

Apuntes del Curso Elementos de Álgebra
(Primera Versión)

Profesor: Pablo Dartnell
Auxiliar: María Isabel Cortés

Capítulo 1

Elementos de Teoría de Grupos.

1.1 Definiciones básicas.

Definición

Un **Monoide** es una estructura algebraica con operación $(M, *)$ tal que:

1. $*$ es asociativa
2. $*$ tiene neutro, $1 \in M$

Definición

Grupo es una estructura con una operación $(G, *)$ tal que:

1. $*$ es asociativa en G
2. $*$ tiene neutro, $1 \in G$
3. todo elemento $x \in G$ tiene inverso $x^{-1} \in G$

Ejemplo: $(\mathbb{Z}, +)$ es grupo

Definición

Un grupo se dice **Abeliano** si la operación es conmutativa

Ejemplo:

Sean $B_n = \{1..n\}$ y $S_n = \sum_n = \{\sigma : B_n \rightarrow B_n/\sigma \text{ es biyección}\}$. S_n es el “conjunto de permutaciones con n letras”. (S_n, \circ) es grupo, con \circ la composición de funciones. Es abeliano si $n \leq 2$. Si $n \geq 3$ no es abeliano.

Las permutaciones se anotan como $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \in S_n$

1. $n \leq 2$

a) $n = 1 \Rightarrow S_n = S_1 = \{id_{\{1\}}\}$, obviamente $(\{id_{\{1\}}\}, \circ)$ es abeliano.

b) $n = 2 \Rightarrow S_n = S_2 = \{\sigma_1, \sigma_2\}$ $\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = id_{\{1,2\}}$ $\sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

\circ	id	σ
id	id	σ
σ	σ	id

\Rightarrow es abeliano.

1. $n \geq 3$, hay $n!$ elementos (permutaciones).

a) $n = 3$

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\sigma \circ \tau \neq \tau \circ \sigma \Rightarrow S_3$ no es abeliano.

b) $n \geq 3$

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}$ $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}$

$\sigma \circ \tau \neq \tau \circ \sigma \Rightarrow S_n$ no es abeliano.

1.2 “Buenas Funciones” entre Grupos: Morfismos

Definición

Sean $(G, *)$, $(H, *_H)$ dos grupos. Un **Morfismo** (u homomorfismo) entre ellos es una función $f : G \rightarrow H$ tal que: $(\forall x, y \in G) f(x * y) = f(x) *_H f(y)$.

Un morfismo como este se suele denotar por $f : (G, *) \rightarrow (H, *_H)$

Nombres especiales:

- Un morfismo inyectivo, se dice MONOMORFISMO.
- Un morfismo sobreyectivo, se dice EPIMORFISMO.
- Un morfismo biyectivo, se dice ISOMORFISMO.
- Un morfismo del grupo $(G, *)$ en si mismo , ENDOMORFISMO .
- Un isomorfismo de $(G, *)$ en si mismo, AUTOMORFISMO.

Observación:

Un morfismo de grupos **realmente** lleva una estructura a la otra. Si $f : (G, *) \rightarrow (H, *_H)$ es morfismo, entonces:

- $f(1_G) = 1_H$
- $(\forall x \in G) f(x^{-1}) = f(x)^{-1}$

*(Ejercicio)***1.3 “Los Buenos Subconjuntos de un Grupo”: Subgrupos.****Definición:**

Sea $(G, *)$ un grupo. Un subconjunto $H \subseteq G$ se dice SUBGRUPO si sólo si :

1. $*$ es cerrado en H . Es decir, $(\forall x, y \in H, x * y \in H)$
2. $(H, *|_H)$ es también un grupo.

Observación:

Si H es un subgrupo de $(G, *)$ el neutro de $*$ en H es el mismo que el neutro de $*$ en G , y $(\forall x \in H)$ el inverso de x para $*$ en H es el mismo que tenía en G . *(Ejercicio)*

Ejercicio:

H subgrupo de $(G, *)$ ssi:

- $*$ es cerrada en H
- $1 \in G$
- $(\forall x \in H) x^{-1} \in H$

Prop

(Caracterización de Subgrupos). $H \subseteq G$ es subgrupo del grupo $(G, *)$ ssi:

1. $H \neq \emptyset$
2. $(\forall x, y \in H) x * y^{-1} \in H$

(EJERCICIO)

Ejercicio:

Sean $(G, *)$ (L, \cdot) dos grupos y $f : G \rightarrow L$ un morfismo. Entonces:

1. Si $H \subseteq G$ es subgrupo $f(H) \subseteq L$ es subgrupo.
2. Si $K \subseteq L$ es subgrupo, entonces $f^{-1}(K) \subseteq G$ es subgrupo .

Definición

Sea $f : (G, *) \rightarrow (L, \cdot)$ un morfismo de grupos . Se definen los siguientes conjuntos:

1. **Núcleo** de $f : \text{Ker} f = f^{-1}\{1\} = \{x \in G / f(x) = 1\} \subseteq G$.
2. **Imagen** de $f : \text{Im} f = f(G) \subseteq L$.

Es fácil probar que $\text{Ker} f$ e $\text{Im} f$ son subgrupos de G y L respectivamente.

Obviamente f sobreyectiva $\Leftrightarrow \text{Im} f = L$.

Prop

f morfismo inyectivo $\Leftrightarrow \text{Ker} f = \{1\}$.

Dem.

\Rightarrow) (EJERCICIO)

\Leftarrow)

Si $x, y \in G$ son tales que $f(x) = f(y) \Rightarrow f(x) * f(y)^{-1} = 1 \Rightarrow f(x) * f(y^{-1}) = 1 \Rightarrow f(x * y^{-1}) = 1$

i.e $x * y^{-1} \in \text{Ker} f = \{1\} \Rightarrow x = y$

1.4 “Buenos Cuocientes en Grupos”.

Definición.

Sea $(G, *)$ un grupo. Una relación de equivalencia \approx en G se dice **compatible** con $*$ ssi:
 $(\forall x, x', y, y' \in G) x \approx x' \wedge y \approx y' \Rightarrow x * y \approx x' * y'$

Observación:

Dada una relación de equivalencia \approx en G compatible con $*$, queda bien definida la operación entre clases: $(\forall [x], [y] \in G/\approx) [x] * [y] = [x * y]$.

$(G/\approx, *)$ es un grupo con neutro $[1]$ y $(\forall [x] \in G/\approx) [x]^{-1} = [x^{-1}]$.

Además, la Sobreyección Canónica $\nu : G \longrightarrow G/\approx$
 $x \longrightarrow [x]$

es un epimorfismo de grupos. (El epimorfismo canónico).

Notar que si \approx es compatible con $*$ en G , entonces $[1] \subseteq G$ es un subgrupo, en efecto:

- $1 \in [1]$
- Si $x, y \in [1] \Rightarrow (x \approx 1 \wedge y \approx 1) \Rightarrow x * y \approx 1 \Rightarrow x * y \in [1]$
- Si $x \in [1] : x \approx 1 \wedge x^{-1} \approx x^{-1}$ (pues \approx es refleja)
 $\Rightarrow 1 \approx x^{-1} \Rightarrow x^{-1} \in [1]$

Además, este subgrupo $H = [1]$ tiene la siguiente propiedad :

$(\forall x \in G)(\forall y \in H) x * y * x^{-1} \in H$ (i.e $(\forall x \in G) x * H * x^{-1} \subseteq H$. En efecto:

$(y \approx 1) \wedge (x \approx x) \wedge (x^{-1} \approx x^{-1}) \Rightarrow x * y * x^{-1} \approx x * 1 * x^{-1} = 1$

y concluimos que $(\forall x \in G) x * H * x^{-1} = H$.

pues $x^{-1} * H * x \subseteq H \Rightarrow H \subseteq x * H * x^{-1}$

Definición

Sea $(G, *)$ un grupo, y $a \in G$. El **Automorfismo Interior** definido por a es:

$$I_a : G \longrightarrow G$$

$$x \longrightarrow I_a(x) = a * x * a^{-1}$$

Ejercicio:

- I_a es un automorfismo
- $I_a \circ I_b = I_{a*b}$
- $I_1 = id_G$
- $I_{a^{-1}} = (I_a)^{-1}$

La clase del 1 en una relación compatible con $*$ es tal que: $(\forall x \in G) I_x(H) = H$ (cerrado para todos los automorfismos interiores).

Definición

Sea $(G, *)$ un grupo. Un subgrupo $H \subseteq G$ se dice **Normal** ssi: $(\forall x \in G) x * H * x^{-1} = H$ (cerrado para los automorfismos interiores)

Notación:

$H \triangleleft G \Leftrightarrow H$ es subgrupo normal de G

Ejercicio:

Sean $(G, *)$, (H, \cdot) dos grupos, y $f : G \rightarrow L$ un morfismo. Probar que $Ker f$ es un subgrupo normal de G .

Definición

Sea $H \subseteq G$ un subgrupo y definamos la siguiente relación en G : $x \approx_H y \Leftrightarrow x^{-1} * y \in H$

Ejercicio:

1. \approx_H es de equivalencia
2. \approx_H es compatible con $*$ $\Leftrightarrow H \triangleleft G$
3. $[1] = H$

Observación:

$x \approx_H y \Leftrightarrow x^{-1} * y \in H \Leftrightarrow y \in x * H$, con $x * H = \{x * h / h \in H\}$ traslación izquierda de x por H

$G \approx_H = \{[x]/x \in G\} = \{x * H/x \in G\}$ $[x] = x * H$ se suele llamar "clase izquierda de x definida por H .

$x \sim_H y \Leftrightarrow y * x^{-1}$ también es de equivalencia en G . con $[x] = H * x$ "clase derecha de x definida por H .

En general , $x * H$ y $H * x$ no tienen por que coincidir , de hecho $H \triangleleft G \Leftrightarrow (\forall x \in G) x * H = H * x$. (\approx_H es la misma que \sim_H ssi $H \triangleleft G$).

G / \approx_H es sólo un conjunto . Adquiere estructura natural de grupo ssi $H \triangleleft G$.

Si $f : G \rightarrow L$ es un morfismo de grupos, entonces $\text{Ker} f \triangleleft G$. A la inversa, todo $H \triangleleft G$ es núcleo de un morfismo. En efecto:

Tomando la relación de equivalencia \approx_H formamos el grupo cociente $L = G / \approx_H$ y el epimorfismo canónico $\nu : G \rightarrow L$ tal que $\nu(x) = [x]$.

Se tiene entonces $\text{Ker} \nu = \{x \in G / \nu(x) = [1] = H\} = H$.

Ejemplo:

Enteros módulo m , $m \geq 1$ en \mathbb{N}

Cuocientes de $(\mathbb{Z}, +) \Leftrightarrow$ subgrupos normales de $(\mathbb{Z}, +)$

$(H \triangleleft G \Leftrightarrow H$ es subgrupo y $\forall x \in \mathbb{Z} x + H + (-x) = H$). De aquí se deduce:

Si $(G, *)$ es grupo abeliano, todo H subgrupo de G es normal.

Prop

Los subgrupos de $(\mathbb{Z}, +)$ son todos de la forma $\{mk/k \in \mathbb{Z}\} = m\mathbb{Z}$ $m \in \mathbb{N}$ fijo.

Dem.

\Leftarrow) Es claro que son Subgrupos.

\Rightarrow) Sea $H \subseteq \mathbb{Z}$ un subgrupo .

- Si $H = \{0\} \Rightarrow H = 0\mathbb{Z}$

- Si $H \neq \{0\}$:

Sea $m \in H$ el más pequeño de los elementos mayores que 0 en H .

Tomemos $h \in H$ un elemento cualquiera. Por el teorema de la división de enteros

$$h = mq + r \quad 0 \leq r < m$$

$\Rightarrow r = h - mq \in H$, pues $h, mq \in H$
 $\Rightarrow r = 0$
 por lo tanto $H = m\mathbb{Z}$

La relación \approx_H asociada a $H = m\mathbb{Z}$ es $x \approx_H y \Leftrightarrow -x + y = mk, k \in \mathbb{Z} \Leftrightarrow x \equiv_m y$
 y entonces resulta que $\mathbb{Z}/\approx_H = \mathbb{Z}_m$ (enteros módulo m)

La operación en \mathbb{Z}_m es suma módulo m .

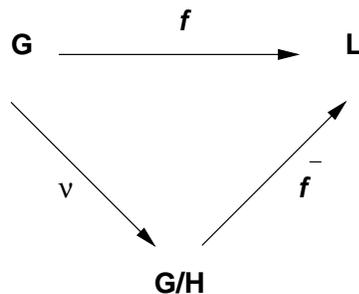
$(m \geq 2) : \mathbb{Z}_m = \{[0], [1], \dots, [m-1]\}$.

Notación:

Si $(G, *)$ es grupo, y $H \triangleleft G$, el cociente G/\approx_H se anota simplemente G/H , y se lee :“G módulo H “

1.4.1 Teorema del Factor

Sean $(G, *)$, (L, \cdot) grupos. $f : (G, *) \rightarrow (L, \cdot)$ morfismo y $H \triangleleft G$, con $H \subseteq \text{Ker} f$.



Entonces $\exists!$ morfismo $\bar{f} : (G/H) \rightarrow (L, \cdot)$ tal que $\bar{f} \circ \nu = f$.(i.e el diagrama conmuta).

Dem.

La ecuación $\bar{f} \circ \nu = f$ significa $\bar{f}([x]) = f(x)$.

Probemos que esta fórmula tiene sentido, i.e $[x] = [x'] \Rightarrow f(x) = f(x')$

$[x] = [x'] \Leftrightarrow x \approx_H x' \Leftrightarrow x^{-1} * x' \in H \Leftrightarrow \exists h \in H \text{ tq } x^{-1} * x' = h$

$\Rightarrow f(x^{-1} * x') = f(h) = 1 \text{ (} h \in \text{Ker} f \text{)} \Rightarrow f(x)^{-1} * f(x') = 1 \Rightarrow f(x) = f(x')$

por lo tanto, la función $\bar{f} : G/H \rightarrow L$ queda bien definida.
 $[x] \rightarrow f(x)$

Es fácil ver que es morfismo:

$\bar{f}([x] * [y]) = \bar{f}([x * y]) = f(x * y) = f(x) * f(y) = \bar{f}([x]) * \bar{f}([y])$

Como $\bar{f}([x])$ está predefinida por $\bar{f} \circ \nu = f$ entonces \bar{f} es único.

Observación:

Se dice que "factorizamos" el morfismo $f : G \rightarrow L$ a través de G/H con $H \subseteq \text{Ker} f$.

Nota:

- $\text{Im} \bar{f} = \text{Im} f$, por lo tanto, \bar{f} epimorfismo $\Leftrightarrow f$ epimorfismo

- $\text{Ker} \bar{f} = \{[x] \in G/H : \bar{f}([x]) = 1\}$
 $= \{[x] \in G/H : f(x) = 1\}$
 $= \{[x] \in G/H : x \in \text{Ker} f\}$
 $=$ Clase de los elementos del $\text{Ker} f$

Veamos que si $x \in \text{Ker} f$, entonces $[x] \in \text{Ker} \bar{f}$:

$y \in [x] \Leftrightarrow x^{-1} * y \in H \Leftrightarrow y \in x * H$, como $\text{Ker} f$ es subgrupo y $H \subseteq \text{Ker} f \Rightarrow x * H \subseteq \text{Ker} f$, por lo tanto, la clase de x si $x \in \text{Ker} f$ sigue en $\text{Ker} \bar{f}$.

De aquí se puede escribir : $\text{Ker} \bar{f} = \text{Ker} f / H$, y así \bar{f} inyectiva $\Leftrightarrow H = \text{Ker} f$.

Corolario

Si $f : G \rightarrow L$ es un epimorfismo, entonces $G/\text{Ker} f \cong L$, y en general, si $f : G \rightarrow L$ es morfismo, entonces $\text{Im} f \cong G/\text{Ker} f$.

1.4.2 Generadores de Subgrupos

Sea $(G, *)$ un grupo y $A \subseteq G$. El subgrupo generado por A se define como:

$$\langle A \rangle = \bigcap_{A \subseteq H \text{ subgrupo de } G} H$$

Ejercicio:

La intersección de una cantidad cualquiera, finita o infinita de subgrupos de G es a su vez un subgrupo de G .

¿Qué es $\langle A \rangle$?

1. Es subgrupo.
2. $\langle A \rangle \supseteq A$.
3. Es el subgrupo de G más pequeño que contiene a A , i.e. si $H \subseteq G$ es subgrupo y $H \supseteq A \Rightarrow H \supseteq \langle A \rangle$.

Prop

1. Si $A \subseteq B \subseteq G$ entonces $\langle A \rangle \subseteq \langle B \rangle$.
2. A es subgrupo de $G \Leftrightarrow A = \langle A \rangle$.
3. $\langle \langle A \rangle \rangle = \langle A \rangle$.

Definición

Si $(G, *)$ es grupo, y $a \in G$, para $n \in \mathbb{Z}$ definimos a^n como:

$$a^0 = 1 \text{ (con 1 el neutro en } G \text{)}$$

$$a^{n+1} = a^n * a \quad n \in \mathbb{N}$$

$$a^n = (a^{-n})^{-1} \text{ si } n < 0$$

Prop

$$(\forall n, m \in \mathbb{Z})(\forall a \in G)$$

- $a^{n+m} = a^n * a^m$
- $(a^n)^m = a^{nm}$

Prop

Si $A \subseteq G$, $A \neq \emptyset$, entonces $\langle A \rangle = \{a_1^{m_1} * \dots * a_n^{m_n} / n \in \mathbb{N}, m_1 \dots m_n \in \mathbb{Z}, a_1 \dots a_n \in A\}$

Definición

Sea $(G, *)$ un grupo. Diremos que G es **cíclico** ssi $(\exists a \in G)$ tal que $G = \{a^n / n \in \mathbb{Z}\}$.

Ejemplos:

- $(\mathbb{Z}, +)$ es cíclico : $\mathbb{Z} = \langle \{1\} \rangle$.
- $(\forall m \geq 1) (\mathbb{Z}_m, +)$ es cíclico: $\mathbb{Z}_m = \langle \{[1]\} \rangle$.

Salvo isomorfismos, estos son los únicos grupos cíclicos que hay. Es decir, si G es cíclico, entonces:

$G \cong (\mathbb{Z}_m, +)$ si G es finito, con $m = |G|$, o bien,

$G \cong (\mathbb{Z}, +)$ si G es infinito

Dem.

Si G es cíclico, $G = \{a^n/n \in \mathbb{Z}\}$. Sea $f: \mathbb{Z} \rightarrow G$
 $n \rightarrow f(n) = a^n$

Es claro que f es un epimorfismo entre $(\mathbb{Z}, +)$ y $(G, *)$.

Veamos que si G es infinito, f es realmente un isomorfismo. Para esto probemos la inyectividad.

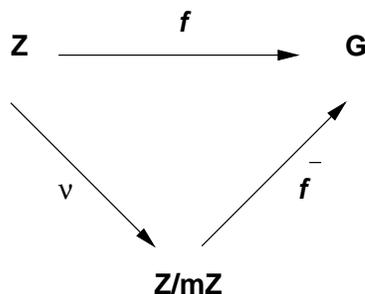
$$\text{Ker } f = \{n \in \mathbb{Z} / f(n) = a^n = 1\}$$

AFIRMACIÓN: no hay ningún $n \neq 0$ en $\text{Ker } f$ (\Leftrightarrow no hay ningún $n > 0$ en $\text{Ker } f$).

Si $n > 0$ está en $\text{Ker } f$, entonces $G = \{a^k/k \in \mathbb{Z}\} = \{1, a, \dots, a^{n-1}\} \Rightarrow G$ es finito $\rightarrow \leftarrow$
 por lo tanto, en este caso, f es isomorfismo.

En general, el núcleo de f será un subgrupo de $\mathbb{Z} : m\mathbb{Z}$, para algún $m \in \mathbb{N}$, y por el teorema del factor

$$\mathbb{Z} \rightarrow G$$



$$G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \text{ . con } m = |G| \text{ para } |G| < \infty.$$

Definición

Sea $(G, *)$ un grupo, y $A \subseteq G$. El **Subgrupo normal generado** por A es:

$$\langle A \rangle_N = \bigcap_{A \subseteq H \triangleleft G} H$$

Ejercicio:

Una intersección cualquiera de subgrupos normales de G es un subgrupo normal.

Observación:

$\langle A \rangle_N$ se caracteriza naturalmente como el subgrupo normal mas pequeño de G que contiene a A .

Claramente $\langle A \rangle \subseteq \langle A \rangle_N$.

Prop

$\langle A \rangle_N = \{I_{x_1}(a_1^{m_1}) * \dots * I_{x_n}(a_n^{m_n}) / n \in \mathbb{N}, m_1 \dots m_n \in \mathbb{Z}, a_1 \dots a_n \in A, x_1 \dots x_n \in G\}$.

La demostración queda de ejercicio.

Conmutadores y Abelianización de un grupo**Definición**

Sea $(G, *)$ un grupo, sean $x, y \in G$. Llamamos **conmutador** de x e y a $[x, y] = x*y*x^{-1}*y^{-1}$.

Es claro que $x * y = y * x \Leftrightarrow [x, y] = 1$.

Observación:

Si $z \in G$, $I_z([x, y]) = [I_z(x), I_z(y)]$. (Mejor aún, si $f : G \rightarrow L$ es morfismo de grupos, y $x, y \in G$, $f([x, y]) = [f(x), f(y)]$), por lo tanto, si $A = \{[x, y] / x, y \in G\}$, entonces, $\langle A \rangle = \langle A \rangle_N = [G, G]$ subgrupo conmutador de G .

Notar que $[G, G] = \{[x_1, y_1] * \dots * [x_n, y_n] / n \in \mathbb{N}, x_1 \dots x_n, y_1 \dots y_n \in G\}$.

Definición

La abelianización de G es $Ab(G) = G/[G, G]$.

Prop

$Ab(G)$ es un grupo abeliano. Mejor aún, $(\forall H \triangleleft G) G/H$ es abeliano $\Leftrightarrow H \supseteq [G, G]$.

Dem.

\Leftarrow) Para $H \triangleleft G$ con $H \supseteq [G, G]$, calculemos los conmutadores de G/H :

Sean $[x], [y] \in G/H$. $[[x], [y]] = [\nu(x), \nu(y)] = \nu[x, y] = [[x, y]] = H$, pues $[x, y] \in H$, pero $H = [1] \Rightarrow [[x], [y]] = [1] \Leftrightarrow [x] * [y] = [y] * [x]$.

\Rightarrow) directo de lo anterior.

Definición

Si G es un grupo, y H, K son subgrupos de G , entonces el “compuesto” de H y K es $HK = \langle H \cup K \rangle$ (subgrupo más pequeño que contiene a H y K).

Evidentemente $HK = \{h_1 * k_1 * \dots * h_n * k_n / n \in \mathbb{N}, h_1 \dots h_n \in H, k_1 \dots k_n \in K\}$

Prop

1. Si $H \triangleleft G$ y $K \triangleleft G$, entonces $HK \triangleleft G$
2. $HK = KH$
3. Si $H \triangleleft G$, $HK = \{h * k/h \in H, k \in K\}$

Dem. (de 3.)

Inducción más lo siguiente:

$$\forall h_1, h_2 \in H \forall k_1, k_2 \in K$$

$$h_1 * k_1 * h_2 * k_2 = h_1 * k_1 * h_2 * k_1^{-1} * k_1 * k_2$$

$$k_1 * h_2 * k_1^{-1} = h' \in H \quad h_1 * h' = h \in H \quad k_1 * k_2 = k \in K .$$

Completar la demostración.

Otro Ejemplo de Cuocientes

Notemos que si X es un conjunto, entonces $(Biy(X), \circ)$ es un grupo, donde

$$Biy(X) = \{f : X \rightarrow X/f \text{ es biyección}\} .$$

Si $X = G$ grupo, tenemos el subgrupo $Aut(G) \subseteq Biy(G)$, con $Aut(G)$ el conjunto de automorfismos de G .

Podemos mirar globalmente los automorfismos interiores como provenientes de la función

$$\begin{aligned} I : G &\longrightarrow Aut(G) \\ a &\longrightarrow I(a) = I_a \end{aligned}$$

que es un morfismo de (G, \cdot) en $(Aut(G), \circ)$.

$I(G) = \{I_a/a \in G\}$, la imagen de este morfismo, es el conjunto de automorfismos interiores de G .

Ejercicio: $I(G) \triangleleft Aut(G)$ (notar que $f \circ I_a \circ f^{-1} = I_{f(a)}$)

¿KerI ?

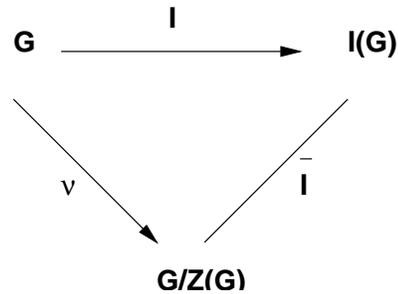
$$a \in KerI \Leftrightarrow I_a = id_G \Leftrightarrow (\forall x \in G) axa^{-1} = x \Leftrightarrow (\forall x \in G) ax = xa \Leftrightarrow (\forall x \in G) a \text{ conmuta con } x$$

Definición

El centro de un grupo (G, \cdot) es $Z(G) = \{a \in G/\forall x \in G ax = xa\}$. Así, $Z(G) = KerI \triangleleft G$.

Directamente del teorema del factor $G/Z(G) \cong I(G)$

El isomorfismo viene dado por la aplicación del teorema del factor al epimorfismo

**Notación:**

La operación $x \rightarrow axa^{-1}$ se suele llamar “conjugación de x por a ”, así, I_a es la conjugación por a en G .

1.4.3 Teorema de Correspondencia**Prop**

Si $f : G \rightarrow L$ es un morfismo de grupos, y $H \subseteq G$ es un subgrupo, se tiene $f^{-1}(f(H)) = (\text{Ker } f)H$.

Dem.

$$x \in f^{-1}(f(H)) \Leftrightarrow f(x) \in f(H) \Leftrightarrow (\exists h \in H) f(x) = f(h) \Leftrightarrow (\exists h \in H) f(xh^{-1}) = 1 \Leftrightarrow (\exists h \in H) xh^{-1} \in \text{Ker } f$$

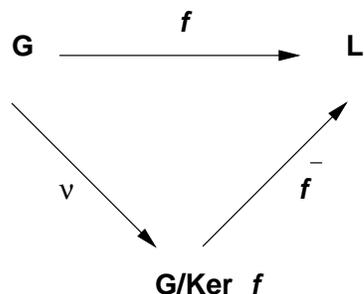
Sea $f : G \rightarrow L$ un epimorfismo de grupos, sabemos del teorema del factor, que

$$\begin{array}{ccc} \bar{f} : G/\text{Ker } f & \longrightarrow & L \\ [x] & \longrightarrow & f(x) \end{array} \text{ es isomorfismo}$$

Así, $\forall H' \subseteq L$ subgrupo, $\bar{f}^{-1}(H') \subseteq G/\text{Ker } f$ es subgrupo. (respectivamente, si $H' \triangleleft L$ respectivamente $\bar{f}^{-1}(H') \triangleleft G/\text{Ker } f$).

$$\begin{aligned} \bar{f}^{-1}(H') &= \{[x] \in G/\text{Ker } f / f(x) \in H'\} \\ &= \{x \cdot \text{Ker } f / x \in f^{-1}(H')\} \\ &= f^{-1}(H')/\text{Ker } f \end{aligned}$$

Con la observación de que $(\forall x \in f^{-1}(H')) [x] = x \cdot \text{Ker } f \subseteq f^{-1}(H') \cdot \text{Ker } f = f^{-1}(H')$, luego los elementos $[x] \in G/\text{Ker } f$, con $x \in f^{-1}(H')$ son elementos de $f^{-1}(H')/\text{Ker } f$.

**Prop**

Hay una correspondencia uno a uno entre subgrupos de G que contienen a $\text{Ker } f$ y subgrupos de L .

Subgrupos de G que contienen a $\text{Ker } f \longleftrightarrow$ Subgrupo de L

$$\begin{array}{ccc}
 f^{-1}(H') & \longleftrightarrow & H' \\
 H & \longrightarrow & f(H)
 \end{array}$$

Más aun , esto induce una correspondencia uno a uno:

Subgrupos normales de G que contienen a $\text{Ker } f \longleftrightarrow$ subgrupos normales de L

$$\begin{array}{ccc}
 f^{-1}(H') \triangleleft G & \longleftrightarrow & H' \triangleleft L \\
 H \triangleleft G & \longrightarrow & f(H) \triangleleft L
 \end{array}$$

Dem.

$f(f^{-1}(H')) = H'$ por que f es sobreyectiva

$f^{-1}(f(H)) = \text{Ker } f \cdot H = H$

(completar parte de subgrupos normales).

Situación usual: $H \triangleleft G$, $\nu : G \rightarrow G/H$

subgrupos de G (normales) \leftrightarrow subgrupos (normales) de G/H que contienen a H .

1.4.4 Teoremas de Isomorfismos**Primer teorema de isomorfismos**

Sea $f : G \rightarrow L$ un epimorfismo de grupos , y sea $H \triangleleft G$, con $H \supseteq \text{Ker } f$. Entonces la función f induce un isomorfismo

$$\begin{array}{ccc}
 \widehat{f} : G/H & \longrightarrow & L/f(H) \\
 [x] & \longrightarrow & [f(x)]
 \end{array}$$

Dem.

Por teorema de correspondencia $f(H) \triangleleft L$

$$f : G \rightarrow L, \nu : L \rightarrow L/f(H).$$

Sea $\tilde{f} = \nu \circ f$, que es epimorfismo, pues f y ν lo son.

El teorema del factor dice que se induce un isomorfismo

$$\bar{f} : G/\text{Ker}\tilde{f} \rightarrow L/f(H)$$

$$[x]_{\text{Ker}\tilde{f}} \rightarrow \tilde{f}(x) = [f(x)]_{f(H)}$$

$$\text{pero Ker}\tilde{f} = \text{Ker}(\nu \circ f) = f^{-1}(\nu^{-1}(1)) = f^{-1}(\text{Ker}\nu) = f^{-1}(f(H)) = H \cdot \text{Ker}f = H$$

Corolario

Si $f : G \rightarrow L$ es epimorfismo de grupos, y $H' \triangleleft L$, f induce un isomorfismo

$$\begin{aligned} \bar{f} : G/f^{-1}(H') &\longrightarrow L/H' \\ [x]_{f^{-1}(H')} &\longrightarrow [f(x)]_{H'} \end{aligned}$$

Dem.

Tomar $H = f^{-1}(H')$ en el teorema anterior y usar correspondencia.

Corolario

(lo que usualmente se llama primer teorema de isomorfismos). Sea G grupo $H, K \triangleleft G$, con $K \subseteq H$. Entonces

$$\begin{aligned} (G/K)/(H/K) &\cong G/H \\ [[x]_K]_{H/K} &\longleftrightarrow [x]_H \end{aligned}$$

Dem.

Notar que $H/K \triangleleft G/K$. Aplicamos el primer teorema de isomorfismos a $\nu : G \rightarrow G/K$, con el subgrupo normal $H \triangleleft G$ que contiene a $\text{Ker}\nu = K$

$$\bar{\nu} : G/H \longrightarrow (G/K)/\nu(H)$$

$$\text{con } \nu(H) = H/K$$

Segundo teorema de isomorfismos

Sea G grupo, H, K subgrupos de G , con $H \triangleleft G$. Entonces :

$$H \cap K \triangleleft G, H \triangleleft HK \text{ y}$$

$$K/H \cap K \cong HK/H$$

$$[x]_{H \cap K} \rightarrow [x]_H$$

Dem.

Considerar:

$$\begin{array}{ccc} & i & \nu \\ K & \hookrightarrow HK & \longrightarrow HK/H \\ x & \hookrightarrow x & \longrightarrow [x]_H \end{array}$$

Ver que $\nu \circ i$ es epimorfismo y calcular su núcleo.

Definición

Un grupo (G, \cdot) se dice finito si el conjunto G es finito. Se llama **Orden** del grupo a su número de elementos: $|G|$.

Proposición

Si (G, \cdot) es grupo finito, y H es un subgrupo de G , entonces $|H| \mid |G|$. (i.e $|H|$ es un divisor de $|G|$).

Dem.

\coprod : unión disjunta con respecto a la relación \approx_H

$$G = \coprod_{[x] \text{ clase de eq. de } \approx_H} [x]$$

$$\Rightarrow |G| = \sum_{xH \text{ es clase}} |xH|, \text{ pero } |xH| = |H|$$

$$\Rightarrow |G| = (\text{número de clases}) \cdot |H|$$

Definición

El cardinal de G/H , i.e., el número de clases de \approx_H se llama índice de H en G , y se anota $[G : H] = |G/H|$.

Fórmula: $|G| = [G : H] |H|$.

Ejemplo: si $|G|$ es primo, los únicos subgrupos de G son $\{1\}$ y G .

1.5 Acciones De Grupos Sobre Conjuntos

Definición

Sea (G, \cdot) un grupo, y $X \neq \emptyset$ un conjunto. Una acción (izquierda) de G en X es una función

$$\begin{array}{ccc} \varphi : G \times X & \longrightarrow & X \\ (g, x) & \longrightarrow & \varphi(g, x) \end{array}$$

(Notación: $\varphi(g, x) = gx$)

con las siguientes propiedades:

1. $(\forall x \in X) 1x = x$
2. $(\forall g, h \in G)(\forall x \in X) g(hx) = (g \cdot h)x$

Observación 1:

Una acción derecha de G sobre X es una función $\psi : X \times G \longrightarrow X$ con las

$$(x, g) \longrightarrow xg = \psi(x, g)$$

siguientes propiedades:

1. $(\forall x \in X) x1 = x$
2. $(\forall g, h \in G)(\forall x \in X) (xg)h = x(g \cdot h)$

Parece una “tomadura de pelo “, pero si a partir de ψ se define $\varphi : G \times X \longrightarrow X$ como $gx = \varphi(g, x) = \psi(x, g) = xg$, se tiene, por la propiedad 2. aplicada a ψ , que $h(gx) = (g \cdot h)x$, lo que no siempre es igual a la propiedad 2. de las acciones izquierdas.

Sin embargo, hay una manera de relacionar acciones izquierdas con derechas mediante lo siguiente:

Si ψ es una acción derecha de G en X , φ dada por $\varphi(g, x) = gx = xg^{-1} = \psi(x, g^{-1})$ es una acción izquierda.

Definición

Una terna (G, X, φ) donde φ es una acción de G en X , se suele llamar G -espacio (izquierdo).

Observación 2 :

Dada una acción φ de G sobre X , podemos definir para cada $g \in G$ la función

$\Phi_g : X \rightarrow X$ mediante $\Phi_g(x) = gx = \varphi(g, x)$. Se tiene:

1. $\Phi_1 = id_X$
2. $\Phi_{gh} = \Phi_g \circ \Phi_h$

De aquí Φ_g es invertible, con $(\Phi_g)^{-1} = \Phi_{g^{-1}}$

De este modo queda definida la función $\Phi : G \longrightarrow \text{Biy}(X)$

$$g \longrightarrow \Phi_g$$

Recordando que $(\text{Biy}(X), \circ)$ es un grupo, 2. dice que $\Phi : (G, \cdot) \rightarrow (\text{Biy}(X), \circ)$ es un morfismo.

Recíprocamente, dado un morfismo $\Psi : (G, \cdot) \rightarrow (\text{Biy}(X), \circ)$ se puede definir $\varphi(g, x) = \Psi_g(x)$ con $\Psi_g = \Psi(g)$, φ resulta ser una acción de G en X , tal que “ su Φ es Ψ ”.

Observación 3:

Si X es un espacio vectorial sobre un cuerpo K y $(\forall g \in G) \Phi_g$ es un isomorfismo lineal de X , entonces se habla de *Representaciones* de G en X .

Ejemplo 1: Acción de G sobre si mismo mediante conjugaciones.

$$X = G \quad \varphi(g, x) = gxg^{-1} = I_g(x)$$

Sabemos que $I : (G, \cdot) \longrightarrow (Aut(G), \circ)$ es un morfismo, y $(Aut(G), \circ)$ es un subgrupo de $(Biy(X), \circ)$, por lo tanto tenemos una acción de G sobre G .

Ejemplo 2: Acción de G sobre si mismo mediante traslaciones (izq).

$$\text{Dado } g \in G, \text{ se define la traslación izquierda por } g \text{ como } T_g: \begin{array}{ccc} G & \longrightarrow & G \\ x & \longrightarrow & T_g(x) = gx \end{array}$$

Evidentemente $\varphi(g, x) = gx$ (producto en G), es una acción de G sobre si mismo, y el morfismo asociado es $T : (G, \cdot) \longrightarrow (Biy(G), \circ)$

Es fácil ver que este morfismo T es inyectivo:

$$\text{Ker } T = \{g \in G / T_g = id_g\} = \{g \in G / (\forall x \in G) gx = x\} = \{1\}$$

Así, G se puede identificar con el subgrupo $T(G)$ (las traslaciones) en $Biy(X)$.

De aquí sale un conocido teorema:

Teorema

Todo subgrupo finito de orden n , es isomorfo a un subgrupo del grupo de permutaciones S_n de n símbolos.

Ejemplo:

$(\mathbb{Z}_3, +)$ es isomorfo a un subgrupo de S_3

+	0	1	2	
0	0	1	2	—————▶ f
1	1	2	0	—————▶ g
2	1	0	2	—————▶ h

$\{f, g, h\} \subseteq S_3$ es el subgrupo isomorfo a $(\mathbb{Z}_3, +)$

Ejemplo:

Sea ahora G un grupo y $H \subseteq G$ un subgrupo (no necesariamente normal).

$$X = G/H = \{[x]/x \in G\} = \{xH/x \in G\}$$

G actúa por traslaciones sobre G/H mediante $g(xH) = (gx)H$.

Definición

Sean (G, X, φ) y (G, Y, ψ) dos G -espacios .Una función $f : X \rightarrow Y$ se dice G -equivariante (con respecto a las acciones φ y ψ) o que f es un morfismo de los G - espacios (G, X, φ) y (G, Y, ψ) , ssi

$$(\forall g \in G)(\forall x \in X) f(gx) = gf(x) \text{ (i.e } f(\varphi(g, x)) = \psi(g, f(x)) \text{) .}$$

Un isomorfismo de G - espacios es un morfismo biyectivo . Se definen de manera natural los monomorfismos, epimorfismos , endomorfismos y automorfismos de G - espacios.

Definición

Sea φ una acción de G sobre X .La acción se dice **transitiva** ssi $(\forall x, y \in X)(\exists g \in G)$ tal que $y = gx$. (G, X, φ) se dice G - espacio homogéneo.

Ejemplo:

G actúa transitivamente sobre cualquier cociente G/H por traslación.

Definición

Sea X un G -espacio, y $x_o \in X$. Llamamos **estabilizador** de x_o (o grupo de isotropía) al conjunto

$$Est(x_o) = \{g \in G / gx_o = x_o\}.$$

Es directo que $Est(x_o)$ es subgrupo de G , y también que $Est(hx_o) = hEst(x_o)h^{-1}$

Así, si la acción es transitiva, todos los estabilizadores de los elementos de X son conjugados entre sí, y por lo tanto, isomorfos.

Teorema

Sea X un G -espacio homogéneo. Sea $x_o \in X$ un elemento cualquiera. Entonces X es isomorfo a $G/Est(x_o)$ (como G -espacios).

Dem.

Sea $f: G \rightarrow X$. Sean $g, h \in G$ tales que $g \approx_{Est(x_o)} h$ i.e.

$$g \rightarrow f(g) = gx_o$$

$$g^{-1}h \in Est(x_o) \Leftrightarrow g^{-1}hx_o = x_o \Leftrightarrow hx_o = gx_o \Leftrightarrow f(x) = f(g) \otimes$$

$$\text{podemos entonces definir } \bar{f}: G/Est(x_o) \rightarrow X$$

$$[g] \rightarrow \bar{f}([g]) = f(g) = gx_o$$

f es sobreyectiva por la transitividad de la acción de G en X , por lo tanto, \bar{f} es sobreyectiva.

\otimes da la inyectividad de \bar{f} , por lo tanto, \bar{f} es biyectiva.

Ejercicio:

Ver que \bar{f} es equivariente, por lo tanto, $X \cong G/Est(x_o)$.

Definición

Sea X un G -espacio. Sea $x_o \in X$, la **órbita** de x_o es $Orb(x_o) = \{gx_o / g \in G\} \subseteq X$.

Observación:

Definamos en X la relación $x \sim_G y \Leftrightarrow (\exists g \in G)$ tal que $y = gx$.

\sim_G es de equivalencia, con $[x_o] = Orb(x_o)$. Así, si $Orb(x_o) \neq Orb(x_1) \Rightarrow Orb(x_o) \cap Orb(x_1) = \emptyset$ y $\bigcup_{x \in X} Orb(x) = X$

Observación:

La acción es transitiva \Leftrightarrow hay una sólo órbita que es todo X .

En general, G actúa sobre cada órbita de forma cerrada:

$x \in Orb(x_o) \Rightarrow gx \in Orb(x_o)$, convirtiéndola en un G -espacio homogéneo.

Así $X = \coprod_{\lambda \in \Lambda} Orb(x_\lambda)$, y cada órbita es un G -espacio homogéneo. (cualquier G -espacio se escribe como unión disjunta de homogéneos) y además $Orb(x_\lambda) \cong G/Est(x_\lambda)$.

Ejemplo:

Volvamos al primer ejemplo, la acción de G sobre si mismo por conjugación.

$$gx = g \cdot x \cdot g^{-1}$$

(Notar que si G es abeliano, $gx = x \forall x, \forall g$).

Sea $x_o \in G$

$$\begin{aligned} Orb(x_o) &= \{gx_o g^{-1} / g \in G\} \\ &= \{ \text{conjugados de } x_o \} \\ &= conj(x_o) \text{ (clase de conjugación de } x_o \text{)} \end{aligned}$$

$$Orb(x_o) \cong G/Est(x_o)$$

$$\begin{aligned} Est(x_o) &= \{g \in G / gx_o = x_o\} \\ &= \{g \in G / g \cdot x_o \cdot g^{-1} = x_o\} \\ &= \{g \in G / g \cdot x_o = x_o \cdot g\} \\ &= Z(x_o) \text{ (centralizador de } x_o \text{)}. \end{aligned}$$

Corolario

El centralizador $Z(g)$ de un elemento cualquiera $g \in G$ es un subgrupo.

Como $G = \coprod_{\lambda \in \Lambda} Orb(x_\lambda)$ (un representante por cada órbita)

$$G = \coprod_{\lambda \in \Lambda} conj(x_\lambda)$$

Notemos que $x \in Z(G) \Leftrightarrow conj(x) = \{x\}$

Así repartiendo la unión en las clases con un elemento y el resto de las clases, queda:

$$G = Z(G) \coprod \left(\coprod_{\lambda \in \Lambda'} conj(x_\lambda) \right)$$

Con Λ' el conjunto que indexa las clases de conjugación con más de un elemento.

Corolario (fórmula de las clases)

Sea G un grupo finito .

$$|G| = |Z(G)| + \sum [G : Z(x_\lambda)]$$

Donde la suma se toma sobre un representante por cada clase de conjugación con más de un elemento.

Aplicación : (Propiedad)

Sea G un grupo finito no trivial (i.e $\neq \{1\}$) , de orden potencia de primo ($|G| = p^n, n \geq 1$ p primo). entonces $|Z(G)| > 1$.

Dem.

Probemos que , en la ecuación de las clases , $p/[G : Z(x_\lambda)]$ para cada uno de los sumandos. En efecto:

$$|G| = p^n = |Z(G)| + [G : Z(x_\lambda)]$$

$$\text{pero } [G : Z(x_\lambda)] = |\text{conj}(x_\lambda)| > 1$$

$$\Rightarrow [G : Z(x_\lambda)] = p^r \quad r \geq 1$$

$$\Rightarrow p / \sum [G : Z(x_\lambda)] , \text{ y como } p \mid |G|$$

$$\Rightarrow p \mid |Z(G)|$$

1.6 Teorema de Cauchy

Definición

Sea G un grupo , $g \in G$. Se llama **orden de g** a $|\langle \{g\} \rangle| = |\{g^n/n \in \mathbb{Z}\}| = O(g)$.

Algunas cosas directas:

Supongamos que g es de orden finito

- Si $g^n = 1 \Rightarrow O(g)/n$
 $\langle \{g\} \rangle \cong \mathbb{Z}/\text{Ker } f = O(g) \cdot \mathbb{Z} \cong \mathbb{Z}_{O(g)}$.
 Mejor aun , $\{n \in \mathbb{Z}/g^n = 1\} = O(g) \cdot \mathbb{Z} = \{ \text{múltiplos de } O(g) \}$
 En particular $O(g) = \min\{n > 0/g^n = 1\}$.
- Si $O(g) = m$ y $x \in \langle \{g\} \rangle$, entonces $x^m = 1$.(pues $(g^r)^m = (g^m)^r$).

Teorema de Cauchy

Sea G un grupo finito y p un primo tal que $p \mid |G|$. Entonces existe un elemento $g \in G$ de orden p .

Dem.

Primero Cauchy débil : caso en que G es un grupo finito abeliano.

Por inducción en $|G|$:

Partida ($|G| = 2$ o $|G|$ primo , el mismo argumento)

Si $|G|$ es primo y $p \mid |G|$, entonces $|G| = p$. En este caso , si $g \in G \setminus \{1\}$, $O(g) > 1$, pero como $O(g) \mid p \Rightarrow O(g) = p$.

Paso inductivo:

Hipótesis de Inducción : la propiedad es cierta para cualquier grupo abeliano de cardinal $< |G|$. Queremos probarlo para G .

Tomemos un elemento $g \in G \setminus \{1\}$. Hay dos casos:

1. $p \mid O(g)$

Se tiene entonces que $O(g) = pr$ para algún r .

$\Rightarrow g^{pr}$ es la primera vez que una potencia de g se hace 1.

por lo tanto, $(g^r)^p = 1$ es la primera vez que una potencia de g^r vale

1. Por lo tanto , $O(g^r) = p$

2. Si p no divide a $O(g)$

Sea $L = G / \langle \{g\} \rangle$ (este cociente tiene sentido pues, por ser G abeliano , todos sus subgrupos son normales).

$$|L| = \frac{|G|}{O(g)}$$

como p no divide a $O(g)$, entonces $p \mid |L|$. Usemos la H.I para L :

$\exists [h] \in L$ de orden p , por lo tanto , $[h]^p = [h^p] = [1] = \langle \{g\} \rangle$

por lo tanto $h^p = g^s$, para algún s

$$\Rightarrow (h^p)^{O(g)} = 1$$

$$\Rightarrow (h^{O(g)})^p = 1$$

\Rightarrow Hay dos posibilidades:

- $h^{O(g)} = 1$
- $O(h^{O(g)}) = p$

Descartemos $h^{O(g)} = 1$:

Si $h^{O(g)} = 1 \Rightarrow [h]^{O(g)} = [1] \Rightarrow p/O(g)$ (pues $O([h]) = p$) $\rightarrow \leftarrow$, pues estamos en el caso p no divide $O(g)$.

Por lo tanto, $h^{O(g)}$ no puede ser 1

$$\Rightarrow O(h^{O(g)}) = p$$

Resuelto para el caso de grupo abeliano.

Caso general: (G no necesariamente abeliano)

Por inducción en $|G|$.

Partida : para $|G|$ primo (basta con $|G| = 2$ abeliano)

Paso inductivo:

Usemos la ecuación de las clases para G

$$|G| = |Z(G)| + \sum [G : Z(x_\lambda)]$$

$Z(G) = G \Leftrightarrow G$ es abeliano (caso anterior).

Supondremos $Z(G) \subsetneq G$.

Analizamos los términos de la sumatoria de la derecha. Por cada clase de conjugación con más de un elemento, se escoge un x_λ . $[G : Z(x_\lambda)]$ es el número de elementos de esta clase de conjugación.

Si $p \nmid |Z(x_\lambda)|$, como $|Z(x_\lambda)| = \frac{|G|}{[G : Z(x_\lambda)]}$ y $[G : Z(x_\lambda)] > 1$

se tiene $|Z(x_\lambda)| < |G|$. por lo tanto, podemos aplicar la H.I a $Z(x_\lambda) \Rightarrow Z(x_\lambda)$ tiene un elemento de orden p .

Supongamos ahora, que $\forall x_\lambda$, p no divide a $Z(x_\lambda)$

$$\Rightarrow (\forall x_\lambda) p \nmid [G : Z(x_\lambda)]$$

$$\Rightarrow p \nmid \sum [G : Z(x_\lambda)] \text{ y como } p \nmid |G|$$

$$\Rightarrow p \nmid |Z(G)|$$

\Rightarrow aplicando H.I, $Z(G)$ tiene elementos de orden p .

Ejercicio:

Si G es abeliano finito, y $|G| = pq$ con p, q primos, entonces G tiene un elemento de orden pq .

1.7 P-Grupos y Teoremas de Sylow

Definición

Sea p un primo. Un grupo G se llama **p -grupo** ssi todo elemento $x \in G$ tiene orden potencia de p .

Ejercicio :

Si G es finito. G es p -grupo $\Leftrightarrow |G|$ es potencia de p

Continuamos con la definición:

- Si G es p -grupo , un p -subgrupo H de G , es un subgrupo de G que es p -grupo.
- Un **p -subgrupo de Sylow** de G es un p -subgrupo maximal con respecto a la inclusión. Es decir ,es p -subgrupo de Sylow ssi es p -subgrupo de G , y no está contenido estrictamente en ningún otro p -subgrupo.

Ejercicios:

1. Si G es un grupo y p es primo , entonces G tiene p -subgrupos de Sylow (eventualmente triviales $\{1\}$) .
2. Si G es finito y $p \mid |G|$, G tiene p -subgrupos de Sylow no triviales.(G no trivial).
3. Si G es un grupo:
 - (a) Si $H \subseteq G$ es un p -subgrupo , los conjugados de H (gHg^{-1} , $g \in H$) son p -subgrupos.
 - (b) Si $P \subseteq G$ es un p -subgrupo de Sylow ,entonces sus conjugados son todos p -subgrupos de Sylow .

Un par de Lemas:

Lema 1

Sea G un grupo y $H \triangleleft G$.Entonces G es un p -grupo $\Leftrightarrow H$ y G/H son p -grupos.

Dem.

\Rightarrow)

Que H es un p -grupo es evidente .

Sea $[g] \in G/H$. Como $g \in G$, $O(g) = p^j$

$\Rightarrow g^{p^j} = 1 \Rightarrow [g]^{p^j} = [g^{p^j}] = [1] \Rightarrow O([g])/p^j \Rightarrow O([g])$ es potencia de p

\Leftarrow)

Sea $g \in G$, $[g] \in G/H$ p -grupo

$\Rightarrow O([g]) = p^j$ algún j

$\Rightarrow [g]^{p^j} = [1] = H$

$\Rightarrow [g^{p^j}] = H$

$\Rightarrow g^{p^j} \in H$ p -grupo

$\Rightarrow O(g^{p^j}) = p^k \Rightarrow g^{p^{j+k}} = 1 \Rightarrow O(g)/p^{j+k}$, por lo tanto , es potencia de p .

Lema 2

Sea G un grupo, $P \subseteq G$ un p -subgrupo de Sylow. Si $g \in G$ es tal que :

- $O(g) = p^j$ algún j , y
- $gPg^{-1} = P$

Entonces $g \in P$.

Observación:

Sea H subgrupo de G . Definimos el **normalizador** de H como $N(H) = \{g \in G / gHg^{-1} = H\}$.

Queda como **Ejercicio** probar que :

1. $N(H)$ es subgrupo de G .
2. $H \triangleleft N(H)$, y es el más grande de los subgrupos de G que contienen a H como subgrupo normal.

El **Lema 2** se puede enunciar de la siguiente manera:

Si P es un p -subgrupo de Sylow de G y $g \in N(P)$ tiene orden potencia de p , entonces $g \in P$.

Dem. (lema 2)

Considerando el normalizador $N(P)$ del grupo P , se tiene:

$$P \triangleleft N(P)$$

$$g \in N(P)$$

Tomemos el cociente $N(P)/P$ y la clase $[g] \in N(P)/P$.

Sea $K = \langle \{[g]\} \rangle \subseteq N(P)/P$.

Recordando el teorema de correspondencia para subgrupos cocientes:

$K = L/P$ con L subgrupo de $N(P)$ que contiene a P .

Probemos que L es un p -grupo. Por el Lema 1

L p -grupo $\Leftrightarrow P$ p -grupo y L/P p -grupo.

K es cíclico generado por $[g]$.

Pero g tiene orden potencia de $p \Rightarrow [g]$ también y $O([g]) = O(L/P)$, por lo tanto, L/P es un p -grupo

$\Rightarrow L$ es un p -grupo. Pero $L \supseteq P$ y P es p -subgrupo de Sylow

$\Rightarrow L = P$, y como $g \in L \Rightarrow g \in P$.

¿Cuántos conjugados tiene el subgrupo K mediante elementos de H ?

Sea G grupo, H y K subgrupos de G .

Queremos calcular $|\{h \cdot K \cdot h^{-1}/h \in H\}|$

Podemos poner este problema en el siguiente contexto:

Estudiar la acción por conjugación del grupo H sobre $S = \{L \subseteq G/L \text{ es subgrupo de } G\}$.

$$\begin{aligned} H \times S &\longrightarrow S \\ (h, l) &\longrightarrow hl = h \cdot l \cdot h^{-1} \end{aligned}$$

La pregunta tiene que ver con $Orb(K)$, ($K \in S$)

Sabemos lo siguiente:

$Orb(K) \cong H/Est(K)$ como H -espacios.

$$\begin{aligned} Est(K) &= \{h \in H/hK = K\} \\ &= \{h \in H/h \cdot K \cdot h^{-1} = K\} = N_H(K) \end{aligned}$$

Normalizador de K en H .

$$\Rightarrow Orb(K) \cong H/N_H(K)$$

(Evidentemente, $N_H(K)$ es subgrupo de H)

Así, si H es finito,

$$|\{h \cdot k \cdot h^{-1}/h \in H\}| = [H : N_H(K)] = \frac{|H|}{|N_H(K)|}$$

Notar que $N(K) = N_G(K)$ así

$$\{g \cdot K \cdot g^{-1}/g \in G\} \cong G/N(K), \text{ y si } G \text{ es finito, } |\{g \cdot K \cdot g^{-1}/g \in G\}| = [G : N(K)].$$

1.7.1 Segundo Teorema de Sylow

Sea G un grupo finito y p un primo. Entonces:

1. El número de p -subgrupos de Sylow de G es $\equiv 1 \pmod{p}$
2. El número de p -subgrupos de Sylow de G es un divisor de $|G|$, mejor aun, este número es $[G : N(P)]$, para P un subgrupo de Sylow dado.
3. Todos los p -subgrupos de Sylow de G son conjugados entre sí.

Dem.

Sea P un p -subgrupo de Sylow, contemos los conjugados de P :

$$|\{gPg^{-1}/g \in G\}| = |Orb(P)|.$$

Se puede ver como G actúa por conjugación sobre sus subgrupos:

$S = \{H \subseteq G/H \text{ subgrupo de } G\}$

$$\begin{aligned} G \times S &\longrightarrow S \\ (g, H) &\longrightarrow gHg^{-1} \end{aligned}$$

Queremos el cardinal de una órbita : $Orb(P) = \{gPg^{-1}/g \in G\}$

Para contar el número de elementos de $Orb(P)$ hacemos actuar por conjugación $P \subseteq G$ sobre $Orb(P)$.

$$|Orb(P)| = \sum_{P' \in Orb(P)} |Orb_P(P')|$$

- Si $P' = P$, $Orb_P(P) = \{hPh^{-1}/h \in P\} = P \Rightarrow |Orb_P(P)| = 1$.
- Si $P' \neq P$, $|Orb_P(P')| = |\{gP'g^{-1}/g \in P\}| = [P : N_P(P')]$
 donde $N_P(P') = \{g \in P/gP'g^{-1} = P'\}$,
 pero $g \in P \Rightarrow O(g)$ es potencia de p , digamos $O(g) = p^k$,
 entonces, por el LEMA 2, y dado que $gP'g^{-1} = P'$ p -subgrupo de Sylow, concluimos que $g \in P'$.
 Por lo tanto, $N_P(P') = P' \cap P$.
 Veamos que $P' \cap P \neq P$, i.e $P' \cap P \subsetneq P$.
 Supongamos que $P' \cap P = P$, i.e que $P \subseteq P' \Rightarrow P' = P$ pues son p -subgrupos de Sylow
 $\rightarrow \leftarrow$
 Por lo tanto, $P' \cap P \subset P$ (subc. estricto)
 $\Rightarrow [P : P \cap P'] > 1$, pero $[P : P \cap P']$ es divisor de p
 $\Rightarrow [P : P \cap P'] = p^j$ para algún $j \geq 1$

$$\Rightarrow |Orb(P)| = 1 + \sum_{P' \neq P} p^j \equiv 1 \pmod{p}$$

¿Hay o no un p -subgrupo de Sylow $H \subseteq G$ que no sea conjugado con P ?

Supongamos que existe tal subgrupo, y contemos todos sus conjugados haciendo actuar a P sobre $\{gHg^{-1}/g \in G\}$. Este conjunto se parte en órbitas, y con los mismos calculos anteriores:

$$|Orb(H')| = |\{gH'g^{-1}/g \in P\}| = [P : N_P(H')] = p^l l \geq 1$$

por lo tanto $p/ |Orb(H')|$, $\forall H'$ conjugado de H

\Rightarrow número de conjugados de $H = 0 \equiv \pmod{p} \rightarrow \leftarrow$ (pues acabamos de probar que los conjugados de un p -subgrupo de Sylow son $\equiv 1 \pmod{p}$).

Así, no hay p -subgrupos de Sylow que no sean conjugados de P .

Esto prueba 3. del teorema, y luego se concluye 1. y 2.

1.7.2 Primer Teorema de Sylow

Sea G un grupo finito, p un primo, tal que $|G| = p^k q$, con q primo relativo de p (i.e p no divide a q), entonces los p -subgrupos de Sylow de G tienen cardinal p^k .

Dem.

Notemos que todos los p -subgrupos de Sylow de G tienen igual cardinal, pues son conjugados, por lo tanto, isomorfos.

Sea P un p -subgrupo de Sylow de G . Lo que queremos probar es que $\frac{|G|}{|P|} = [G : P]$, es decir, que $[G : P]$ no es divisible por p .

Del segundo teorema de Sylow se tiene que $[G : N(P)] = \frac{|G|}{|N(P)|} \equiv 1 \pmod{p}$ (no es divisible por p)

y como $\frac{|G|}{|P|} = \frac{|G|}{|N(P)|} \cdot \frac{|N(P)|}{|P|}$.

Debemos entonces probar que $[N(P) : P]$ no es divisible por p .

Pero:

$[N(P) : P] = |N(P)/P|$ (grupo cociente, pues $P \triangleleft N(P)$)

Así, queremos probar que el orden del grupo $N(P)/P$ no es divisible por p .

Por contradicción, supongamos que el orden de $N(P)/P$ es divisible por p .

Por el teorema de Cauchy, $N(P)/P$ debe tener algún elemento de orden p :

$$O([g]) = p$$

$$\Rightarrow [g]^p = [1] = P$$

$$\Leftrightarrow g^p \in P \Rightarrow (g^p)^{p^j} = 1 \text{ para algún } j.$$

$$g^{p^{j+1}} = 1 \Rightarrow O(g) \text{ es potencia de } p.$$

Pero $g \in N(P) \Rightarrow gPg^{-1} = P$, y como $O(g)$ es potencia de p , por lema 2, se tiene que $g \in P$.

Pero si $g \in P \Rightarrow O([g]) = 1 \rightarrow \leftarrow$

Así p no divide a $|N(P)/P|$

Aplicación

¿Cuántos grupos (salvo isomorfismos) de orden 15 hay?

Sea G un grupo, con $|G| = 15$.

Sea P_3 un 3-subgrupo de Sylow de G

Sea P_5 un 5-subgrupo de Sylow de G

Número de conjugados de $P_3 = \text{Número de 3-subgrupos de Sylow de } G \equiv 1 \pmod{3} = [G : N(P_3)]$

$$[G : N(P_3)][N(P_3) : P_3] = [G : P_3]$$

Número de conjugados de P_3 es un divisor de $[G : P_3] = \frac{|G|}{|P_3|} = \frac{15}{3} = 5$

Hay dos divisores de 5:

1. $1 \equiv 1 \pmod{3}$

2. $5 \equiv 2 \pmod{3}$

Pero sabemos que el número de conjugados de P_3 es $\equiv 1 \pmod{3}$, por lo tanto, descartamos 2. y concluimos que P_3 no tiene más conjugados, i.e $P_3 \triangleleft G$.

$|P_5| = 5$

Número de conjugados de $P_5 \equiv 1 \pmod{5} = [G : N(P_5)]$ divisor de $[G : P_5] = 3 \Rightarrow$ sólo uno, por lo tanto, $P_5 \triangleleft G$.

$P_3 \cap P_5$ es subgrupo de P_3 y P_5 , por lo tanto, debe dividir a $|P_3| = 3$ y a $|P_5| = 5$, $\Rightarrow P_3 \cap P_5 = \{1\}$.

(Se probará más adelante) $\Rightarrow P_3 P_5 \cong P_3 \times P_5$

$G = P_3 P_5 \cong P_3 \times P_5$

pero P_3 y P_5 son cíclicos $\Rightarrow P_3 \cong \mathbb{Z}_3$ y $P_5 \cong \mathbb{Z}_5$, por lo tanto, $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5$.

\Rightarrow Hay sólo un grupo de orden 15

Ejercicio:

¿Cuántos grupos de orden 6 hay ?

Prop

Sea G un grupo de orden p^k , entonces existe una cadena de subgrupos

$G_0 = \{1\} \subset G_1 \subset \dots \subset G_k = G$, con

$|G_i| = p^i \quad i = 0 \dots k$, $G_i \triangleleft G \quad i = 0 \dots k$

Dem.

Necesitaremos la propiedad ya vista siguiente :

Si H es un p - grupo finito no trivial ($|H| > 1$), entonces su centro es no trivial ($|Z(H)| > 1$).

Por inducción en i :

Propiedad para i : \exists cadena $G_0 \subset G_1 \subset \dots \subset G_i$,

con $|G_j| = p^j$, $G_j \triangleleft G$, $\forall j = 0 \dots i$

$i = 0$:

$G_0 = \{1\} \triangleleft G$ es cierta.

Pasemos de i a $i + 1$

Sea $L = G/G_i$ grupo no trivial (pues $i + 1 \leq k$)

$$|L| = [G : G_i] = \frac{|G|}{|G_i|} = \frac{p^k}{p^i} = p^{k-i}$$

$\Rightarrow L$ es p - grupo no trivial

$\Rightarrow Z(L)$ es no trivial . ($|Z(L)| = p^\omega$ con $\omega \geq 1$)

Sea $[g] \in Z(L)$ un elemento de orden p (existe , por teo. de Cauchy)

$$K = \langle \{[g]\} \rangle = \{[g]^t / t \in \mathbb{Z}\} \subseteq L , |K| = p$$

como $K = \langle \{[g]\} \rangle$ es un subgrupo del centro de L , entonces $K \triangleleft L$

Por teorema de correspondencia , $K = H/G_i$, con $H \triangleleft G$, $H \supseteq G_i$, $|H| = [H : G_i] |G_i|$

$$\Rightarrow |H| = p^{i+1}$$

por lo tanto , podemos definir $G_{i+1} = H$ y tenemos

$$G_0 \subset G_1 \subset \dots \subset G_i \subset G_{i+1} , \text{ con } |G_j| = p^j$$

Estudiamos el problema siguiente :

G grupo , H, N subgrupos de G , $N \triangleleft G$. Bajo estas condiciones sabemos que

$$NH = \{nh / n \in N, h \in H\} \text{ (subgrupo de } G \text{)}.$$

Agregamos además la hipótesis de que $N \cap H = \{1\}$. Queremos “entender” NH

Sean $n_1 h_1, n_2 h_2 \in NH$, $(n_1 h_1)(n_2 h_2) = [n_1(h_1 n_2 h_1^{-1})](h_1 h_2)$. Podríamos definir en $N \times H$ una operación $(n_1 h_1)(n_2 h_2) = [n_1(h_1 n_2 h_1^{-1})](h_1 h_2)$

Marco general:

N, H grupos . H actúa de algún modo en N por automorfismos:

$$\begin{aligned} \Phi : H &\longrightarrow \text{Aut}(N) \\ h &\longrightarrow \Phi_h \end{aligned}$$

$$\Phi_h(n_1 n_2) = \Phi_h(n_1) \Phi_h(n_2)$$

$$\Phi_h(n) = hn$$

En esta situación podemos definir el **Producto torcido** o **Producto semidirecto** de N y H por $N \times_\Phi H$.

Como conjunto , $N \times_\Phi H = N \times H$

La operación es $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \Phi_{h_1}(n_2), h_1 \cdot h_2)$

Caso muy particular :

N, H grupos cualquiera , y H actúa en N trivialmente :

$$hn = n \quad \forall n$$

$$\Phi_h(n) = id_N(n) = n$$

En este caso $N \times_\Phi H = N \times H$ con operación componente a componente: $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot n_2, h_1 \cdot h_2)$

Prop

Si N y H son grupos y H actúa sobre N por automorfismos, entonces $N \rtimes_{\Phi} H$, recién definido, es un grupo.

Neutro: $(1, 1) \in N \rtimes_{\Phi} H$

Inverso: $(n, h)^{-1} = (\Phi_{h^{-1}}(n^{-1}), h^{-1})$

Volvamos por un momento a la situación original:

G grupo

N, H subgrupos

$N \triangleleft G$

$N \cap H = \{1\}$

En este caso, H actúa por conjugación sobre N :

$\Phi_h(n) = hnh^{-1} \in N \triangleleft G$ (Φ_h es un automorfismo de N)

Los elementos de $NH \subseteq G$ se multiplicaban mediante

$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \Phi_{h_1}(n_2), h_1 \cdot h_2)$

Prop

La función $f: N \rtimes_{\Phi} H \longrightarrow NH$ es un isomorfismo del grupo $N \rtimes_{\Phi} H$ en el subgrupo de G , NH .

$$(n, h) \longrightarrow n \cdot h$$
Dem.

Que f es isomorfismo es por definición de la operación en $N \rtimes_{\Phi} H$

Que f es sobreyectiva es directo.

La inyectividad de f viene de $N \cap H = \{1\}$

$\text{Ker } f = \{(n, h) / f(n, h) = 1\} = \{(n, h) / n \cdot h = 1\} = \{(n, h) / n = h^{-1}\} = N \cap H$

Prop

G grupo, $N \triangleleft G$, $H \triangleleft G$ y $N \cap H = \{1\}$.

Entonces N y H conmutan, ($\forall n \in N, \forall h \in H, n \cdot h = h \cdot n$)

y $NH \cong N \times H$ ($(n, h) \rightarrow (n, h)$).

Dem.

Sólo hay que probar que N y H conmutan :

Sean $n \in N$, $h \in H$.

$$[n, h] = n \cdot h \cdot n^{-1} \cdot h^{-1} \in N \cap H = \{1\}$$

$$\Rightarrow n \cdot h = h \cdot n$$

$$(\Rightarrow \Phi_h(n) = h \cdot n \cdot h^{-1} = n)$$

En el caso general , si llamamos $G = N \rtimes_{\Phi} H$, podemos considerar los subconjuntos:

$$\tilde{N} = \{(n, 1) / n \in N\} \subseteq G$$

$$\tilde{H} = \{(1, h) / h \in H\} \subseteq G$$

Directamente , \tilde{N} y \tilde{H} son subgrupos de G .

$$\begin{array}{ccc} \varphi_1 : N & \longrightarrow & \tilde{N} \\ n & \longrightarrow & (n, 1) \end{array} \quad \begin{array}{ccc} \varphi_2 : H & \longrightarrow & \tilde{H} \\ h & \longrightarrow & (1, h) \end{array} \quad \text{son isomorfismos.}$$

También :

1. $\tilde{N} \cap \tilde{H} = \{(1, 1)\}$
2. $\tilde{N} \triangleleft G$
3. $\tilde{N}\tilde{H} = G$
4. La acción de H sobre N se convierte en acción por conjugación de \tilde{H} sobre \tilde{N} , vía los isomorfismos φ_1 y φ_2 .

¿Cuántos grupos de orden 6 hay ?

$$|G| = 6 = 2 \cdot 3$$

$$\Rightarrow |P_2| = 2 \Rightarrow P_2 \cong (\mathbb{Z}_2, +)$$

$$|P_3| = 3 \Rightarrow P_3 \cong (\mathbb{Z}_3, +)$$

$$P_2 \cap P_3 = \{1\}$$

Número de conjugados de $P_2 \equiv 1 \pmod{2}$, además debe dividir a 3 $\Rightarrow 1, 3$

Hay dos posibilidades:

1. Existe un 2- subgrupo de Sylow $\Rightarrow P_2 \triangleleft G$
2. Existen 3 2- subgrupos de Sylow \Rightarrow no son normales.

Número de conjugados de $P_3 \equiv 1 \pmod{3}$, divisor de $2 \Rightarrow 1$, por lo tanto, $P_3 \triangleleft G$.

Revisemos las posibilidades para P_2 :

En la situación 1.

$$P_2, P_3 \triangleleft G, P_2 \cap P_3 = \{1\}$$

$$\Rightarrow P_2 P_3 \cong P_2 \times P_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \text{ Abeliano.}$$

Hay, salvo isomorfismos, un sólo grupo abeliano de 6 elementos.

($\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, buscar un isomorfismo).

En la situación 2.

$$G = P_3 P_2 \cong P_3 \rtimes_{\Phi} P_2 \cong \mathbb{Z}_3 \rtimes_{\Phi} \mathbb{Z}_2$$

Si queremos saber más sobre que es G , hay que encontrar los posibles $\mathbb{Z}_3 \rtimes_{\Phi} \mathbb{Z}_2$ (con acción no trivial de \mathbb{Z}_2 en \mathbb{Z}_3).

Acciones por automorfismos de \mathbb{Z}_2 en \mathbb{Z}_3

$$\phi: \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\left. \begin{array}{l} \phi_0 = id_{\mathbb{Z}_3} \\ \phi_1 (\neq id_{\mathbb{Z}_3}) \end{array} \right\} \text{ morfismo: } \phi_1 \circ \phi_1 = id_{\mathbb{Z}_3}$$

Hay que encontrar los posibles automorfismos de \mathbb{Z}_3 Φ_1 :

·) no triviales ($\neq id$)

·) su cuadrado sea la identidad.

Veamos como son los automorfismos de \mathbb{Z}_3 , pero primero, algo más general, los Endomorfismos de \mathbb{Z}_n .

$$f: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$a +_n b \longrightarrow f(a +_n b) = f(a) +_n f(b)$$

$$f(1 + 1) = f(1) + f(1)$$

$$\vdots \quad \quad \quad \vdots$$

$$f(k) = k \cdot f(1)$$

\Rightarrow escogiendo $f(1)$ definimos el endomorfismo.

$$\forall z \in \mathbb{Z}_n, f_z: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$k \longrightarrow kz$$

es endomorfismo, $\text{End}(\mathbb{Z}_n) = \mathbb{Z}_n$

¿Biyectivos?

Aquellos f_z en que z tiene inverso multiplicativo, es decir, f_z en que z es primo relativo con n .

($\text{Aut}(\mathbb{Z}_n), \circ$) $\cong (\mathbb{Z}_n^x, \cdot_n)$ (\mathbb{Z}_n^x : grupo multiplicativo de los invertibles de \mathbb{Z}_n).

$n = 3$

$$(Aut(\mathbb{Z}_3), \circ) \cong (\{1, -1\}, \cdot_3)$$

Ambas f_1 y f_{-1} satisfacen $f_1^2 = f_{-1}^2 = id$. Pero $f_1 = id$, por lo tanto el único automorfismo que sirve para ser ϕ_1 es f_{-1} .

En la acción $\phi : \mathbb{Z}_2 \rightarrow \mathbb{Z}_3$, en el caso 2., $\phi_1 \in Aut(\mathbb{Z}_3)$ debe ser multiplicación por -1 .

El caso 2. es $\mathbb{Z}_2 \times_{\phi} \mathbb{Z}_3$, con :

$(n_1, h_1) \cdot (n_2, h_2) = (n_1 +_3 \phi_{h_1}(n_2), h_1 +_2 h_2) = (n_1 +_3 (-1)^{h_1} n_2, h_1 +_2 h_2)$ Conclusión: Hay dos, salvo isomorfismos, grupos de orden 6 :

1. \mathbb{Z}_6 Abeliano
2. S_3 No Abeliano

Ejercicio:

Mostrar que hay dos grupos de orden 4 : \mathbb{Z}_4 y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1.8 Pequeño estudio de (S_n, \circ)

Recuerdo:

$$X_n = \{1, \dots, n\}$$

$$S_n = \text{Biy}(X_n) = \{\sigma : X_n \rightarrow X_n / \sigma \text{ es biyección}\}$$

(S_n, \circ) es un grupo de orden $n!$. (grupo simétrico de grado n)

$$\text{Notación para } \sigma \in S_n : \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Definición

Un $\sigma \in S_n$ se dice "ciclo de largo k " ($k \leq n$) ssi $\exists i_1, i_2, \dots, i_k$ distintos entre sí en X_n , tales que $\sigma(i_j) = i_{j+1}$ $j = 1, \dots, k-1$ y $\sigma(i) = i$ si $i \notin \{i_1, \dots, i_k\}$.

Observación:

No toda permutación es un ciclo. Por ejemplo :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4 \text{ y no es un ciclo.}$$

σ es producto (composición) de dos ciclos :

$$\tau_1 = (12) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad \tau_2 = (34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1 = \sigma$$

Definición

Dos ciclos $\sigma = (i_1 \dots i_k) \in S_n$ y $\tau = (j_1 \dots j_l) \in S_n$ se dicen “disjuntos” ssi $\{i_1 \dots i_k\} \cap \{j_1 \dots j_l\} = \emptyset$.

Ejercicio:

Si σ y τ son ciclos disjuntos, entonces conmutan

Prop

Todo $\sigma \in S_n \setminus \{1\}$ se escribe de manera única (salvo por el orden de los factores) como producto de ciclos disjuntos (a pares). $\sigma = \sigma_1 \circ \dots \circ \sigma_l$ σ_j y σ_i disjuntos $\forall j \neq i$.

Dem.

Sea $G = \langle \{\sigma\} \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^r\}$ subgrupo de S_n .

Definamos la siguiente acción de G sobre X_n :

$$G \times X_n \longrightarrow X_n$$

$$(\tau, i) \longrightarrow \tau i = \tau(i)$$

Si O_1, \dots, O_l son las órbitas de la acción de G sobre X_n de cardinal > 1 , entonces son disjuntas, y $\sigma = \sigma_1 \dots \sigma_l$, donde σ_j es el ciclo dado por: Tomamos $c \in O_j$, $\sigma_j = (c \sigma(c) \sigma^2(c) \dots \sigma^{m-1}(c))$ con $m_j = |O_j|$ (convencerse de que σ es $\sigma_1 \circ \dots \circ \sigma_l$).

La unicidad (salvo orden de los factores) sale de que si $\sigma = \tilde{\sigma}_1 \circ \dots \circ \tilde{\sigma}_r$, con los $\tilde{\sigma}_j$ ciclos disjuntos, entonces las órbitas (de cardinal > 1) de σ , serán los ciclos de los $\tilde{\sigma}_j$.

Observación:

1. Si $\sigma \in S_n$ es un ciclo de largo k , $O(\sigma) = |\{\sigma^i/i \in \mathbb{Z}\}| = k$
2. Si $\sigma_1, \dots, \sigma_r$ son ciclos disjuntos, $(\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_r)^l = \sigma_1^l \circ \dots \circ \sigma_r^l$. De aquí resulta que si $\sigma \in S_n$, $O(\sigma) = mcm(O(\sigma_1), \dots, O(\sigma_k))$ cuando la descomposición de σ en ciclos disjuntos es $\sigma = \sigma_1 \circ \dots \circ \sigma_k$ $O(\sigma) = mcm(\text{largo de sus ciclos})$.

Algunas fórmulas útiles:

1. Si $\sigma = (i_1 i_2 \dots i_k)$ es un ciclo de largo k , y $\tau \in S_n$ es cualquier permutación, entonces $\tau \sigma \tau^{-1} = (\tau(i_1) \tau(i_2) \dots \tau(i_k))$.
2. $(1 \ 2 \ \dots \ k)(k \ k+1 \ \dots \ l) = (1 \ 2 \ \dots \ k \ k+1 \ \dots \ l)$
3. $(1 \ 2 \ \dots \ k-1 \ k)(k-1 \ k \ k+1 \ \dots \ l) = (1 \ 2 \ \dots \ k-1)(k \ k+1 \ \dots \ l)$

Definición

Una trasposición $\tau \in S_n$ es un ciclo de largo 2 : $\tau = (i_1 i_2)$.

Prop

Toda permutación $\sigma \in S_n$ es producto de trasposiciones.

Prop

Para $n \geq 3$, $Z(S_n) = \{1\}$.

Dem.

Si $\sigma \in S_n$, $\sigma = (i_1 i_2 \dots i_k)(j_1 \dots)$ σ no conmuta con $\tau = (i_k j_1)$.

$\tau \circ \sigma \circ \tau = (i_1 i_2 \dots j_1)(i_k \dots) \neq \sigma$,

si no , $\sigma = (i_2 i_3 \dots)$ σ no conmuta con $\tau = (i_2 i_3)$.

1.8.1 Signo de una permutación

Si $\sigma \in S_n$, la matriz de permutación P_σ , asociada a σ es :

$$p_\sigma = [e_{\sigma(1)} \quad e_{\sigma(2)} \quad \dots \quad e_{\sigma(n)}] \quad \text{con } e_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \end{pmatrix} \leftarrow j \text{ la columna } j \text{ de } I_n$$

Prop

Si $\sigma, \tau \in S_n$, entonces $P_\sigma \cdot P_\tau = P_{\sigma \circ \tau}$

Dem.

Por columnas:

$$\begin{aligned} \text{col}_j(P_\sigma \cdot P_\tau) &= P_\sigma \cdot \text{col}_j(P_\tau) = P_\sigma \cdot e_{\tau(j)} = \sum_{i=1}^n \delta_{i\tau(j)} \cdot e_{\sigma(i)} = e_{\sigma(\tau(j))} \\ &= e_{\sigma \circ \tau(j)} \\ &= \text{col}_j(P_{\sigma \circ \tau}) \end{aligned}$$

Observación:

$\sigma \longrightarrow P_\sigma$ es un morfismo inyectivo de (S_n, \circ) a $(GL(n), \cdot)$
con $GL(n)$: matrices invertibles de $n \times n$.

Definición

El signo de una permutación $\sigma \in S_n$ se define como :

$$\text{sign}(\sigma) = (-1)^\sigma = \det(P_\sigma)$$

Es claro que si τ es trasposición , $(-1)^\tau = -1$. Entonces , si $\sigma \in S_n$ cualquiera , dado que $\sigma = \tau_1 \circ \dots \circ \tau_k$, con τ_1, \dots, τ_k trasposiciones $\Rightarrow P_\sigma = P_{\tau_1} \cdot \dots \cdot P_{\tau_k} \Rightarrow (-1)^\sigma = \det(P_{\tau_1} \cdot \dots \cdot P_{\tau_k}) = (-1)^{\tau_1} \cdot \dots \cdot (-1)^{\tau_k} = (-1) \cdot \dots \cdot (-1) = (-1)^k$

Así , tenemos una función $\text{sgn} : S_n \longrightarrow \{-1, 1\}$ que es un epimorfismo de (S_n, \circ) y $(\{-1, 1\}, \cdot)$
 $\sigma \longrightarrow \text{sgn}(\sigma) = (-1)^\sigma$

Además , $\text{sgn}(\sigma) = 1$ si σ se descompone como un número par de trasposiciones y $\text{sgn}(\sigma) = -1$ si σ se descompone como un número impar de trasposiciones.

Notación:

Si $\sigma \in S_n$ es tal que su signo es 1 , entonces decimos que σ es par , si no , σ se dice impar.

Definición

Llamamos “Grupo Alternante de grado n “ a $A_n = \text{Ker}(\text{sgn}) \triangleleft S_n$ $A_n = \{\sigma \in S_n / \sigma \text{ es par} \}$.

Prop

$$|A_n| = \frac{n!}{2}$$

Dem.

$$S_n/A_n \cong \{-1, 1\} \Rightarrow |S_n/A_n| = \frac{|S_n|}{|A_n|} = 2 \Rightarrow |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Notar que A_n es un subgrupo propio ($\neq S_n$) maximal en S_n :

$$\text{Si } S_n \supseteq H \supseteq A_n \Rightarrow [S_n : A_n] = 2 = [S_n : H][H : A_n]$$

$$\Rightarrow ([S_n : H] = 1 \text{ y } [H : A_n] = 2 \Rightarrow H = S_n) \text{ o } \Rightarrow ([S_n : H] = 2 \text{ y } [H : A_n] = 1 \Rightarrow H = A_n)$$

Observación : esto es una particularidad de los subgrupos de índice primo de un grupo dado.

Prop

A_n está generado por los ciclos de largo 3.

Dem.

1. Un ciclo de largo 3 está en A_n :
 $(i j k) = (i j)(j k) \in A_n$
2. Todo elemento de A_n es producto de ciclos de largo 3 .
 Basta hacerlo para productos $\tau_1\tau_2$ de 2 trasposiciones:
 - (a) $\tau_1 = \tau_2 \Rightarrow \sigma = 1$
 - (b) $(i j)(j k) = (i j k) \quad i \neq j \neq k$
 - (c) $(i j)(k l) = (i j k)(j k l)$ (disjuntos)

Prop

A_n está generado por los cuadrados de los elementos de S_n , es decir , $A_n = \langle \{\sigma^2 / \sigma \in S_n\} \rangle$.

Dem.

1. σ^2 es par
2. Los ciclos de largo 3 son cuadrados.

Definición

Si G es un grupo , un subgrupo H de G , se dice subgrupo característico ssi $\forall f : G \rightarrow G$ automorfismo , $f(H) = H$.

En particular , H subgrupo característico de $G \Rightarrow H \triangleleft G$. La implicancia recíproca no es cierta.

Ejemplo:

Sea $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, todo subgrupo de G es normal , pues es abeliano.

$$H_1 = \mathbb{Z}_2 \times \{0\}$$

$$H_2 = \{0\} \times \mathbb{Z}_2$$

$$H_3 = \{(0, 0), (1, 1)\}$$

Son normales en G , pero no característicos :

$$f(a, b) = (b, a) \text{ intercambia } H_1 \text{ con } H_2$$

$$g(a, b) = (a, a + b) \text{ intercambia } H_3 \text{ con } H_2$$

Prop

A_n es un subgrupo característico de S_n .

Dem.

$$A_n = \langle \{\sigma^2/\sigma \in S_n\} \rangle$$

$$\begin{aligned} \text{Si } f : S_n \rightarrow S_n \text{ es automorfismo} &\Rightarrow f(A_n) = \langle \{f(\sigma^2)/\sigma \in S_n\} \rangle \\ &= \langle \{f(\sigma)^2/\sigma \in S_n\} \rangle \\ &= \langle \{\tau^2/\tau \in S_n\} \rangle \\ &= A_n \end{aligned}$$

Ejercicios

1. Si $f : G \rightarrow K$ es un morfismo de grupos, y $A \subseteq G$, entonces $f(\langle A \rangle) = \langle f(A) \rangle$.
2. Si $f \in \text{End}(S_n)$, entonces $f(A) \subseteq A$.

Corolario

Si $N \triangleleft A_n$ y $f : S_n \rightarrow S_n$ es automorfismo, entonces $f(N) \triangleleft A_n$.

Prop

Si $n \geq 5$, los subgrupos normales de S_n son $\{1\}$, A_n y S_n .

Dem.

Probemos que si $\{1\} \neq N \triangleleft S_n$ entonces $A_n \subseteq N$.

Lo haremos como sigue: probaremos que un N con estas características contiene algún ciclo de largo 3.

Sea $\sigma \in N \setminus \{1\}$, \exists alguna trasposición $\tau \in S_n$ tal que σ no conmuta con τ ($\tau(S_n) = \{1\}$)

$$1 \neq [\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \in N$$

Además $\sigma\tau\sigma^{-1} = \tau_1$ trasposición (conjugado de una trasposición)

por lo tanto, tenemos $\tau_1 \circ \tau \in N \setminus \{1\}$

($\tau_1 \neq \tau$ pues de lo contrario resultaría la identidad)

- Si τ_1 y τ no son disjuntas:
 $\tau_1 = (i, j)$ $\tau = (j, k)$ $\tau_1\tau = (i j k)$ ciclo de largo 3.

- Si τ_1 y τ son disjuntas: tenemos $(i, j)(k, l)$ en N (i, j, k, l distintas entre sí) y, por lo tanto, N contiene todos los productos de dos trasposiciones disjuntas, por lo tanto, contiene a $(kl)(jm)$ $m \notin \{i, j, k, l\}$ ($n \geq 5$) $\Rightarrow (ij)(kl)(kl)(jm) = (ijm) \in N$.

Definición

Un grupo G se dice simple ssi $G \neq \{1\}$ y los únicos subgrupos normales de G son $\{1\}$ y G .

Teorema

Si $n \geq 5$, A_n es simple.

Lema Técnico

Si $\sigma \in S_n$, $n \geq 4$, conmuta con $\tau\sigma\tau \forall \tau \in S_n$ trasposición, entonces $O(\sigma) \leq 2$.

Dem.

Por contradicción:

Si $O(\sigma) > 2 \Rightarrow \sigma$ se escribe en su descomposición en ciclos disjuntos como $\sigma = (i, j, k, \dots)$ (tiene ciclo de largo ≥ 3).

Sea $l \notin \{i, j, k\}$ (esto es posible pues $n \geq 4$) y $\tau = (kl)$

$\tau\sigma\tau = (ijl\dots)$, σ no conmuta con $\tau\sigma\tau$. Calculemos:

$$\sigma \circ \tau\sigma\tau(i) = k \quad \tau\sigma\tau \circ \sigma(i) = l \quad \rightarrow \leftarrow$$

Dem. (Teorema)

Hay que probar que no existe $N \triangleleft A_n$ tal que $N \neq \{1\}$ y $N \neq A_n$.

Por contradicción: supongamos que tenemos algún subgrupo normal propio ($\neq \{1\}$ y $\neq A_n$).

Ejercicio: Probar que si G es grupo y tiene algún subgrupo normal propio, hay uno maximal que lo contiene (Zorn).

Entonces existe un subgrupo normal propio maximal con respecto a la inclusión, que llamaremos $N \Rightarrow N_{S_n}(N) = A_n$.

Por lo tanto, \forall trasposición $\tau \in S_n$ $\tau N \tau \neq N$. Y si $\tau_1, \tau \in A_n$ son trasposiciones $\tau_1 \tau N (\tau_1 \tau)^{-1} = N \Rightarrow \tau N \tau = \tau_1 N \tau_1$.

(N tiene sólo dos conjugados en S_n , N y $\tau N \tau$)

Si consideramos $K = N \cap \tau N \tau$, $K \triangleleft S_n \Rightarrow K = \{1\}$

Por lo tanto, tenemos dos subgrupos normales de A_n , N y $\tau N \tau$, cuya intersección es trivial, por lo tanto, $N(\tau N \tau) \cong N \times \tau N \tau$.

$$\left. \begin{array}{l} N(\tau N \tau) \triangleleft S_n \\ N(\tau N \tau) \subseteq A_n \\ N(\tau N \tau) \supset N \supset \{1\} \end{array} \right\} \Rightarrow N(\tau N \tau) = A_n$$

Como N conmuta con $\tau N \tau$ (dos subgrupos normales con intersección trivial).

Si $\sigma \in N \Rightarrow \sigma$ conmuta con $\tau \sigma \tau \forall$ trasposición τ . Por el lema anterior $\Rightarrow O(\sigma) = 2 \Rightarrow \forall \sigma \in N, \forall \sigma \in \tau N \tau, O(\sigma) \leq 2 \Rightarrow \forall \sigma \in A_n, O(\sigma) \leq 2$
 $\rightarrow \leftarrow$ (pues A_n tiene los ciclos de largo 3).

Capítulo 2

Anillos

2.1 Definiciones Básicas

Sea R un conjunto con dos leyes de composición interna : $+$ y \cdot . $(R, +, \cdot)$ se dice anillo ssi:

1. $(R, +)$ es grupo abeliano
2. \cdot es asociativo en R
3. \cdot distribuye con respecto a $+$ en R
4. \cdot tiene neutro 1 , con $1 \neq 0$, donde 0 es el neutro para $+$. Cuando se tiene esta cuarta propiedad, se habla de “anillo unitario”.

Si además \cdot es conmutativo, el anillo se dice conmutativo.

Nota:

En general, nosotros trabajaremos con anillos unitarios conmutativos.

Ejercicio:

Si $(R, +, \cdot)$ es un anillo, entonces $(\forall a, b \in R)$:

- $a \cdot 0 = 0 \cdot a = 0$
- $-a = (-1) \cdot a$
- $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

Así, 0 no puede tener inverso para \cdot .

Definición

Si $(K, +, \cdot)$ es un anillo conmutativo, se dice cuerpo ssi todo $a \in K \setminus \{0\}$ tiene inverso para \cdot .

Definición

Un anillo no necesariamente conmutativo, en el que todo elemento distinto de 0 tiene inverso para \cdot , se suele llamar “anillo con división”.

Ejercicio :

Un anillo R es cuerpo ssi $(R \setminus \{0\}, \cdot)$ es grupo abeliano.

Definición

Si R es un anillo, un elemento $a \in R \setminus \{0\}$ se dirá “divisor del cero” ssi: $\exists b \in R \setminus \{0\}$ tq. $a \cdot b = 0$ o bien $b \cdot a = 0$.

Definición

Un elemento $a \in R \setminus \{0\}$ se dice “cancelable” para \cdot ssi: $(\forall x, y \in R) \quad a \cdot x = a \cdot y \Rightarrow x = y$ y $x \cdot a = y \cdot a \Rightarrow x = y$

Ejercicio :

- Un anillo R NO tiene divisores del 0 ssi todo $a \in R \setminus \{0\}$ es cancelable para \cdot .
- En un anillo R , todo $a \in R$ con inverso para \cdot es cancelable.
- En un cuerpo K no hay divisores del 0.

Definición

Un “Dominio de integridad” (o “anillo de integridad”) es un anillo conmutativo sin divisores del cero.

Ejemplos :

- $(\mathbb{Z}, +, \cdot)$ es un dominio de integridad.
- Todo cuerpo $(K, +, \cdot)$ es dominio de integridad .(por ejemplo : $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$).
- $(\mathbb{Z}_m, +, \cdot)$ es anillo conmutativo ($m \geq 2$).
 $\mathbb{Z}_m = \{[n]_{\equiv_m} / n \in \mathbb{Z}\}$
 $x \equiv_m y \Leftrightarrow x - y \in m \cdot \mathbb{Z}$
 $\left. \begin{array}{l} n_1 \equiv_m n_2 \\ l_1 \equiv_m l_2 \end{array} \right\} n_1 \cdot l_1 \equiv_m n_2 \cdot l_2$, por lo tanto , $[n_1] \cdot [n_2] = [n_1 \cdot n_2]$ también tiene sentido.
- En \mathbb{Z}_m , $[n]$ no es divisor del cero $\Leftrightarrow [n]$ tiene inverso para $\cdot \Leftrightarrow n$ es primo relativo con m .
- \mathbb{Z}_m es cuerpo $\Leftrightarrow \mathbb{Z}_m$ es dominio de integridad $\Leftrightarrow m$ es primo.

2.2 Anillos de Polinomios

Definición

Si R es un anillo conmutativo , el conjunto de polinomios en una indeterminada x y a coeficientes en R es $R[x] = \{(a_0, a_1, \dots, a_n, \dots) \in R^{\mathbb{N}} / (\exists n_0) \text{ tq } a_n = 0 \forall n \geq n_0\}$.

Definamos las siguientes operaciones en $R[x]$:

- $(a_i)_{i \in \mathbb{N}} + (b_i)_{i \in \mathbb{N}} = (a_i + b_i)_{i \in \mathbb{N}}$
- $(a_i)_{i \in \mathbb{N}} \cdot (b_i)_{i \in \mathbb{N}} = (c_i)_{i \in \mathbb{N}}$, con $c_i = \sum_{j=0}^i a_j \cdot b_{i-j}$

$(R[x], +, \cdot)$ es anillo conmutativo.

Llamamos $x = (0, 1, 0, \dots, 0, \dots) \in R[x]$, de esta forma $x^n = \underbrace{x \cdot \dots \cdot x}_{n \text{ veces}} = (0, \dots, 0, \underset{\uparrow}{1}, 0, \dots)$ y

, por lo tanto , $(a_0, a_1, \dots, a_n, 0, \dots) = \sum_{i=0}^n a_i \cdot x^i$, donde identificamos los elementos $a \in R$ con $(a, 0, \dots, 0, \dots) \in R[x]$. Identificación justificada por el hecho que la función

$f : R \longrightarrow R[x]$ es una inyección que preserva $+$ y \cdot : $f(a+b) = f(a) + f(b)$
 $a \longrightarrow (a, 0, \dots, 0, \dots)$
y $f(a \cdot b) = f(a) \cdot f(b)$.

Notar que : $\sum_{i=0}^n a_i \cdot x^i = \sum_{i=0}^n b_i \cdot x^i \in R[x] \Leftrightarrow a_i = b_i \forall i \in \mathbb{N}$.

Definición

Si $p(x) = \sum_{i \in \mathbb{N}} a_i \cdot x^i \in \mathbb{R}[x]$ definimos su grado como $\text{gr}(p(x)) = \text{Máx}\{n \in \mathbb{N} / a_n \neq 0\}$ ($\neq 0 \Leftrightarrow p(x) \neq 0$) . $\text{gr}(0) = -\infty$.

Convenciones:

$$n + -\infty = -\infty + n = -\infty \quad \forall n \in \mathbb{N} \cup \{-\infty\}$$

$$-\infty < n \quad \forall n \in \mathbb{N}$$

Prop

$\forall p(x), q(x) \in \mathbb{R}[x]$

$$1. \text{gr}(p(x) + q(x)) \leq \text{Máx}\{\text{gr}(p(x), \text{gr}(q(x)))\}$$

$$2. \text{gr}(p(x) \cdot q(x)) \leq \text{gr}(p(x)) + \text{gr}(q(x))$$

Observaciones:

- $\text{gr}(p(x) \cdot q(x)) = \text{gr}(p(x)) + \text{gr}(q(x))$ se tiene cuando NO hay divisores del cero.
- \mathbb{R} es dominio de integridad $\Leftrightarrow \mathbb{R}[x]$ es dominio de integridad.
- Si \mathbb{R} es un cuerpo , se tiene el teorema de la división :Si $p(x), f(x) \in \mathbb{R}[x], f(x) \neq 0$, $\exists! q(x), \exists! r(x) \in \mathbb{R}[x]$ tq.
 $p(x) = q(x) \cdot f(x) + r(x) \quad \text{gr}(r(x)) < \text{gr}(f(x))$.

En general se tiene (aunque \mathbb{R} no sea un cuerpo) : $\forall p(x) \in \mathbb{R}[x], \forall a \in \mathbb{R} p(x) = q(x) \cdot (x - a) + c$ con $c \in \mathbb{R}$.Donde $c = p(a)$, en que $p(a)$ es evaluar la función

$p : \mathbb{R} \longrightarrow \mathbb{R}$ “función polinomial asociada al polinomio $p(x)$ “

$x \longrightarrow p(x)$ “fórmula del polinomio evaluada en el elemento x “.

Es decir , $p(x) = a_0 + a_1 \cdot x + \dots + a_n \cdot x^n \in \mathbb{R}[x]$

$$p(a) = a_0 + a_1 \cdot a + \dots + a_n \cdot a^n \in \mathbb{R}$$

Definición

$a \in \mathbb{R}$ se dice raíz de $p(x) \in \mathbb{R}[x]$ ssi $p(a) = 0$.Se obtiene : a raíz de $p(x)$ ssi $(x - a)$ es un factor de $p(x)$. (i.e $p(x) = q(x) \cdot (x - a)$).

Corolario

Si $a_1, \dots, a_k \in R$ son raíces de $p(x)$ distintas entre sí, entonces $(x-a_1) \cdot (x-a_2) \cdots (x-a_k) / p(x)$.

Corolario

Si $p(x) \in R[x]$ tiene grado $n \in \mathbb{N}$ entonces $p(x)$ admite a lo más n raíces distintas.

Corolario

Si R es infinito y $p(x), q(x) \in R[x]$ entonces las funciones polinomiales $p, q : R \rightarrow R$ son iguales ssi $p(x) = q(x)$.

Dem.

$\Rightarrow \forall a \in R \ p(a) = q(a) \Rightarrow p(x) - q(x)$ tiene a todo $a \in R$ como raíz (infinitas raíces), por lo tanto , su grado debe ser $-\infty \Rightarrow p(x) - q(x) = 0 \Rightarrow p(x) = q(x)$.

Observación:

Si R es finito , $R = \{r_0, \dots, r_k\}$, entonces $p(x) = (x - r_0) \cdot (x - r_1) \cdots (x - r_k) \in R[x]$. $\text{gr}(p(x)) = k + 1 \Rightarrow p(x) \neq 0$. Sin embargo , la función polinomial asociada a $p(x)$ es la función nula ($\forall i \in \{0, \dots, k\} \ p(r_i) = 0$) . Es decir , $p(x)$ y 0 tienen la misma función polinomial asociada.

Definición

Si R y P son anillos , un morfismo (u homomorfismo) de R a P , será una función $f : R \rightarrow P$ tal que:

1. $(\forall r_1, r_2 \in R) \ f(r_1 + r_2) = f(r_1) + f(r_2)$
2. $(\forall r_1, r_2 \in R) \ f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$
3. $f(1_R) = 1_P$

Observación:

1. y 2. no implican 3. Por ejemplo: $f : R \rightarrow P$ Satisface 1. y 2. pero no 3.
 $r \rightarrow f(r) = 0$

Se tienen las nociones de isomorfismo, monomorfismo, epimorfismo ,endomorfismo , automorfismo , etc. como se esperaría.

2.3 Buenos Subconjuntos de un anillo

Definición

Si R es un anillo (conmutativo o no) un **subanillo** S de R será un subconjunto cerrado para $+$ y \cdot , que contiene a $1 \in R$ y tal que con $+$ y \cdot restringidos es anillo .

Definición

Si $(R, +, \cdot)$ es un anillo conmutativo , un **ideal** I en R es un subgrupo de $(R, +)$ tal que : $(\forall r \in R)(\forall x \in I) r \cdot x \in I$, y además $I \subsetneq R$. Si $I = R$ hablamos de **ideal degenerado**.

¿Para que sirven los ideales ? , para hacer cuocientes.

$(R, +)$ es grupo abeliano $\Rightarrow (I, +) \triangleleft (R, +)$ y tiene sentido el grupo abeliano $(R/I, +)$.

$$R/I = \{[x]/x \in R\} \quad [x] = x + I$$

$$[x] + [y] = [x + y]$$

Observemos que :

$$[x] = [x'] \wedge [y] = [y'] \Rightarrow [x \cdot y] = [x' \cdot y']$$

$$x - x' \in I \Leftrightarrow (\exists z \in I) x = x' + z$$

$$y - y' \in I \Leftrightarrow (\exists u \in I) y = y' + z$$

$$x \cdot y = x' \cdot y' + \underbrace{x' \cdot u + y' \cdot z}_{\in I} + \underbrace{z \cdot u}_{\in I} \Rightarrow [x \cdot y] = [x' \cdot y']$$

Tenemos así en R/I dos leyes:

$$[x] + [y] = [x + y]$$

$$[x] \cdot [y] = [x \cdot y]$$

$(R/I, +, \cdot)$ es anillo , con $[1]$ el neutro para \cdot .

Como $I \subset R$, R/I tiene más de un elemento (si $r \notin I \Rightarrow [r] \neq [0] = I$) y , por lo tanto , $1 = [1] \neq 0 = I$.

Prop

Si $f : (R, +, \cdot) \longrightarrow (S, +, \cdot)$ es un morfismo de anillos , entonces $\text{Ker} f = f^{-1}(\{0\})$ es un ideal . Además , todo ideal en R es un núcleo de algún morfismo de anillos.

Dem.

$\text{Ker} f$ es subgrupo de $(R, +)$ y si $x \in \text{Ker} f$ y $r \in R$, $f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0 = 0 \Rightarrow r \cdot x \in \text{Ker} f$. Como $f(1) = 1 \neq 0 \Rightarrow 1 \notin \text{Ker} f$, por lo tanto , $\text{Ker} f$ es ideal en R .

Sea I un ideal de R , la función $\nu : R \longrightarrow R/I$ es un morfismo de anillos.

$$x \longrightarrow [x]$$

$\text{Ker} \nu = I$, por lo tanto , todo ideal es núcleo de un morfismo de anillos.

Observación:

En la definición de ideal se puede reemplazar $I \subsetneq R$, por $1 \notin I$, y queda la misma noción.

Ejemplo:

Ideales en $(\mathbb{Z}, +, \cdot)$.

Subgrupos de $(\mathbb{Z}, +)$: $m \cdot \mathbb{Z}$, $m \in \mathbb{N}$.

$\forall m \neq 1$ $m \cdot \mathbb{Z}$ es ideal de \mathbb{Z} . (para $m = 1$ resulta un ideal degenerado)

2.3.1 Teorema del Factor

Si $f : (R, +, \cdot) \longrightarrow (S, +, \cdot)$ es un morfismo de anillos y $I \subseteq R$ es un ideal, con $I \subseteq \text{Ker} f$, entonces $\exists!$ morfismo de anillos $\bar{f} : R/I \longrightarrow S$ tal que el diagrama siguiente conmuta:

$$\begin{array}{ccc}
 \mathbf{R} & \xrightarrow{\mathbf{f}} & \mathbf{S} \\
 & \searrow \mathbf{v} & \nearrow \bar{\mathbf{f}} \\
 & & \mathbf{R/I}
 \end{array}$$

$f = \bar{f} \circ \nu$ (evidentemente $\bar{f}([x]) = f(x)$.

\bar{f} inyectiva $\Leftrightarrow I = \text{Ker} f$

\bar{f} sobreyectiva $\Leftrightarrow f$ es sobreyectiva .

Ejemplo:

¿Ideales en un cuerpo $(K, +, \cdot)$?

1. Un ideal en un anillo conmutativo NO contiene elementos invertibles (respecto a \cdot) (Ejercicio trivial)
2. En K todo $x \neq 0$ es invertible .

Por lo tanto, el único ideal de un cuerpo es $I = \{0\}$.

Corolario

Si $(K, +, \cdot)$ es un cuerpo y $f : K \rightarrow R$ es un morfismo de anillos, entonces $\text{Ker} f = \{0\}$. i.e f es inyectiva.

Ejemplo:

¿Si K es un cuerpo, Cuáles son los ideales de $(K[x], +, \cdot)$?

Si I es ideal en $K[x]$, entonces $I = p(x) \cdot K[x]$, con $p(x) \in K[x]$ un polinomio fijo de grado distinto de 0.

Dem:

$$\{0\} = 0 \cdot K[x]$$

Supongamos que $I \supset \{0\}$ (contenido estrictamente).

Tomemos $p(x) \in I \setminus \{0\}$ de grado mínimo. Veamos que $(\forall f(x) \in I) f(x) = p(x) \cdot q(x)$ para algún $q(x)$. Para ello, si $f(x) \in I$, dividamos por $p(x)$, obtenemos $f(x) = q(x) \cdot p(x) + r(x)$ con $\text{gr}(r(x)) < \text{gr}(p(x))$.

Notar que $r(x) \in I$, pues $r(x) = \underbrace{f(x)}_{\in I} + \underbrace{-q(x) \cdot p(x)}_{\in I} \in I$, y como $p(x)$ es de grado mínimo dentro de $I \setminus \{0\} \Rightarrow r(x) = 0 \Rightarrow f(x) = q(x) \cdot p(x)$, por lo tanto, $I = p(x) \cdot K[x]$.

Ideales generados por Subconjuntos

Sea R un anillo y $A \subseteq R$. Llamamos ideal generado por A al siguiente conjunto:

$$(A) = \bigcap_{I \text{ es ideal, } I \supseteq A} I$$

Ejercicio:

1. $(A) = \{ \sum_{i=1}^n r_i a_i / n \in \mathbb{N}, a_i \in A, r_i \in R \}$
2. Si $u \in A$ es invertible $\Rightarrow (A) = R$.

Observación:

Si R no fuera conmutativo, sus ideales se definen como:

- $I \subset R$ (inclusión estricta)
- $(I, +)$ subgrupo de $(R, +)$ y $\forall r \in R, \forall x \in I, r \cdot x \in I \wedge x \cdot r \in I$.

Resulta :

$$(A) = \{ \sum_{i=1}^n r_i \cdot x_i \cdot s_i / n \in \mathbb{N}, r_i, s_i \in R, x_i \in A \}$$

Ejemplo de anillos no conmutativos:

1. Sea K un cuerpo , $n \geq 2$. $R = \{(a_{ij})_{i,j=1\dots n} / a_{ij} \in K\}$ matrices de $n \times n$ a coeficientes en K , con la suma y producto de matrices usuales. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ no conmutan.
2. El anillo de división de los cuaterniones:
 $H = \mathbb{R}^4 = \mathbb{R} \times \mathbb{R}^3$, $+$ es componente a componente y \cdot :
 $(a, v) \cdot (b, w) = (a \cdot b - \langle v, w \rangle, a \cdot w + b \cdot v + v \times w)$
 $(a, v)^{-1} = \frac{\overline{(a,v)}}{\|(a,v)\|^2}$ con $\overline{(a, v)} = (a, -v)$

Definición

Un ideal en un anillo R se dice principal si es generado por un elemento.

Definición

Un anillo R se llama “**dominio ideal principal**” (**dip**) ssi es dominio de integridad y todo ideal en él es principal.

Ejemplos:

- El teorema de la división hace a $(\mathbb{Z}, +, \cdot)$ y $(K[x], +, \cdot)$ (K cuerpo) dip.
- Los cuerpos son dip (único ideal el 0).

Ejercicio:

El anillo de los enteros de Gauss $G = \{a + b \cdot i / a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ con $+, \cdot$ de \mathbb{C} son un dip.

Ejercicio:

Sea R un dominio de integridad. Definamos en $R \times R \setminus \{0\}$ la siguiente relación:

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

Sea $K = R \times R \setminus \{0\} / \sim$. Definimos en K :

$$[(a, b)] + [(c, d)] = [a \cdot d + b \cdot c, b \cdot d]$$

$$[(a, c)] \cdot [(c, d)] = [(a \cdot c, b \cdot d)]$$

Probar que estas dos operaciones están bien definidas , y que $(K, +, \cdot)$ es un cuerpo.

Ver que $\varphi : R \longrightarrow K$ es un monomorfismo de anillos y que identificando $a \in R$ con $a \longrightarrow [(a, 1)]$

$$\varphi(a) = [(a, 1)] \in K \text{ entonces } [(a, b)] = \frac{a}{b} (= a \cdot b^{-1}) \forall a, b \in R, b \neq 0 .$$

K se llama el cuerpo de fracciones de R . (Si $R = \mathbb{Z}$, entonces $K = \mathbb{Q}$. Si $R = K[x]$, entonces $K =$ “fracciones racionales”. Si R es un cuerpo k , entonces $K = k$).

Ejercicio:

Mostrar que si P es un cuerpo, y $R \subseteq P$ es subanillo de P , entonces el cuerpo más pequeño incluido en P que contiene a R es isomorfo a $K = \text{“cuerpo de fracciones de } R \text{”}$.

2.4 Algo de Divisibilidad en Anillos

Notemos que si R es un anillo (R^x, \cdot) con $R^x = \{r \in R/r \text{ es invertible}\}$, forma un grupo. Cuando R es conmutativo, R^x es abeliano.

Los elementos $u \in R^x$ se suelen llamar **unidades** de R .

Definición

Diremos que dos elementos a, b son “unitariamente equivalentes” ssi $\exists u \in R^x$ tal que $b = u \cdot a$. (i.e., a, b están en la misma órbita de la acción de (R^x, \cdot) en R por multiplicación).

Notación :

$a \sim b$ (probar que es de equivalencia).

Definición

(Divisibilidad). Sean $a, b \in R$. Decimos que a “divide” a b ssi $(\exists c \in R)$ tal que $b = c \cdot a$.

Observación:

Si $a \sim b \Rightarrow a/b \wedge b/a$.

En general, “/” no es de orden.

Ejercicio:

Ver que en un dominio de integridad $a/b \wedge b/a \Rightarrow a \sim b$. Además, $a/b, a \sim a', b \sim b' \Rightarrow a'/b'$, por lo tanto, se puede definir la relación “/” en R/\sim , y aquí sí es de orden.

2.4.1 Caso en que R es un dip

$$a/b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$$

Notar que $a \sim b \Leftrightarrow (a) = (b)$ (en un dominio de integridad).

Definición

Sean $a, b \in R$. Un elemento $c \in R$ se dice **máximo común divisor** (m.c.d) de a y b ssi:

- Es común divisor : $c/a \wedge c/b$
- Cualquier divisor común de a y b , es también divisor de c : $(\forall d \in R) d/a \wedge d/b \Rightarrow d/c$

Notar que si c es m.c.d de a y b , y $c' \sim c$, entonces c' también es m.c.d de a y b .

En un dominio de integridad, si c es m.c.d de a y b , entonces c' es m.c.d de a y $b \Leftrightarrow c \sim c'$.

Prop

Si R es un dip y $a, b \in R$, con alguno de los dos distinto de 0, entonces $\exists c$ m.c.d de a, b .

Dem.

Considerar $I = (a, b)$, por ser dip, $I = (c)$, con $c \in R$.

$$a \in (c) \Rightarrow c/a$$

$$b \in (c) \Rightarrow c/b$$

, por lo tanto, c es un divisor común de a y b . Sea d un divisor común de a y b :

$$a \in (d) \Rightarrow d/a$$

$$b \in (d) \Rightarrow d/b$$

$$\{a, b\} \in (d) \Rightarrow (c) = (a, b) \subseteq (d) \Rightarrow d/c$$

Notar que $(a, b) = \{\alpha \cdot a + \beta \cdot b / \alpha, \beta \in R\}$, $(a, b) = (c) = \alpha \cdot a + \beta \cdot b / \alpha, \beta \in R$ **Igualdad de Bezout**

Ejercicio:

Dos elementos son “**primos relativos**” si m.c.d entre ellos es 1. a, b primos relativos ssi $(\exists \alpha, \beta \in R) 1 = \alpha \cdot a + \beta \cdot b$.

Corolario

Sea R un dip. Si $a, b, c \in R$, con a, b primos relativos y $a/(b \cdot c)$ entonces a/c .

Dem.

$$a/(b \cdot c) \Rightarrow b \cdot c = \gamma \cdot a, \gamma \in R$$

$$a, b \text{ primos relativos} \Rightarrow 1 = \alpha \cdot a + \beta \cdot b, \alpha, \beta \in R \Rightarrow c = (c \cdot \alpha) \cdot a + \beta \cdot b \cdot c$$

$$\Rightarrow c = (c \cdot \alpha + \beta \cdot \gamma) \cdot a \Rightarrow a/c$$

Definición

Un dominio de integridad R se llama “dominio de factorización única” ssi $(\forall a \in R \setminus \{0\}) \exists p_1, \dots, p_k$ primos únicos salvo por equivalencia unitaria y orden, tal que $a \sim p_1 \cdot p_2 \cdot \dots \cdot p_k$. (unidades con $k = 0$ $a \sim 1 \in R^x$).

Prop

Todo dip es dominio de factorización única .

Dem.

1. Existencia de descomposición en producto de primos para los elementos de $R \setminus R^x$ (no invertibles)

Por contradicción . Sea $S = \{a \in R \setminus R^x / a \text{ no es producto de primos} \}$. Supongamos que $S \neq \emptyset$.

Consideremos para $a \in S$ una cadena estrictamente creciente de ideales: $(a_0) \subset (a_1) \subset \dots \subset (a_n) \subset \dots$ con $a_0 = a$.

Si es que esta cadena está obligada a detenerse en (a_n) , No existe $a_{n+1} \in S$ tal que $(a_n) \subset (a_{n+1})$, por lo tanto , $a_n = c \cdot d$ con $c, d \notin S$. $c, d \notin S \Leftrightarrow$ tienen descomposición en primos $\Rightarrow a_n$ tiene descomposición en primos.

Consideremos el ideal $I = \bigcup_{n \in \mathbb{N}} (a_n)$

Ejercicio : La unión de una cadena de ideales es ideal .

$I = \bigcup_{n \in \mathbb{N}} (a_n)$ es ideal en $R \Rightarrow I = (a)$, $a \in R$.

Pero el generador $a \in I$ debe pertenecer a algún (a_n) , y $a \in (a_n) \Leftrightarrow (a) = I \subseteq (a_n)$, por lo tanto , $I = (a_n) \rightarrow \leftarrow$ la cadena terminó en (a_n) .

$\Rightarrow S = \emptyset$

2. Unicidad de la descomposición

Sea $a \sim p_1 \cdot \dots \cdot p_k \sim q_1 \cdot \dots \cdot q_l$

$p_1 \cdot \dots \cdot p_k \sim q_1 \cdot \dots \cdot q_l \Rightarrow p_k / (q_1 \cdot \dots \cdot q_l)$

(Si p_k y q_1 son primos relativos , $p_k / q_1 (q_2 \cdot \dots \cdot q_l) \Rightarrow p_k / (q_2 \cdot \dots \cdot q_l)$, por lo tanto, en el peor de los casos , esto se detiene en p_k / q_l)

Por lo tanto , $p_k \sim q_i$, algún $i = 1 \dots l$.

Para que la notación sea razonable , intercambiamos q_i y q_l y resulta $p_k \sim q_l \Rightarrow p_1 \cdot \dots \cdot p_{k-1} \sim q_1 \cdot \dots \cdot q_{l-1}$.

Se sigue inductivamente : $p_{k-1} \sim q_{l-1}$ (salvo reordenación)

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ p_{k-j} & \sim & q_{k-j} \end{array}$$

Las dos descomposiciones deben acabar al mismo tiempo (justificar) . Por lo tanto , $(\forall i = 1 \dots l) p_i \sim q_{\sigma(i)}$ para alguna permutación $\sigma \in S_k$.

2.5 Módulos sobre un anillo R

Sea R un anillo , no necesariamente conmutativo . Un módulo izquierdo M (o R -módulo izquierdo) sobre el anillo R , es un grupo abeliano $(M, +)$ (su neutro será 0) dotado de una “ley de composición externa”

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ (r, m) &\longrightarrow rm \end{aligned}$$

Tal que:

1. $1m = m \forall m \in M$
2. $(\forall \alpha, \beta \in R)(\forall m \in M) \alpha(\beta m) = (\alpha\beta)m$
3. $(\forall \alpha, \beta \in R)(\forall m \in M) (\alpha + \beta)m = \alpha m + \beta m$
4. $(\forall \alpha \in R)(\forall m_1, m_2 \in M) \alpha(m_1 + m_2) = \alpha m_1 + \alpha m_2$

Observación:

Se pueden definir R - módulos derechos . Si R es conmutativo coinciden los derechos con los izquierdos y se habla simplemente de R - módulos.

Ejemplos 1:

$R = K$ cuerpo , un K - módulo izquierdo es un K - espacio vectorial.

Ejemplo 2 :

$R = \mathbb{Z}$, los \mathbb{Z} - módulos son exactamente lo mismo que los grupos abelianos. En efecto:

Si $(A, +)$ es grupo abeliano , definimos para $\alpha \in \mathbb{Z}, a \in A$,

$$\alpha a = \begin{cases} \underbrace{a + \dots + a}_{\alpha \text{ veces}} & \text{si } \alpha > 0 \\ 0 & \text{si } \alpha = 0 \\ \underbrace{(-a) + \dots + (-a)}_{-\alpha \text{ veces}} & \text{si } \alpha < 0 \end{cases}$$

Después de multiples inducciones se concluye que A , “con esta multiplicación por escalar” , resulta un \mathbb{Z} - módulo .

Recíprocamente, partiendo con un \mathbb{Z} - módulo M , $(M, +)$ es grupo abeliano. Si $\alpha \in \mathbb{Z}$ y $m \in M$, se tiene lo siguiente:

$$\alpha > 0 \Rightarrow \alpha m = \underbrace{(1 + \dots + 1)}_{\alpha \text{ veces}} m = 1m + \dots + 1m = \underbrace{m + \dots + m}_{\alpha \text{ veces}}$$

$$\alpha = 0 \Rightarrow \alpha m = 0 \quad (\text{propiedad general de } R\text{-módulos : } \forall r \in R, \forall m \in M, r \cdot 0 = 0m = 0)$$

$$\alpha < 0 \Rightarrow -1(\alpha m) = (-1\alpha)m = (\alpha \cdot -1)m = \alpha(-1m)$$

$$\Rightarrow \alpha m = (-\alpha)(-m) = (-m) + \dots + (-m) \quad - \alpha \text{ veces}$$

Ejemplo 3 :

Sea K un cuerpo. Estudiemos los $K[x]$ - módulos

Sea M un $K[x]$ - módulo. Considerando que K puede ser identificado con el subanillo de los polinomios constantes en $K[x]$ ($a \rightarrow a + 0 \cdot x + \dots$). Se puede restringir la “multiplicación por escalar” a escalares de K : $K \times M \rightarrow M$, con lo que M resulta ser un K - espacio vectorial.

Notemos que si tomamos el elemento del anillo $x \in K[x]$

$$x(m_1 + m_2) = xm_1 + xm_2 \quad \forall m_1, m_2 \in M$$

$$x(\alpha m) = \alpha(xm) \quad \forall \alpha \in K, \forall m \in M$$

$$\text{Así, la función } T : M \rightarrow M \\ m \rightarrow xm$$

es una transformación lineal del K - e.v M en sí mismo.

A la inversa, dados un e.v V sobre el cuerpo K , y una transformación lineal $T : V \rightarrow V$, podemos definir una estructura de $K[x]$ - módulo de la siguiente manera:

La suma es la que V trae como K - e.v, la “multiplicación por escalares polinomios”:

$$\text{Si } v \in V \text{ y } p(x) = \sum_{i=0}^n a_i \cdot x^i \in K[x], \text{ definimos } p(T) = \sum_{i=0}^n a_i T^i.$$

Facilmente se prueba que si $p(x), q(x) \in K[x]$ entonces $p \cdot q(T) = p(T) \cdot q(T)$, y de ahí resulta que la “ley de composición externa”

$$K[x] \times V \rightarrow V \\ (p(x), v) \rightarrow p(x)v = p(T)(v)$$

define una estructura de $K[x]$ - módulo en V en la que $xv = T(v)$

2.5.1 Submódulos

Si M es un módulo sobre el anillo R , un submódulo N de M es un subconjunto $N \subseteq M$ tal que :

- $(N, +)$ es subgrupo
- La multiplicación por escalar es cerrada en N : $(\forall r \in R)(\forall n \in N) rn \in N$.

Notar que con estas condiciones , N resulta ser un R - módulo.

Con las mismas demostraciones que en el caso de espacio vectorial , $N \subseteq M$ es submódulo ssi:

1. $N \neq \emptyset$
2. N es cerrado para combinaciones lineales: $(\forall r_1, r_2 \in R)(\forall n_1, n_2 \in N) r_1n_1 + r_2n_2 \in N$

Ejemplo 1:

Los submódulos de un K - módulo: subespacios vectoriales.

Ejemplo 2:

Los submódulos de un \mathbb{Z} - módulo: subgrupos

Ejemplo 3:

Los submódulos de un $K[x]$ -módulo:

El $K[x]$ - módulo es un K - e.v V con $S : V \rightarrow V$ transformación lineal. Si W es submódulo , $W \subseteq V$

- W es s.e.v de V
- Estable por $S : (\forall w \in W) S(w) \in W$, (i.e $S(W) \subseteq W$).

Nota de advertencia :

Sea M un R - módulo . $r \in R, m \in M$

$rm = 0$ NO implica $r = 0 \vee m = 0$, (aunque el anillo no tenga divisores del cero) . NO todas las propiedades de espacios vectoriales se mantienen para módulos.

Ejemplo: en un \mathbb{Z} - módulo puede pasar lo siguiente :

$M = \mathbb{Z}_p$, $p \in \mathbb{Z}, p \neq 0, m = [1]$ se tiene $p[1] = [p] = [0]$.

Definición

Si M es un R - módulo y $m \in M$, se dice que m tiene torsión (o es un elemento de/con torsión) ssi $\exists r \in R \setminus \{0\}$ tal que $rm = 0$.

Ejemplo:

Si R es un dominio de integridad , y M es un R - módulo , entonces : $TM = \{m \in M/m \text{ es de torsión} \}$ es un submódulo de M .

Ejemplo interesante de submódulos:

Sea R anillo conmutativo , tomemos $M = R$, i .e R como R - módulo. (la multiplicación por escalar es la multiplicación del anillo). Los submódulos en este caso , son los ideales (degenerado incluido).

2.5.2 Buenas funciones

Si M y N son R - módulos , un “homomorfismo de R - módulos” (o transformación lineal) es una función $T : M \rightarrow N$ tal que:

- $(\forall x, y \in M) T(x + y) = T(x) + T(y)$
- $(\forall r \in R)(\forall x \in M) T(rx) = rT(x)$

Ejemplo 1:

Si $R = K$ cuerpo , tenemos las transformaciones lineales entre espacios vectoriales.

Ejemplo 2:

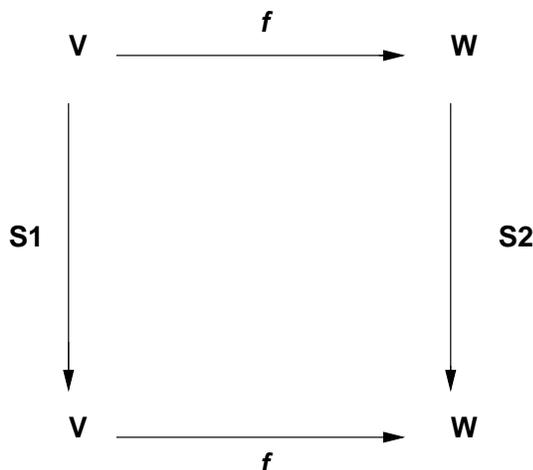
Si $R = \mathbb{Z}$, como \mathbb{Z} - módulo y grupo abeliano es lo mismo , resulta que las transformaciones lineales entre \mathbb{Z} - módulos simplemente son los morfismos de grupos.

Ejemplo 3:

$R = K[x]$. Recordemos que un $K[x]$ -módulo es un espacio vectorial V con una transformación lineal $S : V \rightarrow V$, tal que para el escalar $x \in K[x]$ y un vector $v \in V$, $xv = S(v)$.

Sea $f : V \rightarrow W$ un morfismo de $K[x]$ - módulos , y S_1, S_2 las transformaciones lineales correspondientes a V y W respectivamente.

1. f es K - lineal (lineal entre los e.v V y W)
2. Para $x \in K[x]$, queremos que $f(xv) = xf(v)$ ($\forall v \in V$) , i.e $f(S_1(v)) = S_2f(v) \forall v \in V$



El diagrama conmuta.

2.5.3 Cuocientes

Sea M módulo sobre RR y $N \subseteq M$ un submódulo.

Considerando $(M, +)$ como grupo abeliano, N es subgrupo normal. Podemos calcular entonces $(M/N, +)$ grupo abeliano, donde el cuociente es respecto a $x \sim y \Leftrightarrow y - x \in N$.

Buena propiedad:

$[x] = [y] \wedge v \in R \Rightarrow [rx] = [ry]$, por lo tanto, queda bien definida en M/N la multiplicación por escalar:

$$R \times M/N \longrightarrow M/N$$

$$(r, [x]) \longrightarrow r[x] = [rx]$$

y M/N resulta ser R -módulo con $\nu : M \longrightarrow M/N$ tal que $\nu(x) = [x]$.

La misma serie de teoremas que se tiene para grupos y sus cuocientes vale en esta situación:

Teorema de Correspondencia

Sea M un R -módulo, $N \subseteq M$ submódulo. Hay una correspondencia 1-1 entre submódulos de M que contienen a $N \longleftrightarrow$ submódulos de M/N .

$$N \subseteq P \subseteq M \xrightarrow{\nu} P/N$$

Relevancia de $\text{Ker } f$, $\text{Im } f$ si $f : M \longrightarrow N$ es R -lineal:

- $\text{Ker } f = f^{-1}(\{0\})$ es submódulo de M
- $\text{Im } f = f(M)$ es submódulo de N

- f inyectiva $\Leftrightarrow \text{Ker}f = \{0\}$
- f sobreyectiva $\Leftrightarrow \text{Im}f = N$

Teorema del Factor

Si $f : M \rightarrow N$ es R -lineal y L submódulo de M , con $L \subseteq \text{Ker}f$, entonces $\exists! \bar{f} : M/L \rightarrow N$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc}
 M & \xrightarrow{f} & N \\
 \searrow v & & \nearrow \bar{f} \\
 & M/L &
 \end{array}$$

$$\bar{f}([x]) = f(x)$$

$$f \text{ inyectiva} \Leftrightarrow L = \text{Ker}f \quad (\text{Ker}\bar{f} = (\text{Ker}f)/L)$$

$$f \text{ sobreyectiva} \Leftrightarrow \bar{f} \text{ sobreyectiva} \quad (\text{Im}\bar{f} = \text{Im}f)$$

Ejercicios :

1. Intersección cualquiera de submódulos es submódulo
2. $N + L$ es submódulo de M .

Teoremas de Isomorfismos

1. Si M es un R -módulo y N, L son submódulos, entonces

$$N/(N \cap L) \cong (N + L)/L$$

$$[n]_{N \cap L} \longrightarrow [n]_L$$
2. Si M es R -módulo y $N \subseteq L \subseteq M$ submódulo, entonces

$$(M/N)/(L/N) \cong M/L$$

$$[[x]_N]_{L/N} \longrightarrow [x]_L$$

2.5.4 Sumas , Productos , Sumas directas , etc...

Definición

Si M es un R - módulo y $A \subseteq M$. Se define el submódulo generado por A como :

$$\langle A \rangle = \bigcap_{\substack{N \\ A \subseteq N \\ N \text{ submódulo}}} N$$

$\langle A \rangle$ es un submódulo , y es el más pequeño de los que contienen a A .

Claramente $\langle A \rangle = \{ \sum_{i=1}^n r_i a_i / n \in \mathbb{N}, r_i \in R, a_i \in A \}$. $\langle A \rangle$ consiste en las combinaciones lineales finitas de elementos de A .

Suma de Submódulos

Sea M un R - módulo , y $\{M_\lambda : \lambda \in \Lambda\}$ una familia cualquiera de submódulos de M . La suma de la familia es :

$$+_{\lambda \in \Lambda} M_\lambda = \langle \bigcup_{\lambda \in \Lambda} M_\lambda \rangle$$

$+_{\lambda \in \Lambda} M_\lambda$ consiste en las sumas finitas de elementos en los distintos M_λ , i.e

$$+_{\lambda \in \Lambda} M_\lambda = \{ \sum_{i=1}^n m_{\lambda_i} / n \in \mathbb{N}, \lambda_i \in \Lambda, m_{\lambda_i} \in M_{\lambda_i} \}$$

Definición

La suma se dice directa , y se anota $\bigoplus_{\lambda \in \Lambda} M_\lambda (= +_{\lambda \in \Lambda} M_\lambda)$ ssi :

$$(\forall \tilde{\lambda} \in \Lambda) M_{\tilde{\lambda}} \cap (+_{\lambda \in \Lambda \setminus \{\tilde{\lambda}\}} M_\lambda) = \{0\} .$$

Prop (Ejercicio)

Las siguientes proposiciones son equivalentes:

1. La suma $N = +_{\lambda \in \Lambda} M_\lambda$ es directa
2. Todo $n \in \mathbb{N}$ se escribe de manera única como suma finita de elementos de los M_λ
3. $\forall \{\lambda_1 \dots \lambda_k\} \subseteq \Lambda$, con $\lambda_i \neq \lambda_j$ si $i \neq j$, se tiene que $m_{\lambda_1} + \dots + m_{\lambda_k} = 0$, $m_{\lambda_i} \in M_{\lambda_i} \Rightarrow m_{\lambda_1} = \dots = m_{\lambda_k} = 0$

Producto de una familia de R - módulos

Sea $\{M_\lambda\}_{\lambda \in \Lambda}$ una familia no vacía de R - módulos . Como conjunto , el producto de esta familia es $\prod_{\lambda \in \Lambda} M_\lambda = \{(m_\lambda)_{\lambda \in \Lambda} / m_\lambda \in M_\lambda \forall \lambda \in \Lambda\}$.

$m = (m_\lambda)_{\lambda \in \Lambda}$ se puede entender de manera formal como una “función de elección”:

$$m : \Lambda \longrightarrow \bigcup_{\lambda \in \Lambda} M_\lambda$$

$$\lambda \longrightarrow m(\lambda) = m_\lambda \in M_\lambda$$

Si $M = \prod_{\lambda \in \Lambda} M_\lambda$, podemos darle una estructura de R -módulo . Definamos en M las operaciones $+$ y \cdot :

- $(m_\lambda)_{\lambda \in \Lambda} + (\bar{m}_\lambda)_{\lambda \in \Lambda} = (m_\lambda + \bar{m}_\lambda)_{\lambda \in \Lambda}$ $(m + \bar{m})(\lambda) = m(\lambda) + \bar{m}(\lambda)$
- Multiplicación por escalar en R : $r(m_\lambda)_{\lambda \in \Lambda} = (rm_\lambda)_{\lambda \in \Lambda}$ $(rm)(\lambda) = rm(\lambda)$

Ejercicio:

M , con las operaciones recién definidas , es un R - módulo.

Prop (*Ejercicio*)

Sea $\lambda_o \in \Lambda$. Definamos

$$f_{\lambda_o} : M_{\lambda_o} \longrightarrow M = \prod_{\lambda \in \Lambda} M_\lambda$$

$$m_o \longrightarrow (m_\lambda)_{\lambda \in \Lambda} \quad \text{con } m_\lambda = \begin{cases} 0 & \text{si } \lambda \neq \lambda_o \\ m_o & \text{si } \lambda = \lambda_o \end{cases}$$

f_{λ_o} es un monomorfismo de R - módulos , y por lo tanto , M contiene un submódulo $f_{\lambda_o}(M_{\lambda_o})$ isomorfo a M_{λ_o} (los “vectores” con 0 en todas las componentes distintas a λ_o).

Por otra parte , tenemos las “proyecciones” :

$$\pi_{\lambda_o} : M \longrightarrow M_{\lambda_o}$$

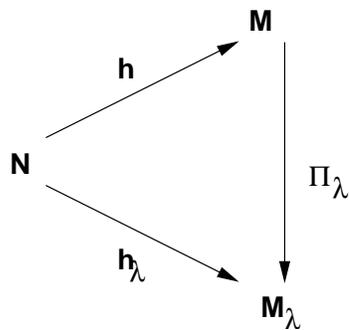
$$(m_\lambda)_{\lambda \in \Lambda} \longrightarrow \pi_{\lambda_o}((m_\lambda)_{\lambda \in \Lambda}) = m_{\lambda_o}$$

$m \longrightarrow m(\lambda_o)$ (evaluación en λ_o). Las proyecciones son epimorfismos de módulos.

Prop

Sea $(M_\lambda)_{\lambda \in \Lambda}$ una familia de R - módulos , y sea N otro R - módulo . \forall familia de morfismos de R - módulos $\{h_\lambda : N \rightarrow M_\lambda\}_{\lambda \in \Lambda}$, $\exists!$ morfismo de R - módulos $h : N \rightarrow M$, con $M = \prod_{\lambda \in \Lambda} M_\lambda$

tal que , ($\forall \lambda \in \Lambda$) el diagrama siguiente conmuta :



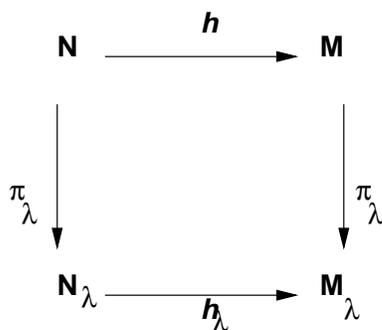
$$\text{i.e } \pi_\lambda \circ h = h_\lambda$$

Dem.

$h(n) = (h_\lambda(n))_{\lambda \in \Lambda}$, la unicidad es directa .

Corolario

Si $\{M_\lambda\}_{\lambda \in \Lambda}$ y $\{N_\lambda\}_{\lambda \in \Lambda}$ son familias de R - módulos , indexadas por el mismo Λ , y $\{h_\lambda : N_\lambda \longrightarrow M_\lambda\}_{\lambda \in \Lambda}$ una familia de transformaciones R - lineales , entonces $\exists!$ morfismo de R -módulos $h : N = \prod_{\lambda \in \Lambda} N_\lambda \longrightarrow \prod_{\lambda \in \Lambda} M_\lambda = M$ tal que $(\forall \lambda \in \Lambda)$ el diagrama siguiente conmuta :



La demostración queda de ejercicio.

Suma directa externa

(No tendremos , a priori , submódulos de un módulo dado).

Sea $\{M_\lambda\}_{\lambda \in \Lambda}$ una familia de R - módulos , sea $\tilde{M} = \{(m_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} M_\lambda / m_\lambda = 0 \text{ para todos los } \lambda \in \Lambda \text{ salvo tal vez , un número finito de ellos (para casi todo } \lambda \in \Lambda)\}$.

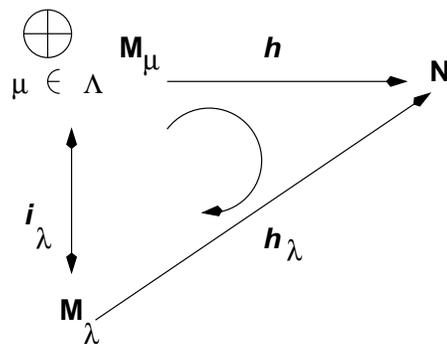
Es directo que \tilde{M} es un submódulo de $M = \prod_{\lambda \in \Lambda} M_\lambda$, llamamos a este submódulo $\tilde{M} \subseteq M$ la “suma directa de los M_λ “.

Observaciones:

1. $(\forall \lambda_o \in \Lambda) \text{ Im}(f_{\lambda_o}) \subseteq \tilde{M}$, por lo tanto , podemos considerar esta función llegando a \tilde{M} , anotemosla $i_{\lambda_o} : M_{\lambda_o} \rightarrow \tilde{M}$ (monomorfismo) (inyección canónica). Podemos entonces identificar M_{λ_o} con $i_{\lambda_o}(M_{\lambda_o}) \subseteq \tilde{M}$.
2. Todo $m \in \tilde{M}$ es suma finita de elementos de los distintos M_λ :
 $m = (m_\lambda)_{\lambda \in \Lambda} = \sum_{\lambda \text{ tq } m_\lambda \neq 0} m_\lambda$, así $\tilde{M} = \langle \bigcup_{\lambda \in \Lambda} M_\lambda \rangle = \sum_{\lambda \in \Lambda} M_\lambda$, además $\tilde{M} = \bigoplus_{\lambda \in \Lambda} M_\lambda$.

Ejercicios:

1. Si $\{M_\lambda\}_{\lambda \in \Lambda}$ es una familia de R - módulos , N es otro R - módulo y $\{h_\lambda : M_\lambda \rightarrow N\}_{\lambda \in \Lambda}$ es una familia de transformaciones R -lineales, entonces $\exists!$ transformación R - lineal $h : \bigoplus_{\lambda \in \Lambda} M_\lambda \rightarrow N$ tal que , $(\forall \lambda \in \Lambda)$ el siguiente diagrama conmuta :



1. Si $\{M_\lambda\}_{\lambda \in \Lambda}$ y $\{N_\lambda\}_{\lambda \in \Lambda}$ son familias de R - módulos y $\{h_\lambda : M_\lambda \rightarrow N_\lambda\}_{\lambda \in \Lambda}$ es una familia de transformaciones lineales , $\exists!$ $h : \bigoplus_{\lambda \in \Lambda} M_\lambda \rightarrow \bigoplus_{\lambda \in \Lambda} N_\lambda$, R -lineal tal que $(\forall \lambda \in \Lambda)$ el diagrama siguiente conmuta :

$$\begin{array}{ccc}
 \bigoplus_{\mu \in \Lambda} \mathbf{M}_\mu & \xrightarrow{h} & \bigoplus_{\mu \in \Lambda} \mathbf{N}_\mu \\
 \updownarrow i_\lambda & & \updownarrow i_\lambda \\
 \mathbf{M}_\lambda & \xrightarrow{h_\lambda} & \mathbf{N}_\lambda
 \end{array}$$

1. Sea $\{M_\lambda\}_{\lambda \in \Lambda}$ una familia de R - módulos y $(\forall \lambda \in \Lambda) N_\lambda \subseteq M_\lambda$ un submódulo , entonces $\bigoplus_{\lambda \in \Lambda} N_\lambda$ es un submódulo de $\bigoplus_{\lambda \in \Lambda} M_\lambda$ y $(\bigoplus_{\lambda \in \Lambda} M_\lambda) / (\bigoplus_{\lambda \in \Lambda} N_\lambda) \cong \bigoplus_{\lambda \in \Lambda} (M_\lambda / N_\lambda)$.

2.5.5 Conjuntos linealmente independientes , Bases

Sea M un R -módulo . Una familia de elementos de M : $\{m_\lambda\}_{\lambda \in \Lambda}$ se dice l.i en M ssi \forall combinación lineal finita tal que $\sum_{\lambda \in I} r_\lambda m_\lambda = 0$ ($I \subseteq \Lambda$ finito , $r_\lambda \in R$) los escalares deben ser 0 : $(\forall \lambda \in I) r_\lambda = 0$

Observación :

$\{m_\lambda\}_{\lambda \in \Lambda}$ es l.i \Leftrightarrow toda subfamilia finita $\{m_\lambda\}_{\lambda \in I}$ ($I \subseteq \Lambda$ finito) es l.i.

Existen módulos SIN familias l.i.

Ejemplo:

$R = \mathbb{Z}$, M un \mathbb{Z} -módulo finito cualquiera . Sabemos que todo $m \in M$ tiene orden $r \in \mathbb{N} \setminus \{0\} \subseteq \mathbb{Z}$ finito , con $r / |M|$, por lo tanto , $rm = 0 \Rightarrow \{m\}$ no es l.i.

La familia vacía es l.i por decreto , por lo tanto , es la única familia l.i dentro de estos módulos .

Ejemplo:

$(\mathbb{Q}, +)$ es un \mathbb{Z} -módulo . $\forall m \in \mathbb{Q} \setminus \{0\}$, $\{m\}$ es l.i .

Ninguna familia con 2 o más elementos de \mathbb{Q} es l.i

(REVISAR).

En R como R - módulo , $\{1\}$ es l.i

Definición

Una **base** de un R - módulo M es una familia l.i que lo genera.

Ejemplo:

1. $\{1\}$ es base de R
2. Ningún \mathbb{Z} - módulo finito (excepto $\{0\}$, cuya base es \emptyset) tiene base.
3. \mathbb{Q} no tiene base como \mathbb{Z} - módulo

Ejercicio:

- Una base es un l.i maximal
- $\{m_\lambda\}_{\lambda \in \Lambda}$ base de M ssi todo $m \in M$ se escribe de manera única como combinación lineal finita de los m_λ .

Definición

Un R - módulo se dirá **libre** si tiene una base.

Ejemplo:

R como R - módulo es libre . $R^n = \prod_{i=1}^n R$ es libre (base canónica).

Caracterización de los R - módulos libres y sus bases**Prop**

Sea M un módulo y $\{m_\lambda\}_{\lambda \in \Lambda}$ una familia de elementos en M , entonces M es libre con base $\{m_\lambda\}_{\lambda \in \Lambda}$ ssi $\forall R$ -módulo N y \forall familia $\{n_\lambda\}_{\lambda \in \Lambda}$ en N $\exists!$ función R - lineal $f : M \rightarrow N$ tal que $(\forall \lambda \in \Lambda) f(m_\lambda) = n_\lambda$.

Dem.

\Rightarrow) M libre con base $\{m_\lambda\}_{\lambda \in \Lambda}$. Tomamos una familia $\{n_\lambda\}_{\lambda \in \Lambda}$ en N y definimos para $m \in M$, $f(m) = \sum_{\lambda \in I} r_\lambda n_\lambda$, donde $m = \sum_{\lambda \in I} r_\lambda m_\lambda$ es la única manera de escribir m como combinación lineal de los elementos de la base.

Es directo que es R - lineal , que $f(m_\lambda) = n_\lambda$, y que esta es la única posible definición de f , pues para que sea lineal , si $f(m_\lambda) = n_\lambda$, entonces $f(\sum_{\lambda \in I} r_\lambda m_\lambda) = \sum_{\lambda \in I} r_\lambda f(m_\lambda)$.

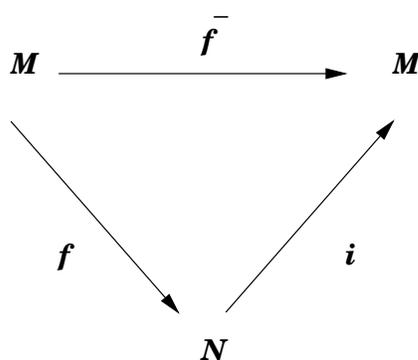
⇐) Supongamos que $\sum_{\lambda \in I} r_\lambda m_\lambda = 0$. Sea $\lambda_o \in I$, y definamos la sgte función $f : M \rightarrow R$ tal que :

$$m_{\lambda_o} \rightarrow 1$$

$m_\lambda \rightarrow 0 \quad \forall \lambda \neq \lambda_o$, pero por hipótesis existe una única función que hace esto, y como $\sum_{\lambda \in I} r_\lambda f(m_\lambda) = f(\sum_{\lambda \in I} r_\lambda m_\lambda) = f(0) = 0$, tenemos que $r_{\lambda_o} 1 = 0 \Rightarrow r_{\lambda_o} = 0$, Si repetimos esto $\forall \lambda \in I$, concluimos que $r_\lambda = 0 \quad \forall \lambda \in I$, por lo tanto, $\{m_\lambda\}_{\lambda \in I}$ es familia l.i

Veamos ahora que $\{m_\lambda\}_{\lambda \in I} = B$ genera M.

Sea $N = \langle B \rangle$ ($\forall \lambda \in \Lambda$) seleccionemos $n_\lambda = m_\lambda \in N \Rightarrow \exists!$ una función lineal $f : M \rightarrow N$ tal que $f(m_\lambda) = m_\lambda$ ($\forall \lambda \in \Lambda$)



Tomemos $\bar{f} : M \rightarrow M$ como la composición $i \circ f$, donde $i : N \hookrightarrow M$ es la inclusión. Como $(\forall \lambda \in \Lambda) \bar{f}(m_\lambda) = i(f(m_\lambda)) = f(m_\lambda) = m_\lambda$. $\bar{f} : M \rightarrow M$ es la única función lineal tal que $m_\lambda \rightarrow m_\lambda$, por lo tanto, $\bar{f} = id_M \Rightarrow \text{Im } \bar{f} = \text{Im}(id_M) = M$, pero de la construcción de \bar{f} , $\text{Im } \bar{f} = \text{Im}(i \circ f) = \text{Im } f \subseteq N = \langle B \rangle$, por lo tanto, $M \subseteq \langle B \rangle (\subseteq M) \Rightarrow M = \langle B \rangle$.

Módulo libre sobre un conjunto A

Sea R anillo conmutativo. Si a es un elemento, podemos construir $R_a = R \times \{a\} = \{(r, a) / r \in R\}$, con la suma $(r, a) + (s, a) = (r + s, a)$, y la multiplicación por escalar en R $r(s, a) = (r \cdot s, a)$.

R_a es un módulo isomorfo a R ($(r, a) \leftrightarrow r$). Como R es un módulo libre con base $\{1\} \Rightarrow R_a$ es libre con base $\{(1, a)\}$. Anotaremos $(1, a) = a \in R_a$, por lo tanto, diremos que R_a es libre con base $\{a\}$. Como $r(1, a) = (r, a)$, se tiene $R_a = \{ra / r \in R\} = Ra$.

Si ahora hacemos esto $\forall a \in A$, tenemos una familia de módulos libres $\{R_a\}_{a \in A}$, con R_a de base $\{a\}$. Anotamos $F_A = \bigoplus_{a \in A} R_a$.

Prop

F_A es libre con base A.

Dem.

$\forall x \in F_A$, x es suma finita de elementos en los sumandos

$$x = \underbrace{x_1}_{\in R a_1} + \cdots + \underbrace{x_k}_{\in R a_k} = r a_1 + \cdots + r_k a_k, \quad r_i \in R, \quad a_i \in A, \quad \text{con esto, } A \text{ genera } F_A, \text{ por otro}$$

lado, si $\sum_{i=1}^k r_i a_i = 0$ para $r_i \in R, a_i \in A$ distintos entre sí.

Recordemos que a_i visto como elemento de F_A es $(0, \dots, 0, a_i, 0, \dots, 0)$, por lo tanto, $\sum_{i=1}^k r_i a_i = (0, \dots, r_j a_j, \dots, 0, \dots, r_i a_i, 0, \dots) = 0 \Leftrightarrow r_j a_j = 0$ en $R a_j \quad \forall j \Leftrightarrow r_j = 0 \quad \forall j$.

Prop

Todo R -módulo es cociente de algún R -módulo libre (mas bien isomorfo).

Dem.

Sea M un R -módulo. Sea $A \subseteq M$ un generador: $\langle A \rangle = M$. Aplicando la construcción anterior, $A \subseteq F_A$.

Por la caracterización de módulo libre con base A , $\exists!$ función lineal $f: F_A \rightarrow M$ tal que $(\forall a \in A) f(a) = a$. f es un epimorfismo \Rightarrow

$$\begin{array}{ccc}
 \mathbf{FA} & \xrightarrow{\mathbf{f}} & \mathbf{M} \\
 & \searrow \mathbf{v} & \nearrow \mathbf{\bar{f}} \\
 & \mathbf{FA/Kerf} &
 \end{array}
 \quad \bar{f}([x]) = f(x)$$

La función lineal inducida en el cociente $\bar{f}: F_A/\text{Ker}f \rightarrow M$, es un isomorfismo.

¿Que hay en $\text{Ker}f$?

$x \in \text{Ker}f \Leftrightarrow x = r_1 a_1 \oplus \cdots \oplus r_k a_k, f(x) = 0$ i.e $x = r_1 a_1 \oplus \cdots \oplus r_k a_k$ tal que $r_1 a_1 + \cdots + r_k a_k = 0$ en M .

Prop

Sean M y N dos módulos libres con bases $\{b_\lambda\}_{\lambda \in \Lambda}$ y $\{c_\lambda\}_{\lambda \in \Lambda}$ respectivamente, ambas de igual cardinal $\Rightarrow M \cong N$.

Dem.

Por la caracterización de módulos libres , $\exists!$ función lineal $f : M \rightarrow N$ tal que $f(b_\lambda) = c_\lambda \forall \lambda \in \Lambda$. Si se prefiere mirar a N como el módulo libre , $\exists!$ función lineal $g : N \rightarrow M$ tal que $g(c_\lambda) = b_\lambda \forall \lambda \in \Lambda$, compongamos :

$$\begin{array}{ccccc} & f & & g & \\ M & \longrightarrow & N & \longrightarrow & M \\ b_\lambda & \longrightarrow & c_\lambda & \longrightarrow & b_\lambda \end{array}$$

$g \circ f : M \rightarrow M$ es lineal tal que $g \circ f(b_\lambda) = b_\lambda$, por lo tanto , por la caracterización de módulos libres , $g \circ f(b_\lambda) = id_M$. Construyendo $f \circ g$, resulta $f \circ g = id_N \Rightarrow f$ y g son isomorfismos inversos uno del otro.

Nota:

Muchas de las propiedades de los espacios vectoriales no valen en general para módulos.

Prop

Si M es un R - módulo libre y $N \subseteq M$ submódulo , entonces N , ni siquiera tiene por que ser libre.

Ejemplo:

$R = (\mathbb{Z}_6, +, \cdot)$ como módulo sobre si mismo . La suma y el producto por escalar son los de R , es libre con base $\{1\}$. Sus submódulos son los ideales. $I = (2) = \{0, 2, 4\}$ es un ideal y no es libre.

Hay casos donde estas cosas andan bien , por ejemplo $R = \mathbb{Z}$ como módulo sobre si mismo. Sus submódulos son los ideales $(n) = n \cdot \mathbb{Z}$, libres con base $\{n\}$ si $n \neq 0$ o \emptyset si $n = 0$.

Teorema

Si R es un dip , L es un R - módulo libre con base $\{b_\lambda\}_{\lambda \in \Lambda}$, y $M \subseteq L$ es un submódulo , entonces M es libre , y tiene una base $\{m_\mu\}_{\mu \in \Gamma}$, $\Gamma \subseteq \Lambda$.

Dem.

Consideremos los subconjuntos $\Lambda' \subseteq \Lambda$ y los submódulos libres de L : $L_{\Lambda'} = \langle \{b_\lambda\}_{\lambda \in \Lambda'} \rangle$. Llamamos $M_{\Lambda'} = M \cap L_{\Lambda'}$.

Interesará considerar aquellos casos en que $M_{\Lambda'}$ es libre , con base $\{m_\mu\}_{\mu \in \Gamma}$ y $|\Gamma'| \leq |\Lambda'|$.

Trabajaremos con tuplas de la forma $(\Lambda', L_{\Lambda'}, M_{\Lambda'}, m' = \{m_\mu\}_{\mu \in \Gamma})$, con las condiciones de más arriba.

Sea A el conjunto de estas tuplas , lo que queremos probar es que A posee un elemento (tupla) para el $\Lambda' = \Lambda$ ($\Rightarrow L_{\Lambda} = L$, $M_{\Lambda} = M$, y por lo tanto , M es submódulo libre de L , con base de cardinal $\leq |\Lambda'| = |\Lambda|$).

Usaremos Zorn. Ordenemos A :

Diremos que

$(\Lambda', L_{\Lambda'}, M_{\Lambda'}, m' = \{m_{\mu}\}_{\mu \in \Gamma'}) \leq (\Lambda'', L_{\Lambda''}, M_{\Lambda''}, m'' = \{m''_{\mu}\}_{\mu \in \Gamma''}) \Leftrightarrow \Lambda'' \subseteq \Lambda'$ ($\Rightarrow M_{\Lambda'} \subseteq M_{\Lambda''}$) y la base m'' de $M_{\Lambda''}$ es una extensión de la base m' de $M_{\Lambda'}$, es decir , $\Gamma' \subseteq \Gamma''$ y $(\forall u \in \Gamma') m_{\mu} = m''_{\mu}$.

\leq es claramente de orden en A .

$A \neq \emptyset$, pues $(\Lambda' = \emptyset, L_{\Lambda'} = \{0\}, M_{\Lambda'} = \{0\}, m' = \emptyset$ ($\Gamma' = \emptyset$)) $\in A$.

Veamos que (A, \leq) tiene las hipótesis que requiere el lema de Zorn:

- $A \neq \emptyset$
- Sea $\{(\Lambda'_i, L_{\Lambda'_i}, M_{\Lambda'_i}, m'_i = \{m_{\mu}^{(i)}\}_{\mu \in \Gamma'_i})\}_{i \in I} = \zeta$ una cadena en A , es decir , una familia totalmente ordenada. P.d.q ζ tiene una cota superior:

Tomemos $\Lambda' = \bigcup_{i \in I} \Lambda'_i \subseteq \Lambda$, y para $M_{\Lambda'}$ tendremos la base $m' = \{m_{\mu}\}_{\mu \in \Gamma'}$, con $\Gamma' = \bigcup_{i \in I} \Gamma'_i$ y $m_{\mu} = m_{\mu}^{(i)}$ si $\mu \in \Gamma'_i$ (está bien definido , por que las bases de los distintos $M_{\Lambda'_i}$ son extensiones de las otras).

P.d m' es l.i y genera $M_{\Lambda'}$

- Lineal independencia :

Una combinación lineal finita de los m_{μ} será una combinación lineal en algún $M_{\Lambda'_i}$, y en ese lugar los $m_{\mu}^{(i)}$ son l.i

- Generan $M_{\Lambda'}$:

$x \in M_{\Lambda'} = L_{\Lambda'} \cap M \Leftrightarrow x \in L_{\Lambda'} = \langle \{b_{\lambda}\}_{\lambda \in \Lambda'} \rangle \wedge x \in M \Rightarrow x$ es combinación lineal finita de los b_{λ} , y los λ que aparezcan estarán todos en algún $\Lambda'_i \Rightarrow x \in L_{\Lambda'_i} \cap M = M_{\Lambda'_i} \Rightarrow x$ es combinación lineal de los $\{m_{\mu}\}_{\mu \in \Lambda'_i} \subseteq m'$.

Evidentemente , $|\Lambda'| \geq |\Gamma'|$ y m' es una extensión de todas las bases m'_i , $\Lambda' \supseteq \Lambda'_i$, por lo tanto , $(\Lambda', L_{\Lambda'}, M_{\Lambda'}, m')$ es una cota superior de la cadena ζ .

Por Zorn , A tiene un elemento maximal $(\Lambda', L_{\Lambda'}, M_{\Lambda'}, m')$.

P.d : para este elemento maximal , $\Lambda' = \Lambda$.

Como de costumbre , al usar Zorn , suponemos que para este elemento maximal , $\Lambda' \subsetneq \Lambda$, y llegaremos a una contradicción haciendo crecer estrictamente este elemento maximal dentro de A .

Tomemos $\lambda_o \in \Lambda \setminus \Lambda'$. Sea $\Lambda'' = \Lambda' \cup \{\lambda_o\}$.

Podría ocurrir que $M_{\Lambda''} = M_{\Lambda'}$, en ese caso $m'' = m'$, y resulta que $(\Lambda', \dots, m') < (\Lambda'', \dots, m'')$, por lo tanto crecería el maximal $\rightarrow \leftarrow$

Si eso no ocurre, $M_{\Lambda''} \supset M_{\Lambda'}$. Veremos que se le puede agregar un elemento a la base de $M_{\Lambda''}$ y habremos crecido estrictamente $\rightarrow \leftarrow$.

Hagámoslo: ¿Qué elementos hay en $M_{\Lambda''}$?

$x \in M_{\Lambda''} \Leftrightarrow x \in M \wedge x \in L_{\Lambda''} (= L_{\Lambda'} \oplus Rb_{\lambda_o})$, por lo tanto, x se puede escribir como $x = y + rb_{\lambda_o}$, con $y \in L_{\Lambda'}$, $r \in R$, y además $x \in M$.

Nuestra tarea:

Encontrar un elemento más para agregar a la base de $M_{\Lambda'}$ y hacer aparecer una base de $M_{\Lambda''}$.

Sea $I = \{r \in R / (\exists y \in L_{\Lambda'}) y + rb_{\lambda_o} \in M_{\Lambda''}\}$. I es un ideal (posiblemente degenerado) en R . Como R es un dip $\Rightarrow I = (r_o)$, para algún $r_o \in R$.

Sea $m_{\lambda_o} = y_o + r_o b_{\lambda_o} \in M_{\Lambda''}$ (existe, pues $r_o \in I$). Veamos que $m' \cup \{m_{\lambda_o}\}$ es base para $M_{\Lambda''}$.

• Lineal independencia

$$\begin{aligned} \text{Sea } sm_{\lambda_o} + \sum r_{\mu} \underbrace{m'_{\mu}}_{\in m'} &= 0 \Leftrightarrow sr_o b_{\lambda_o} + \underbrace{sy_o}_{\in L_{\Lambda'}} + \underbrace{\sum r_{\mu} m'_{\mu}}_{\in M_{\Lambda'} \subseteq L_{\Lambda'}} = 0 \\ \Rightarrow sy_o + \sum r_{\mu} m'_{\mu} \in L_{\Lambda'} &\Rightarrow sy_o + \sum r_{\mu} m'_{\mu} = \sum_{\substack{\lambda \neq \lambda_o \\ \lambda \in A}} t_{\lambda} b_{\lambda} \end{aligned}$$

Como los $\{b_{\lambda}\}$ son l.i $\Rightarrow sr_o = 0$ todos los $t_{\lambda} = 0$, pero en nuestra situación $r_o \neq 0$ (pues $r_o = 0 \Rightarrow M_{\Lambda'} = M_{\Lambda''}$) $\Rightarrow s = 0$, por lo tanto, todos los otros $r_{\mu} = 0$.

• Generador

$M'' = M \cap (L_{\Lambda'} \oplus Rb_{\lambda_o})$. Vimos que un x cualquiera de $M_{\Lambda''}$ es de la forma $x = y + rb_{\lambda_o}$, con $y \in L_{\Lambda'}$, y además $r = sr_o \in I$. Tomando $x - sm_{\lambda_o} = \underbrace{y - sy_o}_{\in \underbrace{L_{\Lambda'} \cap M}_{M_{\Lambda'}}}$, por lo tanto,

$$x - sm_{\lambda_o} = \sum r_{\mu} m_{\mu} \Rightarrow x = sm_{\lambda_o} + \sum r_{\mu} m_{\mu}.$$

Ejercicio:

Si R es un dominio de integridad y L es un R -módulo, entonces todas las bases de L tienen el mismo cardinal.

Ejercicios:

Sea R un anillo conmutativo, $I \subsetneq R$ un ideal.

1. Si M es un R -módulo, definimos $IM = \{ \sum_{i=1}^n s_i m_i / n \in \mathbb{N}, s_i \in I, m_i \in M \}$. Probar que IM es submódulo de M , y de hecho, $IM = \langle \{ sm/s \in I, m \in M \} \rangle$.
2. Sobre M/IM definimos la multiplicación por escalares en el anillo cociente R/I : $[r] \cdot [m] = [rm]$. Ver que esto da una función bien definida $R/I \times M/IM \rightarrow M/IM$ y que con esto, M/IM resulta ser un R/I -módulo.
3. Si $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$, con los M_λ submódulos de M , entonces $IM = \bigoplus_{\lambda \in \Lambda} IM_\lambda$, y de aquí que $M/IM \cong \bigoplus_{\lambda \in \Lambda} M_\lambda/IM_\lambda$, $[\sum m_\lambda] \leftrightarrow \sum [m_\lambda]$, y este isomorfismo es como módulos sobre R y también sobre el anillo.
4. Si M es libre, como R -módulo, de base $B = \{ b_\lambda \}_{\lambda \in \Lambda}$, entonces M/IM es libre como R/I -módulo, con base $\{ [v_\lambda] \}_{\lambda \in \Lambda}$.
5. El ideal $I \subset R$ (estrictamente incluido), se dice **MAXIMAL** ssi es maximal con respecto a la inclusión dentro de los ideales propios de R . i.e, si J es un ideal propio de R y $J \supseteq I \Rightarrow I = J$.
Probar que:
 - (a) Todo ideal propio $J \subset R$ está contenido en algún ideal maximal de R (Zorn). En particular, R siempre tiene ideales maximales.
 - (b) R/I es cuerpo $\Leftrightarrow I$ es ideal maximal de R .
6. Probar que si M es libre, como R -módulo, con dos bases B_1 y B_2 , entonces $|B_1| = |B_2|$.

Definición

Se llama **Rango** de un R -módulo libre, al cardinal de su base.

2.5.6 Módulos finitamente generados

R será un anillo conmutativo.

Definición

Un R -módulo M se dice de “tipo finito” o “**finitamente generado**” ssi $\exists A = \{ a_1, \dots, a_k \} \subseteq M$ finito, tal que $M = \langle A \rangle = \{ \sum_{i=1}^k \lambda_i a_i / \lambda_i \in R \}$.

Ejemplos:

- \mathbb{Q} no es finitamente generado sobre \mathbb{Z} .
- R^n es finitamente generado sobre R , (y libre, con la base canónica)
- Todo grupo abeliano finito es finitamente generado como \mathbb{Z} -módulo.

Definición

Un R -módulo M se dirá cíclico ssi es finitamente generado por un conjunto de la forma $A = \{a\}$.

De aquí en adelante, R será un dip.

¿Cómo son los R -módulos cíclicos?

M cíclico : $M = \langle \{m_o\} \rangle = Rm_o = \{rm_o/r \in R\}$ con $m_o \in M$.

Sabemos que si F es el R -módulo libre con un generador (por ejemplo $F = R$, $\{1\}$ es base), la función

$$\varphi : R(= F) \longrightarrow M = Rm_o$$

$$r(= r1) \longrightarrow rm_o$$

es un epimorfismo

$\Rightarrow M \cong R/\text{Ker}\varphi$. Pero $\text{Ker}\varphi$ es un submódulo de $R \Rightarrow \text{Ker}\varphi = I$, un ideal de R (posiblemente todo R).

Notar que $\text{Ker}\varphi = \{r \in R/rm_o = 0\} = \{r \in R/(\forall m \in M)rm = 0\} =$ “anulador de M ”.

En resumen: un R -módulo cíclico M es isomorfo a $(R/\text{anulador de } M) \cong M$.

Tenemos que $\text{Ker}\varphi =$ anulador de $M = I$ ideal en R , Luego I es principal, $I = (r_o) = R \cdot r_o$ para algún $r_o \in R$.

r_o se llama **anulador minimal**, o bien, **orden de M** .

Así tenemos que $M \cong R/(r_o) = R/R \cdot r_o$ (Lo mismo que ya teníamos para \mathbb{Z} -módulos cíclicos).

Notar que el orden r_o de M está determinado salvo por multiplicación por elementos invertibles. i.e. $(r_o = r_1) \Leftrightarrow (\exists u \in R^x) r_1 = u \cdot r_o$.

Observación:

- $r_o \sim 1 \Leftrightarrow M = \{0\}$
- $r_o = 0 \Leftrightarrow M$ es libre con base $\{m_o\}$

Antes de ver que sucede en el caso general con los R -módulos finitamente generados, estudiemos lo siguiente:

Funciones lineales entre módulos libres

Las funciones lineales entre módulos libres sobre un anillo conmutativo R , se pueden describir (tal como el caso de espacios vectoriales) con matrices a coeficientes en R .

Sean F_1 y F_2 R -módulos libres con bases $B_1 = \{a_1, \dots, a_n\}$ y $B_2 = \{b_1, \dots, b_m\}$ respectivamente.

Una función $f : F_1 \rightarrow F_2$ queda completamente (y únicamente) determinada si conocemos $f(a_1), \dots, f(a_n) \in F_2$.

Por su parte, estas imágenes están completamente determinadas por sus coordenadas en la base B_2 :

$$f(a_j) = r_{1j}b_1 + \dots + r_{mj}b_m, \text{ el vector de coordenadas es } \begin{pmatrix} r_{1j} \\ \vdots \\ r_{mj} \end{pmatrix} = [f(a_j)]_{B_2}.$$

Así, f se representa de manera única por la matriz

$$[f]_{B_1 B_2} = [f] = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \dots & r_{mn} \end{bmatrix}$$

$$[f] \in M_{mn}(R).$$

Hay biyección:

$$L(F_1, F_2) \leftrightarrow M_{mn}(R)$$

$$f \leftrightarrow [f]$$

Más aun, $L(F_1, F_2)$ es un R -módulo ($(f+g)(x) = f(x) + g(x)$ y $(rf)(x) = rf(x)$) que resulta isomorfo (como R -módulo) con el R -módulo $M_{mn}(R)$. (el isomorfismo es la biyección anterior).

A partir de $[f+g] = [f] + [g]$ y $(rf)(x) = rf(x)$, se tiene que si F_1, F_2 y F_3 son libres con bases B_1, B_2 y B_3 respectivamente, y $f : F_1 \rightarrow F_2$, $g : F_2 \rightarrow F_3$ son lineales, entonces $[g \circ f]_{B_1 B_2} = [g]_{B_2 B_3} \cdot [f]_{B_1 B_2}$ (producto usual de matrices).

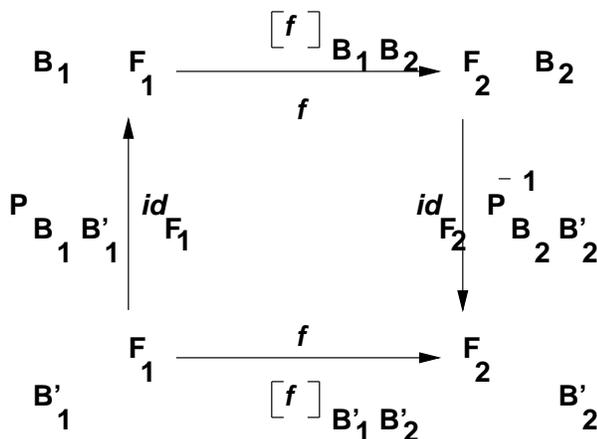
Se tienen los mismos resultados que en álgebra lineal:

• $f : F_1 \rightarrow F_2$ es un isomorfismo $\Leftrightarrow [f]_{B_1 B_2}$ es invertible en $M_{mn}(R)$, con $[f]_{B_1 B_2}^{-1} = [f^{-1}]_{B_1 B_2}$.

• Matrices de Pasaje:

Sean B_1 y B'_1 bases de F_1

$$P_{B_1 B'_1} = [id_{F_1}]_{B_1 B'_1} \quad P_{B'_1 B_1} = [id_{F_1}]_{B'_1 B_1} \quad P_{B_1 B'_1}^{-1} = P_{B'_1 B_1} \quad (\forall x \in F_1)[x]_{B_1} = P_{B_1 B'_1}[x]_{B'_1}$$



$$[f]_{B'_1 B'_2} = P_{B_2 B'_2}^{-1} [f]_{B_1 B_2} P_{B_1 B'_1}$$

Definición

Dos matrices $A, A' \in M_{mn}(\mathbb{R})$ se dicen equivalentes ssi $\exists P \in M_{mm}(\mathbb{R}), Q \in M_{nn}(\mathbb{R})$ invertibles, tales que $A' = P^{-1}AQ$.

(Dos matrices son equivalentes ssi representan a la misma transformación lineal, cambiando las bases).

Ejemplo:

$[2] \in M_{11}(\mathbb{Z})$ no es invertible:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$x \longrightarrow 2x, \text{ su inversa sería } \begin{bmatrix} \frac{1}{2} \end{bmatrix} \notin M_{11}(\mathbb{Z})$$

Nota:

Toda la teoría de determinantes en que las demostraciones NO requieran división, vale para matrices en $M_{nn}(\mathbb{R})$. En particular:

1. $|AB| = |A| \cdot |B|$
2. A es invertible ssi $|A|$ es invertible en \mathbb{R} , y en este caso, $|A^{-1}| = (|A|)^{-1}$

Caso general : R - módulos finitamente generados

Sea $M = \langle \{m_1, \dots, m_n\} \rangle = Rm_1 + \dots + Rm_n$ un módulo finitamente generado sobre el dip R .

Si $F = Ra_1 \oplus \dots \oplus Ra_n$ es un R -módulo libre finitamente generado, Entonces la función

$$\varphi : F \longrightarrow M$$

$$x = r_1a_1 + \dots + r_na_n \longrightarrow r_1m_1 + \dots + r_nm_n$$

es un epimorfismo , y por lo tanto , $M \cong F/\text{Ker}\varphi$.

Por un teorema visto con anterioridad , el submódulo $L = \text{Ker}\varphi \subseteq F$ es también libre , con base de cardinal k , donde $k \leq n$.

Consideremos el caso general en que $L = \text{Im}f$, con $f : F' \rightarrow F$, para F' otro módulo libre finitamente generado. (por ejemplo : $F' = L$, $f = i$, con $i : L \hookrightarrow F$ la inclusión).

Así, el problema de estudiar módulos finitamente generados sobre un dip R , equivale a estudiar módulos del tipo $F/\text{Im}f$, donde $f : F' \rightarrow F$ lineal , F' y F son R -módulos libres de rango finito m y n respectivamente.

Dadas una base B' de F' y B de F , f tiene matriz representante $A = [f]_{B'B}$.

¿Qué sucedería si somos capaces de encontrar una base B' en F' , y otra B en F , de modo que $A = [f]$ tenga la siguiente forma ?

$$\left[\begin{array}{ccc} \delta_1 & & \\ & \delta_r & \\ & & 0 \\ & & & 0 \end{array} \right]$$

¿Qué podemos decir del cuociente $F/\text{Im}f$?

$$B' = \{b_1, \dots, b_m\} \quad B = \{a_1, \dots, a_n\}$$

$$f(b_1) = \delta_1 a_1$$

$$f(b_2) = \delta_2 a_2$$

⋮

$$f(b_r) = \delta_r a_r$$

$$f(b_{r+1}) = \dots = f(b_m) = 0$$

$$\Rightarrow \text{Im}f = R\delta_1 a_1 \oplus \dots \oplus R\delta_r a_r \oplus 0 \quad \text{Además , } F = Ra_1 \oplus \dots \oplus Ra_r \oplus \dots \oplus Ra_n$$

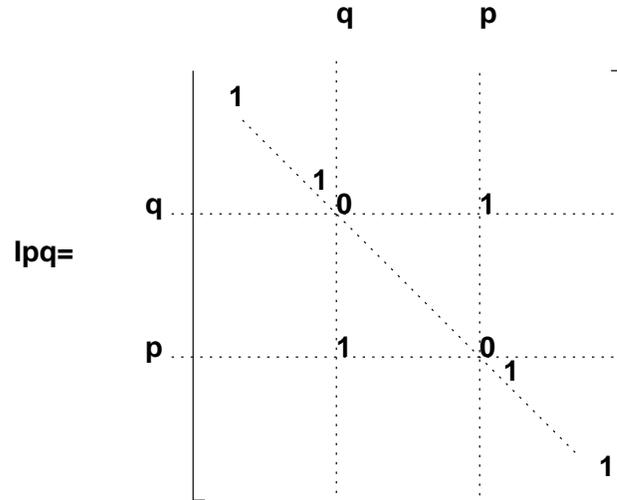
$$\Rightarrow F/\text{Im}f \cong Ra_1/R\delta_1 a_1 \oplus \dots \oplus Ra_r/R\delta_r a_r \oplus Ra_{r+1} \oplus \dots \oplus Ra_n \quad (\text{UN EJERCICIO ANTERIOR})$$

$$\Rightarrow F/\text{Im}f \cong (R/R\delta_1)[a_1] \oplus \dots \oplus (R/R\delta_r)[a_r] \oplus F'' , \text{ con } F'' \text{ libre de base } \{a_{r+1}, \dots, a_n\}$$

$$\text{Así , } F/\text{Im}f \cong R/(\delta_1) \oplus \dots \oplus R/(\delta_r) \oplus F''$$

Concluiríamos entonces , que el módulo original $M \cong F/L = F/\text{Im}f$ es , salvo isomorfismos , una suma finita de módulos cíclicos \oplus un módulo libre de rango finito.

Veamos que A puede ser de la forma que queremos:

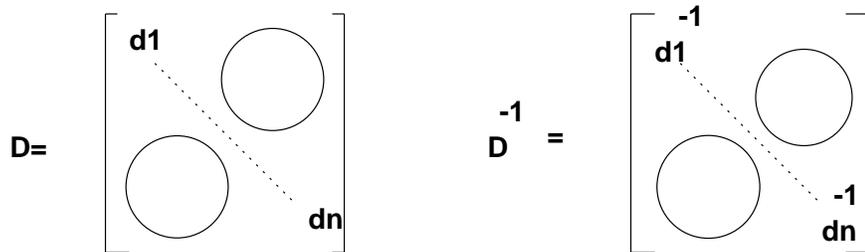


$$I_{pq}^{-1} = I_{pq}$$

$I_{pq} \cdot A$: intercambia filas p y q

$A \cdot I_{pq}$: intercambia columnas p y q

c) Multiplicar filas ($D \cdot A$) o columnas ($A \cdot D$) por elementos invertibles



$$d_1, \dots, d_n \in \mathbb{R}^x$$

2. Además necesitaremos la operación secundaria $S \cdot A$, donde $S = \begin{bmatrix} \alpha & \beta & \circ \\ \gamma & \delta & \circ \\ \circ & \circ & I_{n-2} \end{bmatrix}$ Con

determinante de $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ invertible .

Si $A = \begin{bmatrix} a_{11} & \dots \\ a_{21} & \dots \\ & A' \end{bmatrix}$, queremos obtener $S \cdot A = \begin{bmatrix} m & \dots \\ 0 & \dots \\ & A' \end{bmatrix}$ con $m = \text{mcd}(a_{11}, a_{21})$.

Para esto , debemos escoger de manera apropiada α, β, γ y δ .

$$S \cdot A = \begin{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \cdot \begin{bmatrix} a_{11} & \dots \\ a_{21} & \dots \end{bmatrix} \\ A' \end{bmatrix} = \begin{bmatrix} \alpha a_{11} + \beta a_{21} & \dots \\ \gamma a_{11} + \delta a_{21} & \dots \\ & A' \end{bmatrix}$$

Como R es dip , sabemos que existen $\alpha', \beta' \in R$ tales que $\alpha'a_{11} + \beta'a_{21} = m$. Entonces , si escogemos $\alpha = \alpha'$ y $\beta = \beta'$ tenemos $\alpha a_{11} + \beta a_{21} = m$.

$m/a_{11} \wedge m/a_{21} \Rightarrow \exists \mu, \nu \in R$ tales que $a_{11} = \mu m$ y $a_{21} = \nu m$. Escogamos $\gamma = -\nu$ y $\delta = \mu$, de esta forma tenemos que $\gamma a_{11} + \delta a_{21} = -\nu \mu m + \mu \nu m = 0$. Además $\alpha a_{11} + \beta a_{21} = m \Leftrightarrow \alpha \mu m + \beta \nu m = m \Leftrightarrow \alpha \mu + \beta \nu = 1$, pero $\alpha \mu + \beta \nu = \det \begin{bmatrix} \alpha & \beta \\ -\nu & \mu \end{bmatrix} \Rightarrow$ es invertible.

En resumen : Si escogemos $\alpha, \beta, \gamma,$ y δ de tal forma que $\alpha a_{11} + \beta a_{21} = \text{mcd}(a_{11}, a_{21})$ y $a_{11} = m\delta$, $a_{21} = m(-\gamma)$, se obtiene \bar{A} de la forma deseada.

Para continuar la demostración , necesitaremos el siguiente lema:

Lema

Si $A \neq 0$, es equivalente a una matriz del tipo

$$\left[\begin{array}{c|ccc} \delta & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & & & \\ \vdots & & \mathbf{B} & \\ \mathbf{0} & & & \end{array} \right]$$

con δ divisor de todos los elementos de B .

Dem

Es claro que en la esquina (1, 1) podemos ubicar un elemento distinto de cero , y usarlo para anular , con operaciones secundarias , toda la columna bajo él. Llegamos a lo siguiente:

$$\left[\begin{array}{c|cccc} \mathbf{m} & \cdots & \cdots & \cdots & \cdots \\ \hline \mathbf{0} & \cdots & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \cdots & \cdots & \cdots \end{array} \right]$$

con m divisor de toda la primera columna original.

Paso siguiente: hacemos lo mismo por columnas , con el fin de anular la fila a la derecha de m . Obtenemos:

$$\left[\begin{array}{c|cccc} \mathbf{m1} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{array} \right]$$

con m_1/m . Al siguiente paso obtenemos:

$$\left[\begin{array}{c|cccc} \mathbf{m2} & \cdots & \cdots & \cdots & \cdots \\ \hline \mathbf{0} & \cdots & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \cdots & \cdots & \cdots \end{array} \right]$$

con m_2/m_1

Se genera una sucesión de esquinas $\cdots m_3/m_2/m_1/m_o = m$ cada uno asociado a matrices

$$\left[\begin{array}{c|cccc} \mathbf{mi} & \cdots & \cdots & \cdots & \cdots \\ \hline \mathbf{0} & \cdots & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \cdots & \cdots & \cdots \end{array} \right] \circ \left[\begin{array}{c|cccc} \mathbf{mi} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{array} \right]$$

Afirmamos que los m_i se “estabilizan” .

Consideremos los ideales $(m_o) \subseteq (m_1) \subseteq (m_2) \subseteq \cdots \subseteq (m_i) \subseteq (m_{i+1}) \subseteq \cdots$

Sea $I = \bigcup_{i \in \mathbb{N}} (m_i)$, I es ideal en R , y por ser este un dip , $\exists \bar{m} \in R$ tal que $I = (\bar{m})$.

$\bar{m} \in I \Rightarrow \exists i \in \mathbb{N}$ tal que $\bar{m} \in (m_i) \Rightarrow (\bar{m}) \subseteq (m_i) \subseteq (\bar{m}) \Rightarrow I = (\bar{m}) = (m_i)$, por lo tanto , $(\forall j \geq i) (m_i) = (m_j) \Leftrightarrow m_j = um_i$ con u invertible .

Por lo tanto , en algún momento pasamos de

$$\left[\begin{array}{c|cccc} \mathbf{mi} & \cdots & \cdots & \cdots & \cdots \\ \hline \mathbf{0} & \cdots & \cdots & \cdots & \cdots \\ \vdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \cdots & \cdots & \cdots \end{array} \right] \mathbf{a} \left[\begin{array}{c|cccc} \mathbf{mi} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{array} \right] \text{ (o al revés)}$$

Al ser $m_i = m_{i+1}$ (o $m_i \sim m_{i+1}$) se tiene que $m_i = m_{i+1}$ es un divisor de todos los elementos de la derecha de m_i en la primera matriz , y en vez de hacer este último paso , podemos pivotar por Gauss y anular el resto de la fila sin alterar los ceros bajo m_i . Hemos llegado a :

$$\left[\begin{array}{c|ccc} \mathbf{m} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & & & \\ \vdots & & & \\ \mathbf{0} & & & \end{array} \right] \begin{array}{c} \\ \\ \mathbf{B}' \\ \\ \end{array}$$

Pero aun no se sabe si m divide a las componentes de B' . Para lograr que las divida hacemos lo siguiente :

Si m no divide a $(B')_{ij}$, sumamos la fila i a la primera , y hacemos el mismo procedimiento , se genera

$$\left[\begin{array}{c|ccc} \mathbf{m}' & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & & & \\ \vdots & & & \\ \mathbf{0} & & & \end{array} \right] \begin{array}{c} \\ \\ \mathbf{B}'' \\ \\ \end{array}$$

m' divide a $(B')_{ij}$ y a m .

Terminamos cuando se estabilizan los m . Por inducción se concluye el teorema.

Corolario

Toda matriz cuadrada invertible sobre un dip es equivalente a una matriz diagonal de diagonal invertible.

Observación:

En $R = \mathbb{Z}$ o $R = K[x]$ (K cuerpo) sólo se requieren operaciones primarias , por que las secundarias se pueden obtener a partir de las primarias. Mejor aun , $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{22}(R)$ se puede transformar en $\begin{bmatrix} m & \cdots \\ 0 & \cdots \end{bmatrix}$ (con $m = \text{m.c.d}(a,b)$) sólo a través de operaciones primarias , esto gracias al algoritmo de Euclides.

Corolario

Todo módulo finitamente generado sobre un dip R , es isomorfo a uno del tipo $R/(\delta_1) \oplus \cdots \oplus R/(\delta_k) \oplus F$, con F un módulo libre finitamente generado, y $1 \approx \delta_1/\delta_2/\cdots/\delta_k \neq 0$.

Cuando $R = \mathbb{Z}$, todo grupo abeliano finitamente generado es isomorfo a $\mathbb{Z}_{\delta_1} \oplus \cdots \oplus \mathbb{Z}_{\delta_k} \oplus \mathbb{Z}^m$ con $2 \leq \delta_1/\cdots/\delta_k \neq 0$. Todo grupo abeliano finito es de la forma $\mathbb{Z}_{\delta_1} \oplus \cdots \oplus \mathbb{Z}_{\delta_k}$, $2 \leq \delta_1/\cdots/\delta_k \neq 0$ y el cardinal del grupo es $\prod_{i=1}^k \delta_i$.

Ejemplo:

Si A es abeliano, con $|A| = 24$

$$\begin{array}{ll} \mathbb{Z}_{24} & 3 \cdot 2^3 \\ \mathbb{Z}_{2 \oplus \mathbb{Z}_{12}} & 2 \cdot 3 \cdot 2^2 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 & 2 \cdot 2 \cdot 3 \cdot 2 \end{array}$$

Corolario

Toda matriz $A \in M_{nn}(R)$ es producto de matrices elementales y secundarias. Sobre $R = \mathbb{Z}$ o $R = K[x]$ (K cuerpo), A será producto de elementales.

Ejercicio 1:

Sea M un R -módulo y TM su módulo de torsión

1. Si $f : M \rightarrow M'$ es un isomorfismo de R -módulos, entonces $f(TM) = TM'$.
2. $T(R/(\delta_1) \oplus \cdots \oplus R/(\delta_r) \oplus F) = R/(\delta_1) \oplus \cdots \oplus R/(\delta_r)$
3. $M/TM \cong F$

Corolario

Si R es un dip y M es un módulo sin torsión (i.e. $TM = \{0\}$) y finitamente generado, entonces M es libre.

Ejercicio 2 :

Sea M un R -módulo, $c \in R$ y $f_c : M \rightarrow M$ la multiplicación por c ($f_c(x) = cx$). Anotamos $\text{Im} f_c = cM$. Notar que $cM = (c)M$.

1. Si $M = M_1 \oplus M_2$

- (a) $cM = cM_1 \oplus cM_2$
 (b) $M/cM \cong M_1/cM_1 \oplus M_2/cM_2$
2. Si c y d son primos relativos , entonces $c \cdot R/(d) = R/(d)$
3. Si $d = a \cdot c$ ($a, c \neq 0$) , entonces $c \cdot R/(ac) = (c)/(ac) \cong R/(a)$ y $(R/(ac))/(c \cdot R/(ac)) \cong R/(c)$
4. Si $d = \text{mcd}(c, b)$, entonces $c \cdot R/(b) \cong R/(b/d)$
5. Recuerdo : Si $M = Rm_o$ es un R - módulo cíclico , el anulador de $M = I = \{r \in R/rm_o = 0\} = (r_o)$. $r_o = o(M)$ es el orden de M .
 Probar que : Si M_1, M_2 son módulos cíclicos , entonces $o(M_1)/o(M_2) \Rightarrow o(cM_1)/o(cM_2)$

Teorema

Si R es un dip , todo R - módulo finitamente generado M es isomorfo a $R/(\delta_1) \oplus \cdots \oplus R/(\delta_r) \oplus F$ con $1 \approx \delta_1 / \cdots / \delta_r \neq 0$ y F libre finitamente generado. El rango de F y los δ_i (salvo multiples invertibles) son únicos .

Dem

La existencia del isomorfismo se deduce del teorema anterior.

Veamos que sucede con la unicidad de esta descomposición : Supongamos que $M \cong R/(\delta_1) \oplus \cdots \oplus R/(\delta_r) \oplus F \cong R/(\delta'_1) \oplus \cdots \oplus R/(\delta'_s) \oplus F'$, con $F, F', \delta_i, 1 \leq i \leq r$ y $\delta'_i, 1 \leq i \leq s$ verificando las condiciones del teorema.

Del Ejercicio 1 , se concluye facilmente que $L = R/(\delta_1) \oplus \cdots \oplus R/(\delta_r) \cong L' = R/(\delta'_1) \oplus \cdots \oplus R/(\delta'_s)$ y $F \cong F'$.

Probemos que $r = s$. Por contradicción , supongamos que $r > s$.

Sea p primo tal que $p/\delta_1 \Rightarrow p/\delta_i \forall i \in \{1 \dots r\}$, entonces , del ejercicio 2 , $\frac{R/(\delta_i)}{p \cdot R/(\delta_i)} \cong R/(p)$

Si p/δ'_i , se tiene $\frac{R/(\delta'_i)}{p \cdot R/(\delta'_i)} \cong R/(p)$, si no , p y δ_i son primos relativos $\Rightarrow L'/pL' \cong 0$ (ejercicio 2) .

Así , $L/pL \cong L'/pL'$ equivale a $\underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{r \text{ veces}} \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{\leq s \text{ veces}}$

como p es primo , $I = (p)$ es maximal $\Leftrightarrow R/I = R/(p)$ es cuerpo. El isomorfismo anterior es como $R/(p)$ - módulos , pero por ser $R/(p)$ cuerpo , es un isomorfismo entre $R/(p)$ - e.v $\rightarrow \leftarrow$ pues tienen distinta dimensión ($r > s$) .

Veamos ahora que $\delta_i \sim \delta'_i \forall 1 \leq i \leq s$. Por contradicción , supongamos que $\exists 1 \leq j \leq s$ tal que $\delta_j \not\sim \delta'_j$.

Sea j la última vez que $\delta_i \sim \text{No}\delta'_i$, i.e $\delta'_r \sim \delta_r, \delta'_{r-1} \sim \delta_{r-1}, \dots, \delta'_{i+1} \sim \delta_{i+1}, \delta'_i \text{NO} \sim \delta_i$.

$\delta'_i \text{NO} \sim \delta_i$ significa que δ'_i no divide a δ_i o δ_i no divide a δ'_i , supongamos que δ'_i no divide a δ_i .

Multipliquemos L por δ_i : desde $j = 1$ hasta $j = i$ δ_j/δ_i , por lo tanto, $\delta_i R \subseteq (\delta_j) \Rightarrow \delta_i R/(\delta_j) = 0$. Resulta entonces $R/(\delta_{i+1}/\delta_i) \oplus \dots \oplus R/(\delta_r/\delta_i)$

Como $\delta_{i+1} = \delta'_{i+1}, \dots, \delta_r = \delta'_r$

$L' \cong S \oplus \underbrace{R/(\delta'_i/\text{mcd}(c, \delta_i))}_{\neq 0} \oplus R/(\delta_{i+1}/c) \oplus \dots \oplus R/(\delta_r/c)$ más largo que $L \rightarrow \leftarrow$, por lo tanto

, $\delta_i \sim \delta'_i \forall i = 1 \dots n$.

Definición

- $\delta_1, \dots, \delta_r$ se llaman “factores invariantes” del R - módulo M
- El rango de F se llama rango de M , $r(M)$.

Corolario

Si M es un grupo abeliano, finitamente generado, entonces M se escribe de manera única como $M \cong \mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_r} \oplus \mathbb{Z}^k$, con $1 < q_1/\dots/q_r \neq 0$ naturales únicos, y $k \geq 0$ único, llamado el rango del grupo abeliano.

Sea R un dip. Si M es un R - módulo, su anulador es $I = \{r \in R/(\forall m \in M)\} rm = 0\}$. I es un ideal, por lo tanto, $\exists e \in R$ tal que $I = (e)$. e se llama “anulador minimal”, “anulador principal” o “exponente” de M (si M es cíclico se llama “orden de M ”). Anotamos $e = e(M)$, definido unicamente, salvo multiplicación por elementos invertibles.

Si M es finitamente generado: $M = \langle \{m_1, \dots, m_k\} \rangle = Rm_1 + \dots + Rm_k$.

$r \in \text{Anulador de } M \Leftrightarrow rm_i = 0 \forall 1 \leq i \leq k$, por lo tanto, $I = \{r \in R/rm_i = 0 \forall 1 \leq i \leq k\} = (e)$.

Es directo que $e = e(M) = \text{MCM}\{o(m_1), \dots, o(m_k)\}$, donde $(a) \cap (b) = (\text{MCM}\{o(m_1), \dots, o(m_k)\})$

Sabemos que $M \cong R/(\delta_1) \oplus \dots \oplus R/(\delta_r) \oplus F$

$F \neq \{0\} \Rightarrow e(M) = 0$

$F = \{0\} \Leftrightarrow M$ es de torsión

Entonces $m_1 = [1]_{R/(\delta_1)}, \dots, m_r = [1]_{R/(\delta_r)}$ son generadores de (la copia isomorfa de) M y sus respectivos ordenes son $\delta_1, \dots, \delta_r$, y su MCM es $\delta_r = e(M)$.

Tenemos que si M es finitamente generado, $M = TM \oplus F$, con TM módulo de torsión y FF módulo libre.

Veamos otra descomposición de TM o mejor, supongamos que M es de torsión (otra descomposición de M).

Dado un primo $p \in R$, la **componente p- primaria** de M es $T_p M = \{m \in M / \exists i \geq 0 \text{ tal que } p^i m = 0\}$, para M no necesariamente finitamente generado.

$T_p M$ es un submódulo de M . En efecto:

- $0 \in T_p M$
- Si $m_1, m_2 \in T_p M$, $p^i m_1 = 0$, $p^j m_2 = 0 \Rightarrow p^{i+j}(r m_1 + s m_2) = 0$, $r, s \in R \Rightarrow r m_1 + s m_2 \in T_p M$

Prop

Sea M un R -módulo de torsión. Supongamos que $\{p_\lambda\}_{\lambda \in \Lambda}$ es una familia de primos en R , con cada p_λ un representante de una clase unitaria de primos. Todas las clases representadas una y sólo una vez cada una, entonces $M = \bigoplus_{\lambda \in \Lambda} T_{p_\lambda} M$.

Dem.

Sea $x \in M \setminus \{0\}$, y sea $n \in R$ su orden o anulador minimal ($o(x) = n$).

n no es invertible, si no, $x = 0$. $n \neq 0$, pues x es de torsión.

Sea $n = p_{\lambda_1}^{\alpha_1} \cdots p_{\lambda_k}^{\alpha_k} \cdot u$ la descomposición de n como producto de primos, (u es un elemento invertible). Veamos que $x = x_1 + \cdots + x_k$ con $x_i \in T_{p_{\lambda_i}} M$ $1 \leq i \leq k$.

Sea $n_i = \frac{n}{u p_{\lambda_i}^{\alpha_i}}$, $1 \leq i \leq k$

Ejercicio: (inducción) $\exists \beta_1, \dots, \beta_k \in R$ tal que $\beta_1 n_1 + \cdots + \beta_k n_k = 1$ (puesto que en conjunto, no de a pares, n_1, \dots, n_k son primos relativos: $\text{mcd}(n_1, \dots, n_k) = 1$).

$\Rightarrow x = \beta_1 n_1 x + \cdots + \beta_k n_k x$, $x_i = \beta_i n_i x$ $1 \leq i \leq k$, $p_{\lambda_i}^{\alpha_i} x_i = \beta_i p_{\lambda_i}^{\alpha_i} n_i x = 0 \Rightarrow x_i \in T_{p_{\lambda_i}} M \Rightarrow M = \sum_{\lambda \in \Lambda} T_{p_\lambda} M$.

La suma es directa, esto equivale a: (**Ejercicio**)

Si $x_i \in T_{p_{\lambda_i}} M$ $\lambda_i \neq \lambda_j$ si $i \neq j$ $1 \leq i, j \leq k$, y $x_1 + \cdots + x_k = 0$, entonces $x_i = 0 \forall 1 \leq i \leq k \Rightarrow x_1 = -x_2 - x_3 - \cdots - x_k$, pero $o(x_1) = p_{\lambda_1}^{\alpha_1}$ y $o(-x_2 - x_3 - \cdots - x_k) = p_{\lambda_2}^{\alpha_2} \cdots p_{\lambda_k}^{\alpha_k}$, lo que no es posible si $\alpha_1 \neq 0$, por lo tanto, $\alpha_1 = 0 \Rightarrow x_1 = 0$. Repitiendo el mismo argumento, se concluye que $x_i = 0 \forall 1 \leq i \leq k$.

Ejercicio:

Si $M \neq \{0\}$ es cíclico y de torsión, sabemos que $M \cong R/(\delta)$ $\delta = o(M) = e(M) \in R \setminus (\{0\} \cup R^x)$, $\delta = p_1^{\alpha_1} \cdots p_k^{\alpha_k} u$ p_1, \dots, p_k primos, $u \in R^x$, $\alpha_i \in \mathbb{N} \forall 1 \leq i \leq k$. Entonces $R/(\delta) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$.

Aplicando todo esto resulta lo siguiente: Si M es un R -módulo de torsión finitamente generado, entonces $M \cong \bigoplus_{i=1}^l [R/(p_i^{\alpha_i, 1}) \oplus \cdots \oplus R/(p_i^{\alpha_i, k_i})]$, con p_1, \dots, p_l primos que aparecen

en la descomposición de δ_r , con $\delta_1/\dots/\delta_r$ los factores invariantes. $\alpha_{i,j}$ exponente de p_i en alguno de los δ_j . $R/(p_i^{\alpha_{i,1}}) \oplus \dots \oplus R/(p_i^{\alpha_{i,k_i}}) \cong T_{p_i}M$. Los $p_i^{\alpha_{i,j}}$ se llaman divisores elementales de M .

Ejemplo:

A grupo abeliano de 24 elementos .

$$\begin{array}{lll} \delta_1 = 3 \cdot 2^3 & & \mathbb{Z}_{24} (A_1) \\ \delta_1 = 2 & \delta_2 = 3 \cdot 2 & \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus (A_2) \\ \delta_1 = 2 & \delta_2 = 2 & \delta_3 = 3 \cdot 2 \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 (A_3) \end{array}$$

En términos de divisores elementales :

$$A_1 \cong \underbrace{\mathbb{Z}_3}_{T_3A_1} \oplus \underbrace{\mathbb{Z}_8}_{T_2A_1} \quad A_2 \cong \underbrace{\mathbb{Z}_3}_{T_3A_2} \oplus \underbrace{\mathbb{Z}_4 \oplus \mathbb{Z}_2}_{T_2A_2} \quad A_3 \cong \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2}_{T_2A_3} \oplus \underbrace{\mathbb{Z}_3}_{T_3A_3}$$

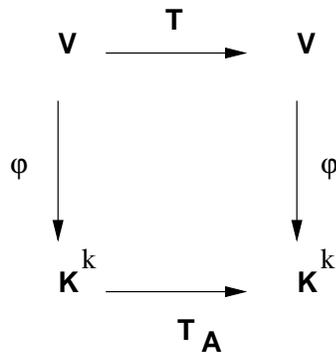
$K[x]$ -Módulos de Torsión Finitamente Generados

Recordemos que si M es $K[x]$ - módulo , entonces $M = V$ espacio vectorial sobre K junto con una transformación lineal $T : V \rightarrow V$ que corresponde a la multiplicación por $x \in K[x]$. Si $v \in V$ y $p(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$, la multiplicación por escalar está definida por $p(x)v = p(T)(v)$ con $p(T) = a_0id + a_1T + \dots + a_nT^n$.

Si V es de dimensión finita y $B = \{v_1, \dots, v_k\}$ es su base , la función $\varphi : V \rightarrow K^k$ tal que

a $v = \lambda_1v_1 + \dots + \lambda_kv_k$ le asigna $\varphi(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix}$, es un isomorfismo de $K[x]$ - módulos :

$$(V, T) \rightarrow (K^k, T_A)$$



con $T_Ax = Ax$, $A = [T]_{BB}$.

Observación:

Si V es e.v de dimensión $n < \infty$ sobre K , sabemos que $L(V, V) \cong M_{nn}(K)$ (como e.v), por lo tanto, $L(V, V)$ es de dimensión n^2 . Entonces, si $T : V \rightarrow V$ es una transformación lineal, $\{T^0, T^1, T^2, \dots, T^k, \dots\} = \{T^k/k \in \mathbb{N}\}$ es l.d $\Rightarrow \exists a_0, a_1, \dots, a_k \in K$ no todos nulos tal que $a_0 T^0 + a_1 T^1 + \dots + a_k T^k = 0$. Si $p(x) = a_0 + a_1 x + \dots + a_k x^k \Rightarrow p(x) \in K[x]/\{0\}$ y $p(T) = 0$.

Sea $I = \{p(x) \in K[x]/p(T) = 0\}$, I es un ideal en $K[x]$, por lo tanto, $I = (m(x))$, pues $K[x]$ es dip. $m(x)$ está únicamente definido, salvo por multiplicación por constantes distintas de cero (i.e, los invertibles en $K[x]$).

$m(x)$ se escoge como el único mónico (coeficiente de la mayor potencia de x es 1) y se llama **polinomio mínimo** de la transformación lineal T . $m(x)$ es el polinomio mónico distinto de cero de menor grado tal que $m(T) = 0$.

$(\forall p(x) \in K[x]) p(T) = 0 \Rightarrow p(x)$ es múltiplo de $m(x)$.

Considerando el par (V, T) como un $K[x]$ -módulo (con T la multiplicación por x) : $m(x)v = 0 \forall v \in V$, por lo tanto, V es de torsión y $m(x)$ es su anulador minimal.

$\{p(x) \in K[x]/p(x) \cdot v = 0 \forall v \in V\}$

$p(x)v = 0 \forall v \in V \Leftrightarrow p(T)v = 0 \forall v \in V \Leftrightarrow p(T) = 0 \in L(V, V)$

$m(x)$ es anulador minimal entonces.

Notar también que, dado que V es de dimensión finita como K -e.v, tiene base $\{v_1 \dots v_n\}$, $(\forall v \in V) v = \underbrace{\lambda_1}_{\in K} v_1 + \dots + \underbrace{\lambda_n}_{\in K} v_n$, pero $K \subseteq K[x]$, por lo tanto, V es generado como $K[x]$ -módulo por $v_1 \dots v_n$.

En resumen, si V es e.v sobre el cuerpo K y $T : V \rightarrow V$ es lineal :

1. $\exists m(x) \in K[x] \setminus \{0\}$, mónico, tal que $m(T) = 0$ y $m(x)$ es el polinomio, distinto de cero, de menor grado que hace esto, más aun, si $P(T) = 0$, para $p(x) \in K[x] \Rightarrow m(x)/p(x)$
2. Considerando V como $K[x]$ -módulo (con $xv = T(v)$) V es de torsión, con anulador minimal $m(x)$ (el polinomio mínimo de T) y finitamente generado.

A la inversa : comenzamos con un módulo M de torsión finitamente generado sobre $K[x]$.

Sabemos que M es un espacio vectorial V sobre K , con una transformación K -lineal $T : V \rightarrow V$. Además $M \cong K[x]/(\delta_1(x)) \oplus \dots \oplus K[x]/(\delta_r(x))$ (como $K[x]$ -módulos), con $\delta_1(x)/\dots/\delta_r(x) \neq 0$ los factores invariantes del módulo, únicos si se piden mónicos (son únicos salvo factores invertibles, i.e constantes distintas de cero).

Veamos primero el caso M cíclico : $M \cong K[x]/(\delta(x))$, con $\delta(x)$ el orden de M . Además $\exists v_o \in V (= M)$, tal que $M = K[x]v_o$, i.e $(\forall v \in V) (\exists p(x) \in K[x]) v = p(T)(v_o) = a_0 v_o + a_1 T(v_o) + \dots + a_k T^k(v_o) \Rightarrow \{v_o, T(v_o), \dots, T^k(v_o), T^{k+1}(v_o), \dots\}$ genera V como espacio vectorial sobre K .

Pero si $p(x) \in K[x]$, podemos dividirlo por $\delta(x) : p(x) = q(x)\delta(x) + r(x)$, con $\text{gr}(r(x)) < \text{gr}(\delta(x)) = n \Rightarrow v = p(T)(v_o) = q(T)\underbrace{\delta(T)(v_o)}_{\delta(x)v_o=0} + r(T)(v_o) = r(T)(v_o) = b_o + b_1T(v_o) + \dots +$

$b_{n-1}T^{n-1}(v_o)$,por lo tanto , $\{v_o, T(v_o), \dots, T^{n-1}(v_o)\}$ generan V como e.v sobre K , i.e V , como e.v sobre K , es de dimensión finita .

Mejor aun : $\{v_o, T(v_o), \dots, T^{n-1}(v_o)\}$ son l.i , y por lo tanto , constituyen una base del e.v sobre el cuerpo K . En efecto :

Si $\lambda_o v_o + \lambda_1 T(v_o) + \dots + \lambda_{n-1} T^{n-1}(v_o) = 0$ $\lambda_i \in K \forall 0 \leq i \leq n-1$, entonces $p(T)(v_o) = 0$, para $p(x) = \lambda_o + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} \Rightarrow p(x)v_o = 0$ en la estructura de $K[x]$ -módulo $\Rightarrow p(x)V = 0$, pues V está generado como $K[x]$ - módulo por $\{v_o\} \Rightarrow p(x)$ es múltiplo de $\delta(x)$, pero $\text{gr}(p(x)) < \text{gr}(\delta(x)) \Rightarrow p(x) = 0 \Rightarrow$ sus coeficientes $\lambda_o = \dots = \lambda_{n-1} = 0$.

¿Cuál es la matriz de T con respecto a la base $B = \{v_o, T(v_o), \dots, T^{n-1}(v_o)\}$ del e.v V ?

$$\begin{array}{ccccccc} v_1 & = & v_o & & Tv_1 & = & Tv_o & = & v_2 \\ v_2 & = & T(v_o) & & Tv_2 & = & T^2v_o & = & v_3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ v_{n-2} & = & T^{n-2}(v_o) & & Tv_{n-1} & = & T^{n-1}v_o & = & v_n \\ v_{n-1} & = & T^{n-1}(v_o) & & Tv_n & = & T^n v_o & = & ? \end{array}$$

Sea $\delta(x) = c_o + c_1x + \dots + c_{n-1}x^{n-1} + x^n$ (el anulador minimal del $K[x]$ -módulo $M = (V, T)$).

Calculemos $T^n v_o : \delta(x)v_o = 0 = c_o v_o + c_1 T v_o + \dots + c_{n-1} T v_o + T^n v_o \Rightarrow T^n v_o = -c_o v_o - c_1 T v_o - \dots - c_{n-1} T^{n-1} v_o = -c_o v_1 - \dots - c_{n-1} v_n$.

Por lo tanto ,

$$\mathbf{A} = [\mathbf{T}]_{\mathbf{B}} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & | & -\mathbf{c}_1 \\ \mathbf{1} & \mathbf{0} & & & | & -\mathbf{c}_2 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & & | & \vdots \\ \vdots & & \mathbf{0} & \mathbf{1} & \mathbf{0} & | & \vdots \\ \vdots & & & \mathbf{0} & \mathbf{1} & \mathbf{0} & | & \vdots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{1} & | & -\mathbf{c}_{\mathbf{n-1}} \end{bmatrix}$$

“Matriz compañera de $\delta(x)$ ” . Anotamos $[T]_B = C_{\delta(x)}$.

Ejercicio:

El polinomio característico de la matriz compañera de $\delta(x)$ es $p_{C_{\delta(x)}} = (-1)^n \delta(x)$. Notar que el polinomio mínimo de T es $\delta(x)$.

Prop

Sea M un $K[x]$ -módulo de modo que $M = (V, T)$, con V e.v sobre K y $T : V \rightarrow V$ la multiplicación por x . Sea $\delta(x) \in K[x] \setminus \{0\}$ mónico. Entonces, M es cíclico de orden $\delta(x)$ ssi V tiene una base B tal que la matriz representante de T en esta base es la matriz compañera de $\delta(x)$.

Dem.

\Rightarrow) Está demostrado

\Leftarrow) $B = \{v_1, \dots, v_n\}$, $\delta(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} + x^n$. $[T]_B = C_{\delta(x)}$ significa :

$$\begin{array}{rcccccc} Tv_1 & = & v_2 & \rightarrow & xv_1 & = & v_2 \\ Tv_2 & = & v_3 & \rightarrow & x^2v_1 & = & v_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ Tv_{n-1} & = & v_n & \rightarrow & x^{n-1}v_1 & = & v_n \\ Tv_n & = & -c_0v_1 - c_1v_2 - \dots - c_{n-1}v_n & & & & \end{array}$$

Como $K[x]$ -módulo, $M = V$ es generado por $\{v_1\}$, i.e M es cíclico.

Además $Tv_n = x^n v_1 = -c_0v_1 - c_1xv_1 - \dots - c_{n-1}x^{n-1}v_1 \Leftrightarrow \delta(x)v_1 = 0$, por lo tanto, $\delta(x)$ anula todo $M = V$.

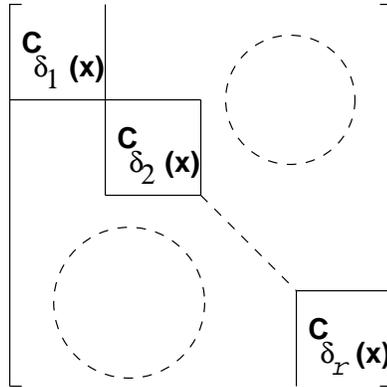
Por ser $V = M$ cíclico, tiene anulador minimal $\delta'(x)$ de grado igual a $\dim V = n$, por ser anulador minimal $\delta'(x)/\delta(x)$, pero $\text{gr}(\delta'(x)) = \text{gr}(\delta(x)) = n$ y ambos son mónicos $\Rightarrow \delta'(x) = \delta(x)$.

Generalicemos para el caso en que M es de torsión finitamente generado sobre $K[x]$: $M \cong K[x]/(\delta_1(x)) \oplus \dots \oplus K[x]/(\delta_r(x))$, con $\delta_1(x)/\dots/\delta_r(x) \neq 0$, $\text{gr}(\delta_1(x)) \geq 1$.

$\delta_r(x)$ es el anulador minimal de todo M , i.e $(\forall v \in V) \delta_r(x)v = \delta_r(T)v = 0$ ($\delta(T) = 0$). Además, cualquier polinomio $p(x)$ tal que $p(T) = 0$, satisface $(\forall v \in V) p(x)v = 0$ i.e $p(x)$ anula todo $M \Rightarrow \delta_r(x)/p(x)$.

Así, $\delta_r(x)$ es el polinomio mínimo $m(x)$ de la transformación lineal T .

Además, el e.v V se descompone como $V = V_1 \oplus \dots \oplus V_r$, con $T(V_i) \subseteq V_i$ y V_i tiene una base tal que la matriz representante de T en ella es $C_{\delta(x)}$, de esta forma, $V = M$ tiene una base (como e.v sobre K) en la que la matriz representante de T es



$\delta_1(x), \dots, \delta_r(x)$ son los factores invariantes del $K[x]$ - módulo M .

Recordando que todo par (V, T) , con V e.v sobre K de dimensión finita , $T : V \rightarrow V$ lineal , es un $K[x]$ -módulo de torsión finitamente generado , concluimos lo siguiente :

Módulos finitamente generados de torsión sobre $K[x]$ ssi e.v de dimensión finita sobre K con una transformación lineal en sí mismo .

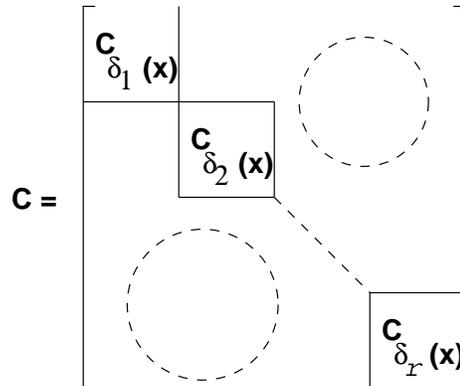
Aplicación a Matrices de $n \times n$ a coeficientes en un Cuerpo

Sea $A \in M_{nn}(K)$. A define una transformación K - lineal

$$T_A : K^n \longrightarrow K^n$$

$$x \longrightarrow Ax$$

(K^n, T_A) produce un $K[x]$ - módulo finitamente generado y de torsión $\Rightarrow \exists!$ lista de polinomios mónicos $\delta_1(x)/\dots/\delta_r(x) \neq 0$ ($\text{gr}(\delta_1(x)) \geq 1$) y una base de K^n , tal que la matriz representante de T_A con respecto a esta base es



“Forma canónica racional de A ”

Además, $\delta_r(x)$ es el polinomio mínimo de A . A es similar a C , pues ambas representan la misma transformación lineal.

Usando que el polinomio característico de $C_{\delta(x)}$ es $(-1)^{\text{gr}(\delta(x))}\delta(x)$ y que el polinomio característico de una matriz de la forma

$$\left[\begin{array}{c|c|c} \mathbf{A}_1 & & \\ \hline & \mathbf{A}_2 & \\ \hline & & \text{---} \end{array} \right] = \text{Polcar}(\mathbf{A}_1)\text{Polcar}(\mathbf{A}_2)\cdots\text{Polcar}(\mathbf{A}_r)$$

es $p_{A_1}p_{A_2}\cdots p_{A_r}$ donde p_{A_i} es el polinomio característico de A_i $1 \leq i \leq r$, y que el polinomio característico de matrices similares es el mismo, resulta:

Corolario 1

Si $A \in M_{nn}(\mathbb{K})$, su polinomio característico es $p_A(x) = (-1)^n \delta_1(x) \cdots \delta_r(x)$. (Salvo signos, $p_A(x)$ es el producto de los factores invariantes de A).

Corolario 2

Si $A \in M_{nn}(\mathbb{K})$ y $m(x)$ es su polinomio minimal, entonces $m(x)/p_A(x)$ (pues $m(x) = \delta_r(x)$).

Corolario 3 (Teorema de Cauchy-Hamilton)

Si $A \in M_{nn}(\mathbb{K})$ y $p_A(x)$ su polinomio característico, entonces $p_A(A) = 0$.

Aplicación de la descomposición primaria de R - módulos finitamente generados de torsión

Sea R un dip y M un R - módulo finitamente generado de torsión $\Rightarrow M \cong \bigoplus_{i=1}^l R/(p_i^{\alpha_{i,1}}) \oplus \cdots \oplus R/(p_i^{\alpha_{i,k_i}})$ (suma finita).

Tomemos $R = \mathbb{K}[x]$ y $p(x) = x - \lambda$, polinomio primo en $\mathbb{K}[x]$ (generalmente hay más polinomios primos). Estudiemos $\mathbb{K}[x]/(p(x)^k)$:

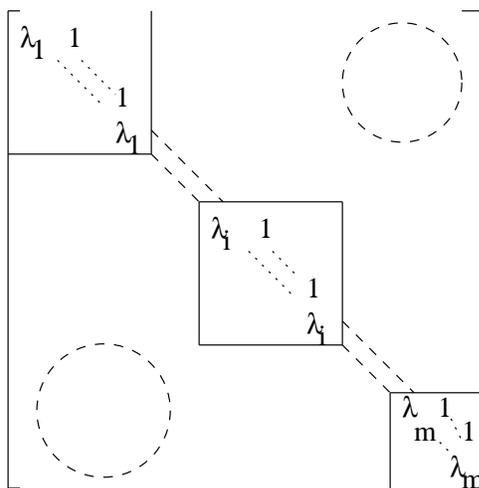
“Bloque de Jordan”

$\{w_1, \dots, w_k\}$ es una base de V por que tiene el número correcto de elementos , y $\dim V = \text{gr}((x - \lambda)^k) = k$ y además es l.i

$\alpha_1(T - \lambda id)^{k-1}v_o + \dots + \alpha_kv_o = 0$, multiplicando por $(T - \lambda id)^{k-1} \Rightarrow \alpha_k = 0$.

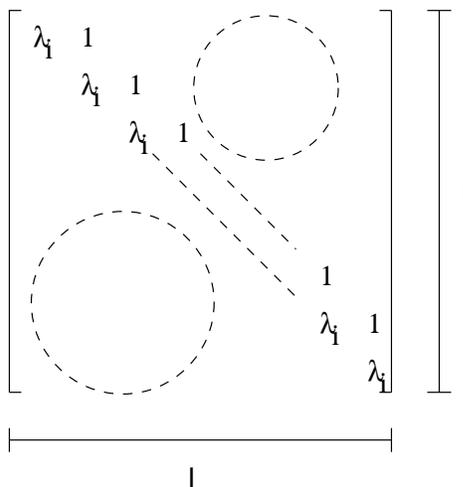
(REVISAR)

Si en $K[x]$ los únicos polinomios primos mónicos son de la forma $x - \lambda$ (por ejemplo $K = \mathbb{C}$) , entonces \forall e.v V de dimensión finita sobre K y $\forall T : V \rightarrow V$ lineal , existe una base B de V tal que la matriz representante de T con respecto a esta base , es de la forma



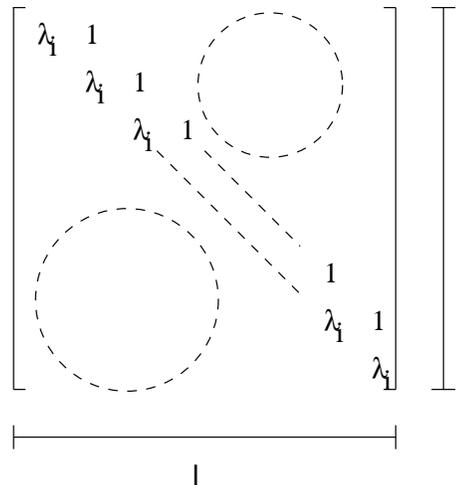
“Forma canónica de Jordan de T ”

$\lambda_1, \dots, \lambda_m$ son los valores propios de T , y los bloques



(en número y tamaño) para cada λ_i están únicamente determinados .

El bloque

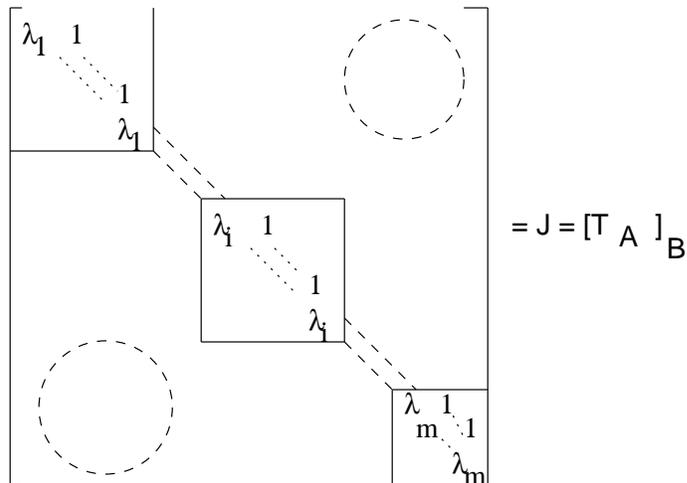


proviene de una parte $\{w_1, \dots, w_l\}$ de la base B (correspondiente al sumando cíclico primario $K[x]/((x - \lambda)^l)$ del módulo (V, T)), que es tal que w_1 es vector propio de $T : Tw_1 = \lambda_i w_1$ (con valor propio asociado λ_i) y w_2, \dots, w_l son vectores propios generados de T , “colas” de w_1 que satisfacen

$$\begin{aligned} Tw_2 &= \lambda_i w_2 + w_1 \\ Tw_3 &= \lambda_i w_3 + w_2 \\ \vdots & \quad \vdots \quad \vdots \quad \vdots \\ Tw_l &= \lambda_i w_l + w_{l-1} \end{aligned}$$

(Esta base viene de un generador w_o en $K[x]/((x - \lambda)^l)$ tal que $(x - \lambda)^l w_o = 0 \rightarrow w_i = (x - \lambda)^{l-i} w_o$ y $(x - \lambda_i)^l w_i = 0 \ i = 1 \dots l$ ($(T - \lambda_i id)^l w_i = 0$)

Si $V = K^n$, $A \in M_{nn}(K)$, $T = T_A : K^n \rightarrow K^n$ con $T_A(x) = Ax$



tal que $PAP^{-1} = J$

Así, A es diagonalizable ssi todos los bloques de Jordan son de $1 \times 1 \Leftrightarrow$ todos los divisores elementales del $K[x]$ - módulo (K^n, T_A) son del tipo $(x - \lambda_i)^1$.

Pregunta: ¿Qué matriz en $K[x]$ hay que “diagonalizar” para obtener los factores invariantes $\delta_1(x), \dots, \delta_r(x)$, en el caso de un $K[x]$ módulo finitamente generado y de torsión (i.e (V, T) , V e.v sobre K de dimensión finita y $T : V \rightarrow V$ lineal) ?

Sea $B = \{v_1, \dots, v_n\}$ base de V (como e.v sobre K) $\Rightarrow \{v_1, \dots, v_n\}$ genera V como $K[x]$ - módulo (pero ya no es l.i). Podemos escribir V como cuociente de un $K[x]$ - módulo libre .

Sea F un $K[x]$ - módulo libre con base $\{b_1, \dots, b_n\}$ ($F \cong K[x]^n$).

Sea φ el único epimorfismo (de $K[x]$ -módulos) de F en V ($= M$) tal que $\varphi(b_i) = v_i \forall i \in \{1, \dots, n\}$. $\varphi : F \rightarrow V$ epimorfismo $\Rightarrow V \cong F/\text{Ker}\varphi$. Estudiemos más en detalle $\text{Ker}\varphi$:

$xv_j = T(v_j) = \sum_{i=1}^n a_{ij}v_i$, donde a_{ij} es el elemento ij de la matriz A de la transformación lineal T en la base B .

$xv_j - \sum_{i=1}^n a_{ij}v_i = 0$ Fórmula en V .

En F : Sea $c_j = xb_j - \sum_{i=1}^n a_{ij}b_i \in F$

$\varphi(c_j) = \varphi(xb_j - \sum_{i=1}^n a_{ij}b_i) = x\varphi(b_j) - \sum_{i=1}^n a_{ij}\varphi(b_i) = xv_j - \sum_{i=1}^n a_{ij}v_i = 0$, por lo tanto, $c_j \in \text{Ker}\varphi$.

Probemos algo mejor : $\text{Ker}\varphi = \langle \{c_1, \dots, c_n\} \rangle$

Sea $L = \langle \{c_1, \dots, c_n\} \rangle$, sabemos que $L \subseteq \text{Ker}\varphi \subseteq F = \langle \{v_1, \dots, v_n\} \rangle$

¿ xb_j módulo L ?

$$[xb_j]_L = [\sum_{i=1}^n a_{ij}b_i]$$

$[x^2b_j]_L = [xxb_j] = x[xb_j] = x[\sum_{i=1}^n a_{ij}b_i] = [\sum_{i=1}^n \lambda_i b_i]$ $\lambda_i \in K$. Inductivamente $x^k b_j \equiv_L \sum_{i=1}^n \lambda_i b_i$ $\lambda_i \in K$, por lo tanto, $\forall p(x) \in K[x]$, $p(x)b_j \equiv_L \sum_{i=1}^n \lambda_i b_i$. así, $\forall z \in F$ $z \equiv_L \sum_{i=1}^n \lambda_i b_i$ $\lambda_i \in K$

En particular, si $z \in \text{Ker}\varphi$:

$$z \equiv_L \sum_{i=1}^n \lambda_i b_i \quad \lambda_i \in K$$

↓

$$0 = \sum_{i=1}^n \lambda_i \varphi(b_i) \Rightarrow 0 = \sum_{i=1}^n \lambda_i v_i \Rightarrow \lambda_1 = \dots = \lambda_n = 0, \text{ es decir,}$$

$$z \in \text{Ker}\varphi \Rightarrow z \equiv_L 0, z \in L.$$

En resumen :

$\varphi : F \rightarrow V$ epimorfismo de $K[x]$ -módulos, $F/\text{Ker}\varphi \cong V$ como $K[x]$ -módulos. $\text{Ker}\varphi = \langle \{c_1, \dots, c_n\} \rangle$.

Sea F' módulo libre de rango n , de base $\{b'_1, \dots, b'_n\}$ y $f : F' \rightarrow F$ la única transformación $K[x]$ - lineal que a b'_i le asigna $f(b'_i) = c_i \forall i \in \{1, \dots, n\}$. Resulta $\text{Im}f = \langle \{c_1, \dots, c_n\} \rangle =$

$\text{Ker}\varphi$, $V \cong F/\text{Im}f$ como $K[x]$ -módulos. Por lo tanto, la matriz a “diagonalizar” para calcular los factores invariantes de V (como $K[x]$ -módulo) es $[f]_{B'B}$

$$\text{columna 1 de esta matriz : } [f(b'_1)]_B = [c_1]_B = [xb_1 - \sum_{i=1}^n a_{i1}b_i]_B = \begin{pmatrix} x - a_{11} \\ -a_{21} \\ \vdots \\ -a_{n1} \end{pmatrix}$$

$$\text{Columna } j : [f(b'_j)]_B = [c_j]_B = [xb_j - \sum_{i=1}^n a_{ij}b_i]_B = \begin{pmatrix} -a_{1j} \\ -a_{2j} \\ \vdots \\ x - a_{jj} \\ \vdots \\ -a_{nj} \end{pmatrix}, \text{ por lo tanto, la matriz}$$

es $xI_n - A$.

Prop

Los factores invariantes de $T : V \rightarrow V$ son los únicos polinomios mónicos $\delta_1(x)/\cdots/\delta_r(x)$ con $\text{gr}(\delta_1(x)) \geq 1$, tal que al “diagonalizar” $xI_n - A$ resulta .

$$\left[\begin{array}{ccc} \delta_1(x) & & \\ & \text{---} & \\ & & \delta_r(x) \\ & & & 0 \\ & & & & 0 \end{array} \right]$$

Ejercicio:

Sea R un dip, $n \in \mathbb{N} \setminus \{0\}$. Miremos los elementos del R -módulo libre R^n como columnas

$$r = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}. \text{ Sean } m_1, \dots, m_n \in R^n \text{ y formemos la matriz } A = [m_1 | \cdots | m_n] \in M_{nn}(R).$$

Sea $\Delta = \det(A)$. Las siguientes proposiciones son equivalentes:

1. El submódulo $M = \langle \{m_1, \dots, m_n\} \rangle \subseteq R^n$ es libre

2. $\{m_1, \dots, m_n\}$ es l.i
3. $\Delta \neq 0$
4. R^n/M es de torsión , finitamente generado . Además :
 - (a) Si $R = \mathbb{Z}$, R^n/M es de torsión finitamente generado $\Leftrightarrow R^n/M$ es finito (grupo abeliano finito) y en este caso $|R^n/M| = |\Delta|$
 - (b) Si $R = K[x]$, K cuerpo , R^n/M es de torsión , finitamente generado $\Leftrightarrow K[x]^n/M$ es de dimensión finita como e.v sobre K , y en este caso , $\text{gr}(\Delta) = \dim_K V$.

Capítulo 3

Teoría de Cuerpos

3.1 Algo más sobre Polinomios

Sean R un anillo conmutativo y $\mathcal{X} = \{x_\lambda\}_{\lambda \in \Lambda}$, con $\Lambda \neq \emptyset$, una familia de elementos que llamaremos “indeterminadas”.

Queremos definir polinomios a coeficientes en el anillo R con variables $x_\lambda : \lambda \in \Lambda$, con el fin de dar sentido a expresiones del tipo $2x_1^2x_2 - 3x_5x_3^3x_4 + x_5 - 7$.

Para formalizar esto (y las operaciones $+$ y \cdot que esperaríamos que existan entre polinomios) definiremos lo siguiente :

Sea $\alpha : \Lambda \longrightarrow \mathbb{N}$ una función tal que $\forall \lambda \in \Lambda$, salvo un número finito de ellos ,
 $\lambda \longrightarrow \alpha(\lambda) = \alpha_\lambda$

$\alpha_\lambda = 0$. Sea \mathcal{F} el conjunto de estas funciones α .

La suma queda bien definida en \mathcal{F} :

Sean $\alpha, \beta \in \mathcal{F}$ $\alpha + \beta : \Lambda \longrightarrow \mathbb{N}$
 $\lambda \longrightarrow \alpha_\lambda + \beta_\lambda$

$+$ es asociativa, conmutativa y tiene neutro 0 . Todo α es cancelable para $+$.

A cada $\alpha \in \mathcal{F}$ le asociamos el monomio $x^\alpha = x_{\lambda_1}^{\alpha_{\lambda_1}} \cdots x_{\lambda_k}^{\alpha_{\lambda_k}}$ donde
 $\{\lambda_1, \dots, \lambda_k\} = \{\lambda \in \Lambda / \alpha_\lambda \neq 0\}$.

El conjunto de polinomios a coeficientes en R con indeterminada $\mathcal{X} = \{x_\lambda\}_{\lambda \in \Lambda}$ será
 $R[\mathcal{X}] = R[\{x_\lambda\}_{\lambda \in \Lambda}] = \bigoplus_{\alpha \in \mathcal{F}} R x^\alpha$. Notar que $(R[\mathcal{X}], +)$ es un R -módulo libre de base $\{x^\alpha\}_{\alpha \in \mathcal{F}}$.

Definimos ahora el producto en $R[\mathcal{X}]$ como sigue :

Para dos elementos de la base : $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$, y luego se extiende linealmente en cada factor :
 $(\sum_{i=1}^n r_i x^{\alpha_i})(\sum_{j=1}^m s_j x^{\beta_j}) = \sum_{\substack{i=1 \dots n \\ j=1 \dots m}} r_i s_j x^{\alpha_i + \beta_j}$

Ejercicio:

1. Probar que tenemos un producto bien definido en $\mathbb{R}[\mathcal{X}]$ y que $(\mathbb{R}[\mathcal{X}], +, \cdot)$ es un anillo conmutativo de neutro $x^o \equiv 1$.
2. La función $\varphi : \mathbb{R} \rightarrow \mathbb{R}[\mathcal{X}]$ tal que a r le asigna $\varphi(r) = rx^o$ es un monomorfismo de anillos, que permite identificar $r \in \mathbb{R}$ con $rx^o \in \mathbb{R}[\mathcal{X}]$.
3. Sean $\lambda \in \Lambda$ y $\alpha \in \mathcal{F}$ tal que

$$\alpha(\mu) = \begin{cases} 1 & \text{si } \mu = \lambda \\ 0 & \text{si } \mu \neq \lambda \end{cases}$$
 Llamando x_λ al elemento x^α , probar que $\forall \beta \in \mathcal{F}$, si $\{\lambda_1, \dots, \lambda_k\} = \{\lambda \in \Lambda / \beta_\lambda \neq 0\}$, entonces $x^\beta = x_{\lambda_1}^{\beta_{\lambda_1}} \cdots x_{\lambda_k}^{\beta_{\lambda_k}}$.
4. Si \mathbb{R} no tiene divisores del 0 $\Rightarrow \mathbb{R}[\mathcal{X}]$ no tiene divisores del 0.
5. $\mathbb{R}[\mathcal{X}]$ tiene la siguiente “propiedad universal”: Si S es un anillo cualquiera, y $\varphi : \mathbb{R} \rightarrow S$ es un homomorfismo de anillos y $\{s_\lambda\}_{\lambda \in \Lambda}$ es una familia de elementos en el anillo S que conmutan entre sí, Entonces $\exists!$ homomorfismo de anillos $\tilde{\varphi} : \mathbb{R}[\mathcal{X}] \rightarrow S$ tal que $\tilde{\varphi}(r) = \varphi(r) \forall r \in \mathbb{R}$, y $\tilde{\varphi}(x_\lambda) = s_\lambda \forall \lambda \in \Lambda$. En particular, si $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ es la identidad, esto significa que, seleccionando para cada incognita x_λ un valor $s_\lambda \in \mathbb{R}$, cada polinomio $\sum r_i x^{\alpha_i} \in \mathbb{R}[\mathcal{X}]$ da origen a su evaluación en la familia $\{s_\lambda\}_{\lambda \in \Lambda}$.
6. Interpretar todo esto en $\mathcal{X} = \{x\}$

3.2 Extensiones de Cuerpos

Sean K y k dos cuerpos. K se dice una extensión de k ($K|_k$) ssi k es subcuerpo de K .

K es un espacio vectorial sobre k , y su dimensión se anota $[K : k] = \dim_k K$. La extensión se dice finita si $[K : k] = \dim_k K$ es finita.

Definición

Sea $K|_k$ una extensión. Un elemento $\alpha \in K$ se dice **algebraico** sobre k ssi $\exists p(x) \in k[x] \setminus \{0\}$, tal que $p(\alpha) = 0$. La extensión $K|_k$ se dice **algebraica** ssi todo $a \in K$ es algebraico sobre k .

Ejemplo: $\mathbb{R}|_{\mathbb{Q}} : \sqrt[3]{2}$ es algebraico sobre \mathbb{Q} , pues $x^3 - 2 \in \mathbb{Q}[x]$ lo tiene como raíz.

Prop

Si la extensión $K|_k$ es finita, entonces es algebraica.

Dem.

Si $a \in K$, entonces $\{1, a, a^2, \dots\} \subseteq K$. Este conjunto no es l.i., pues al ser $\dim_k K < \infty$, cualquier conjunto l.i. será finito $\Rightarrow \exists \lambda_0, \dots, \lambda_n \in k$, no todos nulos, tal que $\lambda_0 1 + \lambda_1 a + \lambda_2 a^2 + \dots + \lambda_n a^n = 0$. Tomando $p(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n \in K[x] \setminus \{0\}$, se tiene $p(a) = 0 \Rightarrow a$ es algebraico.

Definición

Sean $K|_k$ una extensión de cuerpos y $A \subseteq K$. El “subcuerpo de K generado por A sobre k ” será el subcuerpo de K más pequeño que contiene a k y a A . Anotamos $k(A)$.

Este subcuerpo existe y es

$$k(A) = \left\{ \frac{p(a_1 \dots a_n)}{q(a_1 \dots a_n)} / n \in \mathbb{N}, p(x_1 \dots x_n), q(x_1 \dots x_n) \in k[x_1 \dots x_n], a_1 \dots a_n \in A, q(a_1 \dots a_n) \neq 0 \right\}$$

K se dice **finitamente generado** sobre k si A es finito.

Prop

Si $K|_k$ es una extensión finita, entonces K es finitamente generado como cuerpo sobre k .

Dem.

Si $\{v_1 \dots v_n\}$ es base de K como espacio vectorial sobre k , entonces $K = k(v_1, \dots, v_n)$.

Nota: La recíproca de esta propiedad no es cierta. Veamos un ejemplo:

Sean k un cuerpo cualquiera y $k(x)$ el cuerpo cociente de $k[x]$:

$$k(x) = \left\{ \frac{p(x)}{q(x)} / p(x), q(x) \in k[x], q(x) \neq 0 \right\}.$$

$k \subseteq k[x] \subseteq k(x)$, por lo tanto, $k(x)$ es una extensión finitamente generada (generada por x) sobre k y $[k(x) : k] = \infty$.

Polinomio mínimo de un elemento algebraico

Sean $K|_k$ y $a \in K$ algebraico sobre k . Sea $I = \{p(x) \in k[x] / p(a) = 0\}$

- $I \supset \{0\}$ (inclusión estricta), pues a es algebraico sobre k .
- I es un ideal en $k[x]$ (no degenerado, pues $1 \notin I$)

$k[x]$ es un dip, por lo tanto, $I = (m(x))$, con $m(x)$ único generador mónico de grado mínimo. $m(x)$ es primo, si no lo fuera:

$m(x) = p(x)q(x)$ con $\text{gr}(p(x))$ y $\text{gr}(q(x))$ ambos mayores o iguales que 1 y menores que $\text{gr}(m(x))$.

$I = (m(x)) \Rightarrow m(a) = p(a)q(a) = 0 \Rightarrow p(a) = 0 \vee q(a) = 0 \Rightarrow p(x) \in I \vee q(x) \in I$

$\Rightarrow \text{gr}(p(x)) \geq m(x) \vee \text{gr}(q(x)) \geq m(x) \rightarrow \leftarrow$

Por lo tanto, $\exists! m(x) \in k[x]$ primo, mónico y de grado mínimo tal que

$\{p(x) \in k[x] / p(a) = 0\} = m(x) \cdot k[x]$

$m(x)$ se llama “**polinomio mínimo**” o “**polinomio irreducible**” de a con respecto al cuerpo k

Notar que $I = \text{Ker } \varphi$, con φ el morfismo de anillos $\varphi : k[x] \rightarrow K$ tal que a $p(x) \in k[x]$ le asigna $\varphi(p(x)) = p(a)$. Así, la imagen de φ , que anotaremos $k[a]$ es un subanillo de K , y es isomorfo, como subanillo de K , a $k[x]/\text{Ker } \varphi$, de esta forma, $k[a] \cong k[x]/(m(x))$ ($p(a) \rightarrow [p(a)]$).

Notemos que, debido a que $m(x)$ es irreducible, el ideal $I = (m(x))$ es un ideal maximal. En efecto:

Si $J = (p(x))$, no degenerado, es tal que $(m(x)) \subset J$ (inclusión estricta), entonces $p(x)/m(x) \rightarrow \leftarrow$.

I ideal maximal $\Rightarrow k[x]/(m(x))$ cuerpo $\Rightarrow k[a] = \{\lambda_0 + \lambda_1 a + \dots + \lambda_n a^n / n \in \mathbb{N}, \lambda_0 \dots \lambda_n \in k\}$ es un cuerpo, y es el subcuerpo de K generado por k y a . En efecto:

Es claro que $k[a] \subseteq k(a)$.

La otra inclusión es cierta, pues a y k están contenidos en $k[a]$.

Problema Relacionado

Sea k un cuerpo y $p(x) \in k[x]$ un polinomio primo.

¿Existe algún cuerpo K , extensión de k , tal que $p(x)$ tenga al menos una raíz $a \in K$?

Existe, y se construye de la siguiente manera:

Consideremos el ideal $I = (p(x)) \subseteq k[x]$. Este ideal es maximal (pues $p(x)$ es primo), por lo tanto, $E = k[x]/(p(x))$ es cuerpo.

Sea $\gamma : k \rightarrow E$
 $\alpha \rightarrow \gamma(\alpha) = [\alpha]$

γ es un morfismo de cuerpos, por lo tanto, es inyectivo (recordar que el único ideal de un cuerpo es $\{0\}$). Así, k se puede ver como subcuerpo de E (identificando $\alpha \in k$ con $[\alpha] \in E$).

En E hay una raíz para $p(x)$. En efecto:

$E = \{[f(x)] / f(x) \in k[x]\}$, pero si $f(x) = a_0 + a_1 x + \dots + a_n x^n$, entonces $[f(x)] = a_0 + a_1 [x] + \dots + a_n [x]^n \Rightarrow E = \{f([x]) / f(x) \in k[x]\}$.

$[f(x)] = f([x]) = 0 \Leftrightarrow f(x)$ es un múltiplo de $p(x)$, por lo tanto $p([x]) = 0$. De esta forma, concluimos que $[x] \in E$ es raíz de $p(x)$.

Ejemplo:

$k = \mathbb{R}$, $p(x) = x^2 + 1$, polinomio primo en $\mathbb{R}[x]$. $E = \mathbb{R}[x]/(x^2 + 1)$.

Sea $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{R}[x] \Rightarrow [f(x)] = a_0 + a_1[x] + \dots + a_n[x]^n$.

Sabemos que $[x^2 + 1] = 0 = [x]^2 + 1, \Rightarrow [x]^2 = -1$, por lo tanto, $\forall [f(x)] \in E, [f(x)] = a_1 + b[x]$. Así como e.v sobre \mathbb{R} , $E = \langle \{1, [x]\} \rangle$.

$\{1, [x]\}$ son l.i :

Si $\lambda_0 + \lambda_1[x] = 0$ en $E \Rightarrow [\lambda_0 + \lambda_1x] = 0 \Rightarrow \underbrace{\lambda_0 + \lambda_1x}_{\text{grado 1}} = q(x) \underbrace{(x^2 + 1)}_{\text{grado 2}} \Rightarrow \lambda_0 = \lambda_1 = 0$

E es un espacio vectorial de dimensión 2 sobre \mathbb{R} con base $\{1, [x]\}$.

¿Cómo es la multiplicación ?

$$(a + b[x])(c + d[x]) = ac + (ad + bc)[x] + bd[x]^2 = (ac - bd) + (ad + bc)[x]$$

E es isomorfo a los Complejos .

Volvamos al caso general : k un cuerpo y $p(x) \in k[x]$ un polinomio primo. Veamos que $E|_k$ es una extensión finita , con $[E : k] = \text{gr}(p(x))$:

Sea $p(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1} + x^m$ $a_i \in k, \forall i = 1 \dots m - 1$

$p([x]) = a_0 + a_1[x] + \dots + a_{m-1}[x]^{m-1} + [x]^m = 0 \Rightarrow [x]^m = \sum_{i=0}^{m-1} (-a_i)[x]^i$ Por inducción se tiene que $[x]^j = \langle \{1, [x], \dots, [x]^{m-1}\} \rangle \forall j \geq m$. Luego , como espacio vectorial sobre k , E está generado por $\{1, [x], \dots, [x]^{m-1}\}$. Además , esta es una familia l.i sobre k :

Si $\sum_{i=0}^{m-1} \lambda_i [x]^i = 0 \Rightarrow [\sum_{i=0}^{m-1} \lambda_i x^i] = 0 \Rightarrow \sum_{i=0}^{m-1} \lambda_i x^i \in (p(x))$, i.e $\sum_{i=0}^{m-1} \lambda_i x^i = q(x)p(x)$ $q(x) \in k[x]$, pero $\text{gr}(\sum_{i=0}^{m-1} \lambda_i x^i) \leq m - 1 < m = \text{gr}(p(x)) \Rightarrow q(x) = 0 \Rightarrow \sum_{i=0}^{m-1} \lambda_i x^i = 0$ en $k[x] \Rightarrow \lambda_i = 0 \forall i = 0 \dots m - 1$.

El primer resultado era :

$K|_k$ una extensión , $a \in K$ algebraico sobre k , $m(x)$ primo en $k[x]$. K contiene un subcuerpo isomorfo a $k[x]/(m(x))$, donde $m(x)$ tiene a a como raíz , este subcuerpo es $k(a) = k[a] \cong k[x]/(m(x))$, de dimensión finita sobre k , con $[k(a) : k] = \text{gr}(m(x))$.

Así , dado un polinomio $p(x) \in k[x]$ primo , la **extensión minimal** de k en la que $p(x)$ tiene una raíz es $k[x]/(p(x))$.

Consecuencias:

Observación : Si $k \hookrightarrow K \hookrightarrow E$ (cadena de extensiones de cuerpos) , entonces $[E : k] = [K : k][E : K]$, sean finitos o infinitos los cardinales involucrados .

Dem. Si $\{e_\lambda : \lambda \in \Lambda\}$ es una base de E sobre K y $\{f_\mu : \mu \in \Gamma\}$ es una base de K sobre k , entonces $\{f_\mu \cdot e_\lambda : (\mu, \lambda) \in \Gamma \times \Lambda\}$ es una base de E como e.v sobre k . DE aquí:

$E|_k$ es extensión finita $\Leftrightarrow E|_K$ y $K|_k$ son extensiones finitas.

Corolario

Sean $K|_k$ una extensión y $a_1, \dots, a_n \in K$ algebraicos sobre k , entonces $k(a_1, \dots, a_n)|_k$ es una extensión algebraica.

Dem.

Consideremos la siguiente cadena de subcuerpos de K :

$$k = k_0 \hookrightarrow k(a_1) = k_1 \hookrightarrow \dots \hookrightarrow k(a_1 \dots a_n) = k_n . \text{ Notar que } k_{i+1} = k_i(a_{i+1})$$

a_{i+1} es algebraico sobre $k \Rightarrow$ es algebraico sobre $k_i \supseteq k$. Sea $m(x)$ el polinomio irreducible de a_{i+1} sobre k , $m(x) \in k_i[x] \supseteq k[x]$, sin embargo, $m(x)$ podría no ser el polinomio irreducible de a_{i+1} sobre el cuerpo k_i , así, $[k(a_{i+1}) : k_i] < \infty$, concluimos entonces que $k_n|_{k_0} = k(a_1 \dots a_n)|_k$ es una extensión finita, y por lo tanto, algebraica.

Observación: si tenemos la cadena de extensiones de cuerpos $k \hookrightarrow K \hookrightarrow E$ y $a \in E$ es algebraico sobre k , también lo es sobre K .

Corolario

Si $K|_k$ es una extensión con $K = k(a_\lambda : \lambda \in \Lambda)$ y a_λ es algebraico sobre k , $\forall \lambda \in \Lambda$, entonces $K|_k$ es una extensión algebraica.

Dem.

Si $a \in K = k(a_\lambda : \lambda \in \Lambda) \Rightarrow a = \frac{p(a_{\lambda_1} \dots a_{\lambda_n})}{q(a_{\lambda_1} \dots a_{\lambda_n})}$ con $p(x_1 \dots x_n), q(x_1 \dots x_n) \in k[x_1 \dots x_n]$, $q(a_{\lambda_1} \dots a_{\lambda_n}) \neq 0 \Rightarrow a \in k(a_{\lambda_1} \dots a_{\lambda_n}) \subseteq K$, y ya probamos que $k(a_{\lambda_1} \dots a_{\lambda_n})$ es extensión algebraica de k , por lo tanto, a es algebraico sobre k .

Ejercicio:

Dada una cadena de extensiones $k \hookrightarrow K \hookrightarrow E$, $E|_k$ es algebraica ssi $E|_k$ y $K|_k$ son algebraicas.

3.2.1 Cerradura algebraica**Definición**

Un cuerpo K se dice **algebraicamente cerrado** ssi todo polinomio $p(x) \in k[x]$ de grado ≥ 1 tiene raíces en K .

Ejemplo: el teorema fundamental del álgebra asegura que \mathbb{C} es algebraicamente cerrado.

Definición

Una extensión K de un cuerpo k se dice **cerradura algebraica** de k ssi :

1. La extensión $K|_k$ es algebraica.
2. K es algebraicamente cerrado.

Ejemplo: \mathbb{C} es cerradura algebraica de \mathbb{R} .

Ejercicio:

Sea k un cuerpo y $K \supseteq k$ una extensión algebraicamente cerrada . Probemos que existe $k \subseteq \bar{k} \subseteq K$ cerradura algebraica de k :

Sea $\bar{k} = \{a \in K/a \text{ es algebraico sobre } k\}$.Sabemos que :

- \bar{k} es un cuerpo
- $\bar{k}|_k$ es algebraico
- $k \subseteq \bar{k} \subseteq K$

Debemos probar que \bar{k} es algebraicamente cerrado : Sea $f(x) \in \bar{k}[x]$ de grado ≥ 1 .Sabemos que $f(x)$ tiene una raíz $a \in K$.

Sea $E = k(a_0 \dots a_n)$, donde $a_0 \dots a_n \in \bar{k}$ son tales que $f(x) = a_0 + a_1x + \dots + a_nx^n$. E es extensión finita y algebraica sobre k . $f(x) \in E[x]$, a es raíz de $f(x) \Rightarrow a$ es algebraico sobre E .

$k \hookrightarrow E$, $E \hookrightarrow E(a)$ son extensiones finitas $\Rightarrow k \hookrightarrow E(a)$ es extensión finita \Rightarrow es algebraica $\Rightarrow a$ es algebraico sobre $k \Rightarrow a \in \bar{k}$.

Ejercicio:

1. Si K es un cuerpo algebraicamente cerrado , y E es una extensión algebraica de $K \Rightarrow E = K$.
2. Si K es algebraicamente cerrado , todo polinomio $f(x) \in K[x]$ de grado ≥ 1 se descompone en $K[x]$ como $f(x) = a(x - c)$
3. Ningún cuerpo finito es algebraicamente cerrado

Apuntamos ahora a encontrarle una clausura algebraica a cualquier cuerpo k .

Lema

Si k es un cuerpo y $f_1(x) \dots f_n(x)$ son una cantidad finita de polinomios de grado ≥ 1 en $k[x]$, entonces existe una extensión algebraica finita $E|_k$ en la que cada uno de estos polinomios tiene al menos una raíz.

Dem.

Primero tomemos $p_1(x), \dots, p_n(x)$ primos en $k[x]$, con $p_i(x)/f_i(x)$. Extendamos k para que los $p_i(x)$ tengan raíces (y por lo tanto, los $f_i(x)$ también las tendrán).

Sabemos que podemos extender k a $E_1 \cong k[x]/(p_1(x))$ y resulta $E_1 = k(a_1)$, con a_1 raíz de $p_1(x)$ (y $[E_1 : k] = \text{gr}(p_1(x))$). $p_2(x) \in k[x] \subseteq E_1[x]$, pero podría no ser primo en $E_1[x]$. Sea $\tilde{p}_2(x)$ un factor primo de $p_2(x)$ en $E_1[x]$. Sabemos que E_1 se puede extender a $E_2 \cong E_1[x]/(\tilde{p}_2(x))$ y $E_2 = E_1(a_2)$, con a_2 raíz de $\tilde{p}_2(x)$, y por lo tanto, de $p_2(x)$. Así, $E_2 = k(a_1)(a_2) = k(a_1, a_2)$, y como $[E_2 : E_1] < \infty$, entonces $[E_2 : k] < \infty$.

Con el mismo argumento (inducción), extendemos E_2 , $E_3 = E_2(a_3)$, con a_3 raíz de $p_3(x)$ $\dots E_n = E_{n-1}(a_n) = k(a_1 \dots a_n)$ extensión finita de k con a_i raíz de $p_i(x)$.

Lema

Sea k un cuerpo. Existe una extensión algebraica E de k tal que todo polinomio $f(x) \in k[x]$ de grado ≥ 1 tiene al menos una raíz en E . Más aun, si $\{f_\lambda(x)\}_{\lambda \in \Lambda}$ es la familia de todos los polinomios de grado ≥ 1 a coeficientes en k , podemos pedir que $(\forall \lambda \in \Lambda)(\exists a_\lambda \in E)$ raíz de $f_\lambda(x)$ y $E = k(a_\lambda : \lambda \in \Lambda)$.

Dem.

Sea $\mathcal{X} = \{x_\lambda\}_{\lambda \in \Lambda}$. Trabajemos en el “gran” anillo de polinomios a coeficientes en k e indeterminadas en \mathcal{X} : $k[\mathcal{X}]$. Dentro de este anillo, sea I el ideal generado por los elementos de $\{f_\lambda(x)\}_{\lambda \in \Lambda}$, $I = (\{f_\lambda(x)\}_{\lambda \in \Lambda})$. (cosas como $f_1(x_1) + x_3x_4f_2(x_2)$ están en I).

Veamos que I es un ideal no degenerado :

Por contradicción, supongamos que $1 \in I$, i.e $1 = \sum_{i=1}^n g_i(\mathcal{X}) \cdot f_{\lambda_i}(x_{\lambda_i})$, con $g_i(\mathcal{X}) \in k[\mathcal{X}] \forall i = 1 \dots n$.

$f_{\lambda_1}(x_{\lambda_1}) \dots f_{\lambda_n}(x_{\lambda_n})$ son una cantidad finita de generadores. Extendamos k a un cuerpo K en el que $f_{\lambda_1}(x_{\lambda_1}) \dots f_{\lambda_n}(x_{\lambda_n})$ tengan raíces a_1, \dots, a_n respectivamente.

En $K[x] \supseteq k[x]$, $1 = \sum_{i=1}^n g_i(\mathcal{X}) \cdot f_{\lambda_i}(x_{\lambda_i})$ sigue siendo cierto.

Definamos ahora $a_\lambda = \begin{cases} a_i & \text{si } \lambda = \lambda_i \\ 0 & \text{si no} \end{cases}$ y evaluemos $1 = \sum_{i=1}^n g_i(\mathcal{X}) \cdot f_{\lambda_i}(x_{\lambda_i})$ en $x_\lambda = a_\lambda \forall \lambda \in \Lambda \Rightarrow 1 = \sum_{i=1}^n g_i(\mathcal{X}) \cdot f_{\lambda_i}(x_{\lambda_i}) = 0 \rightarrow \leftarrow$, por lo tanto, $1 \notin I$.

Como I es ideal no degenerado, hay algún ideal maximal $J \subset k[\mathcal{X}]$ que lo contiene. Llamemos $E = k[\mathcal{X}]/J$, cuerpo, pues J es maximal.

$$k \xrightarrow{i} k[\mathcal{X}] \xrightarrow{\nu} k[\mathcal{X}]/J = E$$

$\nu \circ i$ es morfismo de cuerpos \Rightarrow es inyectiva, por lo tanto, podemos pensar que $k \subseteq E$. Además, los elementos de E son de la forma $\sum \alpha_i [x_{\lambda_1}]^{e_1} \cdots [x_{\lambda_k}]^{e_k}$, $E = k[[x_\lambda] : \lambda \in \Lambda]$. E está generado a partir de k por $\{[x_\lambda] : \lambda \in \Lambda\}$ y además en $E : f_\lambda([x_\lambda]) = \underbrace{[f_\lambda(x_\lambda)]}_{\in I \subseteq J} = 0$.

Llamando $b_\lambda = [x_\lambda] \in E$, tenemos $E = k(b_\lambda : \lambda \in \Lambda)$, $f_\lambda(b_\lambda) = 0$.

Teorema

Todo cuerpo k tiene clausura algebraica.

Dem.

$E_0 = k$, E_1 la extensión de E_0 del lema anterior, En general, E_{n+1} es la extensión de E_n dada por el lema anterior. Tenemos: $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n \subseteq E_{n+1} \subseteq \cdots$

Sea $K = \bigcup_{n \in \mathbb{N}} E_n$, es cuerpo por ser unión creciente de cuerpos.

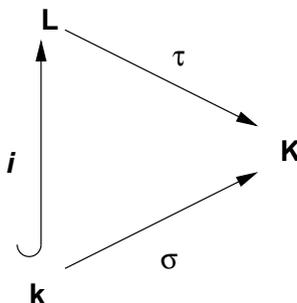
K es algebraico sobre k : Si $a \in K \Rightarrow \exists n \in \mathbb{N}$ tal que $a \in E_n$, pero E_n es algebraico sobre $k \Rightarrow K$ es algebraico sobre k .

K es algebraicamente cerrado: Sea $f(x) = a_0 + \cdots + a_n x^n \in K[x] \Rightarrow \exists m_0, \dots, m_n \in \mathbb{N}$ tales que a_0, \dots, a_n están en E_{m_0}, \dots, E_{m_n} respectivamente, Si E_m es el mayor (con respecto a la inclusión) de estos cuerpos, entonces $f(x) \in E_m[x] \Rightarrow$ tiene raíz en $E_{m+1} \subseteq K$.

3.2.2 Inmersiones

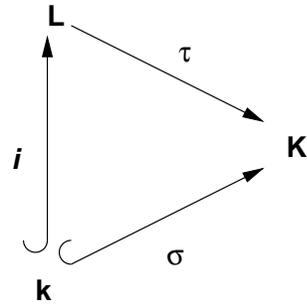
Si k y K son cuerpos, un morfismo de cuerpos $\sigma : k \rightarrow K$ se suele llamar una **inmersión** de k en K . Recordar que σ es necesariamente inyectivo.

Si ahora $L|_k$ es una extensión de cuerpos

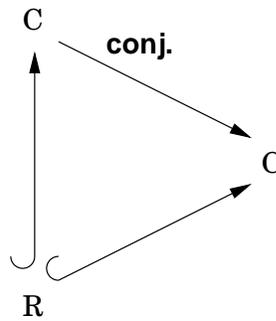


y $\tau : L \rightarrow K$ es una inmersión que extiende σ , se dice que “ τ va sobre σ ”.

Caso particular, si σ es una inclusión, se dice que “va sobre k ”.

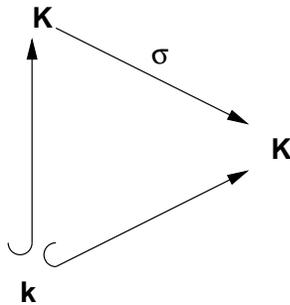


Ejemplo:



Lema

Sea $K|_k$ una extensión algebraica de cuerpos.



Sea σ una inmersión sobre k ($\sigma(x) = x \forall x \in k$), entonces $\sigma : K \rightarrow K$ es un automorfismo de cuerpos.

Dem.

Observación1: Si $\sigma : K \rightarrow K$ es una inmersión sobre k , entonces es una función lineal de K en K con escalares en k : $\sigma(x + y) = \sigma(x) + \sigma(y)$ y $\sigma(\lambda x) = \sigma(\lambda)\sigma(x)$, si $\lambda \in k$ $\sigma(\lambda) = \lambda$, por lo tanto, σ es k -lineal.

Observación2: Así, si $[K : k] < \infty$, este es el teorema de álgebra lineal: función lineal inyectiva de un e.v de dim n a otro de dim n es un isomorfismo.

Hay que probar la sobreyectividad de σ .

Sea $a \in K$ y $E = k(a)$, sabemos que, por ser a algebraico sobre k , $[E : k] = \text{grado del polinomio mínimo de } a \text{ en } k[x] < \infty$.

Probemos que $\sigma(E) \subseteq E$.

Sea $p(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1} + x^n \in k[x]$ el polinomio mínimo de $a \Rightarrow p(a) = b_0 + b_1a + \dots + b_{n-1}a^{n-1} + a^n = 0$. Si aplicamos σ a $p(a)$: $\sigma(p(a)) = 0 = b_0 + b_1\sigma(a) + \dots + b_{n-1}\sigma(a)^{n-1} + \sigma(a)^n \Rightarrow \sigma(a)$ es otra raíz de $p(x)$ en K .

Supongamos que a_1, \dots, a_r son las raíces de $p(x)$ en K . Tratemos de trabajar con $L = k(a_1, \dots, a_r)$, $\sigma(L) = k(\sigma(a_1), \dots, \sigma(a_r))$, por el argumento anterior, $\sigma(a_i)$ es raíz de $p(x)$ en $K \Rightarrow \sigma(L) \subseteq L$ (en realidad, es directamente igual). como $a_1 = a \in L \Rightarrow a = \sigma(a_j)$ algún j .

Un poco más de nomenclatura:

Sea $\sigma : k \rightarrow K$ un morfismo de cuerpos, y sea $p(x) = a_0 + a_1x + \dots + a_nx^n \in k[x]$. Anotamos por $p^\sigma(x)$ al polinomio de $K[x]$ dado por $p^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + \dots + \sigma(a_n)x^n$.

Tenemos un monomorfismo de anillos

$$\begin{array}{ccc} k[x] & \longrightarrow & K[x] \\ p(x) & \longrightarrow & p^\sigma(x) \end{array}$$

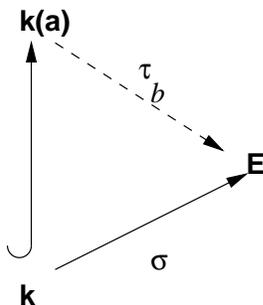
Además, $a \in k$ raíz de $p(x) \Rightarrow \sigma(a) \in K$ raíz de $p^\sigma(x)$.

Lema *

Sean $K|_k$ una extensión de cuerpos, $\sigma : k \rightarrow E$ una inmersión y $a \in K$ algebraico sobre k . Sea $p(x) \in k[x]$ el polinomio mínimo de a . Entonces, por cada raíz $b \in E$ del polinomio $p^\sigma(x) \in E[x]$, existe una única extensión $\tau : k(a) \rightarrow E$ de σ tal que $\tau(a) = b$. Llamemos τ_b a esta extensión. Además, toda extensión de σ a $\tau : k(a) \rightarrow E$ es de la forma τ_b , para algún b raíz de $p^\sigma(x)$ en E .

Dem.

Existencia de τ_b :



Sabemos que :

$$\begin{aligned} k(a) &\cong k[x]/(p(x)) \\ \lambda &\longleftarrow \lambda \in k \\ a &\longleftarrow [x] \end{aligned}$$

Consideremos la función :

$$\begin{aligned} \gamma: k[x] &\longrightarrow E \\ \lambda \in k &\longrightarrow \sigma(\lambda) \in E \quad \gamma(c_0 + c_1x + \cdots + c_nx^n) = \sigma(c_0) + \sigma(c_1)x + \cdots + \sigma(c_n)x^n . \\ x &\longrightarrow b \end{aligned}$$

(Es el único morfismo de anillos que extiende σ a todo $k[x]$ y que manda x en b).

$\gamma(p(x)) = p^\sigma(b) = 0$, por lo tanto , γ se anula en el ideal $(p(x)) \Rightarrow \gamma$ induce un morfismo

$$\begin{aligned} \tilde{\gamma}: k[x]/(p(x)) &\longrightarrow E \\ \lambda \in k &\longrightarrow \sigma(\lambda) \quad . \\ [x] &\longrightarrow b \end{aligned}$$

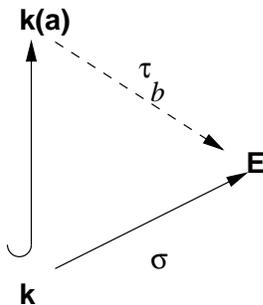
Tenemos entonces que :

$$\begin{array}{ccccc} k(a) & \xrightarrow{f} & k[x]/(p(x)) & \xrightarrow{\tilde{\gamma}} & E \\ \lambda \in k & \longrightarrow & \lambda \in k & \longrightarrow & \sigma(\lambda) \\ a & \longrightarrow & [x] & \longrightarrow & b \end{array}$$

$$\tau_b = \tilde{\gamma} \circ f \text{ es tal que } \begin{cases} \tau_b(\lambda) = \sigma(\lambda) & \text{si } \lambda \in k \\ \tau_b(a) = b \end{cases}$$

La unicidad de τ_b viene del hecho que $k(a)$ está generado por $k \cup \{a\}$ y τ_b está fijo en k y en a . El que todas las extensiones sean de esta forma es directo.

Revisemos la demostración del lema . Tenemos



Recordemos que en $k(a)$ los elementos son de la forma $y = \alpha_0 + \alpha_1 a + \dots + \alpha_n a^n$ con $\alpha_i \in k \forall i = 1 \dots n$ ($y = f(a)$, $f(x) \in k[x]$).

τ_b debiera satisfacer que $\tau_b(\alpha_0) + \tau_b(\alpha_1)\tau_b(a) + \dots + \tau_b(\alpha_n)\tau_b(a)^n = \sigma(\alpha_0) + \sigma(\alpha_1)b + \dots + \sigma(\alpha_n)b^n$. Pero y podría escribirse de varias maneras como polinomio evaluado en a . ¿Cómo garantizamos que $\sigma(\alpha_0) + \sigma(\alpha_1)b + \dots + \sigma(\alpha_n)b^n$ no depende del polinomio que usamos para escribir y ?

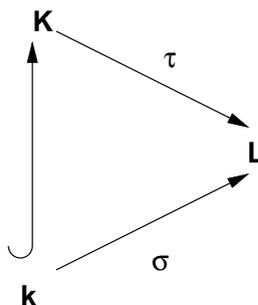
Para resolver este problema, recordemos que $k(a) \cong k[x]/(p(x))$ mediante $\alpha \in k \rightarrow \alpha$, $x \rightarrow [x]$. Definamos entonces:

$$\left. \begin{array}{l} k[x] \rightarrow L \\ \alpha \in k \rightarrow \sigma(\alpha) \\ x \rightarrow b \end{array} \right\} \text{único morfismo de anillos}$$

$q(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_n x^n \rightarrow \varphi(q(x)) = \sigma(\alpha_0) + \sigma(\alpha_1)b + \dots + \sigma(\alpha_n)b^n$ $\varphi(p(x)) = p^\sigma(b) = 0$
 : φ induce un único $\tilde{\varphi} : k[x]/(p(x)) \rightarrow L$ tal que $\alpha_0 + \alpha_1[x] + \dots + \alpha_n[x]^n \rightarrow \sigma(\alpha_0) + \sigma(\alpha_1)b + \dots + \sigma(\alpha_n)b^n$.

Corolario *

Sea $K|_k$ extensión algebraica y $\sigma : k \rightarrow L$ una inmersión de k en un cuerpo algebraicamente cerrado L . Entonces existen inmersiones $\tau : K \rightarrow L$ sobre σ .

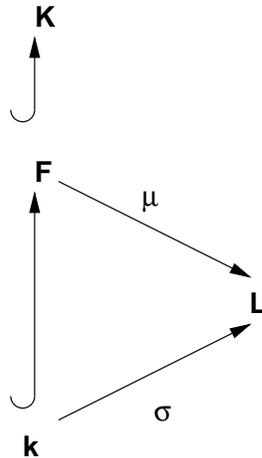


Si además, K es algebraicamente cerrado y L es algebraico sobre $\sigma(k)$, entonces cualquiera de tales τ es un isomorfismo.

Dem.

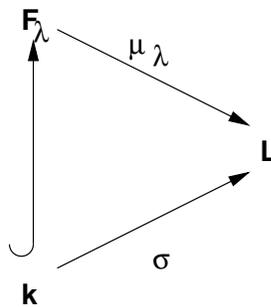
1) Existencia de extensiones $\tau : K \rightarrow L$:

Por Zorn, sea $A = \{\mu : J \rightarrow L/k \subseteq J \subseteq K, \mu|_k = \sigma\}$

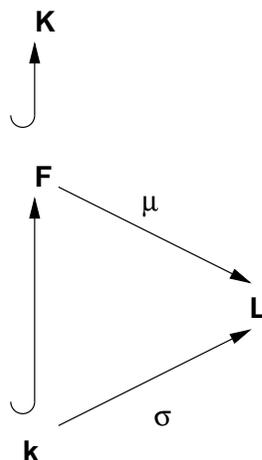


a) A es ordenado : $\mu_1, \mu_2 \in A$, $\mu_1 \preceq \mu_2 \Leftrightarrow \mu_2$ es extensión de μ_1

b) Si $\{\mu_\lambda\}_{\lambda \in \Lambda}$ es una cadena en A

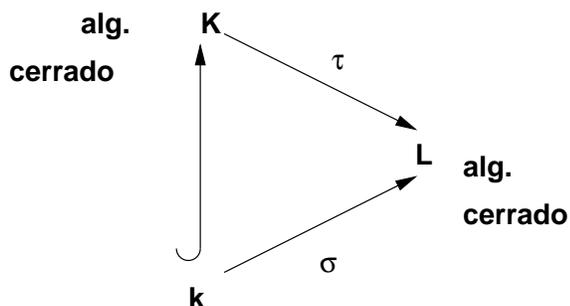


Sea $J = \bigcup_{\lambda \in \Lambda} J_\lambda$. J es un subcuerpo que contiene a k . Definamos $\mu : J \rightarrow L$
 $y \in J_\lambda \rightarrow \mu_\lambda(y)$
 μ está bien definida, y es morfismo de cuerpos sobre σ , por lo tanto, $\mu \in A$, y por definición, es cota superior de la familia $\{\mu_\lambda\}_{\lambda \in \Lambda} \Rightarrow$ Existe un elemento maximal



Si $J \subset K$ (estrictamente incluido), como K es algebraico sobre k , lo es sobre J . Tomando $a \in K \setminus J$, aplicamos el lema con $k = K$, $K = K(a)$ y podemos extender μ por τ a $K(a)$, lo que contradice que μ sea maximal.

2) Tenemos el siguiente diagrama



y queremos probar que τ es isomorfismo. Sólo resta probar que τ es sobreyectiva. Sea $K^\tau = \tau(K) \subseteq L$. k^σ es isomorfo a k y, por lo tanto, también algebraicamente cerrado, tenemos: $k^\sigma \hookrightarrow K^\tau \hookrightarrow L$, con $L|_{k^\sigma}$ algebraica

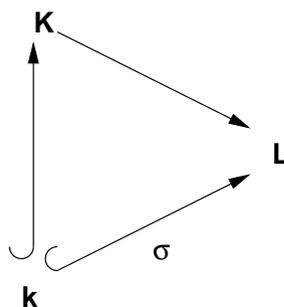
$\Rightarrow L|_{K^\tau}$ extensión algebraica $\Rightarrow L = K^\tau$.

Corolario

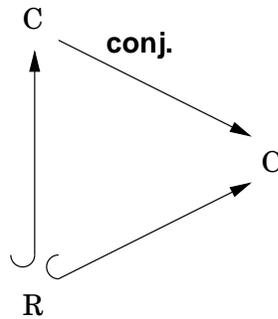
Si $K|_k$ y $L|_k$ son dos cerraduras algebraicas del mismo k , entonces existe un isomorfismo $\tau: K \rightarrow L$ sobre k .

Dem.

Usar el corolario anterior a



Ejemplo: \mathbb{C} es la cerradura algebraica de \mathbb{R} . (teorema fundamental del álgebra)



3.2.3 Cuerpos de descomposición

Definición

Si k es un cuerpo y $f(x) \in k[x]$ es un polinomio de grado ≥ 1 , un “ cuerpo de descomposición para $f(x)$ es una extensión K de k tal que:

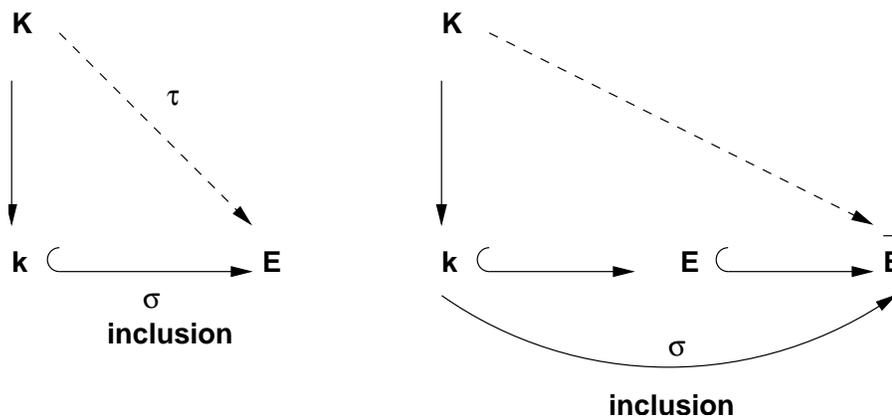
1. $f(x)$ tiene todas sus raíces en K . i.e $f(x)$ se descompone en factores lineales en $K[x]$: $f(x) = \lambda(x - c_1) \cdots (x - c_n)$ con c_1, \dots, c_n las raíces de $f(x)$.
2. K se genera a partir de k mediante las raíces de $f(x)$, i.e $K = k(c_1 \dots c_n)$.

Prop

Si $f(x)$ es de grado ≥ 1 en $k[x]$, entonces:

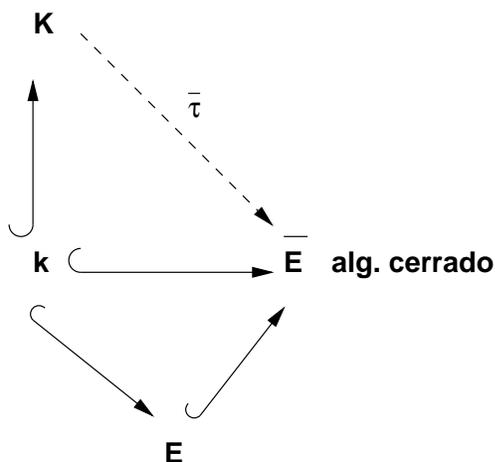
1. Existe un cuerpo de descomposición para $f(x)$.
2. Si $K|_k$ y $E|_k$ son dos cuerpos de descomposición de $f(x)$, entonces existen isomorfismos $\tau : K \rightarrow E$ sobre k (i.e $(\forall x \in k) \tau(x) = x$).

Dem.



Sea \bar{E} cerradura algebraica de E . Notar que \bar{E} , como \bar{E} es algebraico sobre E y E es algebraico sobre k , entonces \bar{E} es algebraico sobre k . Además \bar{E} es algebraicamente cerrado $\Rightarrow \bar{E}$ es cerradura algebraica de k .

Tenemos el siguiente diagrama :



Por un corolario anterior, la inclusión $\bar{\sigma} : k \rightarrow \bar{E}$ se puede extender a una inmersión $\bar{\tau} : K \rightarrow \bar{E}$ sobre k .

Debemos probar que $\bar{\tau}(K) = E$.

Como K y E son cuerpos de descomposición de $f(x) \in k[x]$, entonces, en $K[x] = k(c_1 \dots c_n)$ $f(x) = \lambda(x - c_1) \dots (x - c_n)$ y en $E[x] = k(c'_1 \dots c'_n)$ $f(x) = \lambda(x - c'_1) \dots (x - c'_n)$.

$$\begin{aligned} (\)^{\bar{\tau}} : K[x] &\longrightarrow \bar{E}[x] \text{ morfismo de anillos} \\ g(x) &\longrightarrow g^{\bar{\tau}}(x) \end{aligned}$$

Notar que $f(x) = f^{\bar{\tau}}(x)$

$f(x) = \lambda(x - c_1) \dots (x - c_n) \rightarrow f^{\bar{\tau}}(x) = \lambda(x - \bar{\tau}(c_1)) \dots (x - \bar{\tau}(c_n))$, Así, en \bar{E} , $f(x)$ se descompone en factores primos como $f(x) = \lambda(x - \bar{\tau}(c_1)) \dots (x - \bar{\tau}(c_n))$.

Como $E \subseteq \bar{E}$, $f(x)$ tiene dos descomposiciones en $\bar{E}[x]$:

- 1) $f(x) = \lambda(x - \bar{\tau}(c_1)) \dots (x - \bar{\tau}(c_n))$
- 2) $f(x) = \lambda(x - c'_1) \dots (x - c'_n)$

Por unicidad de descomposición en factores primos, en el dip $\bar{E}[x]$, estas dos descomposiciones son la misma, salvo tal vez el orden de los factores, por lo tanto, $\forall i = 1 \dots n \exists j = 1 \dots n$ tal que $\bar{\tau}(c_i) = c'_j$, $\bar{\tau}(\{c_1, \dots, c_n\}) = \{c'_1, \dots, c'_n\}$ Pero $K = k(c_1, \dots, c_n)$ y $E = k(c'_1, \dots, c'_n)$, por lo tanto, $\bar{\tau}(k) = k(\bar{\tau}(c_1), \dots, \bar{\tau}(c_n)) = k(c'_1, \dots, c'_n) = E$

Definición

Si $F = \{f_\lambda(x)\}_{\lambda \in \Lambda}$ es una familia cualquiera de polinomios de grado ≥ 1 en $k[x]$, un cuerpo de descomposición de la familia es una extensión $K|_k$ tal que

1. Cada $f_\lambda(x)$ de la familia se escribe como producto de factores lineales en K .
2. K está generado a partir de k por las raíces de todos los polinomios de la familia.

Nota:

- El cuerpo de descomposición de $f(x)$ es el de la familia $\{f(x)\}$
- El cuerpo de descomposición de la familia vacía es k .

Ejercicio:

1. F tiene cuerpo de descomposición
2. Si $K|_k$ y $E|_k$ son cuerpos de descomposición de la familia F , entonces son isomorfos sobre k . Más aun, si $\bar{\tau}: K \rightarrow \bar{E}$ es una inmersión de K en la clausura algebraica \bar{E} de E , sobre k , entonces $\bar{\tau}(K) = E$, y define un isomorfismo entre K y E sobre k .

3.3 Aplicación a cuerpos finitos

3.3.1 Definiciones Preliminares

Sea R un anillo conmutativo con unidad. ¿Cuál es el subanillo más pequeño que contiene R ?

En ese anillo deben estar $0, 1, 1+1, 1+1+1, \dots, n \cdot 1, \dots$. Sea $P = \{n \cdot 1/n \in \mathbb{Z}\}$, este el subanillo más pequeño en R . P se suele llamar el “**subanillo primo** de R ”

$(P, +)$ es un grupo cíclico generado por $\{1\}$, por lo tanto, es isomorfo a $(\mathbb{Z}_{|P|}, +)$ si es finito o $(\mathbb{Z}, +)$ si no lo es.

Si P es finito, $|P| = m$ es la primera vez que $\underbrace{1 + \dots + 1}_{m \text{ veces}} = 0$, en caso contrario, $1 + \dots + 1$ se anula.

Si $(P, +) \cong (\mathbb{Z}_m, +)$, el anillo R se dice de “**característica m** ”, si $(P, +) \cong (\mathbb{Z}, +)$, se dice de “**característica 0**”.

Notar que, en el caso de característica m , el isomorfismo

$$\begin{array}{l} P \longrightarrow \mathbb{Z}_m \\ n \cdot 1 \longrightarrow [n] \end{array} \text{ es morfismo de anillos.}$$

Nota:

$$\text{si } \underbrace{1 + \dots + 1}_{m \text{ veces}} = 0 \Rightarrow (\forall a \in R) \underbrace{a + \dots + a}_{m \text{ veces}} = a(\underbrace{1 + \dots + 1}_{m \text{ veces}}) = 0$$

Si R no tiene divisores del 0 (dominio de integridad) su característica es 0 o primo. En efecto :

Sabemos que si R no es finito, en cualquier caso, su característica es 0, por lo tanto, sólo basta probar la afirmación para R finito de característica m .

Supongamos que m no es primo (recordar que $\{1, 0\} \subseteq R$, por lo tanto, $m \geq 2$) $\Rightarrow \exists k \geq 2$, $l \leq m - 1$ tal que $m = k \cdot l$. Llamemos $a = k \cdot 1$ y $b = l \cdot 1$, ambos son distintos de 0, pues k y l son menores que m y la primera vez que una suma de “unos” se anula es con m . Pero $a \cdot b = (k \cdot l)1 = m1 = 0 \Rightarrow a$ y b son divisores del 0 $\rightarrow \leftarrow$.

Notar que en este caso, R de característica prima m , el subanillo primo $(P, +, \cdot)$ es un cuerpo (pues es isomorfo al cuerpo $(\mathbb{Z}_m, +, \cdot)$) llamado **subcuerpo primo**.

Observación:

En general, el anillo R es un módulo sobre cualquier subanillo, en particular sobre su subanillo primo, por lo tanto, si R es de característica prima, entonces R es un espacio vectorial sobre el subcuerpo primo.

Caso $R = k$, con k cuerpo

No tiene divisores del 0, por lo tanto, es de característica 0 o p prima.

1. Caso característica p prima: k será espacio vectorial sobre el subcuerpo primo $k_p \cong (\mathbb{Z}_p, +, \cdot)$. Así, k es una extensión de $k_p \cong \mathbb{Z}_p$. k será un e.v. vectorial de dimensión finita (no podría tener una base infinita) sobre k_p . Si $\dim_{k_p} k = n$, entonces $k \cong k_p^n \cong (\mathbb{Z}_p)^n$ como e.v.
2. Caso característica 0: El subanillo primo P es isomorfo a $(\mathbb{Z}, +, \cdot)$. Si tomamos los cocientes entre elementos de P , resulta un subcuerpo, el subcuerpo más pequeño en k , llamado subcuerpo primo de k (anotamos $k_{\mathbb{Q}}$), que es isomorfo a $(\mathbb{Q}, +, \cdot)$. k es una extensión de $k_{\mathbb{Q}}$ y, por lo tanto, un e.v. sobre $k_{\mathbb{Q}}$.

Teorema 1

Si k es un cuerpo finito, entonces $|k| = p^n$, donde $p = \text{car}(k)$ primo, y $1 \leq n \in \mathbb{N}$.

Para la demostración del siguiente teorema necesitaremos los siguientes resultados:

Lema

En característica p , $(a + b)^{p^i} = a^{p^i} + b^{p^i}$, $i \in \mathbb{N}$.

Dem.

$$(a + b)^p = \sum_{j=0}^p \binom{p}{j} a^j b^{p-j} = a^p + b^p + \underbrace{\sum_{0 < j < p} \binom{p}{j} a^j b^{p-j}}_0$$

Por inducción sobre i se concluye.

¿Cómo saber si un polinomio tiene raíces repetidas ?

Si $g(x) \in k[x]$ tiene a a como raíz repetida , entonces $(x - a)^m q(x) = g(x)$.

Cuando k es un cuerpo , definimos la derivada , como la única función k - lineal $D : k[x] \rightarrow k[x]$, tal que $D(x^n) = nx^{n-1}$ (ejercicio). Se prueba facilmente que si $f(x), g(x) \in k[x]$, entonces $D(f(x), g(x)) = D(f(x)) \cdot g(x) + f(x) \cdot D(g(x))$.

De lo anterior concluimos que a es raíz múltiple de $g(x) \in k[x] \Leftrightarrow a$ es raíz de $g(x)$ y $D(g(x))$

Teorema 2

$\forall p$ primo , $\forall n \geq 1$, hay cuerpo finitos F de p^n elementos.

Dem.

¿Dónde buscar F ?

Si F existe , deberá ser una extensión algebraica de \mathbb{Z}_p (F_p) , pues $\dim_{\mathbb{Z}_p} F = n$ finito (ext. finita \Rightarrow ext. algebraica).

Comencemos con $K = \overline{\mathbb{Z}_p}$, la cerradura algebraica de \mathbb{Z}_p (ext. algebraica más grande posible de \mathbb{Z}_p) . Llamemos $q = p^n$. Queremos buscar en $K = \overline{\mathbb{Z}_p}$ un subcuerpo de q elementos .

Para la búsqueda : Si F existiera , tomamos $G = (F \setminus \{0\}, \cdot)$ grupo multiplicativo con $q - 1$ elementos $\Rightarrow (\forall x \in G) x^{q-1} = 1 \Rightarrow x^q = x$. Tendríamos entonces : $(\forall x \in F) x^q = x$.

Sea ahora $f(x) = x^q - x \in \mathbb{Z}_p[x] \subseteq K[x]$.Sea F el cuerpo de descomposición de $x^q - x$ (se puede buscar dentro de K) . Mostremos que $F = \{\text{raíces de } x^q - x\}$

$\{\text{raíces de } x^q - x\}$ es cuerpo , en efecto :

Si $a, b \in \{\text{raíces de } x^q - x\}$

- $(a \cdot b)^q = a^q \cdot b^q = a \cdot b \Rightarrow a \cdot b \in \{\text{raíces de } x^q - x\}$
- Si $a \neq 0$, $(\frac{1}{a})^q = \frac{1}{a^q} = \frac{1}{a} \Rightarrow a$ tiene inverso en $\{\text{raíces de } x^q - x\}$
- $1^q = 1 \Rightarrow 1 \in \{\text{raíces de } x^q - x\}$
- $0^q = 0 \Rightarrow 0 \in \{\text{raíces de } x^q - x\}$
- Por el lema anterior $(a + b)^q = a^q + b^q = a + b \Rightarrow (a + b) \in \{\text{raíces de } x^q - x\}$
- $(-a)^q = (-1)^q a^q = (-1)^q a$.
 Si $p \geq 3$, $(-1)^q = -1 \Rightarrow (-a)^q = -a$.
 Si $p = 2$, $(-a)^q = a$, pero $a + a = 0 \Rightarrow a = -a \Rightarrow (-a)^q = -a$, por lo tanto $-a \in \{\text{raíces de } x^q - x\}$.

Así, $\{ \text{raíces de } x^q - x \}$ es cuerpo.

¿Cuántos elementos tiene ?

Lo ideal es que tenga q elementos, es decir, que sean q raíces distintas.

Para esto calculemos la derivada de $f(x) = x^q - x$: $Df(x) = qx^{q-1} - 1 = -1$, no tiene raíces, por lo tanto, $f(x)$ no tiene raíces repetidas.

Podemos concluir entonces que $F = \{ \text{raíces de } x^q - x \}$ es un cuerpo con $q = p^n$ elementos.

Teorema 3

Si p es primo y $n \geq 1$, entonces dos cuerpos cualquiera K y F con p^n elementos son isomorfos.

Dem.

Los elementos de F y de K satisfacen la ecuación $x^q - x = 0$. Pero $x^q - x \in \mathbb{Z}_p[x]$ tiene a lo más q raíces, y en F (y también en K) hay q raíces, por lo tanto, F (y también K) es cuerpo de descomposición de $x^q - x$ sobre \mathbb{Z}_p , por lo tanto, $F \cong K$.

Notación: Si $q = p^n$, se suele anotar como F_q al cuerpo finito con q elementos.

Teorema 4

1. Sea F un subcuerpo de F_q . Entonces $|F| = p^j$, con j/n
2. $\forall j/n, \exists!$ subcuerpo F de F_q con $r = p^j$ elementos.

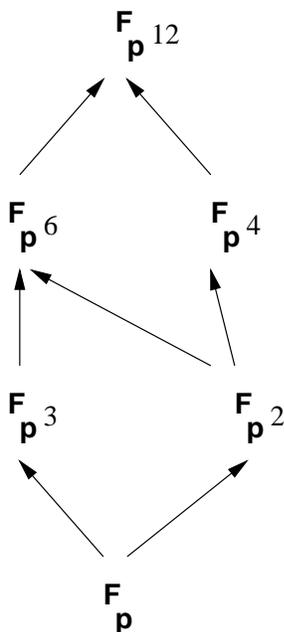
Dem.

La demostración queda de ejercicio, pero se pueden tomar en cuenta las siguientes indicaciones:

1. Si $k \hookrightarrow K \hookrightarrow E$, entonces $[E : k] = [E : K] \cdot [K : k]$.
2. Probar que $(r-1)/(q-1)$, además si G es grupo abeliano con $m = q-1$ elementos y l/m , entonces existe $H \subseteq G$ con l elementos.

Ejemplo:

Estructura de Subgrupos de F_{12}

**Ejercicio:**

Si k es un cuerpo cualquiera y $(G, \cdot) \subseteq (k^x, \cdot)$ es un subgrupo multiplicativo finito, entonces (G, \cdot) es cíclico.

Dem.

Como (G, \cdot) es finito, (G, \cdot) es cíclico ssi $(G, \cdot) \cong (\mathbb{Z}_n, +)$, con $n = |G|$.

Sea $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ la descomposición de n en producto de primos distintos entre sí.

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1} \cdots p_l^{\alpha_l}} \cong \underbrace{\mathbb{Z}_{p_1^{\alpha_1}}}_{T_{p_1}(\mathbb{Z}_n)} \oplus \cdots \oplus \underbrace{\mathbb{Z}_{p_l^{\alpha_l}}}_{T_{p_l}(\mathbb{Z}_n)}$$

Lo que haremos para la demostración es entonces tomar una componente primaria cualquiera $T_p(G) = \{a \in G/a^{p^j} = 1, \text{ algún } j\}$ de G , y probar que es cíclico.

Sea $H = T_p(G)$ una componente p -primaria, $H = \{x \in G/x^{p^j} = 1, \text{ algún } j\} = \{x \in G/O(\langle x \rangle) = p^j, \text{ algún } j\}$.

Si H fuera cíclico como queremos, entonces $H = \langle a \rangle$, $O(a) = p^l$. p^l será el máximo orden de elementos en H .

Sea $p^l = \text{Max}\{O(x)/x \in H\}$ y a un elemento de H de orden p^l . Claramente: $p^l = O(a) = |\langle a \rangle|/|H|$. Además, $(\forall x \in H) x^{p^l} = 1$, pues $O(x) = p^j \leq p^l$.

Recordar que H es subgrupo de (k^x, \cdot) . Así, los elementos de H son raíces en k del polinomio $x^{p^l} - 1$, y este polinomio no puede tener más de p^l raíces $\Rightarrow |H| \leq p^l$, por lo tanto, $|H| = p^l$, y como el subgrupo $\langle a \rangle \subseteq H$ tiene también p^l elementos $\Rightarrow \langle a \rangle = H$.

Ejercicio:

1. Sea $K|_k$ una extensión de cuerpos con $K = \bar{k}$ (cerradura algebraica de k). Sea $a \in K$, y sea $p(x)$ el polinomio mínimo de a en $k[x]$. Si r es la multiplicidad de $p(x)$ (i.e , en la descomposición de $p(x)$ en $K[x]$, $(x - a)$ aparece elevado a r), entonces , todas las raíces de $p(x)$ en K tienen multiplicidad r .
2. $\text{Car}(k) = 0 \Rightarrow r = 1$

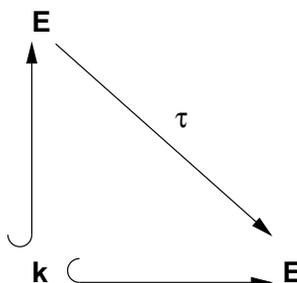
Dem.

1. $p(x) = (x - a_1)^{r_1} \cdots (x - a_l)^{r_l}$ en $K[x]$, con $a_1 \dots a_l$ las raíces de $p(x)$ en $K[x]$ de multiplicidades $r_1 \dots r_l$ respectivamente . Podemos tomar $a_1 = a$ y , por lo tanto , $r_1 = r$.

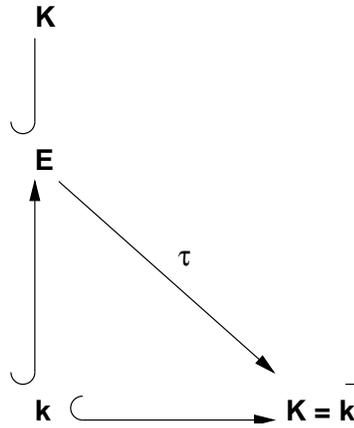
(Esta descomposición de $p(x)$ es válida también en $E = k(a_1 \dots a_l) \subseteq K$, el cuerpo de descomposición de $p(x)$).

Veamos que ocurre si existe una inmersión sobre k $\tau : E \rightarrow E$ tal que $\tau(a_1) = a_2$. Si tal cosa ocurriera , $p(x) = (x - a_1)^{r_1} \cdots (x - a_l)^{r_l} = p^\tau(x) = (x - \tau(a_1))^{r_1} \cdots (x - \tau(a_l))^{r_l} = (x - a_2)^{r_1} (x - \tau(a_2))^{r_2} \cdots (x - \tau(a_l))^{r_l}$, otra descomposición en factores lineales de $p(x)$ en $E[x] \Rightarrow$ debe ser la misma , salvo el orden de los factores , \Rightarrow el factor $(x - a_2)^{r_2}$ de la primera descomposición debe coincidir con el factor $(x - a_2)^{r_1}$ de la nueva descomposición $\Rightarrow r_1 = r_2$. Con esto , probaríamos 1. del ejercicio.

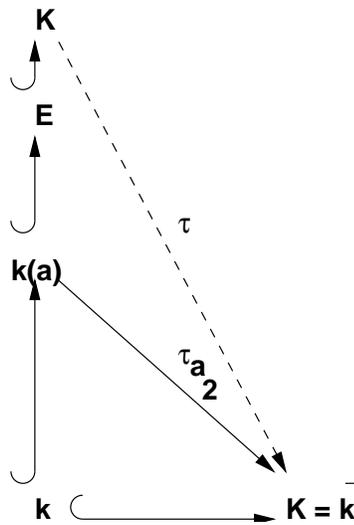
Buscamos



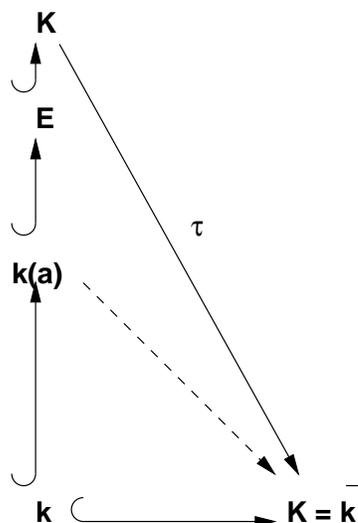
Nuestra situación es:



Primero, extendamos σ (inclusión) a $\tau_{a_2} : k(a) \rightarrow K$. Obtenemos:



usando el Corolario $*$, podemos extender la inmersión τ_{a_2} a toda la extensión algebraica E de $k(a)$. Llegamos a $\tau : E \rightarrow K$ extensión de τ_{a_2}



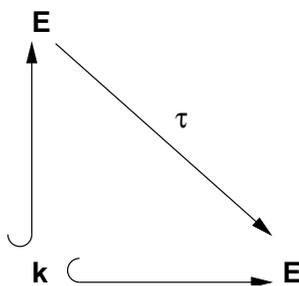
τ extiende la inclusión y además $\tau(a) = \tau(a_2)$. El único problema es como asegurar que $\tau(E) \subseteq E$.

$$E = k(a_1 \dots a_l) \Rightarrow \tau(E) = k(\tau(a_1) \dots \tau(a_l)) .$$

¿Qué valores tienen $\tau(a_1) \dots \tau(a_l)$?

$$p(x) = (x - a_1)^{r_1} \dots (x - a_l)^{r_l} , p(x) = p^\tau(x) = (x - \tau(a_1))^{r_1} \dots (x - \tau(a_l))^{r_l} \text{ en } K[x] \\ \Rightarrow \tau(a_1) \dots \tau(a_l) \text{ son las raíces de } p(x) \text{ en } K \Rightarrow \tau(E) = k(\tau(a_1) \dots \tau(a_l)) = k(a_1 \dots a_l) = E .$$

Así



Por lo tanto , $r_1 = r_2$ (del mismo modo , $r_1 = r_j \forall j = 1 \dots l$)

2. Hay que probar que en característica 0 , $r = 1$. Es decir , si $p(x) \in k[x]$ es irreducible de grado ≥ 1 , no tiene raíces repetidas.

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in k[x] \text{ irreducible}$$

$$Dp(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1 \in k[x] .$$

Si $a \in \bar{k}$ es raíz repetida de $p(x)$, entonces también es raíz de $Dp(x)$ $\rightarrow \leftarrow$ pues $\text{gr}(Dp(x)) < \text{gr}(p(x))$, lo que contradice que $p(x)$ sea el polinomio mínimo de a .

Ejemplo de un polinomio irreducible con raíces múltiples

Sea α un elemento no algebraico sobre $\mathbb{Z}_2 = \mathbb{F}_2$, y $k = \mathbb{Z}_2(\alpha)$ (Ejemplo: tomar $k = \mathbb{Z}_2(x) = \left\{ \frac{p(x)}{q(x)} / p(x), q(x) \in \mathbb{Z}_2[x], q(x) \neq 0 \right\}$ $\alpha = x$). Entonces α no tiene raíz cuadrada en k (es decir, x no se puede escribir como $\left(\frac{p(x)}{q(x)} \right)^2$ con $p(x), q(x) \in \mathbb{Z}_2[x]$).

Notar que: $\text{Car} k = 2$ (su subcuerpo primo es \mathbb{Z}_2) y tiene un elemento α sin raíz cuadrada. Tomemos el polinomio $p(x) = x^2 - \alpha \in k[x]$. $p(x)$ es irreducible.

Extendamos k a $E = k(b)$ con b raíz de $p(x)$.

$b^2 - \alpha = 0$ en $E \Rightarrow b^2 = \alpha \Rightarrow p(x) = x^2 - b^2$ en $E[x]$. Pero estamos en característica 2 $\Rightarrow p(x) = x^2 - b^2 = (x - b)^2 \Rightarrow b$ es una raíz doble de $p(x)$.

Observación:

Si $\text{Car} k = p$, la función $k \rightarrow k$ es un morfismo de cuerpos. $(y + z)^p = y^p + z^p$ es un morfismo aditivo inyectivo. Si además k es finito \Rightarrow es sobreyectivo.

En particular, si k es finito y $\text{Car} k = p \Rightarrow$ todo elemento de k tiene raíz p -ésima (y también p^j -ésima en k) en k .

Retomemos la teoría de extensiones de cuerpos:

Teorema

Las siguientes propiedades de una extensión algebraica $K|_k$ son equivalentes:

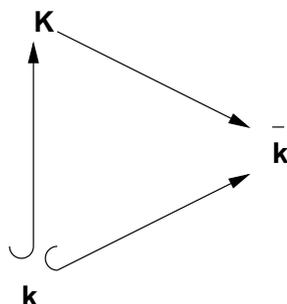
1. K es cuerpo de descomposición sobre k de una familia de polinomios irreducibles a coeficientes en k .
2. Todo polinomio irreducible $p(x) \in k[x]$ que tiene una raíz $a \in K$, se descompone completamente en factores lineales en $K[x]$.
3. Sea \bar{k} una cerradura algebraica de k que contiene a K (por ejemplo $\bar{k} = \bar{K}$), cualquier inmersión $\sigma : K \rightarrow \bar{k}$ sobre k es un automorfismo de K .

Dem.

2. \Rightarrow 1.

Sea \mathcal{F} la familia de todos los polinomios irreducibles $p(x) \in k[x]$ que tienen una raíz $a \in K$, 2. dice que cada polinomio de esta familia se descompone en factores lineales en $K[x]$. Sus raíces generan K sobre k pues todo $a \in K$ es raíz de algún polinomio irreducible en $k[x]$: su polinomio mínimo en $k[x]$.

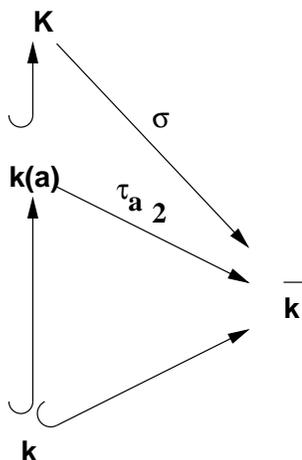
3. \Rightarrow 2.



Sea $p(x) \in k[x]$ irreducible con una raíz $a \in K$. Sabemos que en $\bar{k}[x]$, $p(x)$ se descompone en factores lineales : $p(x) = \lambda(x - a_1) \cdots (x - a_n)$.

Necesitamos probar que $a_1 \dots a_n$, las raíces de $p(x)$, están en $K \subseteq \bar{k}$.

Con un argumento ya usado antes, se puede extender la inclusión $k \hookrightarrow \bar{k}$ a un morfismo $\tau_{a_2} : k(a) \rightarrow \bar{k}$ tal que $\tau_{a_2}(a) = a_2$, y luego este, a un morfismo $\sigma : K \rightarrow \bar{k}$.



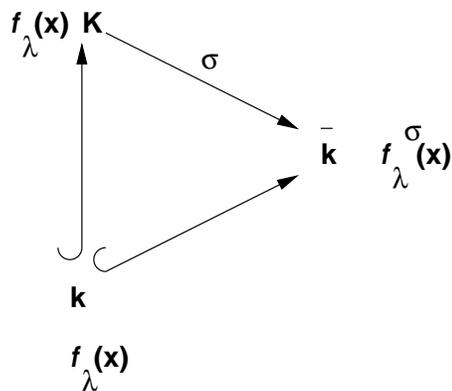
σ es una extensión de $\tau_{a_2} \Rightarrow \sigma(a) = \tau_{a_2}(a) = a_2$, pero 3. dice que $\sigma(K) = K$, por lo tanto $a_2 \in K$. (lo mismo para $a_3 \dots a_n$).

1.) \Rightarrow 3.)

K es cuerpo de descomposición de $\{f_\lambda(x)\}_{\lambda \in \Lambda}$, familia de polinomios irreducibles, entonces K se genera sobre k con las raíces de los f_λ .

Probemos entonces que si $a_1 \dots a_n$ son las raíces de uno de estos f_λ , entonces $\sigma(a_1) \dots \sigma(a_n) \in K$. $f_\lambda(x) = \mu(x - a_1) \cdots (x - a_n)$ en $K[x]$, $\mu \in k$.

Consideremos $K[x] \longrightarrow \bar{k}[x]$
 $p(x) \longrightarrow p^\sigma(x)$



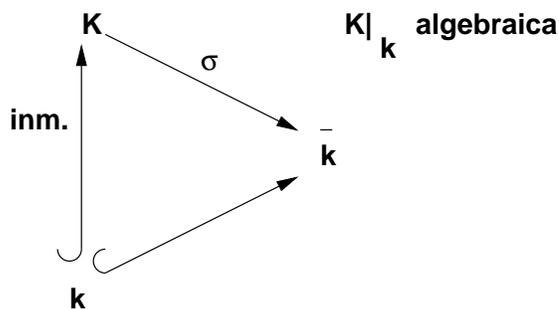
$$f_\lambda(x) = \mu(x - a_1) \cdots (x - a_n) \text{ en } K[x]$$

\Updownarrow

$$f_\lambda^\sigma(x) = \mu(x - \sigma(a_1)) \cdots (x - \sigma(a_n)) \text{ en } \bar{k}[x]$$

Tenemos dos descomposiciones del mismo polinomio en $\bar{k}[x] \Rightarrow$ son iguales , salvo orden $\Rightarrow \forall i, \exists j$ tal que $\sigma(a_i) = a_j \in K \Rightarrow \sigma(K) \subseteq K$.

Tenemos entonces el siguiente diagrama :



σ inmersión sobre k , $K|_k$ algebraica \Rightarrow por un ejercicio anterior , σ es automorfismo.

Definición

Una extensión algebraica con estas tres propiedades equivalentes , se dice **normal**.

Observación:

Recordemos las tres propiedades equivalentes que caracterizan a una extensión normal.

a) En la propiedad 1. , la familia de polinomios irreducibles puede tomarse como una familia de polinomios cualquiera , i.e , la frase “ polinomios irreducibles” puede ser reemplazada por “polinomios”.

b) En la propiedad 2. no se puede eliminar la palabra irreducible . Demos un ejemplo de ello :

Sean $a \in k$ y $q(x) \in k[x]$, tal que este último no tenga raíces en K . Sea $p(x) = (x - a)q(x)$, $p(x) \in k[x]$ (evidentemente no es irreducible), $p(x)$ tiene una raíz $a \in K$ y no se descompone en factores lineales en $k[x]$.

Ejemplo:

Toda extensión $K|_k$ de grado 2 (i.e $[K : k] = 2$) es normal .

Dem.

Sea $p(x) \in k[x]$ irreducible con alguna raíz $a \in K$.Supongamos que $a \notin k$. Consideremos su polinomio mínimo sobre k .

Afirmamos que $\text{gr}(p(x)) = 2$.

$$\underbrace{k \hookrightarrow k(a)}_{\text{grado del pol.min.}} \hookrightarrow K$$

$k(a) \cong k[x]/(p(x))$, además $k(a) = K$

$$[K : k] = \underbrace{[K : k(a)]}_1 [k(a) : k] \Rightarrow [k(a) : k] = 2 .$$

Ejemplo:

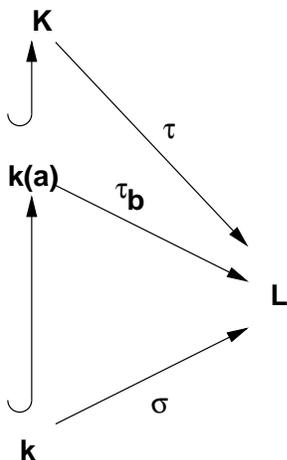
Ejemplo de una extensión que no es normal .

Consideremos $\mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q}(\sqrt[4]{2})$ como una extensión de \mathbb{Q} . Sea $p(x) = x^4 - 2 \in \mathbb{Q}[x]$, veamos que este polinomio es irreducible en $\mathbb{Q}[x]$.

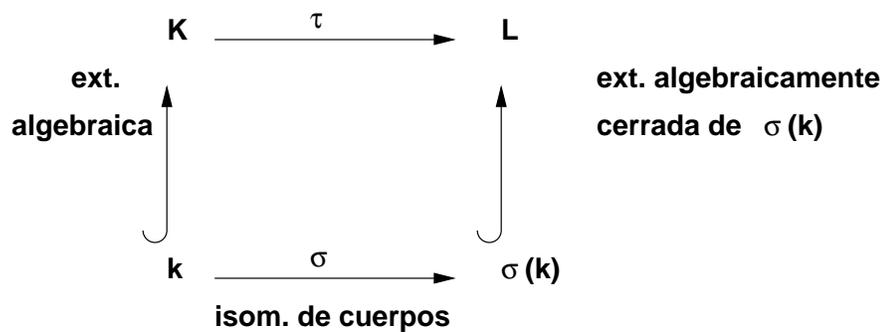
$p(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$ en $\mathbb{C}[x]$. Es fácil ver que ningún producto de estos cuatro factores (excepto de los cuatro juntos) está en $\mathbb{Q}[x] \Rightarrow p(x)$ es el polinomio mínimo de $\sqrt[4]{2}$ sobre \mathbb{Q} , sin embargo , $p(x)$ tiene una raíz $\sqrt[4]{2}$ en $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathbb{R}$, pero no las dos siguientes : $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$.

Notar que $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[4]{2}]$. Ambas extensiones en la cadena : $\mathbb{Q}(\sqrt{2})|_{\mathbb{Q}}$ y $\mathbb{Q}(\sqrt[4]{2})|_{\mathbb{Q}(\sqrt{2})}$ son de grado 2 , por lo tanto ,normales .Sin embargo , $\mathbb{Q}(\sqrt[4]{2})|_{\mathbb{Q}}$ no lo es .

Continuemos con el estudio de extensiones de inmersiones :



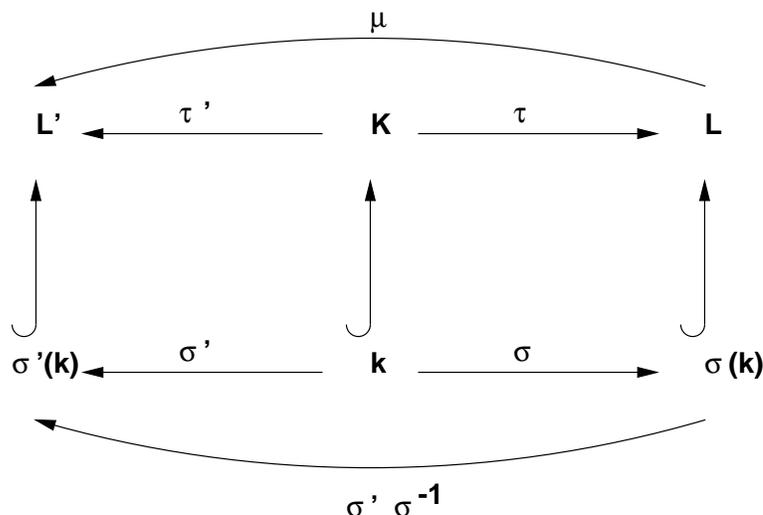
El mismo diagrama :



Notar que , dado que $K|_k$ es extensión algebraica , entonces $\tau(k)$ es extensión algebraica de $\tau(k) = \sigma(k)$, por lo tanto , $\tau(k) \subseteq$ “Clausura algebraica de $\sigma(k)$ dentro de L ” .

Así , L se puede reemplazar (y no se pierden ni se ganan extensiones τ de σ) por la clausura algebraica $\overline{\sigma(k)} \subseteq L$. Supondremos en lo que sigue que $L = \overline{\sigma(k)}$.

¿Qué sucede si tenemos dos situaciones como las anteriores ?



Por el corolario *, el isomorfismo $\sigma' \circ \sigma^{-1} : \sigma(k) \rightarrow \sigma'(k)$ se extiende a un isomorfismo $\mu : L' \rightarrow L$ (dado que L' , además de ser algebraicamente cerrado es algebraico sobre $\sigma'(k)$, y L , además de ser algebraico sobre $\sigma(k)$ es algebraicamente cerrado).

Si definimos los siguientes conjuntos :

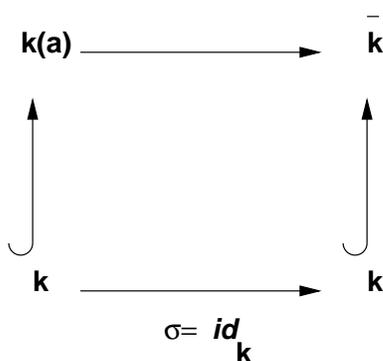
$$\text{Ext}(\sigma) = \{ \tau : K \rightarrow L/\tau \text{ es una inmersión extensión de } \sigma \}$$

$$\text{Ext}(\sigma') = \{ \tau : K \rightarrow L'/\tau \text{ es una inmersión extensión de } \sigma' \}$$

Se deduce entonces que la función $\varphi : \text{Ext}(\sigma) \rightarrow \text{Ext}(\sigma')$ es una biyección .

$$\tau \rightarrow \mu \circ \tau = \tau'$$

En un caso simple : $K = k(a)$, a algebraico sobre k . ¿Qué se puede decir sobre el número de extensiones de σ ?



Si $p(x)$ es el polinomio mínimo de a , del lema * , por cada raíz b de $p(x)$, hay una y sólo una extensión $\tau_b : k(a) \rightarrow \bar{k}$, y estas son todas las extensiones de σ que hay . Por lo tanto , σ tiene tantas extensiones como el número de raíces (distintas entre si) de $p(x)$. Sabemos que todas las raíces de $p(x)$ tienen multiplicidad r , por lo tanto , si las raíces distintas de $p(x)$ son $b_1 \dots b_l$, $p(x) = [(x - a_1) \cdots (x - a_n)]^r$, por lo tanto , $\text{gr}(p(x)) = r \cdot l = n \Rightarrow$ número de extensiones es $\leq n$.

Definición

Llamamos grado de separabilidad de la extensión $k(a)|_k$ al número de extensiones de σ . Anotamos $[k(a) : k]_s \leq [k(a) : k]$. Notar que $[k(a) : k]_s / [k(a) : k]$.

Esta definición se generaliza para cualquier extensión $K|_k$.

Prop

Sea $k \hookrightarrow K \hookrightarrow E$ una cadena de extensiones algebraicas. Entonces :

1. $[E : k]_s = [K : k]_s \cdot [E : K]_s$.
2. Si K es una extensión finita $[K : k]_s \leq [K : k]$.

Dem.

Probemos 2. a partir de 1.

K extensión finita $\Leftrightarrow K = k(a_1 \dots a_n)$ con $a_1 \dots a_n$ algebraicos sobre k .

Tenemos la siguiente cadena

$$k \hookrightarrow k(a_1) \hookrightarrow \dots \hookrightarrow k(a_1 \dots a_{n-1})(a_n) = K$$

En cada uno de estos pasos aplicamos que $[k(a) : k]_s / [k(a) : k]$. Obtenemos:

$$[k(a_1) : k]_s \leq_{\text{divisor de}} [k(a_1) : k]$$

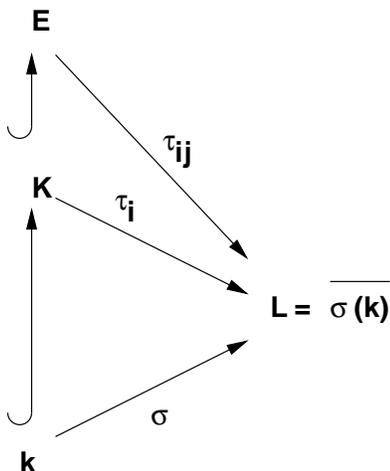
⋮

$$[k(a_1 \dots a_n) : k(a_1 \dots a_{n-1})]_s \leq_{\text{divisor de}} [k(a_1 \dots a_n) : k(a_1 \dots a_{n-1})]$$

multiplicando y usando 1.

$$[K : k]_s \leq_{\text{divisor de}} [K : k]$$

Demostremos 1.



Sea $\text{Ext}(\sigma) = \{\tau_i\}_{i \in I}$ la familia de todas las extensiones de σ a morfismos de K en L , $[K : k]_s = |\text{Ext}(\sigma)| = |I|$. Para cada $i \in I$, sea $\text{Ext}(\tau_i) = \{\tau_{ij}\}_{j \in J_i}$ la familia de extensiones de τ_i a inmersiones de E en L ($\forall i \in I$) $[E : K]_s = |\text{Ext}(\tau_i)| = |J_i|$. Entonces, llamando $\text{Ext}_E(\sigma)$ a la familia de todas las extensiones posibles de σ a un morfismo de E en L , resulta $\text{Ext}_E(\sigma) = \{\tau_{ij} : i \in I, j \in J_i\}$ y $|\text{Ext}_E(\sigma)| = [E : k]_s = \left| \prod_{i \in I} J_i \right| = \sum_{i \in I} |J_i| = |I| [E : K]_s = [K : k]_s [E : k]_s$

Definición

Una extensión finita $K|_k$ se dice **separable** ssi $[K : k]_s = [K : k]$.

- Si $E|_k$ es una extensión algebraica de k , un elemento $a \in E$ se dice separable sobre k ssi $k(a)|_k$ es una extensión separable (ssi el polinomio mínimo de a en $k[x]$ no tiene raíces repetidas).
- Un polinomio $f(x) \in k[x]$ se dice separable ssi $f(x)$ no tiene raíces repetidas en su cuerpo de descomposición.
- Si $K|_k$ es una extensión algebraica (finita o infinita), decimos que es separable si toda subextensión finita es separable (i.e , si \forall subcuerpo $k \subseteq F \subseteq K$, $F|_k$ es separable).

Propiedades simples

1. Si $k \hookrightarrow K \hookrightarrow E$ es una cadena de extensiones finitas, entonces $E|_k$ es separable $\Leftrightarrow E|_K$ y $K|_k$ son separables.
2. Si $k \hookrightarrow K \hookrightarrow E$ es una cadena de extensiones algebraicas, entonces, si $a \in E$ es separable sobre k , también lo es sobre K .

Dem.

Para demostrar 1., usar lo siguiente:

$$[E : k]_s = [E : K]_s \cdot [K : k]_s \quad [E : k] = [E : K] \cdot [K : k].$$

Demostremos 2. :

Si $p_k(x)$ es el polinomio mínimo de a en $k[x]$ y $p_K(x)$ es su polinomio mínimo en $K[x] \Rightarrow p_K(x)/p_k(x)$ en $K[x]$, por lo tanto, si $p_k(x)$ no tiene raíces repetidas, entonces $p_K(x)$ tampoco.

Prop

Una extensión algebraica $K|_k$ es separable ssi toda $a \in K$ es separable sobre k .

Dem.

\Rightarrow)

$k(a)$ es extensión finita sobre k , por lo tanto, por definición de $K|_k$ separable, debe ser separable.

\Leftarrow)

Sea $F|_k$ una subextensión finita de $K|_k$. Entonces $F = k(a_1 \dots a_n)$, con $a_1 \dots a_n \in K$. Tenemos la siguiente cadena:

$$k \hookrightarrow k(a_1) \hookrightarrow k(a_1, a_2) \hookrightarrow \dots \hookrightarrow F$$

Aplicando las dos propiedades anteriores se concluye.

Prop

1. Sea $K = k(a_\lambda : \lambda \in \Lambda)$ extensión de k por la familia $\{a_\lambda\}_{\lambda \in \Lambda}$ de elementos algebraicos. Entonces $K|_k$ es separable $\Leftrightarrow a_\lambda$ separable $\forall \lambda \in \Lambda$.
2. Si $k \hookrightarrow K \hookrightarrow E$ es una cadena de extensiones algebraicas, entonces $E|_k$ es separable $\Leftrightarrow E|_K$ y $K|_k$ son separables.

La demostración queda de ejercicio.

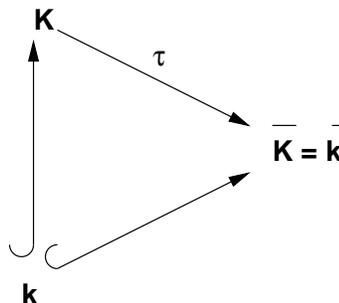
Observación:

En cuerpos de característica 0, los polinomios irreducibles tienen raíces simples (no repetidas), por lo tanto, toda extensión algebraica en característica 0 es separable.

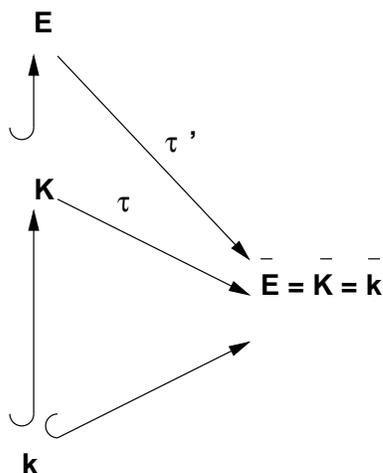
Ejemplo :

Extensión normal "generada" por una extensión finita $K|_k$

Sea $K|_k$ una extensión finita no necesariamente normal,



Probar que el cuerpo E , subcuerpo de \overline{K} , generado por $\{\tau(K)/\tau$ inmersión de K en \overline{K} sobre $k\}$ es una extensión finita de K , normal sobre k , y la menor posible. Tenemos :



Si existe tal E , este debe contener a $\tau(K)$, $\forall \tau : K \rightarrow \overline{K}$ inmersión sobre k . En efecto : si $\tau : K \rightarrow \overline{K}$ es inmersión sobre k , debe poder extenderse a $\tau' : E \rightarrow \overline{K}$ inmersión sobre k , y por la normalidad de $E|_k \Rightarrow \tau'(E) = E \Rightarrow \tau(K) = \tau'(K) \subseteq \tau'(E) = E$. Notar que tales inmersiones $\tau : K \rightarrow \overline{K}$ sobre k son un número finito : Hay $[K : k]_s \leq [K : k] < \infty$. Sean $\tau_1 \dots \tau_r$ tales inmersiones .Sea E el cuerpo más pequeño que contiene a $\tau_1(K) \dots \tau_r(K)$ (subcuerpo de \overline{K}). Si $E|_k$ es normal, buscamos:

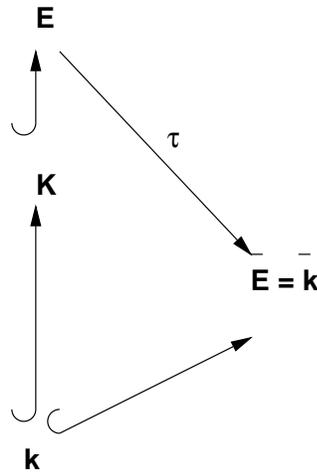
Definición:

Sean K_1, K_2 dos subcuerpos de un cuerpo L . El compuesto de K_1 y K_2 , que se anota K_1K_2 (o $K_1 \vee K_2$), es el subcuerpo más pequeño de L que contiene a K_1 y a K_2 . Este subcuerpo es:

$$K_1K_2 = \left\{ \frac{\sum x_i y_i}{\sum x'_i y'_i} / x_i, x'_j \in K_1, y_i, y'_j \in K_2, \sum x'_i y'_i \neq 0 \right\}$$

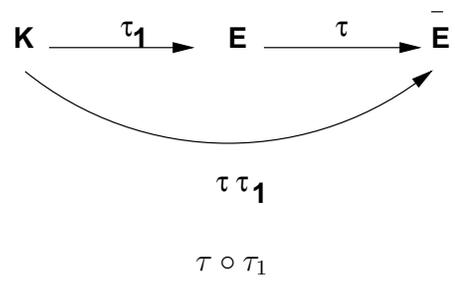
$$K_1K_2 = K_1(K_2) = K_2(K_1) \text{ y } K_1K_2 \dots K_n = K_n(\dots K_3(K_2K_1) \dots) .$$

En el caso del ejemplo, $E = \tau_1(K) \dots \tau_r(K)$. Probaremos luego que $E|_k$ es extensión finita.



Sea $\tau : E \rightarrow \bar{E}$ una inmersión sobre k .

$$\tau(E) = \tau(\tau_1(K) \cdots \tau_r(K)) = \tau(\tau_1(K))\tau(\tau_2(K)) \cdots \tau(\tau_r(K)) = \tau \circ \tau_1(K)\tau \circ \tau_2(K) \cdots \tau \circ \tau_r(K).$$



es inmersión sobre $k \Rightarrow$ es algún τ_j

Como τ es inyectiva : $i \neq j \Rightarrow \tau \circ \tau_i \neq \tau \circ \tau_j \Rightarrow |\{\tau \circ \tau_i/i = 1 \dots r\}| = r$, por lo tanto , $\{\tau \circ \tau_i/i = 1 \dots r\} = \{\tau_i/i = 1 \dots r\} \Rightarrow \tau \circ \tau_1(K)\tau \circ \tau_2(K) \cdots \tau \circ \tau_r(K) = \tau_1(K) \cdots \tau_r(K) = E$

Sólo resta ver que si $K_1|_k$ y $K_2|_k$ son dos extensiones finitas de k , con $k, K_1, K_2 \subseteq L$ cuerpo , entonces $K_1K_2|_k$ es extensión finita. $[K_1K_2 : k] = [K_1K_2 : K_1] \underbrace{[K_2 : k]}_{\text{finito}}$. Esperaríamos que

$$[K_1K_2 : K_1] \leq [K_1 : k]$$

1) Si $K_1 = k(a)$

$K_1K_2 = k(a)K_2 = K_2(k(a)) = K_2(a)$, luego

$$\underbrace{[K_2(a) : K_2]}_{\text{gr}(q(x)), q(x) \in K_2[x]} \leq \underbrace{[k(a) : k]}_{\text{gr}(p(x))} \Rightarrow q(x)/p(x)$$

2) $[K_2(a) : K_2] \leq [k(a) : k]$

$$[K_2(a_1, a_2) : K_2] = [K_2(a_1, a_2) : K_2(a_2)][K_2(a_2) : K_2] \leq [k(a_1a_2) : k(a_2)][k(a_2) : k] = [k(a_1a_2) : k]$$

Por lo tanto , $[K_1K_2 : k] \leq [K_1 : k][K_2 : k]$

Así , por ejemplo , $[\tau_1(K) \dots \tau_r(K) : k] \leq [K : k]^r$

Definición

Sea $K|_k$ extensión de cuerpos . Un elemento $a \in K$ se dice **primitivo** para $K|_k$ ssi $K = k(a)$. En tal caso , $K|_k$ se llama extensión primitiva.

Teorema del elemento primitivo

Sea $K|_k$ extensión algebraica:

1. $K|_k$ es primitiva ssi existe un número finito de “cuerpos intermedios” para la extensión.
Es decir , $|\{\text{Fcuerpo } / k \subseteq F \subseteq K\}| < \infty$.
2. Si la extensión $K|_k$ es finita separable , entonces es primitiva .

Dem.

Caso K finito :

Lo único ha probar , es que toda extensión siempre tiene primitivos.

Consideremos $(K \setminus \{0\}, \cdot)$, es grupo finito \Rightarrow es cíclico $\Leftrightarrow \exists a \in K \setminus \{0\}$ tal que $K \setminus \{0\} = \{a^n : n \in \mathbb{N}\} \Rightarrow K = k(a)$.

Caso K no finito:

Demostremos primero 1.

\Rightarrow)

a elemento primitivo $\Leftrightarrow K = k(a)$. Sea $p(x) \in k[x]$ el polinomio mínimo de a .

Si F es cuerpo intermedio , entonces $K = F(a)$. Sea $p_F(x) \in F[x]$ el polinomio mínimo de a en F .

$k \subseteq F$, entonces , como $p_F(x)$ se anula en $a \Rightarrow p_F(x)/p(x)$.

$p(x)$ tiene un número finito de divisores (en su su cuerpo de descomposición) , por lo tanto , si probamos que : F y F' cuerpos intermedios $\Rightarrow p_F(x) \neq p_{F'}(x)$, estaríamos demostrando 1.

Veamos que $p_F(x)$ determina F . Sea F' el cuerpo construido a partir de k agregando los coeficientes del polinomio $p_F(x) \in F[x]$. Obviamente $k \subseteq F' \subseteq F$, probaremos que en realidad $F' = F$.

Como F' se construye a partir de los coeficientes de $p_F(x)$, entonces $p_F(x) \in F'[x]$, además $p_F(a) = 0$. Pero también $p_F(x)$ es irreducible en $F'[x]$, por lo tanto $p_F(x)$ es el polinomio mínimo de a en $F'[x]$: $p_F(x) = p_{F'}(x)$.

Además $F(a) = K = F'(a)$, luego :

$$[K : F] = \text{gr}(p_F(x)) = \text{gr}(p_{F'}(x)) = [K : F'] \Rightarrow [K : F'] = [K : F][F : F'] \Rightarrow [F : F'] = 1 \Rightarrow F = F'$$

Así , si $p_F(x)$ es el polinomio a coeficientes en $F[x]$, entonces F está generado sobre k por los coeficientes de $p_F(x)$.

\Leftrightarrow)

Si hay un número finito de cuerpos intermedios $\Rightarrow K = k(a)$

algún a . $[K : k]$ finito $\Rightarrow K = k(a_1 \dots a_n)$.

Probaremos por inducción en n que $(\forall n \in \mathbb{N})$, si $K = k(a_1 \dots a_n)$ entonces $K = k(a)$, para algún a .

Paso clave es con $n = 2$ (\Rightarrow paso inductivo) .

$$k(a_1 \dots a_{n+1}) = k(a_1 \dots a_n)(a_{n+1}) ,$$

$$\text{H.I} \Rightarrow k(a_1 \dots a_n) = k(a') \Rightarrow$$

$$k(a_1 \dots a_{n+1}) = k(a_1 \dots a_n)(a_{n+1}) = k(a'a_{n+1}) = k(a'') \quad (n = 2) .$$

$n = 2$: Queremos probar que $K = k(a_1, a_2) = K = k(a)$ algún $a \in K$.

Aquí usaremos K infinito $\Rightarrow k$ infinito

Para λ en k , sea $a^\lambda = a_1 + \lambda a_2$, y sea $F_\lambda = k(a^\lambda) = k(a_1 + \lambda a_2)$.

Existe un número finito de subcuerpos F_λ y un número infinito de elementos $\lambda \Rightarrow \exists \lambda_1, \lambda_2 \in k$, $\lambda_1 \neq \lambda_2$ tal que $F_{\lambda_1} = F_{\lambda_2} = F$.

$$a_1 + \lambda_1 a_2 \in F$$

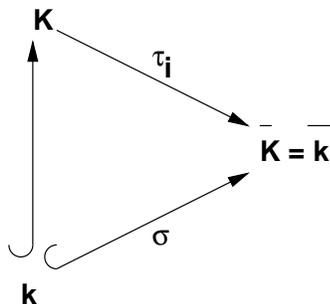
$$a_1 + \lambda_2 a_2 \in F$$

$$\text{restando: } \underbrace{(\lambda_1 - \lambda_2)}_{\neq 0 \in k} a_2 \in F \Rightarrow a_2 \in F , \quad a_1 = \underbrace{(a_1 + \lambda_2 a_2)}_{\in F} - \underbrace{\lambda_2 a_2}_{\in F} \Rightarrow a_1 \in F$$

$$a_1, a_2 \in F \Rightarrow K \subseteq F \subseteq K$$

Probemos 2.

$$K|_k \text{ finita separable} \Leftrightarrow [K : k]_s = [K : k] = n$$



Hay n inmersiones distintas entre si $\tau_1 \dots \tau_n : K \rightarrow \bar{K} = \bar{k}$ sobre k .

Igual que en la demostración anterior , basta probar la propiedad para $K = k(a_1, a_2)$ y luego aplicar inducción.

Sea $f(x) \in K[x]$ el polinomio siguiente:

$$f(x) = \prod_{1 \leq i < j \leq n} ((a_1 + xa_2)^{\tau_i} - (a_1 + xa_2)^{\tau_j}) \in \overline{K}[x]$$

$f(x) \neq 0$ en $\overline{K}[x]$.

Como $\forall i < j$, $\tau_i \neq \tau_j \Rightarrow \tau_i(a_1) \neq \tau_j(a_1) \vee \tau_i(a_2) \neq \tau_j(a_2)$

Por lo tanto, cada factor de $f(x)$ es distinto de 0 $\Rightarrow f(x)$ tiene sólo un número finito de raíces en $\overline{K} \Rightarrow$ como $k \subseteq K$ es infinito, habrá al menos un $\lambda \in k$ tal que $f(\lambda) \neq 0$.

Para este λ : $\tau_i(\underbrace{a_1 + \lambda a_2}_a) \neq \tau_j(a_1 + \lambda a_2)$ para $i < j$

$\Rightarrow \{\tau_i(a)\}_{i=1}^n$ son n elementos distintos en \overline{K} .

Si $p(x) \in k[x]$ es el polinomio mínimo de $a \Rightarrow p^{\tau_i}(x) = p(x)$

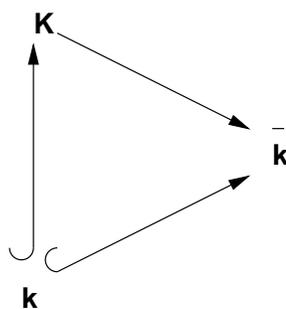
\Rightarrow como $p(a) = 0$, $p(\tau_i(a)) = p^{\tau_i}(\tau_i(a)) = 0$. Luego, $p(x)$ tiene como raíces al menos a los n elementos distintos $\tau_1(a) \dots \tau_n(a) \Rightarrow \text{gr}(p(x)) \geq n$

$[K : k] = n \Rightarrow k(a) \in K$.

Ejercicio: Encontrar los cuerpos intermedios de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]|_{\mathbb{Q}}$.

3.4 Teoría de Galois

Sea $K|_k$ una extensión de cuerpos algebraica. La extensión se dice **de Galois** ssi es normal y separable.



- El **Grupo de Galois** de una extensión $K|_k$ es por definición $G = \text{Gal}(K|_k) = \{\sigma : K \rightarrow K / \sigma \text{ es automorfismo sobre } k\}$
- Dado un cuerpo K , y G un grupo de automorfismos de K , el **cuerpo fijo** de G es $K^G = \{x \in K / \sigma(x) = x, \forall \sigma \in G\}$

3.4.1 Teorema fundamental de la teoría de Galois

Sea $K|_k$ una extensión finita de Galois . Entonces la función γ , que toma subgrupos del grupo $G = \text{Gal}(K|_k)$ y entrega cuerpos intermedios $k \subseteq F \subseteq K$, dada por H (subgrupo de G) $\rightarrow K^H = F$, es una biyección decreciente (i.e , $H_1 \subseteq H_2 \Leftrightarrow K^{H_1} \supseteq K^{H_2}$).

$\forall H$ subgrupo de G , la extensión $K|_{K^H}$ es de Galois , y $\text{Gal}(K|_{K^H}) = H$, además $|H| = [K : K^H]$.

Por otra parte , $H \triangleleft G \Leftrightarrow K^H|_k$ es de Galois , y se tiene una biyección entre subgrupos normales H de G y subextensiones de Galois $F|_k$ de $K|_k$. Además , cuando $H \triangleleft G$

$$\begin{aligned} G/H &\cong \text{Gal}(K^H|_k) . \\ [\sigma] &\rightarrow \sigma|_{K^H} \end{aligned}$$

Antes de demostrar el teorema , demos una aplicación de él :

Teorema fundamental del álgebra

$$\overline{\mathbb{R}} = \mathbb{C}$$

Dem.

Aparte de la teoría del álgebra que utilizaremos en la demostración , necesitaremos las dos propiedades siguientes (de naturaleza topológica de \mathbb{R}) :

1. Todo $r \geq 0$ en \mathbb{R} tiene exactamente una raíz cuadrada $\alpha \geq 0$ en \mathbb{R} . En efecto , $\alpha = \sup\{q \in \mathbb{Q}/q \geq 0, q^2 \leq r\}$.
2. Todo polinomio $p(x) \in \mathbb{R}[x]$ de grado impar , tiene al menos una raíz en \mathbb{R} :

$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ mónico , n impar.

Si $x \neq 0$, $p(x) = x^n \left(1 + \frac{a_{n-1}}{x} + \dots + \frac{a_0}{x^n}\right)$ como función

$$\begin{array}{ccc} p(x) & \longrightarrow & \infty \\ x \rightarrow \infty & & \end{array} \quad \begin{array}{ccc} p(x) & \longrightarrow & -\infty \\ x \rightarrow -\infty & & \end{array}$$

Por lo tanto , $\exists x_1, x_2 \in \mathbb{R}$ tal que $p(x_1) < 0$, $p(x_2) > 0$, y como p es continua , $\exists \bar{x} \in \mathbb{R}$ tal que $p(\bar{x}) = 0$.

Notar que de 1. se deduce que todo $z \in \mathbb{C}$ tiene raíz cuadrada en \mathbb{C} :

Si $z = a + bi$, entonces $z = (x + yi)^2$, con $x + yi = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i \text{sgn}(b) \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \right)$.

Y por lo tanto , cualquier ecuación de segundo grado a coeficientes en \mathbb{C} tiene sus raíces en \mathbb{C} .

Consecuencia: \mathbb{C} no tiene extensiones de grado 2 .

Probar que $\overline{\mathbb{R}} = \mathbb{C}$, equivale a probar que $\overline{\mathbb{C}} = \mathbb{C}$, y esto equivale a probar que toda extensión finita $E|_{\mathbb{C}}$ es \mathbb{C} .

Sea E una extensión finita de \mathbb{C} . Entonces E es una extensión finita de \mathbb{R} .

Como la característica de todos estos cuerpos es 0, todas las extensiones son separables, pero $E|\mathbb{R}$ podría no ser normal, por lo tanto, $E|\mathbb{R}$ podría no ser Galois.

Usando un ejercicio anterior, podemos extender E a la "extensión normal generada por E " : $\mathbb{K} = \sigma_1(E) \cdots \sigma_r(E)$, con $\sigma_1 \dots \sigma_r$ las inversiones de E en \bar{E} sobre \mathbb{R} .

$\mathbb{K}|\mathbb{R}$ es de Galois, por lo tanto, podemos aplicar el teorema fundamental. Llamemos $G = \text{Gal}(\mathbb{K}|\mathbb{R})$.

1) Probaremos que $|G| = 2^m$, para algún m .

Sea $P \subseteq G$ un 2-subgrupo de Sylow, $|P| = 2^r$, con $|G| = 2^r \cdot l$, con l impar. Sea F el cuerpo fijo de P : $F = K^P = \{x \in K / \sigma(x) = x, \forall \sigma \in P\}$.

T.f de Galois: $\mathbb{K}|_F$ es de Galois, $P = \text{Gal}(\mathbb{K}|_F)$, $|P| = [K:F]$

$$\text{Luego, } [F:\mathbb{R}] = \frac{[K:\mathbb{R}]}{[K:F]} = \frac{2^r \cdot l}{2^r} = l$$

Deduciremos usando 2. que $F = \mathbb{R}$:

Sea $a \in F$ y $p(x)$ su polinomio mínimo en $\mathbb{R}[x]$. $\text{gr}(p(x)) = [\mathbb{R}(a) : \mathbb{R}] / [F : \mathbb{R}]$ impar $\Rightarrow \text{gr}(p(x))$ es impar $\Rightarrow p(x)$ tiene alguna raíz en \mathbb{R} . Pero $p(x)$ es irreducible en $\mathbb{R} \Rightarrow p(x) = x - a$ (grado 1) $\Rightarrow a \in \mathbb{R} \Rightarrow l = 1 \Rightarrow [K:\mathbb{R}] = 2^r$.

Notando que K es extensión de E , y por lo tanto, de \mathbb{C} , se tiene $[K:\mathbb{C}] = \frac{[K:\mathbb{R}]}{[\mathbb{C}:\mathbb{R}]} = 2^{r-1}$.

Consideremos K como extensión de \mathbb{C} . Al ser $\mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow K \Rightarrow K|\mathbb{C}$ es de Galois.

Sea $\bar{G} = \text{Gal}(K|\mathbb{C})$, $|\bar{G}| = [K:\mathbb{C}] = 2^{r-1}$. \bar{G} es un 2-grupo, y tendrá subgrupos (normales en \bar{G}) de todos los ordenes intermedios. En particular, $\exists H \subseteq \bar{G}$ tal que $|H| = 2^{r-2}$ (a menos que $r = 1$ y $K = \mathbb{C}$).

$$\text{Sea } L = K^H, 2^{r-2} = |H| = [K:L] \Rightarrow [L:\mathbb{C}] = \frac{[K:\mathbb{C}]}{[K:L]} = \frac{2^{r-1}}{2^{r-2}} = 2$$

Lo que no puede ser, pues por 1., \mathbb{C} no tiene extensiones de orden 2, por lo tanto, $2^{r-1} = 1 \Rightarrow K = \mathbb{C}$.

Demostración del teorema fundamental de Galois

Lema 1

Sean $K|_k$ extensión de Galois y $G = \text{Gal}(K|_k)$.

1. $K^G = k$
2. Si H es subgrupo de G y $F = K^H$, entonces $K|_F$ es extensión de Galois.

Dem.

1.

$$G = \{ \sigma : K \rightarrow K / \sigma \text{ automorfismo tq } \sigma(x) = x \ \forall x \in k \}$$

$$K^G = \{ x \in K / \sigma(x) = x, \forall \sigma \in G \}$$

Por definición de G , $k \subseteq K^G$. Probemos la otra inclusión :

Sea $a \in K^G$ y $p(x)$ su polinomio mínimo en $k[x]$. $a \in k \Leftrightarrow k(a) = k \Leftrightarrow [k(a) : k] = \text{gr}(p(x)) = 1$

.

Como $K|_k$ es separable, $p(x)$ tiene raíces simples, por lo tanto, hay que probar que $p(x)$ tiene una sola raíz a .

Por cada raíz $b \in \bar{K}$ de $p(x)$, $\exists!$ extensión de la inclusión $k \hookrightarrow \bar{K}$ a $\tau_b : k(a) \rightarrow \bar{K}$.

$\bar{K}|_{k(a)}$ es algebraica, por lo tanto, τ_b se puede extender a $\sigma : K \rightarrow \bar{K}$. Obviamente σ también será una extensión de la inclusión $k \hookrightarrow \bar{K}$.

$K|_k$ es normal $\Rightarrow \sigma(K) = K$. Tenemos entonces $\sigma : K \rightarrow K$ automorfismo de K sobre k , i.e $\sigma \in G$.

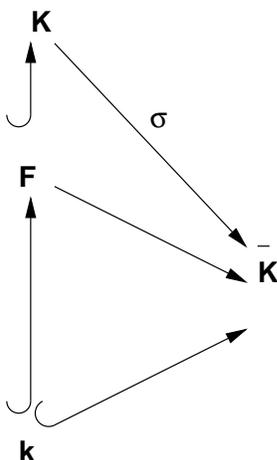
$a \in K^G \Rightarrow \sigma(a) = a$, pero dado que σ extiende a τ_b , $\sigma(a) = \tau_b(a) = b \Rightarrow b = a \Rightarrow$ la única raíz de $p(x)$ es a , y por ser de multiplicidad 1, concluimos que $p(x)$ tiene sólo una raíz.

2.

$k \hookrightarrow F \hookrightarrow K$. Queremos demostrar que $F|_k$ es normal y separable (de Galois).

La separabilidad de $F|_k$ se desprende de la separabilidad de $K|_k$.

Para la normalidad de $K|_F$:



Si $\sigma : K \rightarrow \bar{K}$ es inmersión sobre F , lo es sobre $k \Rightarrow \sigma(K) = K$, por lo tanto, $K|_F$ es normal

.

($F|_k$ podría no ser normal).

Corolario

Sean $K|_k$ extensión de Galois y $G = \text{Gal}(K|_k)$. Definamos los siguientes conjuntos y funciones:

$$\mathcal{C} = \{F/ k \subseteq F \subseteq K \text{ cuerpo intermedio}\}$$

$$\mathcal{A} = \{H/H \text{ subgrupo de } G\}$$

$$\begin{array}{ccc} \eta: \mathcal{C} & \longrightarrow & \mathcal{A} \\ F & \longrightarrow & \text{Gal}(K|_F) \end{array} \quad \begin{array}{ccc} \gamma: \mathcal{A} & \longrightarrow & \mathcal{C} \\ H & \longrightarrow & K^H \end{array}$$

$\gamma \circ \eta: \mathcal{C} \longrightarrow \mathcal{C}$ es $\text{id}_{\mathcal{C}}$. Así, η es inyectiva y γ es sobreyectiva.

Dem.

Sea $F \in \mathcal{C}$, por 2. del lema anterior, $K|_F$ es de Galois. Sea $H = \text{Gal}(K|_F)$ ($H = \eta(F)$). Aplicando 1. del lema 1 a la extensión $K|_F \Rightarrow K^H = F$ ($\gamma(\eta(F)) = F$).

Ejercicio:

Sea $K|_k$ extensión de Galois y $G = \text{Gal}(K|_k)$. Sean H_1, H_2 dos subgrupos de G y $F_1 = K^{H_1}, F_2 = K^{H_2}$. Entonces:

1. $H_1 \subseteq H_2 \Leftrightarrow F_1 \supseteq F_2$
2. Sea $H = H_1 \cap H_2$ y $F = K^H$, entonces $F = F_1 F_2$.
3. Si $H = H_1 H_2 = \langle H_1 \cup H_2 \rangle$ y $F = K^H$, entonces $F = F_1 \cap F_2$.

Lema 2

Sea $K|_k$ una extensión algebraica y separable tal que $\exists n \geq 1, n \in \mathbb{N} (\forall a \in K)[k(a) : k] \leq n$. Entonces la extensión $K|_k$ es finita con $[K : k] \leq n$.

Dem.

Sea $r = \text{Max}\{\bar{r}/\bar{r} = [k(a) : k], \text{ para algún } a \in K\}$. Sea $a \in K$ tal que $[k(a) : k] = r$.

Supongamos que $k(a) \neq K$. Sea $b \in K \setminus k(a)$. Tomemos $k(a, b) = k(a)(b)$, extensión finita de k , separable \Rightarrow tiene elementos primitivos, i.e $\exists c \in k(a, b) \subseteq K$ tq $k(a, b) = k(c)$. Pero $k(a) \subset k(a, b)$ (inclusión estricta) $\Rightarrow r = [k(a) : k] < [k(a, b) : k] = [k(c) : k] \rightarrow \leftarrow$, por lo tanto, $K = k(a) \Rightarrow [K : k] = r \leq n$.

Teorema de Artin

Sea K un cuerpo . Sea G un grupo finito de autoorfismos de K . Sea $K^G = k$. Entonces $K|_k$ es de Galois , con $\text{Gal}(K|_k) = G$, $[K : k] = |G| = n$.

Dem.

Sea $a \in K$. Sean $\sigma_1 \dots \sigma_r$ una cantidad maximal de elementos de G tal que $\sigma_1(a) \dots \sigma_r(a)$ son todos distintos de 0 . Notar que la identidad es uno de estos r elementos.

Sea $p(x) = (x - \sigma_1(a)) \cdots (x - \sigma_r(a))$. $p(a) = 0$

Para cada $\sigma \in G$, $p^\sigma(x) = (x - \sigma\sigma_1(a)) \cdots (x - \sigma\sigma_r(a))$, por lo tanto , los elementos de G dejan invariantes los coeficientes de $p(x)$, i.e están en $k = K^G$, por lo tanto , a es algebraico sobre $k \Rightarrow K|_k$ es algebraica.

Además , $p(x)$ tiene raíces distintas en K , por lo tanto , $q(x)$, el polinomio mínimo de a , que divide a $p(x)$, tiene raíces simples $\Rightarrow a$ es separable $\Rightarrow K|_k$ es separable.

Por último , $p(x)$ tiene r raíces \Rightarrow el número de raíces de $q(x)$ es $\leq r \Rightarrow \text{gr}(q(x)) \leq r \leq n \Rightarrow [k(a) : k] \leq n$. Por el lema 2 : $K|_k$ es una extensión finita , con $[K : k] \leq n$.

Falta probar $G = \text{Gal}(K|_k)$, $[K : k] = |G| = n$

La inclusión $G \subseteq \text{Gal}(K|_k)$ es directa .

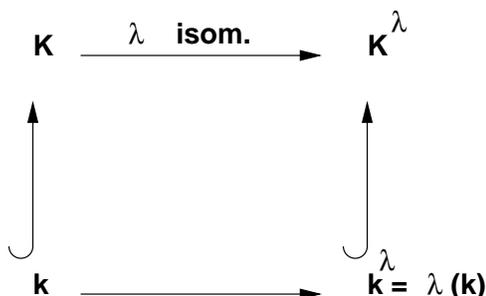
$n = |G| \leq |\text{Gal}(K|_k)| = [K : k]_s = [K : k] \leq n$, por lo tanto , $G = \text{Gal}(K|_k)$ y $[K : k] = n$.

Corolario

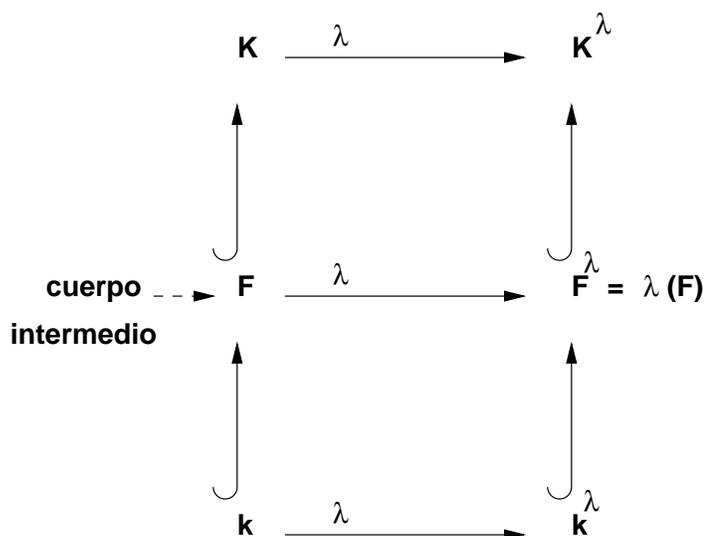
$$\text{id} \begin{cases} \mathcal{C} \longrightarrow \mathcal{A} \longrightarrow \mathcal{C} \\ \text{F} \longrightarrow \text{Gal}(K|_F) \\ \text{H} \longrightarrow K^H \end{cases}$$

Por el teorema de Artin , $\text{Gal}(K|_{K^H}) = H$ (la composición que faltaba) .

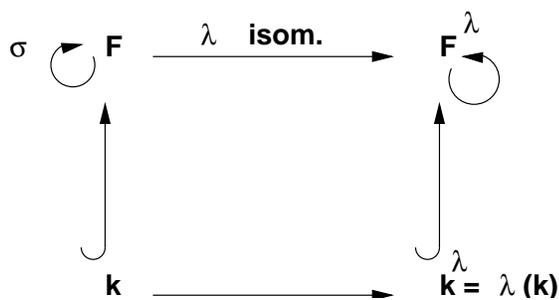
Para terminar de probar el teorema fundamental de la teoría de Galois consideremos la siguiente situación:



$K|_k$ extensión de Galois $\Leftrightarrow K^\lambda|_{k^\lambda}$ es de Galois



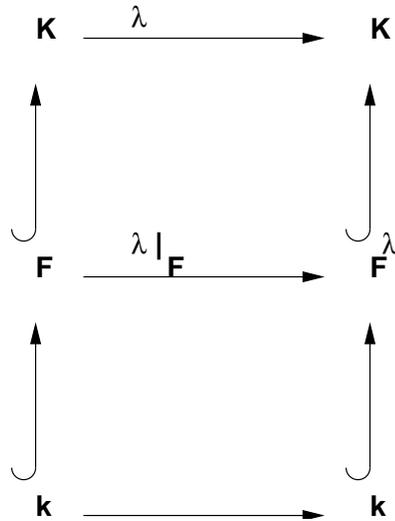
¿Qué relación hay entre $\text{Gal}(F|_k)$ y $\text{Gal}(F^\lambda|_{k^\lambda})$?



$$\text{Gal}(F|_k) \cong \text{Gal}(F^\lambda|_{k^\lambda}) \quad \text{Gal}(K|_F) \cong \text{Gal}(K^\lambda|_{F^\lambda})$$

$$\sigma \rightarrow \lambda \circ \sigma \circ \lambda^{-1}$$

Caso que nos interesará:



$$\lambda \circ \text{Gal}(\mathbf{K}|\mathbf{F}) \circ \lambda^{-1} = \text{Gal}(\mathbf{K}|\mathbf{F}^\lambda)$$

Si $\mathbf{K}|\mathbf{k}$ es de Galois y \mathbf{F} cuerpo intermedio, con estas consideraciones se prueba la siguiente propiedad:

Prop

Si $\mathbf{K}|\mathbf{k}$ es de Galois, \mathbf{F} cuerpo intermedio, $G = \text{Gal}(\mathbf{K}|\mathbf{k})$, $H = \text{Gal}(\mathbf{K}|\mathbf{F})$, entonces $\mathbf{F}|\mathbf{k}$ es de Galois $\Leftrightarrow H \triangleleft G$, y en este caso, la restricción $\sigma \in G$, $\sigma|_{\mathbf{F}} : \mathbf{F} \rightarrow \mathbf{F}$ es un epimorfismo de G en $\text{Gal}(\mathbf{F}|\mathbf{k})$, con H su núcleo y $\mathbf{F}|\mathbf{k}$ es de Galois, $G/H \cong \text{Gal}(\mathbf{F}|\mathbf{k})$.