simétricos en $F[X_1,\dots,X_n]$ son un subanillo de $F[X_1,\dots,X_n]$, y las funciones racionales simétricas son un subcuerpo de $F(X_1,\dots,X_n)$.

Definición. Sea F cuerpo. Los *polinomios simétricos elementales* de $F[X_1,\dots,X_n]$ son, para $r = 1,\dots,n$:

$$s_r = \sum_{1\leqslant i_1<\dots<i_r\leqslant n} X_{i_1}\dots X_{i_r}$$

En otras palabras, s_r es la suma de todos los monomios que pueden construirise multiplicando r indeterminadas distintas. Explícitamente, son:

$$\begin{aligned} s_1 &= X_1 + \dots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \dots + X_2X_3 + X_2X_4 + \dots + X_{n-1}X_n \\ &\vdots \\ s_n &= X_1\dots X_n \end{aligned}$$

Observación 2.10.2. Los polinomios simétricos elementales son polinomios simétricos.

Definición. Sea F cuerpo, y $s_1,\dots,s_n$ los polinomios simétricos elementales de $F[X_1,\dots,X_n]$. El *polinomio general de grado n sobre F* es:

$$(X - X_1)\dots(X - X_n) = X^n - s_1X^{n-1} + s_2X^{n-2} - \dots + (-1)^n s_n \in F(s_1,\dots,s_n)[X] \quad (2.7)$$

El teorema que sigue justifican la nomenclatura de *elementales*: toda función racional simétrica es una función racional en los polinomios simétricos elementales. Se puede probar además que todo polinomio simétrico es un polinomio en los polinomios simétricos elementales (teorema fundamental de los polinomios simétricos); no lo haremos porque no es central a nuestras motivaciones.

Teorema 2.78 (fundamental de las funciones racionales simétricas)**.** *El cuerpo de las funciones racionales simétricas de $F(X_1, \dots, X_n)$ es $F(s_1, \dots, s_n)$. Además la extensión $F(s_1, \dots, s_n) \subset F(X_1, \dots, X_n)$ es de Galois, y su grupo de Galois es S_n.*

Demostración. Consideremos el polinomio $p(X) = (X - X_1) \dots (X - X_n) \in F(X_1, \dots, X_n)[X]$. La ecuación (2.7) nos muestra que $p \in F(s_1, \dots, s_n)[X]$ y que las las indeterminadas $X_1, \dots, X_n$ son raíces de p, i.e. son algebraicas sobre $F(s_1, \dots, s_n)$. Como p es separable, entonces $F(X_1, \dots, X_n)$ es el cuerpo de descomposición de p sobre $F(s_1, \dots, s_n)$, por lo tanto la extensión $F(s_1, \dots, s_n) \subset F(X_1, \dots, X_n)$ es de Galois.

El grupo de Galois $G := \mathrm{Gal}_{F(s_1,\dots,s_n)}^{F(X_1,\dots,X_n)}$ es el grupo de Galois del polinomio p, por lo tanto G se identifica con un subgrupo (transitivo) de S_n. En particular $|G| \leqslant n!$.

Por otro lado tenemos la identificación $S_n \subset \mathrm{Aut}(F(X_1, \dots, X_n))$ como en la definición de polinomios simétricos. Los polinomios simétricos elementales $s_1, \dots s_n$ son polinomios simétricos, luego son fijados por los elementos de S_n. En otras palabras, $F(s_1, \dots, s_n) \subset \mathrm{Fix}(S_n)$.

Tenemos la torre de cuerpos $F(s_1, \dots, s_n) \subset \mathrm{Fix}(S_n) \subset F(X_1, \dots, X_n)$. La transitividad de grados nos da:

$$|F(X_1, \dots, X_n) : F(s_1, \dots, s_n)| = |F(X_1, \dots, X_n) : \mathrm{Fix}(S_n)||\mathrm{Fix}(S_n) : F(s_1, \dots, s_n)|$$

Por un lado, como $F(s_1, \dots, s_n) \subset F(X_1, \dots, X_n)$ es de Galois, entonces

$$|F(X_1, \dots, X_n) : F(s_1, \dots, s_n)| = |G| \leqslant n!$$

Por otro lado, por el corolario 2.49 se tiene que $\mathrm{Fix}(S_n) \subset F(X_1, \dots, X_n)$ es de Galois, luego

$$|F(X_1, \dots, X_n) : \mathrm{Fix}(S_n)| = |\mathrm{Gal}_{\mathrm{Fix}(S_n)}^{F(X_1,\dots,X_n)}| = |S_n| = n!$$

Entonces necesariamente $|\mathrm{Fix}(S_n) : F(s_1, \dots, s_n)| = 1$, i.e. $\mathrm{Fix}(S_n) = F(s_1, \dots, s_n)$. Como recién dijimos, $\mathrm{Fix}(S_n) \subset F(X_1, \dots, X_n)$ es de Galois, i.e. $F(s_1, \dots, s_n) \subset F(X_1, \dots, X_n)$.

Por lo tanto $\mathrm{Fix}\left(\mathrm{Gal}_{F(s_1,\dots,s_n)}^{F(X_1,\dots,X_n)}\right) = F(s_1, \dots, s_n) = \mathrm{Fix}(S_n) \Rightarrow \mathrm{Gal}_{F(s_1,\dots,s_n)}^{F(X_1,\dots,X_n)} = S_n$. □

Corolario 2.79. *Sea F cuerpo. El grupo de Galois del polinomio general de grado n sobre F es S_n.*

Demostración. Como $F(X_1, \dots, X_n)$ es el cuerpo de descomposición del polinomio general de grado n sobre $F(s_1, \dots, s_n)$, entonces por el teorema anterior su grupo de Galois es $\mathrm{Gal}_{F(s_1,\dots,s_n)}^{F(X_1,\dots,X_n)} = S_n$.

□

Corolario 2.80. *Sea G grupo finito. Entonces existen F, K cuerpos, $F \subset K$ de Galois tales que $G \simeq \mathrm{Gal}_F^K$.*

Demostración. Por el teorema de Cayley, $G \simeq H < S_n = \mathrm{Gal}_{L(s_1,\dots,s_n)}^{L(X_1,\dots,X_n)}$ para algún $n \in \mathbb{N}$ y L cuerpo cualquiera. Entonces por el corolario 2.49, $\mathrm{Gal}_{\mathrm{Fix}(H)}^{L(X_1,\dots,X_n)} \simeq H \simeq G$. □

Observación 2.10.3. El corolario anterior nos dice que un grupo finito cualquiera se puede ver como grupo de Galois de una extensión de cuerpos. Cabe preguntarse si puede verse como grupo de Galois de una extensión finita de $\mathbb{Q}$: éste es el *problema de Galois inverso*, que es un problema abierto.

Un *cuerpo de números algebraicos* (o más sencillamente, un *cuerpo de números*) es una extensión finita de $\mathbb{Q}$.

2.11. Extensiones ciclotómicas

Notación. En esta sección notaremos $\zeta_n := e^{\frac{2\pi i}{n}}$ a la primera raíz n-ésima primitiva de la unidad, y $\mu_n = \{\text{raíces } n\text{-ésimas de 1 sobre } \mathbb{Q}\}$.

Observación 2.11.1. $\mu_d \subset \mu_n \iff d \mid n$.

Definición. El cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$ es el cuerpo $\mathbb{Q}(\zeta_n)$ llamado *cuerpo ciclotómico de raíces n-ésimas de la unidad*.

Definición. El *n-ésimo polinomio ciclotómico* $\phi_n \in \mathbb{C}[X]$ es el polinomio mónico cuyas raíces son las raíces n-ésimas primitivas de la unidad:

$$\phi_n(X) := \prod_{\substack{z \in \mu_n \\ z \text{ primitiva}}} (X - z) = \prod_{\substack{1 \leqslant a < n \\ \mathrm{mcd}(a,n)=1}} (X - \zeta_n^a)$$

Observación 2.11.2. $X^n - 1 = \prod_{d \mid n} \phi_d$. En efecto,

$$X^n - 1 = \prod_{z \in \mu_n} (X - z) = \prod_{d \mid n} \prod_{\substack{z \in \mu_d \\ z \text{ primitiva}}} (X - z) = \prod_{d \mid n} \phi_d$$

La segunda igualdad se obtiene agrupando los elementos de orden d en μ_n, para todo $d \mid n$.

En particular, comparando los grados obtenemos la identidad de teoría de números

$$n = \sum_{d \mid n} \varphi(d)$$

Además obtenemos una manera de calcular por recurrencia los polinomios ciclotómicos:

$$\phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \phi_d}$$

Ejemplo 2.11.3.

$$\begin{aligned}
\phi_3(X) &= \frac{X^3 - 1}{X - 1} = X^2 + X + 1 \\
\phi_4(X) &= \frac{X^4 - 1}{X^2 - 1} = X^2 + 1 \\
\phi_5(X) &= \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1 \\
\phi_6(X) &= \frac{X^6 - 1}{(X-1)(X+1)(X^2 + X + 1)} = X^2 - X + 1
\end{aligned}$$

Teorema 2.81. *$\phi_n \in \mathbb{Z}[X]$, es mónico, irreducible y de grado $\varphi(n)$.*

Demostración. Obviamente es mónico de grado $\varphi(n)$. Hay que ver que sus coeficientes son enteros y que es irreducible.

- $\phi_n \in \mathbb{Z}[X]$: por inducción en n. Para $n = 1$ es obvio. Supongamos que vale para $1 \leqslant d < n$. Entonces

$$X^n - 1 = \phi_n \cdot \prod_{\substack{d \mid n \\ d<n}} \phi_d = \phi_n \cdot f \quad \text{para cierto } f \in \mathbb{Z}[X]$$

por hipótesis de inducción.

Por un lado tenemos $X^n - 1 = \phi_n f$ en $\mathbb{Q}[X]$. Por otro lado, como $X^n - 1, f \in \mathbb{Z}[X]$, existen $q, r \in \mathbb{Z}[X]$ tales que $X^n - 1 = qf + r$, donde $r = 0$ o gr $r <$ gr q. Por la unicidad de la división entera en $\mathbb{Q}$, debe ser $q = \phi_n$ y $r = 0$, luego $\phi_n \in \mathbb{Z}[X]$.

- ϕ_n es irreducible: por absurdo supongamos que $\phi_n = fg$ con $f, g \in \mathbb{Z}[X]$ mónicos, f irreducible.

Sea ζ una raíz n-ésima primitiva de la unidad que es raíz de f (esto implica que $f = m_{\zeta,\mathbb{Q}}$ pues f es irreducible), y sea p primo tal que $p \nmid n$. Entonces ζ^p es raíz n-ésima primitiva de 1, luego ζ^p debe ser raíz de ϕ_n, luego de f o de g.

Supongamos que ζ^p es raíz de g, i.e. $g(\zeta^p) = 0$. Entonces ζ es raíz de $g(X^p)$, y como $f = m_{\zeta,\mathbb{Q}}$, se tiene que $f(X) \mid g(X^p)$ en $\mathbb{Z}[X]$. Por lo tanto existe $h \in \mathbb{Z}[X]$ tal que $g(X^p) = f(X)h(X)$.

Reduciendo módulo p, se obtiene $\overline{g}(X^p) = \overline{f}(X)\,\overline{h}(X)$ en $\mathbb{Z}_p[X]$. Pero como todo $u \in \mathbb{Z}_p$ cumple $u^p = u$, podemos sacar el exponente p para afuera, y $(\overline{g}(X))^p = \overline{f}(X)\,\overline{h}(X)$ en $\mathbb{Z}_p[X]$. Como $\mathbb{Z}_p[X]$ es un dominio de factorización única, se tiene que $\overline{f}$ y $\overline{g}$ tienen un factor en común en $\mathbb{Z}_p[X]$.

Pero $\phi_n = fg \Rightarrow \overline{\phi_n} = \overline{f}\,\overline{g}$ en $\mathbb{Z}_p[X]$, luego $\overline{\phi_n} \in \mathbb{Z}_p[X]$ tiene una raíz múltiple. Entonces $X^n - 1 \in \mathbb{Z}_p[X]$ tiene una raíz múltiple, pues tiene a $\overline{\phi_n}$ como factor. Esto es absurdo pues todas las raíces de $X^n - 1$ son diferentes en cualquier cuerpo de característica que no divide a n.

Entonces ζ^p debe ser raíz de f, para toda ζ raíz de f. Luego ζ^a es raíz de f para todo a tal que $\mathrm{mcd}(a, n) = 1$, pues si $a = p_1 \dots p_k$ es producto de primos que no dividen a n, entonces ζ^{p_1} es raíz de f, luego $(\zeta^{p_1})^{p_2}$ es raíz de f, $\dots$, $\zeta^{p_1 \cdots p_k} = \zeta^a$ es raíz de f.

Esto significa exactamente que toda raíz n-ésima primitiva de la unidad es raíz de f, luego por definición de ϕ_n, se tiene $f = \phi_n$, pero f es irreducible, luego ϕ_n es irreducible. □

Corolario 2.82. $|\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \varphi(n)$. *En particular si p es primo,* $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = p - 1$.

Demostración. $\phi_n = m_{\zeta_n,\mathbb{Q}}$ y gr $\phi_n = \varphi(n)$. □

Teorema 2.83. *El grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ es isomorfo a $\mathbb{Z}_n^*$. En particular es abeliano.*

Demostración. Definimos $\psi : \mathbb{Z}_n^* \to \mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}$, $\overline{a} \mapsto \sigma_a$, donde σ_a se define como $\sigma_a|_{\mathbb{Q}} = \mathrm{id}$ y $\sigma_a(\zeta_n) = \zeta_n^a$. Esto nos da efectivamente un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\zeta_n)$.

ψ es un morfismo:

$$\sigma_a\sigma_b(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^b)^a = \zeta_n^{ab} = \sigma_{ab}(\zeta_n) \Rightarrow \sigma_a\sigma_b = \sigma_{ab} \quad \forall a, b$$

ψ es sobreyectiva: si $\sigma \in \mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}$, entonces manda ζ_n en otra raíz n-ésima primitiva de 1, pues son las raíces del polinomio irreducible ϕ_n. Luego $\sigma = \sigma_a$ para cierto a tal que $1 \leqslant a < n$, $\mathrm{mcd}(a, n) = 1$, luego ψ es sobreyectivo.

Además hay precisamente $\varphi(n)$ tales a diferentes, y $|\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}| = \varphi(n) = |\mathbb{Z}_n^*|$, luego ψ es biyectivo. □

Ejemplo 2.11.4. $\mathbb{Q} \subset \mathbb{Q}(\zeta_5)$ es de Galois, y $\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_5)} = \mathbb{Z}_5^* \simeq \mathbb{Z}_4$. Es un ejemplo de una extensión de Galois de $\mathbb{Q}$ de grado 4, con grupo de Galois cíclico.

Observación 2.11.5. Una extensión de cuerpos $F \subset K$ se dice *abeliana* si su grupo de Galois es abeliano. Tenemos entonces que $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ es abeliana.

[DF], p. 599 prueba que: si $n = p_1^{a_1} \dots p_k^{a_k}$ es la descomposición en primos de n, entonces

$$\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)} \simeq \mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}\left(\zeta_{p_1^{a_1}}\right)} \times \cdots \times \mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}\left(\zeta_{p_k^{a_k}}\right)}$$

Usando esto y el teorema chino de los restos, [DF] prueba que el problema de Galois inverso para grupos abelianos se resuelve con extensiones ciclotómicas: dado G grupo abeliano finito existe K subcuerpo de un cuerpo ciclotómico tal que $G \simeq \mathrm{Gal}_{\mathbb{Q}}^{K}$. El recíproco también vale:

Teorema (Kronecker-Weber): Todo cuerpo de números con grupo de Galois abeliano es isomorfo a un subcuerpo de un cuerpo ciclotómico.

Terminamos la sección con una aplicación de los cuerpos ciclotómicos a las construcciones con regla y compás.

Teorema 2.84. *El n-ágono regular es constructible con regla y compás si y sólo si $\varphi(n)$ es una potencia de 2.*

Demostración. Usaremos el teorema 2.27.

La construcción del n-ágono regular es equivalente a la construcción de las raíces n-ésimas de la unidad, pues son los vértices del n-ágono regular inscrito en el círculo unitario.

La construcción de $\zeta_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$ es equivalente a la construcción de su parte real, $a := \cos\frac{2\pi}{n} = \frac{1}{2}(z_n + \overline{\zeta_n}) = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$. Multiplicando esta identidad por ζ_n, obtenemos que ζ_n satisface la ecuación cuadrática en $\mathbb{Q}(a)$:

$$\zeta_n^2 - 2a\zeta_n + 1 = 0$$

Por lo tanto $|\mathbb{Q}(\zeta_n) : \mathbb{Q}(a)| = 2$, pues es $\leqslant$ y no es igual ya que $\zeta_n \in \mathbb{C}\backslash\mathbb{R}$ y $\mathbb{Q}(a) \subset \mathbb{R}$.

Entonces la torre $\mathbb{Q} \subset \mathbb{Q}(a) \subset \mathbb{Q}(\zeta_n)$ nos da que $|\mathbb{Q}(a) : \mathbb{Q}| = \varphi(n)/2$.

Por lo tanto si el n-ágono regular es constructible, entonces $\varphi(n)$ debe ser potencia de 2.

Recíprocamente, si $\varphi(n) = 2^{m'}$, entonces $\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}$ es abeliano de orden potencia de 2, luego el subgrupo $\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(a)}$ también lo es. Supongamos que es de orden 2^m para cierto $m < m'$. Como un p-grupo tiene subgrupos de todos los órdenes, se tiene

$$\mathrm{Gal}_{\mathbb{Q}}^{\mathbb{Q}(a)} = G_m > G_{m-1} > \cdots > G_0 = \{\mathrm{id}\}$$

donde cada subgrupo es de índice 2 en el siguiente.

Tomando cuerpos fijos, por la correspondencia de Galois se obtiene una serie de extensiones cuadráticas de $\mathbb{Q}$ que termina en $\mathbb{Q}(a)$, luego a es constructible. □

Observación 2.11.6. Un *primo de Fermat* es un número primo que es de la forma $2^n + 1$ para algún $n \in \mathbb{N}$. Fermat probó que si $2^n + 1$ es primo entonces n es una potencia de 2.

Se puede probar que $\varphi(n)$ es una potencia de 2 si y sólo si $n = 2^k p_1 \dots p_k$ para algún k y primos de Fermat $p_1, \dots, p_k$ diferentes.

Ejercicios

Ej. 56 — La demostración del teorema 2.83 se puede retocar para probar que si F es un cuerpo de característica cero entonces $\mathrm{Gal}_F^{F(\zeta_n)}$ es un subgrupo de $\mathbb{Z}_n^*$, y en particular es abeliano.

2.12. Extensiones trascendentes

[8]En esta sección consideramos extensiones de cuerpos por cuerpos de tamaño mucho mayor.

Definición. Sea $F \subset \Omega$ extensión de cuerpos. Decimos que $\alpha_1, \ldots, \alpha_n \in \Omega$ son *algebraicamente dependientes* sobre F si existe $f \in F[X_1, \ldots, X_n]$, $f \neq 0$ tal que $f(\alpha_1, \ldots, \alpha_n) = 0$.

Son *algebraicamente independientes* si no son algebraicamente dependientes, i.e. si

$$\sum_{1 \leqslant i_1, \ldots, i_n \leqslant n} a_{i_1,\ldots,i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n} = 0 \Rightarrow a_{i_1,\ldots,i_n} = 0 \quad \forall i_1, \ldots, i_n, \quad \text{donde } a_{i_1,\ldots,i_n} \in F$$

Decimos que un subconjunto $A \subset \Omega$ es algebraicamente independiente sobre F si lo son todos sus subconjuntos finitos. Si no, es algebraicamente dependiente.

Ejemplo 2.12.1. $\alpha \in \Omega$ es algebraicamente independiente sobre F si y sólo si es trascendente sobre F.

Observación 2.12.2. Si pedimos que f sea un polinomio homogéneo de grado 1, obtenemos la definición de elementos linealmente (in)dependientes.

Definición. Sea $F \subset \Omega$ extensión de cuerpos, $\alpha_1, \ldots, \alpha_n \in \Omega$. Decimos que la extensión $F \subset F(\alpha_1, \ldots, \alpha_n)$ es *puramente trascendente* si $\alpha_1, \ldots, \alpha_n$ son algebraicamente independientes sobre F.

Una extensión $F \subset \Omega$ es puramente trascendente si existe un subconjunto $A \subset \Omega$ que es algebraicamente independiente sobre F y tal que $\Omega = F(A)$.

Ejemplo 2.12.3. $\mathbb{Q} \subset \mathbb{Q}(\pi, \sqrt{2})$ es trascendente (pues π lo es), pero no puramente trascendente. Explícitamente, si $f = Y^2 - 2 \in \mathbb{Q}[X, Y]$ entonces $f \neq 0$ y $f(\pi, \sqrt{2}) = 0$.

Definición. Sea $F \subset \Omega$ extensión de cuerpos. Una *base de trascendencia* para Ω sobre F es un subconjunto algebraicamente independiente $A \subset \Omega$ tal que $F(A) \subset \Omega$ es una extensión algebraica.

Una aplicación estándar del lema de Zorn nos da el siguiente

Teorema 2.85. *Toda extensión de cuerpos $F \subset \Omega$ tiene una base de trascendencia. Más aún, todas las bases de trascendencia de una extensión fija tienen el mismo cardinal.*

Esto habilita la siguiente

Definición. Sea $F \subset \Omega$ extensión de cuerpos. El *grado de trascendencia* de la extensión es el cardinal de una base de trascendencia.

Tenemos una analogía con el álgebra lineal dada por el siguiente cuadro:

Álgebra lineal	Trascendencia
Independencia lineal	Independencia algebraica
Base	Base de trascendencia
Dimensión	Grado de trascendencia

[8]No se trata de ahondar en la teoría de las extensiones trascendentes, sino de dar un pantallazo general de las definiciones y teoremas más básicos, y de algunos teoremas sorprendentes.

Ejemplo 2.12.4.

- Una extensión es algebraica si y sólo si su grado de trascendencia es 0 (una base de trascendencia es $\varnothing$).
- $\{\pi\}$ es una base de trascendencia para $\mathbb{Q} \subset \mathbb{Q}(\pi, \sqrt{2})$, luego esta extensión tiene grado de trascendencia 1.
- $F \subset F(X_1, \ldots, X_n)$ es una extensión puramente trascendente, de grado de trascendencia n.

  Observar que dar el anillo de polinomios en n variables con coeficientes en F, $F(X_1, \ldots, X_n)$, es lo mismo que dar F junto con una extensión puramente trascendente $F \subset F(\alpha_1, \ldots, \alpha_n)$. En otras palabras, "es lo mismo" una indeterminada que un elemento trascendente.
- El grado de trascendencia de $\mathbb{Q} \subset \mathbb{R}$ es el continuo, i.e. $\mathfrak{c} = |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.
- No se sabe si el grado de trascendencia de $\mathbb{Q} \subset \mathbb{Q}(\pi, e)$ es 1 o 2. En otras palabras, no se sabe si π y e son algebraicamente independientes. Por lo tanto no se sabe por ejemplo si $\pi + e$ es trascendente. Sin embargo, se sabe que e^π (la *constante de Gelfond*) es trascendente: esto es consecuencia del siguiente teorema, que respondió afirmativamente al séptimo problema de Hilbert:

  Teorema de Gelfond-Schneider (1934): Si $\alpha, \beta \in \mathbb{C}$ son números algebraicos, $\alpha, \beta \neq 0, 1$, y si $\beta \notin \mathbb{Q}$, entonces α^β es trascendente.

  En efecto, $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i}$.

  Otra consecuencia de este teorema es que $2^{\sqrt{2}}$ y $\sqrt{2}^{\sqrt{2}}$ son trascendentes.

Otro teorema sorprendente es el teorema de Lüroth:

Teorema 2.86 (Lüroth)**.** *Si $F \subset F(t)$ es una extensión simple y trascendente de F, entonces todo cuerpo E tal que $F \subsetneq E \subset F(t)$ es también una extensión simple y trascendente de F.*

Observación 2.12.5. El teorema de Lüroth dice, en otras palabras, que todo subcuerpo de un cuerpo de funciones racionales en una variable (distinto del cuerpo base) es también un cuerpo de funciones racionales en una variable.

En dos variables, el teorema es cierto en característica 0 (teorema de Castelnuovo): todo subcuerpo de $F(X, Y)$ distinto de F es isomorfo a $F(X)$ o a $F(X, Y)$.

Para tres variables o más el teorema es falso incluso sobre $\mathbb{C}$.

2.13. Extensiones inseparables

En esta sección estudiaremos las extensiones inseparables. En el corolario 2.39 vimos que toda extensión algebraica de un cuerpo de característica cero es separable. Por lo tanto en esta sección trabajaremos siempre con cuerpos de característica $p > 0$.

Definición. Sea k cuerpo de característica p, $f \in k[X]$ un polinomio no constante. El *grado de inseparabilidad* de f es la mayor potencia p^n, $n \geqslant 0$ tal que $f(X) = g(X^{p^n})$ para algún $g \in k[X]$.

Observación 2.13.1. La anterior definición tiene sentido: g no puede ser constante pues f no lo es, y gr $f(X) =$ gr $g(X^{p^n}) = p^n$ gr $g(X)$, entonces necesariamente hay un máximo n que cumple $f(X) = g(X^{p^n})$.

La siguiente proposición muestra que en un cuerpo de característica p todas las raíces de un polinomio irreducible tienen la misma multiplicidad, que es el grado de inseparabilidad del polinomio:

Proposición 2.87. *Sea k cuerpo de característica p y $f \in k[X]$ un polinomio irreducible con grado de inseparabilidad p^n. Entonces f se escinde en su cuerpo de descomposición sobre k de la siguiente manera:*

$$f(X) = a_0(X - a_1)^{p^n} \dots (X - a_r)^{p^n}$$

donde $a_1, \dots, a_r$ son distintos dos a dos.

Demostración. Sea $g \in k[X]$ tal que $f(X) = g(X^{p^n})$. Entonces g no es un polinomio en X^p, pues si $g(X) = h(X^p)$ entonces $f(X) = h(X^{p^{n+1}})$ contradiciendo la maximalidad de n.

Además g es irreducible. En efecto, supongamos que $g(X) = u(X)v(X)$. Entonces $f(X) = u(X^{p^n})v(X^{p^n})$: como f es irreducible esto implica que uno de los dos factores, por ejemplo $u(X^{p^n})$, es constante. En este caso debe ser $u(X)$ constante, y g es irreducible.

Por la proposición 2.40 debe ser g un polinomio separable, luego en una clausura algebraica L de k, se tiene:

$$g(X) = a_0(X - b_1) \dots (X - b_r)$$

para ciertos $b_1, \dots, b_r \in L$ distintos dos a dos.

Sea $a_i = \sqrt[p^n]{b_i}$ una raíz de $X^{p^n} - b_i$ en L. Tenemos entonces, por el lema 2.71:

$$f(X) = g(X^{p^n}) = a_0(X^{p^n} - a_1^{p^n}) \dots (X^{p^n} - a_r^{p^n}) = a_0(X - a_1)^{p^n} \dots (X - a_r)^{p^n} \qquad \square$$

Definición. Sea K cuerpo. Un polinomio $f \in K[X]$ se dice *puramente inseparable* si tiene exactamente una raíz (sin contar multiplicidades) en su cuerpo de descomposición.

Sea $F \subset K$ extensión de cuerpos. Decimos que es *puramente inseparable* si todo elemento $\alpha \in K$ es raíz de un polinomio en $F[X]$ puramente inseparable.

Observación 2.13.2.

1. Un polinomio $f \in F[X]$ es a la vez separable y puramente inseparable si y sólo si $f = X - c$ para algún $c \in F$. Por lo tanto un elemento $\alpha \in K$ es raíz de un polinomio en $F[X]$ separable y puramente inseparable si y sólo si $\alpha \in F$.

2. $F \subset K$ es puramente inseparable si y sólo si todos los polinomios mínimos de los elementos de K sobre F son puramente inseparables, si y sólo si todo elemento $\alpha \in K \backslash F$ es raíz de un polinomio irreducible e inseparable.

Ejemplo 2.13.3. Sea F cuerpo de característica p. Un polinomio $f \in F[X]$ de la forma $f(X) = X^{p^n} - b$ es puramente inseparable. En efecto, si $a = \sqrt[p^n]{b}$ es una raíz de f en su cuerpo de descomposición, aplicando el lema 2.71:

$$f(X) = X^{p^n} - b = X^{p^n} - a^{p^n} = (X - a)^{p^n}$$

Teorema 2.88. *Una extensión de cuerpos de característica p, $F \subset K$ es puramente inseparable si y sólo si para todo $\alpha \in K$ existe $n \in \mathbb{N}$ tal que $\alpha^{p^n} \in F$.*

Demostración. ($\Rightarrow$) Sea $\alpha \in K$. Entonces $m_{\alpha,F}$ es puramente inseparable y es irreducible, luego la proposición 2.87 y el ejemplo 2.13.3 nos dan que α es raíz de un polinomio de la forma $c(X - b)^{p^n} = c(X^{p^n} - a)$, i.e. $\alpha^{p^n} = \frac{a}{c} \in F$.

($\Leftarrow$) Sea $\alpha \in K$. Entonces $\alpha^{p^n} =: a \in F$, y α es raíz del polinomio puramente inseparable $X^{p^n} - c$. □

Ejemplo 2.13.4. La extensión $\mathbb{F}_p(t^p) \subset \mathbb{F}_p(t)$, donde t es una indeterminada sobre $\mathbb{F}_p$, i.e. un elemento trascendente sobre $\mathbb{F}_p$, es puramente inseparable. En efecto, un elemento $f \in \mathbb{F}_p(t)$ es de la forma:

$$f = \frac{\sum_{i=1}^{p-1} a_i t^i}{\sum_{j=1}^{p-1} b_j t^j}$$

para ciertos $a_i, b_j \in \mathbb{F}_p$. Si lo elevamos a la potencia p, i.e. si le aplicamos el endomorfismo de Frobenius, obtenemos:

$$f^p = \frac{\sum_{i=1}^{p-1} a_i^p t^{pi}}{\sum_{j=1}^{p-1} b_j^p t^{pj}} \in \mathbb{F}_p(t^p)$$

luego por la proposición anterior, $\mathbb{F}_p(t)$ es puramente inseparable sobre $\mathbb{F}_p(t^p)$.

Lema 2.89. *Sea F cuerpo de característica p, $f \in F[X]$ un polinomio puramente inseparable de raíz α en su cuerpo de descomposición. Entonces existe $m \in \mathbb{Z}^+$ y $c \in K^*$ tal que*

$$f(X) = c\,(m_{\alpha,F}(X))^m$$

Demostración. Por inducción en gr f. Si gr $f = 1$ es obvio. Supongamos que vale para polinomios de grado $\leqslant n$, donde $n = \text{gr } f$.

Como $m_{\alpha,F} \mid f$, se tiene $f = g m_{\alpha,F}$ con gr $g \leqslant n$. Pero f es puramente inseparable de raíz α, entonces g debe serlo también. Por hipótesis de inducción $g(X) = c\,(m_{\alpha,F}(X))_0^m$ para algún $c \in K^*$, $m_0 \in \mathbb{Z}^+$, de donde

$$f(X) = g(X) m_{\alpha,F}(X) = c\,(m_{\alpha,F}(X))^{m_0+1}$$

Con $m_0 + 1 = m \in \mathbb{Z}^+$ se deduce la tesis. □

Proposición 2.90. *Sea F cuerpo de característica p. Un polinomio $f \in F[X]$ es puramente inseparable si y sólo si:*

$$f(X) = c(X^{p^n} - a)^m$$

para ciertos $c \in F^*$, $n, m \in \mathbb{N}$.

Demostración. ($\Leftarrow$) Un polinomio de esa forma es puramente inseparable. En efecto, por el ejemplo 2.13.3:

$$f(X) = c(X^{p^n} - a)^m = c\left((X-b)^{p^n}\right)^m = c\,(X-b)^{p^n m}$$

($\Rightarrow$) Por el lema 2.89, $f(X) = c\,(m_{\alpha,F}(X))^m$ para ciertos $c \in K^*$, $m \in \mathbb{Z}^+$. Como f es puramente inseparable, $m_{\alpha,F}$ lo es también; además es un polinomio irreducible, luego aplicándole la proposición 2.87 se tiene $m_{\alpha,F}(X) = X^{p^n} - a$ para ciertos $a \in F$, $n \in \mathbb{N}$. Pero entonces:

$$f(X) = c\,(m_{\alpha,F}(X))^m = c\left(X^{p^n} - a\right)^m$$ □

Corolario 2.91. *Sea $F \subset K$ extensión de cuerpos de característica p, $f \in K[X]$ polinomio puramente inseparable. Entonces $F \subset \mathrm{Desc}_F(f)$ es una extensión puramente inseparable.*

Definición. Dada una extensión de cuerpos $F \subset K$ y $\alpha \in K$, diremos que α es *separable*, *inseparable*, o *puramente inseparable* sobre F si es raíz respectivamente de un tal polinomio en $F[X]$.

Definición. Sea $F \subset K$ extensión de cuerpos de característica p.

El mayor subcuerpo de K que es separable sobre F se llama *clausura separable* de F en K, y se denota K_F^s. El *grado de separabilidad* de la extensión se define como $|K_F^s : F|$.

El mayor subcuerpo de K que es puramente inseparable sobre F se llama *clausura puramente inseparable* o *clausura perfecta* de F en K, y se denota K_F^P. El *grado de inseparabilidad* de la extensión se define como como $|K_F^P : F|$.

Observación 2.13.5. El conjunto de todos los elementos de K separables (resp. puramente inseparables) sobre F forma un cuerpo (verificarlo), así que es la clausura separable (resp. perfecta) de F en K.

El teorema 2.88 nos dice que la clausura perfecta de F en K es el conjunto de los elementos α de K tales que $\alpha^{p^n} \in F$ para algún $n \in \mathbb{N}$, i.e. K_F^P consiste de adjuntarle a F todas las raíces p^n-ésimas de sus elementos, para todo $n \in \mathbb{Z}^+$.

La siguiente proposición justifica el nombre de *clausura perfecta*:

Proposición 2.92. *Sea $F \subset L$ extensión de cuerpos de característica p tal que L es una clausura algebraica de F. Entonces L_F^P, notado $F^{p^{-\infty}}$, es el menor subcuerpo perfecto de L que contiene a F.*

Demostración. Para cada $r \in \mathbb{Z}^+$, se define:

$$F^{p^{-r}} := \{\alpha \in L : \alpha^{p^r} \in F\}$$

i.e. $F^{p^{-r}}$ es el resultado de adjuntarle a F todas sus raíces p^r-ésimas de sus elementos. Es un subcuerpo de L, y tenemos la torre infinita:

$$F \subset F^{p^{-1}} \subset F^{p^{-2}} \subset \cdots \subset F^{p^{-r}} \subset \ldots$$

De esta manera, por el teorema 2.88 resulta que

$$F^{p^{-\infty}} = \bigcup_{r=1}^{\infty} F^{p^{-r}} \tag{2.8}$$

Por la proposición 2.41, para ver que $F^{p^{-\infty}}$ es perfecto basta ver que $(F^{p^{-\infty}})^p = F^{p^{-\infty}}$. Esto es obvio de la igualdad (2.8) y de observar que $(F^{p^{-r}})^p = F^{p^{-(r-1)}}$.

Es el menor: sea $E \subset L$ un subcuerpo perfecto que contiene a F. Si $\alpha \in F^{p^{-\infty}}$, entonces $\alpha \in F^{p^{-r}}$ para algún $r \in \mathbb{Z}^+$, i.e. $\alpha^{p^r} \in F \subset E$ que es perfecto: $\alpha^{p^r} = \beta^{p^r}$ para algún $\beta \in E$. Por lo tanto $\alpha = \beta \in E$, probando que $F^{p^{-\infty}} \subset E$. □

El siguiente teorema nos dice que podemos partir una extensión algebraica cualquiera en una parte separable y una puramente inseparable:

Teorema 2.93. *Sea $F \subset K$ extensión algebraica de cuerpos de característica p. Entonces la extensión $K_F^s \subset K$ es puramente inseparable. Por lo tanto, si consideramos la torre*

$$F \subset K_F^s \subset K$$

tiene el primer tramo separable y el segundo puramente inseparable.

Demostración. Sea $\alpha \in K$. Sea p^n el grado de inseparabilidad de $m_{\alpha,F}$. Entonces $m_{\alpha,F}(X) = g(X^{p^n})$ para algún $g \in F[X]$. Por lo tanto $g(\alpha^{p^n}) = m_{\alpha,F}(\alpha) = 0$.

Por un lado, g no es un polinomio en X^p, pues si $g(X) = h(X^p)$ entonces $f(X) = h(X^{p^{n+1}})$ contradiciendo la maximalidad de n.

Por otro lado, g es irreducible. En efecto, supongamos que $g(X) = u(X)v(X)$. Entonces $m_{\alpha,F}(X) = u(X^{p^n})v(X^{p^n})$: como $m_{\alpha,F}$ es irreducible esto implica que uno de los dos factores, por ejemplo $u(X^{p^n})$, es constante. En este caso debe ser $u(X)$ constante, y g es irreducible.

Por la proposición 2.40 debe ser g un polinomio separable, luego α^{p^n} es raíz de un polinomio separable, de donde $\alpha^{p^n} \in K_F^s$: por el teorema 2.88 se deduce que $K_F^s \subset K$ es puramente inseparable. □

Isaacs ([Isa], p.301) indica que una extensión algebraica $F \subset K$ puede no poseer un cuerpo intermedio que sea puramente inseparable sobre F y que cumpla que K es separable sobre él.

Demostremos el teorema que auguramos en la observación 2.4.5:

Teorema 2.94. *Sea $F \subset K$ una extensión algebraica tal que todo polinomio no constante en $F[X]$ tiene una raíz en K. Entonces K es algebraicamente cerrado.*

Demostración. Caso 1: $F \subset K$ es separable. Para ver que K es algebraicamente cerrado basta ver que es una clausura algebraica de F: sea $f \in F[X]$ no constante, y veamos que tiene una raíz en K. Basta probarlo para f irreducible. Podemos suponer sin pérdida de generalidad que además es mónico.

Por hipótesis f tiene una raíz $\alpha \in K$, y por lo tanto $f = m_{\alpha,F}$. Al ser $F \subset K$ separable, se tiene que f es separable.

Sea $E = \mathrm{Desc}_F(f)$: es el cuerpo de descomposición de un polinomio en $F[X]$ separable, luego la extensión $F \subset E$ es de Galois, y por lo tanto es separable (y es finita). Por el teorema del elemento primitivo, se tiene $E = F(\beta)$ para algún $\beta \in E$. Sea $g = m_{\beta,F}$.

Por hipótesis g tiene una raíz $\gamma \in K$. Por el teorema de extensión 2.12, $E = F(\beta)$ y $F(\gamma) \subset K$ son F-isomorfos. Pero entonces $F(\gamma)$ es un cuerpo de descomposición para f sobre F que está incluido en K, de donde f se escinde sobre K, y K es una clausura algebraica de F.

Caso 2: $F \subset K$ es una extensión inseparable de cuerpos de característica p. Veamos que $K_F^P = \{\alpha \in K : \alpha^{p^n} \in F \text{ para algún } n \in \mathbb{N}\}$ es perfecto:

Si $\alpha \in K_F^P$, entonces $\alpha^{p^n} \in F$ para algún $n \in \mathbb{N}$, por lo tanto $X^{p^{n+1}} - \alpha^{p^n} \in F[X]$: por hipótesis tiene una raíz $\beta \in K$. Pero entonces:

$$0 = \beta^{p^{n+1}} - \alpha^{p^n} = (\beta^p - \alpha)^{p^n} \Rightarrow \beta^p = \alpha$$

Además $\beta^{p^{n+1}} = \alpha^{p^n} \in F$, de donde $\beta \in K_F^P$. Esto muestra que $(K_F^P)^p = K_F^P$, i.e. K_F^P es perfecto.

Como K_F^P es perfecto y $K_F^P \subset K$ es algebraica, entonces $K_F^P \subset K$ es separable (proposición 2.42). Si probamos que todo polinomio no constante $g \in K_F^P[X]$ tiene una raíz en K, entonces ya terminamos pues estamos en el caso 1.

Sea $g(X) = a_0 + a_1 X + \cdots + a_n X^n \in K_F^P[X]$ no constante. Sea $r \in \mathbb{N}$ suficientemente grande como para garantizar que $(a_i)^{p^r} \in F$ para todo $i = 0, \ldots, n$. Entonces:

$$g(X)^{p^r} = a_0^{p^r} + a_1^{p^r} X^{p^r} + \cdots + a_n^{p^r} X^{np^r} \in F[X]$$

Por hipótesis, $g(X)^{p^r}$ tiene una raíz $\alpha \in K$. Pero si $g(\alpha)^{p^r} = 0$, entonces debe ser $g(\alpha) = 0$, y α es raíz de f, terminando la demostración. $\square$

2.14. Solubilidad por radicales

En esta sección nos proponemos dar una condición necesaria y suficiente para que una ecuación $p(X) = 0$, donde p es un polinomio con coeficientes en un cuerpo de característica cero, sea resoluble por radicales. Como corolario, probaremos el famoso teorema de Abel, que dice que el polinomio general de grado $n \geqslant 5$ no es resoluble por radicales.

Para simplificar un poco el trabajo lo probaremos para polinomios sobre cuerpos de característica cero. Una demostración en general se encuentra, por ejemplo en [We], [Rot2] o [Rot3].

Definición. Una *extensión pura de tipo m* es una extensión $F \subset F(u)$ donde $u^m \in F$ para algún $m \geqslant 1$. Una extensión $F \subset K$ es *radical* si existe una torre de cuerpos (que llamaremos *torre radical*)

$$F = K_0 \subset K_1 \subset \cdots \subset K_t = K \tag{2.9}$$

donde las extensiones $K_i \subset K_{i+1}$ son puras para todo $i = 0, \ldots, t-1$.

Decimos que $f \in F[X]$ es *resoluble por radicales* si existe una torre como (2.9) tal que f se escinde sobre K_t (i.e. tal que $\mathrm{Desc}_F(f) \subset K_t$ [9]).

Observación 2.14.1.

1. Toda extensión radical es finita.
2. Si $F \subset E \subset K$ es una torre tal que $F \subset E$ y $E \subset K$ son extensiones radicales, entonces $F \subset K$ es una extensión radical.

Ejemplo 2.14.2. Intuitivamente, un polinomio es resoluble por radicales si podemos obtener sus ceros mediante extracciones sucesivas de raíces. Veamos un par de ejemplos.

Si $f = X^2 + bx + c \in \mathbb{Q}[X]$, entonces sus dos raíces son $\frac{-b \pm \sqrt{b^2-4c}}{2}$, donde $u = \sqrt{b^2-4c}$ denota una raíz de $X^2 - (b^2 - 4c)$. Entonces $\mathbb{Q} \subset \mathbb{Q}(u)$ es una extensión pura (pues $u^2 \in \mathbb{Q}$), y $\mathbb{Q}(u)$ es el cuerpo de descomposición de f sobre $\mathbb{Q}$.

Si $f = X^{10} - 5X^5 + 5 \in \mathbb{Q}[X]$, entonces sus diez raíces cumplen:

$$u^5 = \frac{5 \pm \sqrt{5}}{2} \quad \Rightarrow \quad u = \sqrt[5]{\frac{5 \pm \sqrt{5}}{2}}$$

Consideremos la torre de cuerpos:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{5}, \omega) \subset \mathbb{Q}(\sqrt{5}, \omega, \alpha) \subset \mathbb{Q}(\sqrt{5}, \omega, \alpha, \beta) = K$$

donde ω es una raíz quinta primitiva de la unidad, y:

$$\alpha = \sqrt[5]{\frac{5 + \sqrt{5}}{2}}, \qquad \beta = \sqrt[5]{\frac{5 - \sqrt{5}}{2}}$$

donde las raíces quintas fueron elegidas arbitrariamente (i.e. α y β corresponden a la elección de *una* raíz de $X^5 - \frac{5+\sqrt{5}}{2}$ y $X^5 - \frac{5-\sqrt{5}}{2}$ respectivamente). Es una torre de extensiones puras como en (2.9).

[9] Kronecker introdujo la siguiente terminología sugerente. Los elementos de K_t que no están en F se llaman *irracionalidades*; las que están en $\mathrm{Desc}_F(f)$ se dicen *naturales* y las que no *accesorias*.

Tenemos que todas las raíces de f son $\omega^i\alpha$ y $\omega^i\beta$ para $i = 1, \dots, 5$, de donde f se escinde sobre K. Por lo tanto el cuerpo de descomposición para f sobre $\mathbb{Q}$ está incluido en K, lo cual prueba que f es resoluble por radicales.

En este ejemplo, $\sqrt{5}$ y ω son irracionalidades accesorias: precisamos adjuntarlas para poder construir α y β que son irracionalidades naturales.

Observación 2.14.3. La definición de "polinomio resoluble por radicales" parece en un principio capturar en efecto lo que queremos definir, pero el ejemplo anterior puede hacer surgir un cierto escepticismo. Adjuntamos una raíz quinta primitiva de la unidad. Según la definición, no hay problema (la adjunción resulta obviamente una extensión pura). Pero una raíz quinta primitiva de la unidad es $e^{\frac{2\pi i}{5}} = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right)$. Ciertamente no parece ser el tipo de elementos que tenemos en mente adjuntar cuando hablamos de ecuaciones resolubles por *radicales*. Que haya una "expresión por radicales" para las raíces n-ésimas de la unidad es un resultado de Gauss, cuya demostración puede consultarse por ejemplo en [T], pp. 203-207.

Proposición 2.95. *Sea $F \subset K$ una extensión radical. Entonces se puede tomar una torre de cuerpos como en (2.9) donde $K_i \subset K_{i+1}$ es una extensión pura de tipo primo, para todo $i = 0, \dots, t-1$.*

Demostración. Basta probar que podemos reemplazar cada extensión pura de la torre dada por una torre donde cada cuerpo es una extensión pura de tipo primo del anterior. Sea entonces $k \subset k(u)$ una extensión pura de tipo m. Descompongamos $m = p_1 \dots p_k$ como producto de primos. Entonces

$$k \subset k(u^{m/p_1}) \subset k(u^{m/p_1 p_2}) \subset \cdots \subset k(u)$$

es una torre de extensiones puras tal que $k(u^{m/p_1 \dots p_i}) \subset k(u^{m/p_1 \dots p_{i+1}})$ es de tipo p_{i+1}. □

La siguiente proposición justifica que en característica cero podamos limitarnos a considerar extensiones radicales de Galois sin perder generalidad.

Proposición 2.96. *Sea $F \subset K$ una extensión radical. Sea N la clausura normal de la extensión. Entonces $F \subset N$ es radical.*

Demostración. Sea $F \subset K$ una extensión radical: existen $u_1, \dots, u_t$ tales que

$$F \subset F(u_1) \subset F(u_1, u_2) \subset \cdots \subset F(u_1, \dots, u_t) = K$$

es una torre radical. Sea E la clausura normal de $F \subset K$. Afirmo que

$$E = F\left(\{\sigma(u_i) : \sigma \in \mathrm{Gal}_F^E, i = 1, \dots, t\}\right)$$

En efecto, como vimos en la proposición 2.57,

$$E = \mathrm{Desc}_F\left(m_{u_1,F} \dots m_{u_t,F}\right) = F(\{\text{raíces de } m_{u_1,F} \dots m_{u_t,F}\})$$

La observación 2.9.1 nos da que $\{\text{raíces de } m_{u_i,F}\} = \{\sigma(u_i) : \sigma \in \mathrm{Gal}_F(m_{u_i,F})\}$. Veamos que también es igual a $\{\sigma(u_i) : \sigma \in \mathrm{Gal}_F^E\}$.

($\subset$): Podemos extender cada $\sigma \in \mathrm{Gal}_F(m_{u_i,F})$ a un $\tilde{\sigma} \in \mathrm{Gal}_F^E$ por el teorema 2.31 de extensión al cuerpo de descomposición, tomando a $m_{u_1,F} \dots m_{u_t,F} \in F[X]$ como polinomio.

($\supset$): Si $\sigma \in \mathrm{Gal}_F^E$, entonces σ se restringe a un F-isomorfismo $F(u_i) \to F(\sigma(u_i))$, luego por el corolario 2.13 u_i y $\sigma(u_i)$ deben ser raíces del mismo polinomio irreducible con coeficientes

en F. Por lo tanto $\sigma(u_i)$ es raíz de $m_{u_i,F}$.

Sea $B_i = F\left(\{\sigma(u_j) : 1 \leqslant j \leqslant i, \sigma \in \mathrm{Gal}_F^E\}\right)$. Escribamos $\mathrm{Gal}_F^E = \{1, \sigma, \tau, \dots\}$. Lo recién probado nos dice que $E = B_t$. Veamos que $F \subset E = B_t$ es radical, por inducción en t.

Si $t = 1$, se tiene que $E = B_1$. Afirmo que

$$F \subset F(u_1) \subset F(u_1, \sigma(u_1)) \subset F(u_1, \sigma(u_1), \tau(u_1)) \subset \cdots \subset B_1$$

es una torre radical para la extensión $F \subset B_1$. En efecto, si $u_1^m \in F$, entonces $\tau(u_1)^m = \tau(u_1^m) \in \tau(F) = F$, luego $\tau(u_1)^m \in F \subset F(u_1, \sigma(u_1))$.

Supongamos ahora que $F \subset B_i$ es radical. Se tiene que $B_{i+1} = B_i(\{\sigma(u_{i+1}) : \sigma \in \mathrm{Gal}_F^E\})$. Si probamos que $B_i \subset B_{i+1}$ es radical, entonces $F \subset B_{i+1}$ es radical por la observación 2.14.1.

Si $u_{i+1}^m \in B_i = F(u_1, \dots, u_i)$, entonces $\sigma(u_{i+1})^m = \sigma(u_{i+1}^m) \in F(\sigma(u_1), \dots, \sigma(u_i)) \subset B_i$.

Como $E = B_t$, esto termina la demostración. □

Observación 2.14.4. Si además F es de característica cero, entonces $F \subset N$ es de Galois, ya que toda extensión finita de un cuerpo de característica cero es separable (corolario 2.39) y en este caso la clausura normal es la clausura de Galois (corolario 2.58).

Lema 2.97. *Sea F de característica cero y consideremos la torre*

$$F = K_0 \subset K_1 \subset \cdots \subset K_t$$

donde $K_i \subset K_{i+1}$ es una extensión pura de tipo p_i primo para todo i. Supongamos que F contiene todas las raíces p_i-ésimas de la unidad para todo i.

a) Sea $K = K_t$. Si $F \subset K$ es normal, entonces Gal_F^K es un grupo resoluble.

b) Si $f \in F[X]$ es resoluble por radicales y $\mathrm{Desc}_F(f) \subset K_t$, entonces $\mathrm{Gal}_F(f)$ es resoluble.

Demostración. a) Sea $G_i = \mathrm{Gal}_{K_i}^K$ para todo $i = 0, \dots, t$. Se tiene

$$\mathrm{Gal}_F^K = G_0 > G_1 > \cdots > G_t = \{e\} \tag{2.10}$$

Se tiene que $K_1 = K_0(u)$, donde $u^{p_1} \in K_0$. Afirmo que K_1 es el cuerpo de descomposición de $f = X^{p_1} - u^{p_1}$ sobre K_0. En efecto, como $p_i \neq \mathrm{car}\, F$, las raíces de este polinomio son $u, \omega u, \dots, \omega^{p_1-1}u$ donde ω es una raíz p_1-ésima primitiva de la unidad. Como por hipótesis $\omega \in K_0$, se deduce lo afirmado.

Pero f es un polinomio separable, por lo tanto $K_0 \subset K_1$ es una extensión de Galois. Observar que $K_0 \subset K$ es de Galois porque K_0 es de característica cero. Por el teorema fundamental de la teoría de Galois aplicado a la torre $K_0 \subset K_1 \subset K$, se tiene que $\mathrm{Gal}_{K_1}^K \lhd \mathrm{Gal}_{K_0}^K$, i.e. $G_1 \lhd G_0$, y $G_0/G_1 \simeq \mathrm{Gal}_{K_0}^{K_1}$. Pero $p_1 = |K_1 : K_0| = |\mathrm{Gal}_{K_0}^{K_1}|$, por lo tanto $\mathrm{Gal}_{K_0}^{K_1} \simeq \mathbb{Z}_{p_1}$ cíclico de orden primo.

Repitiendo este argumento para cada i, se deduce que la serie (2.10) es una serie abeliana para Gal_F^K .

b) Por la proposición anterior podemos suponer que $F \subset K_t$ es normal. Por la parte anterior se tiene que $\mathrm{Gal}_F^{K_t}$ es resoluble.

Sea $E = \mathrm{Desc}_F(f)$. Tenemos una torre $F \subset E \subset K_t$. De nuevo, como F es de característica cero y $F \subset E$, $F \subset K_t$ son normales, entonces son de Galois. Por el teorema fundamental de la teoría de Galois, deducimos que $\mathrm{Gal}_F^{K_t}/\mathrm{Gal}_E^{K_t} \simeq \mathrm{Gal}_F^E$. Entonces Gal_F^E es cociente de un grupo resoluble, por lo tanto es resoluble.

□

Teorema 2.98. *Sea F de característica cero, $f \in F[X]$. Si f es resoluble por radicales entonces su grupo de Galois es resoluble.*

Demostración. Como f es resoluble por radicales, existe una torre radical

$$F = K_0 \subset K_1 \subset \cdots \subset K_t$$

tal que $E \coloneqq \mathrm{Desc}_F(f) \subset K_t$. Sea $m = p_1 \dots p_t$. Sea $E^\star \coloneqq \mathrm{Desc}_E(X^m - 1)$, i.e. $E^\star = E(\Omega)$ donde Ω es el conjunto de todas las raíces m-ésimas de la unidad.

Sea $F^\star = F(\Omega)$. Entonces $F^\star$ contiene todas las raíces m-ésimas de la unidad, luego contiene todas las raíces p_i-ésimas de la unidad. Además se tiene que $E^\star = \mathrm{Desc}_{F^\star}(f)$. Tenemos la torre radical

$$F^\star = K_0(\Omega) \subset K_1(\Omega) \subset \cdots \subset K_t(\Omega)$$

que muestra que $f \in F^\star[X]$ es resoluble por radicales, y como $E \subset K_t$, entonces $E^\star \subset K_t(\Omega)$. Estamos en las hipótesis del lema anterior: tenemos pues que $\mathrm{Gal}_{F^\star}(f) = \mathrm{Gal}_{F^\star}^{E^\star}$ es resoluble.

Consideremos la torre $F \subset F^\star \subset E^\star$. Recordando que F es de característica cero, tenemos que $F \subset E^\star$ es de Galois pues $E^\star = \mathrm{Desc}_F(f \cdot (X^m - 1))$, y $F \subset F^\star$ también es de Galois, por lo tanto por el teorema fundamental de la teoría de Galois, se tiene que $\mathrm{Gal}_{F^\star}^{E^\star} \lhd \mathrm{Gal}_F^{E^\star}$, y:

$$\frac{\mathrm{Gal}_F^{E^\star}}{\mathrm{Gal}_{F^\star}^{E^\star}} \simeq \mathrm{Gal}_F^{F^\star}$$

Tenemos que $\mathrm{Gal}_{F^\star}^{E^\star}$ es resoluble; afirmo que $\mathrm{Gal}_F^{F^\star}$ también lo es. En efecto, es abeliano (el grupo de Galois del cuerpo de descomposición de $X^n - 1$ sobre un cuerpo de característica cero es abeliano: es el ejercicio 56). Por lo tanto $\mathrm{Gal}_F^{E^\star}$ es resoluble (es una extensión de grupos resolubles).

Ahora consideramos la torre $F \subset E \subset E^\star$. De nuevo, $F \subset E$ y $F \subset E^\star$ son de Galois, luego

$$\frac{\mathrm{Gal}_F^{E^\star}}{\mathrm{Gal}_E^{E^\star}} \simeq \mathrm{Gal}_F^E$$

y en conclusión Gal_F^E es resoluble por ser cociente de un grupo resoluble. □

Ya podemos probar que, para cualquier $n \geqslant 5$, no es posible dar una fórmula general que mediante sumas, productos y extracción de raíces exprese los ceros de cualquier polinomio de grado n:

Corolario 2.99 (Abel)**.** *El polinomio general de grado n sobre un cuerpo F (de característica cero) no es resoluble por radicales, para $n \geqslant 5$.*

Demostración. Ya vimos en el corolario 2.79 que el grupo de Galois del polinomio general de grado n es S_n, que ya probamos (corolario 1.83) que no es resoluble para $n \geqslant 5$. □

Observación 2.14.5. El teorema anterior vale en característica positiva. Esta observación justifica los paréntesis del anterior corolario.

Nos dirigimos ahora a probar el recíproco del teorema anterior.

Lema 2.100. *Sea $F \subset K$ una extensión de Galois de grado primo p. Si F contiene una raíz p-ésima primitiva de la unidad, entonces $F \subset K$ es una extensión pura de tipo p.*

Demostración. Como $|K : F| = p$, el grupo de Galois Gal_F^K tiene orden p, y por lo tanto es cíclico. Sea σ un generador de Gal_F^K.

Por el teorema de Lagrange, $\sigma^p = \mathrm{id}$, de donde σ es raíz del polinomio $X^p - 1$. Además σ no es raíz de ningún polinomio no nulo de menor grado que p. En efecto, si $f = a_0 + a_1 X + \cdots + a_n X^n \in F[X]$ con $n < p$ es un polinomio no nulo tal que $f(\sigma) = 0$, entonces

$$a_0 \mathrm{id} + a_1 \sigma + \cdots + a_n \sigma^n = 0$$

es una combinación lineal nula no trivial de $\{\mathrm{id}, \sigma, \ldots, \sigma^{p-1}\}$ que son morfismos de cuerpos diferentes, contradiciendo la independencia lineal de caracteres (corolario 2.46).

Observar que $\sigma : K \to K$ es una F-transformación lineal. En efecto, si $a \in F$ y $v \in K$, $\sigma(au) = \sigma(a)\sigma(u) = a\sigma(u)$ pues $\sigma|_F = \mathrm{id}$.

Tenemos entonces que $X^p - 1$ es el polinomio mínimo (en el sentido de álgebra lineal) de la F-transformación lineal $\sigma : K \to K$. Sabemos de álgebra lineal que las raíces del polinomio mínimo de una transformación lineal son los valores propios de σ, por lo tanto todas las raíces p-ésimas de la unidad son raíces de $X^p - 1$.

Por hipótesis, F contiene una raíz p-ésima primitiva de la unidad, llamémosle ω. Las raíces p-ésimas de la unidad forman un grupo, por lo tanto $\omega^{-1} \in F$ también es una raíz p-ésima de la unidad (de hecho, también es primitiva, porque invertir es un automorfismo en un grupo abeliano, y un automorfismo lleva generadores en generadores). Existe entonces un vector propio $z \in E$ de σ tal que $\sigma(z) = \omega^{-1} z$. Observar que $z \notin F$ pues $z \notin \mathrm{Fix}(\mathrm{Gal}_F^K) = F$, ya que $F \subset K$ es de Galois. Tenemos entonces:

$$\sigma(z^p) = (\sigma(z))^p = (\omega^{-1})^p z^p = z^p$$

de donde $z^p \in \mathrm{Fix}(\mathrm{Gal}_F^K) = F$.

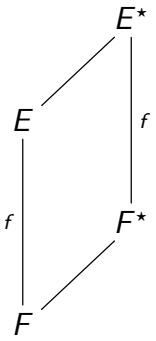
Afirmo que $K = F(z)$, terminando la demostración. Tenemos la torre $F \subset F(z) \subset K$, entonces por transitividad de grados es

$$|K : F| = |K : F(z)||F(z) : F|$$

El lado izquierdo vale p. En el lado derecho, $|F(z) : F| \neq 1$ pues $z \notin F$. En conclusión, como p es primo, debe ser $|K : F(z)| = 1$, i.e. $K = F(z)$. □

Lema 2.101 (Irracionalidades accesorias)**.** *Sea F cuerpo, $f \in F[X]$, $E = \mathrm{Desc}_F(f)$. Si $F \subset F^\star$ es un una extensión de cuerpos y $E^\star = \mathrm{Desc}_{F^\star}(f)$ es tal que $E \subset E^\star$, entonces la restricción*

$\mathrm{Gal}_{F^\star}^{E^\star} \to \mathrm{Gal}_F^E$, $\sigma \mapsto \sigma|_E$ *es un homomorfismo inyectivo.*



Demostración. Tenemos que $E = F(\Omega)$ y $E^\star = F^\star(\Omega)$ donde Ω es el conjunto de raíces de f. Sea $\sigma \in \mathrm{Gal}_{F^\star}^{E^\star}$.

σ permuta Ω y deja fijo $F^\star$, por lo tanto deja fijo F. Por lo tanto $\sigma|_E \in \mathrm{Gal}_F^E$.

La restricción es un morfismo. Para ver que es inyectivo, sea $\sigma \in \mathrm{Gal}_{F^\star}^{E^\star}$ tal que $\sigma|_E = \mathrm{id}$. En este caso, σ deja fijo $F^\star$ y deja fijo $E = F(\Omega)$, por lo tanto deja fijo $F^\star(\Omega) = E^\star$, i.e. $\sigma = \mathrm{id}$. □

Teorema 2.102. *Sea F cuerpo de característica cero. Sea $F \subset E$ extensión de Galois tal que Gal_F^E es resoluble. Entonces existe una extensión radical de F que contiene a E.*

En particular, si $f \in F[X]$ tiene grupo de Galois $\mathrm{Gal}_F(f)$ resoluble entonces es resoluble por radicales.

Demostración. Sea $G = \mathrm{Gal}_F^E$. Como G es finito y resoluble, entonces G tiene una serie de composición con factores de orden primo. En particular, el penúltimo término de la serie es un subgrupo normal H de índice primo. Sea $p = |G : H|$. Sea ω una raíz p-ésima primitiva de la unidad, que existe en el cuerpo de descomposición de $X^p - 1$ sobre F pues F tiene característica cero.

1er **caso**: $\omega \in F$. Hacemos inducción en $|E : F|$. El caso base es trivial.

Tenemos que $\mathrm{Fix}(H) \subset E$ es una extensión de Galois, y $\mathrm{Gal}_{\mathrm{Fix}(H)}^E = H$ es resoluble pues es un subgrupo de G que es resoluble.

Ahora, $|E : \mathrm{Fix}(H)| < |E : F|$, entonces por hipótesis de inducción obtenemos una torre radical

$$\mathrm{Fix(H)} = R_0 \subset R_1 \subset \cdots \subset R_t$$

tal que $E \subset R_t$.

Por otro lado, como $H \lhd G$ y $|G : H| = p$, por el teorema fundamental de la teoría de Galois $F \subset \mathrm{Fix}(H)$ es una extensión de Galois de grado p.

Estamos en las hipótesis del lema 2.100: se tiene que $\mathrm{Fix}(H) = F(z)$ donde $z^p \in F$, i.e. $F \subset \mathrm{Fix}(H)$ es una extensión pura, por lo tanto es radical, y $\mathrm{Fix}(H) \subset R_t$ también lo es, por lo tanto $F \subset R_t$ es una extensión radical de F que contiene a E.

2° **caso**: $\omega \notin F$. Sea $F^\star = F(\omega)$, $E^\star = E(\omega)$.

Afirmación: $F \subset E^\star$ es de Galois.

Demostración: Como $F \subset E$ es de Galois, es el cuerpo de descomposición de un polinomio separable $f \in F[X]$. Si $f = X^p - 1$ entonces $E = E^\star$ y ya está. Si $f \neq X^p - 1$, entonces

$E^\star$ es el cuerpo de descomposición de $f \cdot (X^p - 1) \in F[X]$. Este polinomio es separable pues $f \neq X^p - 1$ y $X^p - 1$ es separable e irreducible, ya que car $F = 0$ y $\omega \notin F$.

Tenemos entonces $F \subset F^\star \subset E^\star$, con $F \subset E^\star$ de Galois, por lo tanto $F^\star \subset E^\star$ es de Galois (teorema fundamental de la teoría de Galois).

Sea $G^\star = \mathrm{Gal}_{F^\star}^{E^\star}$. Por el lema 2.101, hay un monomorfismo de grupos $\psi : G^\star \to G$. Por lo tanto $G^\star$ es isomorfo a un subgrupo de G que es resoluble, de donde $G^\star$ es resoluble.

Como $\omega \in F^\star$, por el caso 1 existe una torre radical

$$F^\star = R_0^\star \subset R_1^\star \subset \cdots \subset R_m^\star$$

con $E^\star \subset R_m^\star$. Pero $F^\star = F(\omega)$ es una extensión pura, de donde $F \subset R_m^\star$ es una extensión radical tal que $E \subset R_m^\star$, pues $E \subset E^\star \subset R_m^\star$. □

Observación 2.14.6. El teorema anterior *no* vale en característica positiva.

Niccolò Fontana Tartaglia y Girolamo Cardano probaron (1535-1545) que un polinomio de grado 3 era resoluble por radicales, dando una fórmula explícita. En 1545 Luigi Ferrari probó que un polinomio de grado 4 era resoluble por radicales, también dando una fórmula. Estas fórmulas son aburridas de demostrar, sin embargo podemos demostrar ahora que existen fórmulas por radicales para las raíces de polinomios de grado 3 y 4:

Corolario 2.103. *Si F es un cuerpo de característica cero, entonces todo polinomio $f \in F[X]$ de grado $\leqslant 4$ es resoluble por radicales.*

Demostración. El grupo de Galois de f es un subgrupo de S_4 que es resoluble (ejemplo 1.11.7), y por lo tanto es resoluble. □

Capítulo 3

Representaciones de grupos finitos

3.1. Definiciones básicas

Notación. Si V es un espacio vectorial, notaremos

$$\mathrm{GL}(V) := \mathrm{Aut}(V) = \{\text{transformaciones lineales } V \to V \text{ invertibles}\}$$

Definición. Sea G grupo. Una *representación lineal* o simplemente *representación* de G es un par (V, ρ) [1] donde V es un k-espacio vectorial y $\rho : G \to \mathrm{GL}(V)$ es un morfismo de grupos. El *grado* de la representación es $\dim_k V$.

Una *representación matricial* de grado n de G sobre un cuerpo k es un morfismo de grupos $\rho : G \to \mathrm{GL}_n(k)$.

Si V es un espacio vectorial tal que (V, ρ) es una representación de un grupo G, decimos que V es un *G-módulo*.

Si $k = \mathbb{C}$ diremos que (V, ρ) es una representación *compleja*.

Notación. A veces notaremos ρ_g en vez de $\rho(g)$ para alivianar la notación.

Observación 3.1.1. Eligiendo una base, i.e. eligiendo un isomorfismo $\mathrm{GL}(V) \simeq \mathrm{GL}_n(k)$, es lo mismo dar una representación lineal finita que dar una representación matricial.

Ejemplo 3.1.2. Veamos cómo lucen las representaciones de $\mathbb{Z}_m = \langle a \rangle$ de grado n:

Si $\rho : \mathbb{Z}_m \to \mathrm{GL}_n(\mathbb{C})$ es morfismo de grupos, entonces $\rho(a^i) = A^i$ para algún $A \in \mathrm{GL}_n(\mathbb{C})$.

Afirmación: ρ es representación si y sólo si $A^m = I_n$.

Demostración: ($\Rightarrow$) $A^m = \rho(a^m) = \rho(e) = I_n$.

($\Leftarrow$) Sean $0 \leqslant r, k < m$.

Si $0 \leqslant r + k < m$ entonces $\rho(a^r a^k) = \rho(a^{r+k}) = A^{r+k} = A^r A^k$.

Si $r + k \geqslant m$ entonces

$$\rho(a^r a^k) = \rho(a^m a^{r+k-m}) = \rho(a^{r+k-m}) \overset{r+k\leq 2m}{=} A^{r+k-m} = A^{r+k-m} A^m = A^{r+k}$$

Comparar la siguiente proposición con 1.48.

Proposición 3.1. *"Es lo mismo" dar una representación de G en V que dar una acción $\cdot : G \times V \to V$ tal que $g \cdot -$ sea lineal para todo $g \in G$.*

[1] A veces sobreentenderemos el espacio vectorial o el morfismo, diciendo que V o que ρ es una representación de G.

Demostración. La relación fundamental es $g \cdot - = \rho(g)$.

($\Rightarrow$) Consideramos $\cdot : G \times V \to V$, $(g, v) \mapsto \rho(g)(v)$. Es lineal pues $\rho(g)$ lo es, para todo $g \in G$.

Es una acción: $e \cdot v = \rho(e)(v) = v$ para todo $v \in V$;
$g_1 g_2 \cdot v = \rho(g_1 g_2)(v) = \rho(g_1)(\rho(g_2)(v)) = g_1 \cdot (g_2 \cdot v)$ para todo $g_1, g_2 \in G$, $v \in V$.

($\Leftarrow$) Definimos $\rho : G \to \mathrm{GL}(V)$ mediante $\rho(g)(v) = g \cdot v$ para todo $g \in G$, $v \in V$.

Está bien definido, i.e. $\rho(g) \in \mathrm{GL}(V)$ para todo $g \in G$, pues la acción es lineal.

Es morfismo de grupos: $\rho(g_1 g_2)(v) = g_1 g_2 \cdot v = g_1 \cdot (g_2 \cdot v) = \rho(g_1)(\rho(g_2)(v))$ para todo $g_1, g_2 \in G$, $v \in V$. □

Definición. Sean (V_1, ρ_1) y (V_2, ρ_2) representaciones de un grupo G. Decimos que $\varphi : V_1 \to V_2$ es un *morfismo de G-módulos*, o *G-mapa*, si es lineal y respeta la acción de G, i.e. $\varphi(g \cdot v) = g \cdot \varphi(v)$ para todo $g \in G$, $v \in V_1$.

Equivalentemente, si $\varphi(\rho_1(g)(v)) = \rho_2(g)(\varphi(v))$ para todo $g \in G$, $v \in V_1$. Es decir, si el siguiente diagrama conmuta para todo $g \in G$:

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

Dos representaciones son *isomorfas*, o *equivalentes* si existe un morfismo de G-módulos entre ellas que sea un isomorfismo lineal, i.e. si existe un *isomorfismo de G-módulos*.

Observación 3.1.3.
- Si un G-mapa es invertible, su inversa es un G-mapa; la composición de G-mapas es un G-mapa, etc.
- Para un morfismo de G-módulos se tiene $\varphi \circ \rho_1(g) = \rho_2(g) \circ \varphi$ para todo $g \in G$. Si además φ es un isomorfismo, entonces se tiene $\rho_2(g) = \varphi \circ \rho_1(g) \circ \varphi^{-1}$ para todo $g \in G$.
- Problema básico de la teoría de representaciones: clasificar las representaciones de un grupo G a menos de isomorfismo (i.e. conjugación por un isomorfismo).

Definición. Sea (V, ρ) una representación. Una *subrepresentación* es la restricción $(W, \rho|_W)$ donde W es un subespacio vectorial G-invariante, i.e. $\rho(g)(W) \subset W$ para todo $g \in G$. De esta manera, una subrepresentación es una representación.

Una representación es *irreducible* si no admite subrepresentaciones propias, i.e. si V no tiene subespacios propios G-invariantes.

Los siguientes ejemplos acarrean verificaciones sencillas que se dejan como ejercicio para el lector.

Ejemplo 3.1.4. Sea G grupo.

- La *representación trivial* es tal que $\rho(g) = \mathrm{id}$ para todo $g \in G$.
- Si (V_1, ρ_1) y (V_2, ρ_2) son representaciones de G, la suma directa $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$ es una representación.

- Si (V_1, ρ_1) y (V_2, ρ_2) son representaciones de G sobre k, el producto tensorial $(V_1 \otimes_k V_2, \rho_1 \otimes \rho_2)$ es una representación.
- Si (V, ρ) es una representación de G y W es una subrepresentación, el cociente V/W es una representación, con $g \cdot \overline{v} = \overline{g \cdot v}$.
- Si (V, ρ) es una representación, el dual V^* también es una representación, con la acción $G \times V^* \to V^*$, $g \cdot f \mapsto f(g^{-1} \cdot -)$.

Definición. Una representación es *completamente reducible* si se descompone como suma directa de subrepresentaciones irreducibles; de lo contrario es *indescomponible*.

Observación 3.1.5. Al contrario que con espacios vectoriales y como con módulos, si $W \subset V$ es una subrepresentación, no necesariamente se tiene $V = W \oplus V/W$: una representación puede no ser irreducible y ser indescomponible, pues una subrepresentación puede no tener un complemento. Sin embargo, el teorema de Maschke más adelante nos va a dar condiciones suficientes para que esto no suceda.

A continuación presentamos una tercera estructura equivalente a la de representación lineal y a la de representación matricial.

Definición. Sea R anillo conmutativo. Una *R-álgebra* A es un anillo con una estructura de R-módulo compatible, i.e. tal que $a(r_1 r_2) = (ar_1)r_2 = r_1(ar_2)$ para todo $a \in A$, $r_1, r_2 \in R$.

De esta manera, un álgebra es una estructura algebraica con tres operaciones: suma, producto por escalar y producto. El ejemplo arquetípico es el siguiente:

Ejemplo 3.1.6. Si R es un anillo conmutativo, el anillo de matrices $M_n(R)$ es una R-álgebra.

Observación 3.1.7. Recordemos que si R es un anillo y X es un conjunto, podemos pensar al R-módulo libre de base X, notado $R[X]$, como el R-módulo de sumas formales:

$$R[X] = \left\{ \sum_{\substack{g \in G \\ \text{finita}}} \alpha_x x : \quad \alpha_x \in R \quad \forall x \in X \right\}$$

Si G es un grupo y consideramos $R[G]$, el R-módulo libre de base G, podemos usar el producto de G para introducir un producto en $R[G]$ de tal manera que sea una R-álgebra:

Definición. Sean G grupo, R anillo conmutativo. El *álgebra de grupo* $R[G]$ es el R-módulo libre de base G, en el que consideramos la estructura de R-álgebra dada por el producto siguiente: si $\lambda_g, \mu_h \in R$ para todo $g, h \in G$,

$$\left(\sum_{\substack{g \in G \\ \text{finita}}} \lambda_g g \right) \left(\sum_{\substack{h \in G \\ \text{finita}}} \mu_h h \right) = \sum_{g,h \in G} \lambda_g \mu_h gh$$

Proposición 3.2. *Sea k cuerpo. "Es lo mismo" dar una representación sobre k (de grado n) que dar un $k[G]$-módulo a izquierda (libre de rango n).*

Demostración. Si V es un $k[G]$-módulo a izquierda, $\rho : G \to \mathrm{GL}(V)$, $\rho(g)(v) = gv$ define una representación de G sobre k.

Recíprocamente, si $\rho : G \to \mathrm{GL}(V)$ es una representación, podemos dotar a V de una estructura de $k[G]$-módulo a izquierda de la siguiente manera:

$$\left(\sum_{\substack{g\in G\\ \text{finita}}} \lambda_g g\right) v = \left(\sum_{\substack{g\in G\\ \text{finita}}} \lambda_g \rho(g)(v)\right) \qquad \square$$

De esta manera, muchos teoremas sobre representaciones pueden traducirse a teoremas acerca de los $k[G]$-módulos. Por ejemplo, una subrepresentación es un $k[G]$-submódulo; un G-mapa es un morfismo de $k[G]$-módulos. No será éste el punto de vista que adoptemos en general.

Ejemplo 3.1.8. Recordemos que todo anillo R es un módulo sobre sí mismo mediante la acción regular, $r \cdot s = rs$ para todo $r, s \in R$.

Sea k cuerpo. Entonces $k[G]$ es un módulo sobre sí mismo: la *representación regular* de G sobre k es la representación asociada a la estructura de $k[G]$-módulo de $k[G]$.

Escrita como representación, es la representación $\rho : G \to \mathrm{GL}(k[G])$ definida como $\rho(g)(v) = gv$. Más explícitamente:

$$\rho(g)\left(\sum_{\substack{h\in G\\ \text{finita}}} \mu_h h\right) = \sum_{\substack{h\in G\\ \text{finita}}} \mu_h gh$$

Más sucintamente, podemos definir $\rho(g)$ explicitándolo en la base de $k[G]$ y extendiendo por linealidad: $\rho(g)(h) = gh$ para todo $g, h \in G$.

En realidad, la recién descrita es la representación regular *a izquierda*, pues estamos considerando la acción regular a izquierda $r \cdot s = rs$. La representación regular *a derecha* es la que proviene de la acción regular a derecha $r \cdot s = sr^{-1}$.

Lema 3.3. *Sea G grupo finito, R anillo conmutativo. Sea $\mathbf{cl}(G)$ el conjunto de clases de conjugación de G. Sea $e_c = \sum_{g\in c} g$ para cada $c \in \mathbf{cl}(G)$. Entonces el centro de $R[G]$ es el submódulo generado por los elementos de la forma*

$$\sum_{c\in \mathbf{cl}(G)} \lambda_c e_c, \quad \lambda_c \in R$$

En otras palabras, los e_c, $c \in \mathbf{cl}(G)$ son una base de $Z(R[G])$.

Demostración. Como G es base de $R[G]$, un elemento $x = \sum_{g\in G} \lambda_g g \in R[G]$ arbitrario está en el centro de $R[G]$ si y sólo si conmuta con todos los elementos $h \in G$, i.e. si $hxh^{-1} = x$ para todo $h \in G$. Entonces, si $h \in G$:

$$\begin{aligned} x \in Z(R[G]) &\iff h\left(\sum_{g\in G} \lambda_g g\right) h^{-1} = \sum_{g\in G} \lambda_g g \\ &\iff \sum_{g\in G} \lambda_g hgh^{-1} = \sum_{g\in G} \lambda_g g \\ &\iff \sum_{g\in G} \lambda_{g^{-1}hg} g = \sum_{g\in G} \lambda_g g \end{aligned}$$

usando que $g \mapsto hgh^{-1}$ es biyectiva, de inversa $g \mapsto h^{-1}gh$. Pero esto implica que la asociación $g \mapsto \lambda_g$ es constante en las clases de conjugación, por lo tanto el centro de $R[G]$ está formado por los elementos de la forma

$$\sum_{c \in \mathbf{cl}(G)} \lambda_c e_c, \quad \lambda_c \in R$$ □

Ejercicios

Ej. 57 — La representación $\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$ dada por $t \cdot (x, y) = (x, x + ty)$ no es irreducible pero es indescomponible.

Ej. 58 — Generalizando la representación dual, si V, W son representaciones de un grupo G sobre k, entonces $\mathrm{Hom}_k(V, W)$ es una representación, con la acción

$$G \times \mathrm{Hom}_k(V, W) \to \mathrm{Hom}_k(V, W), \quad (g \cdot f)(v) = g \cdot f(g^{-1} \cdot v)$$

Ej. 59 — Sea G grupo finito, V una representación de G. Para todo $v \in V$ existe una subrepresentación $W \subset V$ de grado finito tal que $v \in W$.

3.2. Primeros teoremas

Proposición 3.4. *Sea $f : V \to W$ un morfismo de G-módulos. Entonces* $\ker f \subset V$ *e* $\operatorname{Im} f \subset W$ *son G-invariantes.*

Demostración. Si $v \in \ker f$, entonces $f(g \cdot v) = g \cdot f(v) = g \cdot 0 = 0 \Rightarrow g \cdot v \in \ker f$.
Si $w \in \operatorname{Im} f \Rightarrow w = f(u)$ para algún $u \in V$. Entonces $g \cdot w = g \cdot f(u) = f(g \cdot u) \in \operatorname{Im} f$. □

Lema 3.5 (Schur)**.** *Si V, W son representaciones irreducibles de G y $f : V \to W$ es un G-mapa, entonces:*

1. *$f = 0$ o f es un isomorfismo,*
2. *Si $V = W$ y $k = \mathbb{C}$ (o k es algebraicamente cerrado), entonces $f = \lambda I$ para algún $\lambda \in k$.*

Demostración. 1. $\ker f \subset V$ es G-invariante, entonces como V es irreducible:

$\ker f = V \Rightarrow f = 0$, o

$\ker f = \{0\}$ y f es inyectiva. Como $\operatorname{Im} f \subset W$ es G-invariante y W es irreducible, entonces $\operatorname{Im} f = \{0\} \Rightarrow f = 0$ o $\operatorname{Im} f = W$, y f es sobreyectiva, luego un isomorfismo.

2. Como $\mathbb{C}$ es algebraicamente cerrado, existe $\lambda \in \mathbb{C}$ valor propio de f. Sea $v_0 \neq 0$ un vector propio de valor propio λ.

   Probemos que $f = \lambda I$. Para esto consideremos la transformación lineal $f_\lambda : V \to V$, $f_\lambda(v) = f(v) - \lambda v$. Veamos que $f_\lambda = 0$, en cuyo caso terminamos.

   f_λ es un G-mapa:

$$g \cdot f_\lambda(v) = g \cdot f(v) - g \cdot \lambda v = f(g \cdot v) - \lambda g \cdot v = f_\lambda(g \cdot v)$$

   Como $f_\lambda(v_0) = 0$ y $v_0 \neq 0$, como V es irreducible debe ser $\ker f_\lambda = V$, i.e. $f_\lambda = 0$. □

El siguiente teorema nos da condiciones suficientes para que toda subrepresentación tenga un complemento: el grupo debe ser finito y la característica del cuerpo debe ser nula o no dividir al orden del grupo. En realidad se puede probar que estas condiciones son también necesarias.

Recordemos primero que una *proyección* de un espacio vectorial V sobre un subespacio W es una transformación lineal $T : V \to W$ tal que $T|_W = \mathrm{id}$. Es equivalente dar una proyección que dar una transformación lineal $T : V \to V$ tal que $T^2 = T$, tomando como subespacio a $\operatorname{Im} T$.

Teorema 3.6 (Maschke)**.** *Sea G grupo finito, (V, ρ) una representación de G. Si car $k = 0$ o car $k \nmid |G|$, entonces todo subespacio G-invariante W posee (al menos) un complemento G-invariante. Es decir, existe U subespacio G-invariante tal que $V = W \oplus U$.*

Demostración. Basta encontrar una proyección p_0 de V sobre W que sea un G-mapa, pues entonces $\ker p_0$ e $\operatorname{Im} p_0$ son subespacios G-invariantes, y $V = \ker p_0 \oplus \operatorname{Im} p_0 = \ker p_0 \oplus W$.

Sea $q : V \to V$ una proyección de V sobre W, i.e. q es una transformación lineal tal que $\operatorname{Im} q = W$ y $q|_W = \mathrm{id}$. Definimos $p_0 : V \to V$ como

$$p_0 = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ q \circ \rho_{g^{-1}}$$

Aquí hemos usado la hipótesis de que $|G|$ es finito, y además es invertible por las hipótesis sobre car k. Veamos que p_0 es la proyección que estamos buscando.

$\operatorname{Im} p_0 = W$:

$(\subset)$: $\rho_g \circ q \circ \rho_{g^{-1}}(v) = \rho_g(q(\rho_{g^{-1}}(v))) \in W$, pues como q es proyección, $q(\rho_{g^{-1}}(v)) \in W$, luego como W es G-invariante, $\rho_g(q(\rho_{g^{-1}}(v))) \in W$, para todo $g \in G, v \in V$, luego $p_0(v) \in W$ para todo $v \in V$, i.e. $\operatorname{Im} p_0 \subset W$.

$(\supset)$ Dado $w \in W$,

$$\begin{aligned} p_0(w) &= \frac{1}{|G|} \sum_{g \in G} \rho_g q(\rho_{g^{-1}}(w)) \overset{q|_W = \mathrm{id}}{=} \frac{1}{|G|} \sum_{g \in G} \rho_g \rho_{g^{-1}}(w) \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_{gg^{-1}}(w) = \frac{1}{|G|} \sum_{g \in G} w = \frac{1}{|G|} |G|\, w = w \end{aligned}$$

luego $w \in \operatorname{Im} p_0 \quad \forall w \in W \Rightarrow W \subset \operatorname{Im} p_0$. Más aún, $p_0|_W = \mathrm{id}$: hemos demostrado que p_0 es una proyección sobre W.

Veamos que p_0 es un G-mapa, concluyendo la demostración. Dado $v \in V$, $g_0 \in G$:

$$\begin{aligned} p_0(\rho_{g_0}(v)) &= \frac{1}{|G|} \sum_{g \in G} \rho_g \, q \, \rho_{g^{-1}}(\rho_{g_0}(v)) \\ &= \frac{1}{|G|} \sum_{g \in G} \overbrace{\rho_{g_0} \rho_{g_0{}^{-1}}}^{\mathrm{id}} \rho_g \, q \, \rho_{g^{-1} g_0}(v) \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_{g_0} \rho_{g_0{}^{-1} g} \, q \, \rho_{g^{-1} g_0}(v) \\ &= \rho_{g_0} \left(\frac{1}{|G|} \sum_{g \in G} \rho_{g_0{}^{-1} g} \, q \, \rho_{g^{-1} g_0}(v) \right) \\ &\overset{*}{=} \rho_{g_0} \left(\frac{1}{|G|} \sum_{h \in G} \rho_h \, q \, \rho_{h^{-1}}(v) \right) \\ &= \rho_{g_0}(p_0(v)) \end{aligned}$$

La igualdad * se deduce de que $g_0^{-1} g = h$ es una biyección de G, i.e. cuando g se mueve por todo G, también $g_0^{-1} g$ recorre todo G. □

Adoptando la perspectiva de los módulos sobre el álgebra de grupo, el teorema de Maschke dice que si G es un grupo finito tal que car $k = 0$ o car $k \nmid |G|$, entonces el álgebra de grupo $k[G]$ es un anillo semisimple.

Corolario 3.7 (Completa reducibilidad)**.** *Sea G grupo finito, V una representación de G de grado finito tal que car $k = 0$ o car $k \nmid |G|$. Entonces V es completamente reducible.*

Demostración. Por inducción en $n = \dim_k V$. Supongo que vale para espacios de dimensión menor que n.

Si V es irreducible ya está.

Si no, tiene un subespacio propio G-invariante, $U \subset V$.

$\dim_k U < n$, luego por hipótesis de inducción existen subrepresentaciones irreducibles $U_1, \dots, U_r \subset U$ tales que $U = U_1 \oplus \cdots \oplus U_r$.

Además por el teorema de Maschke U tiene un complemento U', que también cumple $\dim_k U' < n$, luego por hipótesis de inducción existen subrepresentaciones irreducibles $U'_1, \dots, U'_k \subset U'$ tales que $U' = U'_1 \oplus \cdots \oplus U'_k$.

Pero entonces $V = U \oplus U' = U_1 \oplus \cdots \oplus U_r \oplus U'_1 \oplus \cdots \oplus U'_k$ donde cada uno de los subespacios es G-invariante e irreducible, luego V es completamente reducible. □

Podemos encontrar distintas descomposiciones de V en suma directa de subrepresentaciones irreducibles. Pero partiendo de una descomposición en irreducibles y juntando todas las representaciones irreducibles equivalentes en un sólo sumando, obtenemos una descomposición canónica, llamada *descomposición isotípica*.

Notación. $V^{\oplus n} := \overbrace{V \oplus \cdots \oplus V}^{n \text{ veces}}$.

Teorema 3.8 (Descomposición isotípica)**.** *Sean V, W representaciones complejas de un grupo finito G. Sean*

$$V = V_1 \oplus \cdots \oplus V_n, \quad W = W_1 \oplus \cdots \oplus W_n$$

descomposiciones en irreducibles.[2] *Escribamos ahora*

$$V = V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k}, \qquad \text{donde } V_i \not\simeq V_j \text{ si } i \neq j \tag{3.1}$$

$$W = W_1^{\oplus m_1} \oplus \cdots \oplus W_k^{\oplus m_k}, \quad \text{donde } W_i \not\simeq W_j \text{ si } i \neq j \tag{3.2}$$

[2] *Entonces si $\varphi : V \to W$ es un G-mapa, se tiene que φ respeta la descomposición: para cada i, $\varphi(V_i^{\oplus n_i}) \subset W_j^{\oplus m_j}$ para algún j. En particular, esta descomposición en irreducibles es única a menos de isomorfismo.*

Demostración. En las descomposiciones (3.1) y (3.2) podemos reordenar los sumandos de tal manera que si V_i es isomorfo a algún W_j, entonces $i = j$. Explícitamente, los ponemos al comienzo de la descomposición: si no hay ningún V_i isomorfo a ningún W_j, no hacemos nada; en caso contrario tomemos el mayor $r \in \{1, \dots, k\}$ tal que $V_i \simeq W_i$ para todo $i = 1, \dots, r$.

Consideremos la descomposición en bloques de φ asociada a las descomposiciones de V y W como en (3.1) y (3.2). Explícitamente, sea $\iota_i : V_i^{\oplus n_i} \to V$ la inclusión, y $\pi_j : W \to W_j^{\oplus m_j}$ la proyección. Dado $\varphi : V \to W$ un G-mapa no nulo, consideremos "lo que φ hace en $W_j^{\oplus m_j}$ cuando actúa restringida a $V_i^{\oplus n_i}$":

$$\varphi_{ij} : V_i^{\oplus n_i} \to W_j^{\oplus m_j}, \qquad \varphi_{ij} = \pi_j \circ \varphi \circ \iota_i$$

[2] Podemos suponer que la cantidad de sumandos diferentes que aparecen en V y que aparecen en W son los mismos: si no lo son, completamos el menor con sumandos nulos.

Basta pues probar que $\varphi_{ij} = 0$ para todo $i \neq j$, pues entonces $\varphi(V_i^{\oplus n_i}) \subset W_i^{\oplus m_i}$ que es lo que queremos probar.

Consideremos los bloques afuera de la diagonal, i.e. los φ_{ij} con $i \neq j$. Si $\tilde{V}_i := V_i^{\oplus n_i}$ y $\tilde{W}_j := W_j^{\oplus m_j}$, tenemos $\varphi_{ij} : \tilde{V}_i \to \tilde{W}_j$.

La única manera de descomponer $\tilde{V}_i$ y $\tilde{W}_j$ en irreducibles es $\tilde{V}_i = \overbrace{V_i \oplus \cdots \oplus V_i}^{n_i \text{ veces}}$ y $\tilde{W}_j = \overbrace{W_j \oplus \cdots \oplus W_j}^{m_j \text{ veces}}$. En efecto, si V_1 y V_2 son irreducibles, las subrepresentaciones irreducibles de $V_1 \oplus V_2$ son sólo V_1 y V_2 (convencerse), y así n veces.

Ahora consideramos la descomposición en bloques de φ_{ij} asociada a estas descomposiciones de $\tilde{V}$ y $\tilde{W}$: son todas de la forma $\tilde{\varphi}_{ij} : V_i \to W_j$. Como $i \neq j$, entonces por cómo ordenamos las descomposiciones (3.1) y (3.2) se tiene que $V_i \not\simeq W_j$, luego por el lema de Schur todos los bloques $\tilde{\varphi}_{ij} = 0$. Entonces $\varphi_{ij} = 0$ si $i \neq j$, es lo que queríamos probar.

En particular, si tomamos $\varphi = \mathrm{id}_V$ y dos descomposiciones de V en irreducibles como en (3.1) y (3.2) (con $W = V$), lo que tenemos es que $r = k$ (i.e. $V_i \simeq W_i$ para todo $i = 1, \ldots, k$) y $n_i = m_i$ para todo i: la descomposición es única a menos de isomorfismo. □

Observación 3.2.1. Sea V una representación de un grupo G. El conjunto

$$V^G := \{v \in V : g \cdot v = v \quad \forall g \in G\}$$

de puntos fijos para la acción $G \times V \to V$ es un subespacio G-invariante de V.

Proposición 3.9. *Sea V una representación de un grupo finito G sobre k, donde car $k = 0$ o car $k \nmid |G|$. La transformación lineal $\epsilon : V \to V$ definida como*

$$\epsilon = \frac{1}{|G|} \sum_{g \in G} \rho_g$$

es un G-mapa, y es una proyección de V sobre V^G.

Demostración. ϵ es un G-mapa: dados $v \in V$, $g_0 \in G$,

$$\epsilon(\rho_{g_0}(v)) = \frac{1}{|G|} \sum_{g \in G} \rho_g(\rho_{g_0}(v)) = \frac{1}{|G|} \sum_{g \in G} \rho_{gg_0}(v) = \frac{1}{|G|} \sum_{h \in G} \rho_h(v) = \epsilon(v)$$

usando que $gg_0 = h$ es una biyección de G. Por otro lado,

$$\begin{aligned} \rho_{g_0}(\epsilon(v)) &= \rho_g\left(\frac{1}{|G|} \sum_{g \in G} \rho_g(v)\right) = \frac{1}{|G|} \sum_{g \in G} \rho_{g_0}\rho_g(v) \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_{g_0 g}(v) = \frac{1}{|G|} \sum_{h \in G} \rho_h(v) = \epsilon(v) \end{aligned}$$

usando que $g_0 g = h$ es una biyección de G. Esto muestra que ϵ es un G-mapa. Además tenemos $\rho_g(\epsilon(v)) = \epsilon(v)$.

$\mathrm{Im}\ \epsilon = V^G$:
$(\subset)$: $u = \epsilon(v) \Rightarrow \rho_g(u) = \rho_g(\epsilon(v)) = \epsilon(v) = u \Rightarrow u \in V^G$.

$(\supset)$: $v \in V^G \Rightarrow \epsilon(v) = \frac{1}{|G|}\sum_{g\in G} \rho_g(v) = \frac{1}{|G|}\sum_{g\in G} v = \frac{1}{|G|}|G|v = v \Rightarrow v \in \text{Im } \epsilon$.

$\epsilon^2 = \epsilon : \epsilon(\epsilon(v)) = \frac{1}{|G|}\sum_{g\in G} \rho_g(\epsilon(v)) = \frac{1}{|G|}\sum_{g\in G} \epsilon(v) = \frac{1}{|G|}|G|\epsilon(v) = \epsilon(v)$. □

Definición. El operador ϵ definido en la proposición anterior se llama *operador de Reynolds*.

Ejercicios

Ej. 60 — Sean V, W representaciones de un grupo G sobre k. Notemos $\text{Hom}_G(V, W) = \{G\text{-mapas de } V \text{ en } W\}$ y consideremos la representación $\text{Hom}_k(V, W)$. Entonces $(\text{Hom}_k(V, W))^G = \text{Hom}_G(V, W)$.

Ej. 61 — Sea G grupo finito, V una representación compleja de grado finito. Existe un producto interno en V preservado por la acción de G, i.e. tal que $\langle g \cdot v, g \cdot w\rangle = \langle v, w\rangle$ para todo $v, w \in V, g \in G$. Además, si la representación es irreducible, el producto interno es único a menos de multiplicar por un escalar.

3.3. Caracteres

Definición. El *carácter* de una representación (V, ρ) de un grupo G es el morfismo de grupos $\chi_V(g) := \mathrm{Tr}(\rho(g))$, donde Tr denota la traza de la transformación lineal.

El carácter se dice *irreducible* si la representación es irreducible; el *grado* del carácter es el grado de la representación.

El *núcleo* del carácter es $\ker \chi := \ker \rho$.

Observación 3.3.1. En la sección de teoría de cuerpos dimos otra definición de carácter de un grupo. No son equivalentes, más bien la anterior es un caso particular de éste, como veremos en la proposición 3.27.

Lo fantástico de los caracteres es que determinan la representación a menos de isomorfismo: éste es el gran resultado de esta sección.

La siguiente proposición tiene varias aplicaciones:

Proposición 3.10. *Sea (V, ρ) una representación compleja de un grupo G. Entonces para cada $g \in G$, V admite una base formada por vectores propios de ρ_g, y los valores propios son raíces de la unidad.*

Demostración. Sea $g \in G$. Restringimos ρ a $\rho : G \to \mathrm{GL}(\langle g \rangle)$.

Como $k = \mathbb{C}$, ρ_g tiene un valor propio $\alpha_1 \in \mathbb{C}$. Sea $v_1 \in V$, $v_1 \neq 0$ un vector propio de valor propio α_1. Tenemos entonces $\rho_g(v_1) = \alpha_1 v_1$, y en general $\rho_{g^n}(v_1) = \alpha_1^n v_1$.

Definamos $W_1 := \langle v_1 \rangle \subset V$: es una subrepresentación compleja del grupo cíclico $\langle g \rangle$.

Si $\langle g \rangle$ es infinito, entonces $\langle g \rangle \simeq \mathbb{Z}$, y $\mathrm{GL}(\langle g \rangle) \simeq \{\mathrm{id}, \varphi\}$ donde $\varphi : 1 \mapsto -1$. Para cualquiera de los dos automorfismos de $\mathbb{Z}$ existe una base de $\mathbb{Z} \simeq \langle g \rangle$ formada por vectores propios.

Si $\langle g \rangle$ es finito, por el teorema de Maschke existe $V_1 \subset \langle g \rangle$ subrepresentación tal que $V = W_1 \oplus V_1$.

Repitiendo el mismo razonamiento con V_1 encontramos una subrepresentación $W_2 = \langle v_2 \rangle$ y una descomposición $V_1 = W_2 \oplus V_2$, de manera que $V = W_1 \oplus W_2 \oplus V_2$.

Tras una cantidad finita de pasos, $V_n = \{0\}$, y llegamos a una descomposición en subrepresentaciones $V = W_1 \oplus W_n$ donde $W_i = \langle v_i \rangle$ y cada v_i es vector propio de ρ_g. Obtenemos que $\{v_1, \ldots, v_n\}$ es una base de V formada por vectores propios de ρ_g.

Además, la matriz asociada a ρ_g en esta base es diagonal, y los elementos de la diagonal son sus valores propios α_i. Como existe $n \in \mathbb{Z}^+$ tal que $g^n = 1$, necesariamente $\alpha_i^n = 1$ para todo i, luego los valores propios α_i son raíces de la unidad. □

Observación 3.3.2. En la proposición anterior, en general no es posible elegir una base de V tal que la matriz asociada a ρ_g sea diagonal simultáneamente para todo $g \in G$.

Definición. Si $\alpha \in \mathbb{C}$ es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$, decimos que es un *entero algebraico*.

El anillo de los enteros algebraicos se denota $\mathbb{A}$.

Corolario 3.11. *Si χ es un carácter complejo de un grupo finito, entonces $\chi : G \to \mathbb{A}$. En otras palabras, los valores que toman los caracteres de los grupos finitos son enteros algebraicos.*

Demostración. En efecto, por la proposición 3.10 se tiene que $\chi(g) = \epsilon_1 + \cdots + \epsilon_n$ donde $\epsilon_1, \ldots, \epsilon_n \in \mathbb{C}$ son raíces de la unidad, luego raíces de un polinomio de la forma $X^k - 1$: en particular, son enteros algebraicos. □

Recordemos que por definición el núcleo de un carácter es el núcleo de la representación de la que proviene. El siguiente corolario nos muestra que si conocemos los valores del carácter asociado a una representación, entonces conocemos el núcleo de la representación, y en particular podemos afirmar si ésta es fiel o no.

Corolario 3.12. *Sea (V, ρ) representación de un grupo finito G. Se tiene:*

$$\ker \chi = \{g \in G : \chi(g) = \chi(1)\}$$

Demostración. ($\subset$): $g \in \ker \rho \iff \rho(g) = I_n$ donde n es el grado de la representación. Por lo tanto $\chi(g) = \mathrm{Tr}(\rho(g)) = n = \dim V = \chi(1)$.

($\supset$): Supongamos que $\chi(g) = \chi(1) = n$. Por la proposición 3.10, existe una base de V para la que $\rho(g)$ se corresponde con una matriz diagonal, y $\chi(g) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de la diagonal, con los ϵ_i raíces de la unidad. La única manera de que sumar n números complejos de módulo 1 dé n es que todos valgan 1, i.e. $\epsilon_i = 1$ para todo i. Pero entonces $\rho(g) = I_n$, luego $g \in \ker \rho = \ker \chi$. □

Proposición 3.13. *Sean (V, ρ_V) y (W, ρ_W) representaciones sobre k de un grupo G.*

1. $\chi_V(hgh^{-1}) = \chi_V(g) \quad \forall g, h \in G.$
2. $\chi_V(1) = \dim_k V.$
3. $\chi_{V \oplus W} = \chi_V + \chi_W.$
4. $\chi_{V \otimes_k W} = \chi_V \chi_W.$
5. $\chi_{V^*}(g) = \chi_V(g^{-1}) \quad \forall g \in G.$
6. $\chi_V(g^{-1}) = \overline{\chi_V(g)} \quad \forall g \in G$ *si V es una representación compleja.*

Demostración.

1. Es bien conocido de álgebra lineal que la traza es invariante por conjugación.
2. $\chi_V(1) = \mathrm{Tr}(\mathrm{id}) = 1$.
3. $\chi_{V \oplus W}(g) = \mathrm{Tr}(\rho_V \oplus \rho_W(g)) = \mathrm{Tr}(\rho_V(g)) + \mathrm{Tr}(\rho_W(g)) = \chi_V(g) + \chi_W(g)$ pues la matriz asociada a $(\rho_V \oplus \rho_W)(g)$ es una matriz en bloques $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ donde A, B son matrices asociadas a $\rho_V(g), \rho_W(g)$ respectivamente (en bases adecuadas).
4. Análogamente al ítem anterior: recordemos que si $A = (a_{ij})$ y B son las matrices asociadas a $\rho_V(g)$ y a $\rho_W(g)$ respectivamente, la matriz asociada a $(\rho_V \otimes \rho_W)(g)$ es el producto de Kronecker, $A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$. Basta pues observar que $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\ \mathrm{Tr}(B)$.

5. Sea $\mathcal{B} = \{v_1, \ldots, v_n\}$ una base de V, y $\mathcal{B}^* = \{v_1^*, \ldots, v_n^*\}$ la base dual. Sea $A = (a_{ij})$ la matriz asociada a la transformación lineal $V \to V$, $v \mapsto g^{-1} \cdot v$ en la base $\mathcal{B}$, y sea (a_{ij}^*) la matriz asociada a la transformación lineal $V^* \to V^*$, $f \mapsto g \cdot f$ en la base $\mathcal{B}^*$. Tenemos:
$$g^{-1} \cdot v_i = \sum_j a_{ij} v_j, \qquad g \cdot v_i^* = \sum_j a_{ij}^* v_j^*$$
luego por definición de base dual, $a_{ii}^* = (g \cdot v_i^*)(v_i) = v_i^*(g^{-1} \cdot v_i) = a_{ii}$. Sumando para todo i obtenemos que $\chi_{V^*}(g) = \chi_V(g^{-1})$.

6. Sea $g \in G$. Por la proposición 3.10 podemos elegir una base de V tal que la matriz asociada a ρ_g sea una matriz diagonal (α_{ij}) cuya diagonal está formada por raíces de la unidad. En particular $|\alpha_{ii}| = 1$, luego $\alpha_{ii}^{-1} = \overline{\alpha_{ii}}$. Entonces
$$\chi_V(g^{-1}) = \sum_i \alpha_{ii}^{-1} = \sum_i \overline{\alpha_{ii}} = \overline{\sum_i \alpha_{ii}} = \overline{\chi_V(g)} \qquad \square$$

Dos representaciones isomorfas determinan el mismo carácter:

Proposición 3.14. *Si V, W son dos representaciones de G isomorfas, entonces $\chi_V = \chi_W$.*

Demostración. Sea $\theta : V \to W$ isomorfismo de G-módulos: se tiene entonces $\rho_V(g) = \theta^{-1} \circ \rho_W(g) \circ \theta$ para todo $g \in G$. Por lo tanto, aplicando la propiedad 1) anterior,
$$\chi_V(g) = \mathrm{Tr}(\rho_V(g)) = \mathrm{Tr}(\theta^{-1} \circ \rho_W(g) \circ \theta) = \mathrm{Tr}(\rho_W(g)) = \chi_W(g) \quad \forall g \in G \qquad \square$$

En general cuando hablamos de los caracteres de un grupo G estamos pensando en los caracteres asociados a las diferentes representaciones sobre un cuerpo fijo (por lo general $\mathbb{C}$) del grupo. La proposición anterior nos dice que dos caracteres diferentes provienen de representaciones cuyas clases de isomorfismo son diferentes.

Definición. Si G es un grupo finito, definimos en el espacio vectorial $\mathbb{C}^G$ de las funciones $G \to \mathbb{C}$ el producto interno
$$\langle f, h \rangle = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{h(g)}$$

Lema 3.15. *Si V, W son representaciones de grado finito sobre k de un grupo G, entonces tenemos un isomorfismo de G-módulos:*
$$\mathrm{Hom}_k(V, W) \simeq V^* \otimes_k W$$

Demostración. El espacio vectorial $\mathrm{Hom}_k(V, W)$ es una representación de G por el ejercicio 58.

Sea $\phi : V^* \otimes_k W \to \mathrm{Hom}_k(V, W)$ definida en los tensores elementales como $\phi(f \otimes w)(v) = f(v)w$. Es sencillo verificar con la propiedad universal del producto tensorial que ϕ es una transformación lineal bien definida.

Es un isomorfismo lineal: sean $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_m\}$ bases de V y W respectivamente. Considerando la base dual $\{v_1^*, \ldots, v_n^*\}$ de V^*, los tensores $v_i^* \otimes w_j$ forman una base de $V^* \otimes_k W$. Basta ver que los $\phi(v_i \otimes w_j)$ forman una base de $\mathrm{Hom}_k(V, W)$. Esta verificación es un ejercicio sencillo de álgebra lineal que queda a cargo del lector.

Para ver que ϕ es un G-mapa, veamos que $\phi(g \cdot (f \otimes w)) = g \cdot \phi(f \otimes w)$. Hay varias representaciones en juego: arriba de cada igualdad se indica la acción de G sobre qué espacio vectorial se está usando.

Por un lado,

$$\begin{aligned}\phi(g \cdot (f \otimes w))(v) &\overset{V^* \otimes W}{=} \phi((g \cdot f) \otimes (g \cdot w))(v) \\ &\overset{\text{def. de } \phi}{=} (g \cdot f)(v)\, g \cdot w \\ &\overset{V^*}{=} f(g^{-1} \cdot v)\, g \cdot w \\ &\overset{\text{linealidad de } g \cdot -}{=} g \cdot (f(g^{-1} \cdot v)w)\end{aligned}$$

Por otro lado,

$$\begin{aligned}(g \cdot \phi(f \otimes w))(v) &\overset{\mathrm{Hom}_k(V,W)}{=} g \cdot [(\phi(f \otimes w))(g^{-1} \cdot v)] \\ &\overset{\text{def. de } \phi}{=} g \cdot (f(g^{-1} \cdot v)w)\end{aligned}$$

□

Teorema 3.16 (Ortonormalidad de caracteres)**.** *Sean V, W representaciones complejas irreducibles de un grupo G. Entonces*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 0 & si\ V \not\simeq W \\ 1 & si\ V \simeq W \end{cases}$$

Demostración. Por los ejercicios 58 y 60, tenemos que $\mathrm{Hom}(V, W)$ es una representación compleja de G tal que $(\mathrm{Hom}(V, W))^G = \mathrm{Hom}_G(V, W)$.

Por lo tanto en este caso el operador de Reynolds es

$$\epsilon : \mathrm{Hom}(V, W) \to \mathrm{Hom}_G(V, W), \quad \epsilon = \frac{1}{|G|} \sum_{g \in G} \rho_g$$

Como ϵ es una proyección sobre $\mathrm{Hom}_G(V, W)$, se tiene:

$$\mathrm{tr}(\epsilon) = \dim \mathrm{Im}\ \epsilon = \dim \mathrm{Hom}_G(V, W) = \begin{cases} 0 & \text{si } V \not\simeq W \\ 1 & \text{si } V \simeq W \end{cases} \tag{3.3}$$

donde en la última igualdad aplicamos el lema de Schur a las representaciones irreducibles complejas V y W.

Por otro lado:

$$\mathrm{tr}(\epsilon) = \mathrm{tr}\left(\frac{1}{|G|} \sum_{g \in G} \rho_g\right) \overset{\text{tr es lineal}}{=} \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}(V,W)}(g) \tag{3.4}$$

Aplicando el lema 3.15 y la propiedad 3.13, se tiene:

$$\chi_{\mathrm{Hom}(V,W)} = \chi_{V^* \otimes W} = \chi_{V^*} \chi_W = \overline{\chi_V} \chi_W$$

Usando esta igualdad en la ecuación (3.4) e igualando a (3.3), junto con la definición del producto interno se obtiene:

$$\langle \chi_W, \chi_V \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_W(g) = \begin{cases} 0 & \text{si } V \not\simeq W \\ 1 & \text{si } V \simeq W \end{cases}$$

En conclusión, como $\langle \chi_V, \chi_W \rangle = \overline{\langle \chi_W, \chi_V \rangle}$ se deduce:

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 0 & \text{si } V \not\simeq W \\ 1 & \text{si } V \simeq W \end{cases}$$ □

Corolario 3.17. *Si dos representaciones complejas irreducibles tienen el mismo carácter entonces son isomorfas.*

Demostración. Supongamos que V, W son dos tales representaciones pero que no son isomorfas. Entonces la ortonormalidad de caracteres nos dice que $\langle \chi_V, \chi_W \rangle = 0$. Por lo tanto necesariamente χ_V, χ_W han de ser diferentes, pues si fueran iguales, el producto interno tomaría la forma $\langle \chi_V, \chi_W \rangle = \frac{1}{|G|} \sum a_i \overline{a_i} = \frac{1}{|G|} \sum |a_i|^2 > 0$, donde $a_i = \chi_V(g_i)$. □

Corolario 3.18. *Sea (V, ρ) una representación compleja de un grupo G, y sea $V = V_1 \oplus \cdots \oplus V_n$ una descomposición de V en subrepresentaciones irreducibles. Entonces para cada carácter irreducible χ de G, el número de subespacios V_i de carácter χ es $\langle \chi_V, \chi \rangle$.*

Demostración. Si a es el número de V_i de carácter χ, entonces la ortonormalidad de caracteres implica que

$$\langle \chi_V, \chi \rangle = \langle \chi_{V_1 \oplus \cdots \oplus V_n}, \chi \rangle = \langle a_1 \chi_{V_1} + \cdots + a_n \chi_{V_n}, \chi \rangle = \sum_{j=1}^{n} a_j \langle \chi_{V_j}, \chi \rangle = a$$ □

En otras palabras, la cantidad de veces que aparece χ en una descomposición en irreducibles de V es $\langle \chi_V, \chi \rangle$. Esto nos dice que V es la suma directa de tantas representaciones irreducibles de carácter χ como el valor de $\langle \chi_V, \chi \rangle$. De aquí deducimos

Corolario 3.19. *Dos representaciones de un grupo finito G son isomorfas si y sólo si determinan el mismo carácter.*

Demostración. Sean V, W representaciones de G de igual carácter. Por la completa reducibilidad podemos considerar descomposiciones en subrepresentaciones irreducibles, $V = V_1 \oplus \cdots \oplus V_n$, $W = W_1 \oplus \cdots \oplus W_k$. Sea a la cantidad de veces que aparece un carácter irreducible χ de G en esta descomposición de V. Entonces como $\chi_V = \chi_W$, se tiene $a = \langle \chi_V, \chi \rangle = \langle \chi_W, \chi \rangle$, i.e. χ también aparece en la descomposición de W a veces.

Esto vale para todo carácter irreducible χ de G, por lo tanto con el corolario 3.17 concluimos que en las descomposiciones de V y de W aparecen los mismos sumandos a menos de reordenación, luego $V \simeq W$. □

Corolario 3.20. *Todo carácter χ de un grupo finito G se descompone de forma única como combinación lineal de caracteres irreducibles $\chi = n_1 \chi_1 + \cdots + n_k \chi_k$ para ciertos $n_i \in \mathbb{N}$.*

Demostración. Sea V una representación de G de carácter χ. Por completa reducibilidad podemos descomponer V en irreducibles, $V = V_1 \oplus \cdots \oplus V_n$. De esta manera, $n_i = \langle \chi_V, \chi_{V_i} \rangle$ nos da la combinación lineal deseada, y cualquier otra descomposición en irreducibles nos da la misma combinación lineal, pues los caracteres que aparecen son los mismos. □

Corolario 3.21. *Si un carácter de un grupo finito se descompone en irreducibles como* $\chi = n_1\chi_1 + \cdots + n_k\chi_k$*, entonces se cumple* $\langle \chi, \chi \rangle = \sum_{i=1}^{k} n_i^2$*. En particular* χ *es irreducible si y sólo si* $\langle \chi_V, \chi_V \rangle = 1$.

Demostración. Descomponemos V en irreducibles, $V = V_1 \oplus \cdots \oplus V_n$. Se tiene $\chi_V = n_1\chi_1 + \cdots + n_k\chi_k$ para ciertos $n_i \in \mathbb{N}$. De esta manera,

$$\langle \chi_V, \chi_V \rangle = \langle n_1\chi_1 + \cdots + n_k\chi_k, n_1\chi_1 + \cdots + n_k\chi_k \rangle = \sum_{i=1}^{k} n_i^2$$

Por la descomposición de V, deducimos que:

$$\begin{aligned} V \text{ es irreducible} &\iff \text{existe } i \text{ tal que } n_i = 1 \text{ y } n_j = 0 \text{ para todo } j \neq i \\ &\iff \sum_{i=1}^{k} n_i^2 = 1 \\ &\iff \langle \chi_V, \chi_V \rangle = 1 \end{aligned}$$

□

Ahora vemos que el número de caracteres irreducibles de un grupo finito es finito.

Teorema 3.22. *Un grupo finito* G *tiene un número finito de caracteres irreducibles complejos* $\chi_1, \ldots, \chi_k$ *cuyos grados* n_i *verifican la relación:*

$$|G| = \sum_{i=1}^{k} n_i^2$$

Demostración. Para demostrar esto consideramos la representación regular de G (recordar el ejemplo 3.1.8). Si χ_{reg} es el carácter asociado a esta representación, se tiene:

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{si } g = 1 \\ 0 & \text{si no} \end{cases}$$

En efecto, $\chi_{\text{reg}}(1) = \dim_{\mathbb{C}} \mathbb{C}[G] = |G|$; y la traza de la matriz asociada a multiplicar por un elemento no trivial es cero, pues la matriz tiene ceros en la diagonal (i.e. si $g \neq e$, $gh \neq h$).

Ahora bien, si χ es un carácter irreducible de G asociado a una representación V, se tiene:

$$\langle \chi_{\text{reg}}, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\text{reg}}(g)\chi(g^{-1}) = \frac{1}{|G|}\chi_{\text{reg}}(1)\chi(1) = \chi(1) = \dim_{\mathbb{C}} V$$

Es decir, todo carácter irreducible aparece en la representación regular tantas veces como su grado.

Tenemos entonces que si $\chi_{\text{reg}} = n_1\chi_1 + \cdots + n_k\chi_k$ es la descomposición de χ_{reg} en caracteres irreducibles, los caracteres χ_i resultan ser todos los caracteres irreducibles de G, y n_i es el grado de χ_i. Por lo tanto:

$$|G| = \chi_{\text{reg}}(1) = n_1\chi_1(1) + \cdots + n_k\chi_k(1) = n_1^2 + \cdots + n_k^2$$

□

Observación 3.3.3. Cabe destacar que en la demostración anterior probamos que todo carácter irreducible aparece en la representación regular tantas veces como su grado.

Vamos a refinar ahora el teorema anterior diciendo exactamente cuántos caracteres irreducibles tiene un grupo finito.

Definición. Sea G un grupo finito. Una *función de clases*, o *función central*, es una función $f : G \to \mathbb{C}$ tal que $f(g^{-1}hg) = f(h)$ para todo $h, g \in G$. Notaremos $\mathcal{C}(G, \mathbb{C})$ al conjunto de funciones centrales de G.

Ejemplo 3.3.4. Los caracteres son funciones centrales.

Proposición 3.23. *Sea G un grupo finito. Entonces $\mathcal{C}(G, \mathbb{C}) \subset \mathbb{C}^G$ es un $\mathbb{C}$-subespacio vectorial, y su dimensión es el número de clases de conjugación de G.*

Demostración. Claramente, la suma y el producto por un escalar de funciones centrales es una función central.

Si $C_1, \ldots, C_n$ son las clases de conjugación de G y $c_1, \ldots, c_n$ son representantes, entonces

$$f_i : G \to \mathbb{C}, \quad f_i(g) = \begin{cases} 1 & \text{si } g \in C_i \\ 0 & \text{si no} \end{cases}$$

son una base de $\mathcal{C}(G, \mathbb{C})$.

Son linealmente independientes: si $\sum_{i=1}^n \lambda_i f_i = 0$, entonces $\sum_{i=1}^n \lambda_i f_i(c_j) = 0 \Rightarrow c_j = 0$ para todo $j = 1, \ldots, n$.

Generan $\mathcal{C}(G, \mathbb{C})$: si $f \in \mathcal{C}(G, \mathbb{C})$, entonces definiendo $\lambda_i := f(c_i)$, se tiene $f = \sum_{i=1}^n \lambda_i f_i$. $\square$

Observación 3.3.5. La proposición anterior nos da que hay a lo sumo tanto caracteres irreducibles de un grupo finito como clases de conjugación de G. En efecto, si $F = \{\chi \in \mathcal{C}(G, \mathbb{C}) : \chi \text{ es carácter irreducible de } G\}$, por ortogonalidad de caracteres se tiene que F es linealmente independiente. Entonces $|F| \leqslant \dim \mathcal{C}(G, \mathbb{C}) =$ número de clases de conjugación de G.

Nos dirigimos ahora a probar que en realidad esta cota siempre se alcanza, i.e. siempre hay tantos caracteres irreducibles de G como clases de conjugación.

Observación 3.3.6. La transformación lineal $\mathbb{C}^G \to \mathbb{C}[G]$, $\phi \mapsto \sum_{g \in G} \phi(g) g$ es un isomorfismo de $\mathbb{C}$-espacios vectoriales. El lema 3.3 nos dice que bajo este isomorfismo, $\mathcal{C}(G, \mathbb{C})$ se corresponde con el centro de $\mathbb{C}[G]$. Por lo tanto si $\phi \in \mathcal{C}(G, \mathbb{C})$, podemos identificar ϕ con

$$x = \sum_{g \in G} \phi(g) g \in Z(\mathbb{C}[G]).$$

Lema 3.24. *Sea (V, ρ) una representación compleja irreducible de grado n de un grupo G. Pensemos V como $\mathbb{C}[G]$-módulo a izquierda. Sea $\phi \in \mathcal{C}(G, \mathbb{C})$ una función central, que por la observación anterior podemos identificar con*

$$x = \sum_{g \in G} \phi(g) g \in Z(\mathbb{C}[G]).$$

Entonces, para todo $v \in V$, se cumple:

$$xv = \frac{|G|}{n} \langle \phi, \overline{\chi_V} \rangle v$$

Demostración. La función $f : V \to V$, $v \mapsto xv$ es un morfismo de $\mathbb{C}[G]$-módulos. En efecto, el producto por escalar se conserva pues $x \in Z(\mathbb{C}[G])$: si $y \in \mathbb{C}[G], v \in V$, se tiene $f(yv) = xyv = yxv = yf(v)$.

El lema de Schur nos dice entonces que existe $\alpha \in \mathbb{C}$ tal que $f(v) = \alpha v$ para todo $v \in V$. Sólo tenemos que ver que $\alpha = \frac{|G|}{n}\langle \phi, \overline{\chi_V}\rangle$. Para ello usamos la linealidad de la traza:

$$n\alpha = \mathrm{Tr}(f) = \mathrm{Tr}\left(\sum_{g\in G} \phi(g)\rho_g\right) = \sum_{g\in G} \phi(g)\mathrm{Tr}(\rho_g) = \sum_{g\in G} \phi(g)\chi_V(g) = |G|\langle \phi, \overline{\chi_V}\rangle \qquad \square$$

Teorema 3.25. *Si G es un grupo finito, sus caracteres irreducibles forman una base ortonormal de $\mathcal{C}(G, \mathbb{C})$.*

Demostración. Sean $\chi_1, \ldots, \chi_k$ los caracteres irreducibles diferentes de G. Como los caracteres son ortogonales, entonces son linealmente independientes. Sólo resta ver que generan $\mathcal{C}(G, \mathbb{C})$. Basta ver que los caracteres conjugados $\overline{\chi_1}, \ldots, \overline{\chi_k}$ generan $\mathcal{C}(G, \mathbb{C})$, observando que $\langle \overline{\chi_i}, \overline{\chi_j}\rangle = \langle \chi_j, \chi_i\rangle$ implica que los caracteres conjugados son ortogonales luego linealmente independientes.

Sea $\psi \in \mathcal{C}(G, \mathbb{C})$, y sea

$$\phi := \psi - \sum_{i=1}^{k} \langle \psi, \overline{\chi_i}\rangle \overline{\chi_i} \in \mathcal{C}(G, \mathbb{C})$$

Basta probar que $\phi = 0$.

ϕ es tal que $\langle \phi, \overline{\chi_j}\rangle = 0$ para todo j: en efecto, por ortonormalidad de los caracteres conjugados:

$$\langle \phi, \overline{\chi_j}\rangle = \left\langle \psi - \sum_{i=1}^{k} \langle \psi, \overline{\chi_i}\rangle \overline{\chi_i}\,,\ \overline{\chi_j} \right\rangle = \langle \psi, \overline{\chi_j}\rangle - \sum_{i=1}^{k} \langle \psi, \overline{\chi_i}\rangle \langle \overline{\chi_i}, \overline{\chi_j}\rangle = \langle \psi, \overline{\chi_j}\rangle - \langle \psi, \overline{\chi_j}\rangle = 0$$

Sea $x \in Z(\mathbb{C}[G])$ el elemento correspondiente a ϕ a través del isomorfismo $\mathbb{C}^G \to \mathcal{C}(G, \mathbb{C})$, i.e. $x = \sum_{g\in G} \phi(g)g \in Z(\mathbb{C}[G])$ (observación 3.3.6).

Sea (V, ρ) una representación de G. Si es irreducible, el lema 3.24 nos dice que

$$xv = \frac{|G|}{n}\langle \phi, \overline{\chi_V}\rangle v = 0$$

pues recién probamos que $\langle \phi, \overline{\chi}\rangle = 0$ para cualquier carácter irreducible χ de G.

Si no es irreducible, llegamos a la misma conclusión descomponiéndolo en suma directa de subrepresentaciones irreducibles: si $V = V_1 \oplus \cdots \oplus V_n$ para ciertos V_i irreducibles, entonces $\chi_V = \chi_{V_1} + \cdots + \chi_{V_n} = 0$ pues $\chi_{V_i} = 0$ por ser caracteres irreducibles de G.

Apliquemos esto a la representación regular de G, i.e. a $V = \mathbb{C}[G]$ con la acción regular. Entonces para $v = 1$, obtenemos:

$$0 = x1 = \sum_{g\in G} \phi(g)g$$

de donde necesariamente $\phi = 0$. $\square$

La proposición 3.23 junto con el teorema nos dan el número exacto de caracteres irreducibles de un grupo finito:

Corolario 3.26. *El número de caracteres irreducibles de un grupo finito G es igual al número de clases de conjugación de G.*

3.4. Ejemplos y aplicaciones

3.4.1. Representaciones de grado 1

En la sección de teoría de cuerpos definimos un carácter de un grupo G como un morfismo de grupos $G \to K^*$ donde K es un cuerpo. La siguiente proposición nos dice que es lo mismo dar uno de esos caracteres que dar una representación de grado 1 del grupo.

Proposición 3.27. *Sea G grupo y K cuerpo. "Es lo mismo" dar un morfismo de grupos $\varphi : G \to K^*$ que dar una representación de grado 1 de G sobre K.*

Demostración. ($\Rightarrow$) Sea $\varphi : G \to K^*$ un morfismo de grupos. Entonces $\rho : G \to K^* \simeq \mathrm{GL}(K)$ es un morfismo de grupos: es una representación de grado 1 de G sobre el K-espacio vectorial K.

($\Leftarrow$) Sea (V, ρ) una representación de G sobre K de grado 1. Sea $v_0 \in V \backslash \{0\}$. Dado $g \in G$, existe un único escalar $\varphi(g) \in K$ tal que $\rho(g)(v_0) = \varphi(g)v_0$, y como $\rho(g) \in \mathrm{GL}(V)$ entonces $\varphi(g) \neq 0$.

Esto define una función $\varphi : G \to K^*$. Es un morfismo de grupos: si $g, h \in G$,

$$\begin{aligned}\varphi(gh)v_0 = \rho(gh)(v_0) = \rho(g)(\rho(h)(v_0)) = \rho(g)(\varphi(h)v_0)\\ = \varphi(h)\rho(g)(v_0) = \varphi(h)\varphi(g)v_0 = \varphi(g)\varphi(h)v_0\end{aligned}$$

Como v_0 no es el vector nulo, entonces $\varphi(gh) = \varphi(g)\varphi(h)$. □

Teorema 3.28. *Un grupo finito G es abeliano si y sólo si todos sus caracteres irreducibles tienen grado 1. En este caso hay tantos caracteres irreducibles como $|G|$.*

Demostración. Sea h el número de clases de conjugación de G. El grupo G es abeliano si y sólo si la clase de conjugación de cada elemento es trivial, i.e. si y sólo si $|G| = h$.

Si $n_1, \ldots, n_h$ son los grados de los caracteres irreducibles de G (corolario 3.26), entonces satisfacen (teorema 3.22) $n_1^2 + \cdots + n_h^2 = |G|$. Por lo tanto $|G| = h \iff n_i = 1$ para todo $i \iff$ todos los caracteres irreducibles tienen grado 1. □

3.4.2. Tablas de caracteres

Para determinar una representación compleja de un grupo finito G basta determinar sus caracteres irreducibles, que hay tantos como clases de conjugación de G. Por lo tanto poniendo los caracteres irreducibles de G en una tabla, estamos determinando todas las posibles representaciones de G.

Definición. Sea G grupo finito, $C_1, \ldots, C_n$ las clases de conjugación, $g_1, \ldots, g_n$ sendos representantes, y $\chi_1, \ldots, \chi_n$ los caracteres irreducibles de G. La *tabla de caracteres* de G es la matriz $n \times n$ cuya entrada (i, j) es $\chi_i(g_j)$. Por convención tomamos $g_1 = 1$: la primera fila corresponde pues a la representación trivial.

Observación 3.4.1. La primera fila siempre consiste de unos; la primera columna corresponde a los grados de las representaciones.

Ejemplo 3.4.2. Sea $\varphi : S_n \to \mathrm{GL}_n(\mathbb{C})$, definida en la base canónica $\{e_1, \ldots, e_n\}$ de $\mathrm{GL}_n(\mathbb{C})$ como $\varphi(\sigma)(e_i) = e_{\sigma(i)}$. Ésta es la *representación estándar* de S_n. Se tiene:

$$\varphi_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi_{(123)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Ejemplo 3.4.3. Sea $\rho : S_3 \to \mathrm{GL}_2(\mathbb{C})$ definida en los generadores (12),(123) como

$$\rho_{(12)} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \rho_{(123)} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

y sea $\psi : S_3 \to \mathrm{GL}_1(\mathbb{C})$ definida como $\psi_\sigma = \mathrm{id}$ para todo σ. Entonces:

$$(\rho \oplus \psi)_{(12)} = \begin{pmatrix} -1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (\rho \oplus \psi)_{(123)} = \begin{pmatrix} -1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

En el ejemplo 3.4.5 probaremos que ρ es irreducible, y al final habremos probado que la representación $\rho \oplus \psi$ es equivalente a la representación estándar.

Ejemplo 3.4.4. Sea la acción $S_n \times \mathbb{C} \to \mathbb{C}$, definida como $\sigma \cdot z = \epsilon(\sigma)z$: define una representación no trivial de S_n de grado 1, llamada *representación alternada* de S_n.

Ejemplo 3.4.5. Determinemos la tabla de caracteres de S_3.

Sabemos que S_3 tiene 3 clases de conjugación: $\{\mathrm{id}\}, \{(12)(23)(13)\}, \{(123)(132)\}$. Por lo tanto S_3 tiene 3 caracteres irreducibles, cuyos grados d_1, d_2, d_3 satisfacen la relación

$$d_1^2 + d_2^2 + d_3^2 = 1$$

La única solución posible a menos de reordenación de esta ecuación es $d_1 = 1, d_2 = 1, d_3 = 2$: hay dos representaciones irreducibles de grado 1 y una representación irreducible de grado 2.

Deben ser entonces la representación alternada y una representación irreducible de grado 2. Consideremos ρ la del ejemplo 3.4.3.

Afirmación: ρ es irreducible.

Demostración: Basta ver que $\langle \chi_\rho, \chi_\rho \rangle = 1$. Como los caracteres son funciones centrales, para calcular el producto interno basta ver cuánto valen en un conjunto de representantes de las clases de conjugación. $\chi_\rho(\mathrm{id}) = 2$, $\chi_\rho((12)) = 0$, y $\chi_\rho((123)) = -1$. Como hay tres transposiciones y dos 3-ciclos, se tiene:

$$\langle \chi_\rho, \chi_\rho \rangle = \frac{1}{6}(2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2) = 1$$

y ρ es irreducible. □

Ya podemos entonces calcular la tabla de caracteres de S_3.

S_3	1 id	3 (12)	2 (123)
χ_{id}	1	1	1
χ_{alt}	1	-1	1
χ_ρ	2	0	-1

Observar que la representación estándar de S_3 está dada por las matrices:

$$\varphi_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi_{(123)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

y por lo tanto su carácter toma los valores:

	id	(12)	(123)
χ_{est}	3	1	0

Comparando con la tabla de caracteres de S_3 observamos que $\chi_{\text{est}} = \chi_\rho + \chi_{\text{id}}$, y por lo tanto si ψ es la representación trivial, la representación estándar es equivalente a $\rho \oplus \psi$.

Ejercicios

Ej. 62 — Generalizar la representación 3.4.3 para conseguir una representación irreducible de grado $n-1$ de S_n.

Bibliografía

[A] P. Aluffi, *Algebra: Chapter 0*, 2009, Graduate Studies in Mathematics, Volume 104, AMS

[DF] D. Dummit & R. Foote, *Abstract Algebra, Third Edition*, 2004, John Wiley & Sons, Inc., US

[F] W. Fulton & J. Harris, *Representation Theory: A First Course*, 1991, Springer-Verlag New York, Inc.

[H] T. Hungerford, *Algebra*, 1974, Springer-Verlag New York, Inc.

[J] N. Jacobson, *Basic Algebra I*, 1974, W.H. Freeman and Company, US

[K] G. Karpilovsky, *Topics in Field Theory*, 1989, North-Holland, Amsterdam

[KC] K. Conrad, *Galois groups of cubics and quartics (not in characteristic 2)*, disponible en http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf

[KM] M.I. Kargapolov, Ju.I. Merzljakov, *Fundamentals of the Theory of Groups*, 2ª ed., 1979, Springer-Verlag New York, Inc.

[I1] C. Ivorra Castillo, *Álgebra*, disponible en http://www.uv.es/ivorra/Libros/Algebra.pdf

[I2] C. Ivorra Castillo, *Representaciones de grupos finitos*, disponible en http://www.uv.es/ivorra/Libros/Representaciones.pdf

[Isa] I.M. Isaacs, *Algebra: A Graduate Course*, 1994, Wadsworth Inc., US

[M1] J.S. Milne, *Group Theory*, disponible en http://www.jmilne.org/math/CourseNotes/GT.pdf

[M2] J.S. Milne, *Fields and Galois Theory*, disponible en http://www.jmilne.org/math/CourseNotes/ft.html

[Rob] D.J.S. Robinson, *A Course in the Theory of Groups, Second Edition*, 1996, Springer-Verlag New York, Inc.

[Rom] S. Roman, *Field Theory, Second Edition*, 2006, Springer-Verlag New York, Inc.

[Rot1] J.J. Rotman, *An Introduction to the Theory of Groups: Fourth Edition*, 1995, Springer-Verlag New York, Inc.

[Rot2] J.J. Rotman, *Advanced Modern Algebra*, 2002, Prentice-Hall, US

[Rot3] J.J. Rotman, *Galois Theory*, 1990, Springer-Verlag New York, Inc.

[T] J.P. Tignol, *Galois' Theory of Algebraic Equations*, 2001, World Scientific Publishing Co., Singapur

[We] S. Weintraub, *Galois Theory*, 2006, Springer Science+Business Media Inc., US

[Wi] M. Wild, *The Groups of Order Sixteen Made Easy*, disponible en http://math.sun.ac.za/~wild/MarcelWild-HomePage_files/Groups16AMM.pdf

Índice alfabético

Índice de notaciones