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 $(\mathrm{M}, *)$ tal que:

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

Definición

Grupo es una estructura con una operación $(\mathrm{G}, *)$ tal que:

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

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

Definición

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

Ejemplo:

Sean $B_n = \{1..n\}$ y $S_n = \sum_n = \{\sigma : B_n \to B_n / \sigma \text{ es biyección}\}$ .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 $(\mathrm{G} *), (\mathrm{H}, *_{\mathrm{H}})$ dos grupos . Un **Morfismo** (u homomorfismo) entre ellos es una función $f : \mathrm{G} \to \mathrm{H}$ tal que: $(\forall x, y \in \mathrm{G})\ f(x * y) = f(x) *_{\mathrm{H}} f(y)$.

Un morfismo como este se suele denotar por $f : (\mathrm{G}, *) \to (\mathrm{H}, *_{\mathrm{H}})$

Nombres especiales:

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

Observación:

Un morfismo de grupos **realmente** lleva una estructura a la otra. Si $f : (\mathrm{G}, *) \to (\mathrm{H}, *_{\mathrm{H}})$ es morfismo, entonces:

- $f(1_{\mathrm{G}}) = 1_{\mathrm{H}}$
- $(\forall x \in \mathrm{G})\ f(x^{-1}) = f(x)^{-1}$

(***Ejercicio***)

1.3 "Los Buenos Subconjuntos de un Grupo": Subgrupos.

Definición:

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

1. $*$ es cerrado en H . Es decir, $(\forall x, y \in \mathrm{H}, x * y \in \mathrm{H})$
2. $(\mathrm{H}, * \,|_{\mathrm{H}})$ es tambiénun grupo.

Observación:

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

Ejercicio:

H subgrupo de $(\mathrm{G}, *)$ ssi:

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

Prop

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

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

(EJERCICIO)

Ejercicio:

Sean (G, $*$) (L, $\cdot$) dos grupos y $f : \mathrm{G} \to \mathrm{L}$ un morfismo.Entonces:

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

Definición

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

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

Es fácil probar que Ker$f$ e Imf son subgrupos de G y L respectivamente.
Obviamente f sobreyectiva$\Leftrightarrow Imf =$ L .

Prop

f morfismo inyectivo $\Leftrightarrow Kerf = \{1\}$.

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 $x * y^{-1} \in Kerf = \{1\} \Rightarrow x = y$

1.4 "Buenos Cuocientes en Grupos".

Definición.

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

Observación:

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

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

Además, la Sobreyección Canónica $\begin{array}{rccc} \nu: & \mathrm{G} & \longrightarrow & \mathrm{G}/\sim \\ & x & \longrightarrow & [x] \end{array}$

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

Notar que si $\approx$es compatible con $*$ en G , entonces $[1] \subseteq \mathrm{G}$ 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 $\mathrm{H} = [1]$tienelasiguientepropiedad :

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

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

Definición

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

$$\begin{array}{rccc} I_a: & \mathrm{G} & \longrightarrow & \mathrm{G} \\ & x & \longrightarrow & I_a(x) = a * x * a^{-1} \end{array}$$

Ejercicio:

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

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

Definición

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

Notación:

$\mathrm{H} \triangleleft \mathrm{G} \Leftrightarrow \mathrm{H}$ **es subgrupo normal de** G

Ejercicio:

Sean $(\mathrm{G}, *)$, $(\mathrm{H}, \cdot)$ dos grupos, y $f : \mathrm{G} \to \mathrm{L}$ un morfismo.Probar que $Kerf$ es un subgrupo normel de G .

Definición

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

Ejercicio:

1. $\approx_{\mathrm{H}}$ es de equivalencia
2. $\approx_{\mathrm{H}}$ es compatible con $* \Leftrightarrow \mathrm{H} \triangleleft \mathrm{G}$
3. $[1] = \mathrm{H}$

Observación:

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

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

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

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

$\mathrm{G}/\approx_{\mathrm{H}}$ es sólo un conjunto . Adquiere estructura natural de grupo ssi $\mathrm{H} \triangleleft \mathrm{G}$.

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

Tomando la relación de equivalencia $\approx_{\mathrm{H}}$ formamos el grupo cuociente $\mathrm{L} = \mathrm{G}/\approx_{\mathrm{H}}$ y el epimorfismo canónico $\nu : \mathrm{G} \to \mathrm{L}$ tal que $\nu(x) = [x]$.

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

Ejemplo:

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

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

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

Si $(\mathrm{G}, *)$ 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 $\mathrm{H} \subseteq \mathbb{Z}$ un subgrupo .

- Si $\mathrm{H} = \{0\} \Rightarrow \mathrm{H} = 0\mathbb{Z}$
- Si $\mathrm{H} \neq \{0\}$:
  Sea $m \in \mathrm{H}$ el más pequeño de los elementos mayores que 0 en H.
  Tomemos $h \in \mathrm{H}$ un elemento cualquiera.Por el teorema de la división de enteros
  $h = mq + r\, 0 \leq r < m$

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

La relación $\approx_{\mathrm{H}}$ asociada a $\mathrm{H} = m\mathbb{Z}$ es $x \approx_{\mathrm{H}} y \Leftrightarrow -x + y = mk, k \in \mathbb{Z} \Leftrightarrow\ x \equiv_m\ y$

y entonces resulta que $\mathbb{Z}/\approx_{\mathrm{H}} = \mathbb{Z}_m$ (enteros módulo m)

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

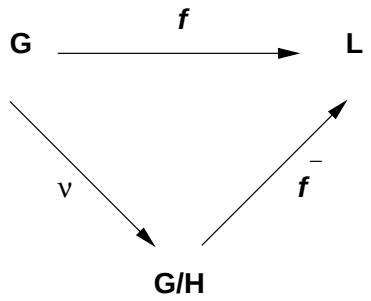
$(m \geq 2) : \mathbb{Z}_m = \{[0], [1], ..., [m-1]\}$.

Notación:

Si $(\mathrm{G}, *)$ es grupo, y $\mathrm{H} \triangleleft \mathrm{G}$, el cuociente $\mathrm{G}/\approx_{\mathrm{H}}$ se anota simplemente G/H , y se lee :"G módulo H "

1.4.1 Teorema del Factor

Sean $(\mathrm{G}, *)$, $(\mathrm{L}, \cdot)$ grupos. $f : (\mathrm{G}, *) \to (\mathrm{L}, \cdot)$ morfismo y $\mathrm{H} \triangleleft \mathrm{G}$, con $\mathrm{H} \subseteq Kerf$.



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

Dem.

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

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

$[x] = [x'] \Leftrightarrow x \approx_{\mathrm{H}} x' \Leftrightarrow x^{-1} * x' \in \mathrm{H} \Leftrightarrow \exists\, h \in \mathrm{H}\ tq\, x^{-1} * x' = h$

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

por lo tanto, la función $\overline{f}:\ \begin{array}{ccc} \mathrm{G/H} & \longrightarrow & \mathrm{L} \\ [x] & \longrightarrow & f(x) \end{array}$ queda bien definida.

Es fácil ver que es morfismo:

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

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

Observación:

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

Nota:

- $\mathrm{Im}\overline{f} = \mathrm{Im}f$, por lo tanto, $\overline{f}$ epimorfismo$\Leftrightarrow$ f epimorfismo
- $\begin{aligned} \mathrm{Ker}\overline{f} &= \{[x] \in \mathrm{G/H} : \overline{f}([x]) = 1\} \\ &= \{[x] \in \mathrm{G/H} : f(x) = 1\} \\ &= \{[x] \in \mathrm{G/H} : x \in \mathrm{Ker}f\} \\ &= \text{Clase de los elementos del } \mathrm{Ker}f \end{aligned}$

  Veamos que si $x \in \mathrm{Ker}f$, entonces $[x] \subseteq \mathrm{Ker}f$:
  $y \in [x] \Leftrightarrow x^{-1} * y \in \mathrm{H} \Leftrightarrow y \in x * \mathrm{H}$, como $\mathrm{Ker}f$ es subgrupo y $\mathrm{H} \subseteq \mathrm{Ker}f \Rightarrow x * \mathrm{H} \subseteq \mathrm{Ker}f$, por lo tanto, la clase de x si $x \in \mathrm{Ker}f$ sigue en $\mathrm{Ker}f$.
  De aquí se puede escribir : $\mathrm{Ker}\overline{f} = \mathrm{Ker}f/\mathrm{H}$, y así $\overline{f}$ inyectiva $\Leftrightarrow \mathrm{H} = \mathrm{Ker}f$.

Corolario

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

1.4.2 Generadores de Subgrupos

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

$$< A >= \bigcap_{A \subseteq \mathrm{H} subgrupo\, de\, \mathrm{G}} \mathrm{H}$$

Ejercicio:

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

¿Qué es $< A >$?

1. Es subgrupo.
2. $< A > \supseteq A$.
3. Es el subgrupo de G más pequeño que contiene a A , i.e. si $\mathrm{H} \subseteq \mathrm{G}$ es subgrupo y $\mathrm{H} \supseteq A \Rightarrow \mathrm{H} \supseteq < A >$.

Prop

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

Definición

Si $(G, *)$ es grupo, y $a \in$ G , para $n \in \mathbb{Z}$ definimos a^n como:
$a^0 = 1$ (con 1 el neutro en G)
$a^{n+1} = a^n * a \;\; n \in \mathbb{N}$
$a^n = (a^{-n})^{-1}$ 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 $< A >= \{a_1^{m_1} * ... * a_n^{m_n} / n \in \mathbb{N}, m_1 ... m_n \in \mathbb{Z}, a_1 ... a_n \in A\}$

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

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 $f: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longrightarrow & f(n) = a^n \end{array}$

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.

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

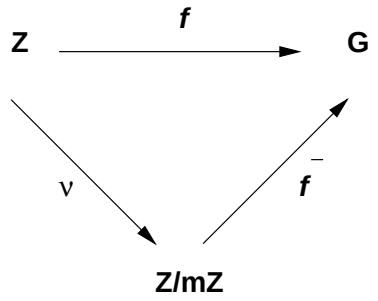
AFIRMACIÓN: no hay ningún $n \neq 0$ en $\text{Ker} f$ ($\Leftrightarrow$ no hay ningún $n > 0$ en $\text{Ker} f$).

Si $n > 0$ está en $\text{Ker} f$, entonces $G = \{a^k / k \in \mathbb{Z}\} = \{1, a, .., a^{n-1}\} \Rightarrow$ 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

$\mathbb{Z} \longrightarrow G$



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

Definición

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

$< A >_N = \bigcap_{A \subseteq H \lhd G} H$

Ejercicio:

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

Observación:

$< A >_N$ se caracteriza naturalmente como el subgrupo normal mas pequeño de G que contiene a A .

Claramente $< A > \subseteq < A >_N$.

Prop

$< A >_N = \{I_{x_1}(a_1^{m_1}) * \cdots * I_{x_n}(a_n^{m_n})/n \in \mathbb{N}, m_1 \ldots m_n \in \mathbb{Z}, a_1 \ldots a_n \in A,\ x_1 \ldots x_n \in \mathrm{G}\}$.

La demostración queda de ejercicio.

Conmutadores y Abelianización de un grupo

Definición

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

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

Obsrvación:

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

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

Definición

La abelianización de G es $Ab(\mathrm{G}) = \mathrm{G}/[\mathrm{G}, \mathrm{G}]$.

Prop

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

Dem.

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

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

$\Rightarrow$) 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 $\mathrm{HK} =< \mathrm{H} \cup \mathrm{K} >$ (subgrupo más pequeño que contiene a H y K).

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

Prop

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

Dem. (de 3.)

Inducción más lo siguiente:

$\forall\, h_1, h_2 \in \mathrm{H}\ \forall\, k_1, k_2 \in \mathrm{K}$

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

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

Completar la demostración.

Otro Ejemplo de Cuocientes

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

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

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

Podemos mirar globalmente los automorfismos interiores como provenientes de la función

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

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

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

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

¿Ker$I$?

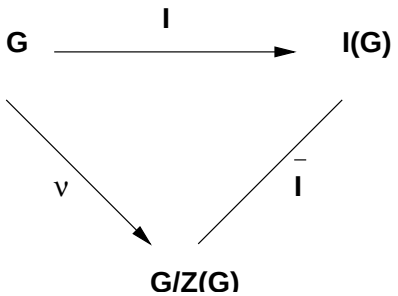
$a \in \mathrm{Ker}I \Leftrightarrow I_a = id_{\mathrm{G}} \Leftrightarrow (\forall x \in \mathrm{G})\, axa^{-1} = x \Leftrightarrow (\forall x \in \mathrm{G})\, ax = xa \Leftrightarrow (\forall x \in \mathrm{G})$ a conmuta con x

Definición

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

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

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



Notación:

La operación $x \to axa^{-1}$ 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 $f : \mathrm{G} \to \mathrm{L}$ es un morfismo de grupos , y $\mathrm{H} \subseteq \mathrm{G}$ es un subgrupo , se tiene $f^{-1}(f(\mathrm{H})) = (\mathrm{Ker}f)\mathrm{H}$.

Dem.

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

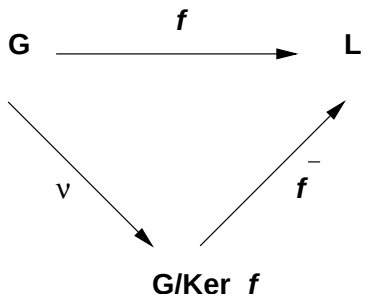
Sea $f : \mathrm{G} \to \mathrm{L}$ un epimorfismo de grupos , sabemos del teorema del factor , que

$$\begin{array}{rccl} \overline{f}: & \mathrm{G}/\mathrm{Ker}f & \longrightarrow & \mathrm{L} \quad \text{es isomorfismo} \\ & [x] & \longrightarrow & f(x) \end{array}$$

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

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

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



Prop

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

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

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

Más aun , esto induce una correspondencia uno a uno:

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

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

Dem.

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

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

(completar parte de subgrupos normales).

Situación usual: $\mathrm{H} \triangleleft \mathrm{G}$, $\nu : \mathrm{G} \to \mathrm{G/H}$

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

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

Dem.

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

$f : \mathrm{G} \to \mathrm{L}$, $\nu : \mathrm{L} \to \mathrm{L}/f(\mathrm{H})$.

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

El teorema del factor dice que se induce un isomorfismo

$\overline{f} : \mathrm{G}/\mathrm{Ker}\widetilde{f} \to \mathrm{L}/f(\mathrm{H})$

$[x]_{\mathrm{Ker}\widetilde{f}} \to \widetilde{f}(x) = [f(x)]_{f(\mathrm{H})}$

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

Corolario

Si $f : \mathrm{G} \to \mathrm{L}$ es epimorfismo de grupos , y $\mathrm{H}' \triangleleft \mathrm{L}$, f induce un isomorfismo

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

Dem.

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

Corolario

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

$$\begin{array}{ccc} (\mathrm{G}/\mathrm{K})/(\mathrm{H}/\mathrm{K}) & \cong & \mathrm{G}/\mathrm{H} \\ [[x]_{\mathrm{K}}]_{\mathrm{H}/\mathrm{K}} & \longleftrightarrow & [x]_{\mathrm{H}} \end{array}$$

Dem.

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

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

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

Segundo teorema de isomorfismos

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

$\mathrm{H} \cap \mathrm{K} \triangleleft \mathrm{G}$, $\mathrm{H} \triangleleft \mathrm{H}\,\mathrm{K}$ y

$\mathrm{K}/\mathrm{H} \cap \mathrm{K} \cong \mathrm{H}\,\mathrm{K}/\mathrm{H}$

$[x]_{\mathrm{H} \cap \mathrm{K}} \to [x]_{\mathrm{H}}$

Dem.

Considerar:

$$\begin{array}{ccccc} & i & & \nu & \\ \mathrm{K} & \hookrightarrow & \mathrm{H\,K} & \longrightarrow & \mathrm{H\,K/H} \\ x & \hookrightarrow & x & \longrightarrow & [x]_{\mathrm{H}} \end{array}$$

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

Definición

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

Proposición

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

Dem.

$\coprod$: unión disjunta con respecto a la relación $\approx_{\mathrm{H}}$

$\mathrm{G} = \coprod_{[x] clase\, de\, eq.\, de \approx_{\mathrm{H}}} [x]$

$\Rightarrow \mid \mathrm{G} \mid = \sum_{x\mathrm{H}\, es\, clase} \mid x\mathrm{H} \mid$, pero $\mid x\mathrm{H} \mid = \mid \mathrm{H} \mid$

$\Rightarrow \mid \mathrm{G} \mid =$ (número de clases) $\cdot$ H

Definición

El cardinal de G/H , i.e , el número de clases de $\approx_{\mathrm{H}}$ se llama índice de H en G , y se anota $[\mathrm{G} : \mathrm{H}] = \mid \mathrm{G/H} \mid$.

Fórmula: $\mid \mathrm{G} \mid = [\mathrm{G} : \mathrm{H}] \mid \mathrm{H} \mid$.

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

1.5 Acciones De Grupos Sobre Conjuntos

Definición

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

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

(Notación: $\varphi(g,x) = gx$)
con las siguientes propiedades:

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

Observación 1:

Una acción derecha de G sobre X es una función $\psi : \begin{array}{ccc} X \times \mathrm{G} & \longrightarrow & X \\ (x,g) & \longrightarrow & xg = \psi(x,g) \end{array}$ con las siguientes propiedades:

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

Parece una "tomadura de pelo ", pero si a partir de ψ se define $\varphi : \mathrm{G} \times X \longrightarrow X$ 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 $g \in \mathrm{G}$ la función
$\Phi_g : X \to X$ 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 $\Phi : \begin{array}{ccc} \mathrm{G} & \longrightarrow & Biy(X) \\ g & \longrightarrow & \Phi_g \end{array}$
Recordando que $(Biy(X), \circ)$ es un grupo , 2. dice que $\Phi : (\mathrm{G}, \cdot) \to (Biy(X), \circ)$ es un morfismo.

Reciprocamente , dado un morfismo $\Psi : (\mathrm{G}, \cdot) \to (Biy(X), \circ)$ 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 $(\forall g \in \mathrm{G})\ \Phi_g$ 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.***

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

Sabemos que $I: \begin{array}{ccc} (\mathrm{G},\cdot) & \longrightarrow & (Aut(\mathrm{G}),\circ) \\ g & \longrightarrow & I_g \end{array}$ es un morfismo, y $(Aut(\mathrm{G}),\circ)$ es un subgrupode $(Biy(X),\circ)$, por lo tanto tenemos una acción de G sobre G .

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

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

Evidentemente $\varphi(g,x) = gx$ (producto en G) , es una acción de G sobre si mismo , y el morfismo asociado es $T: \begin{array}{ccc} (\mathrm{G},\cdot) & \longrightarrow & (Biy(\mathrm{G}),\circ) \\ g & \longrightarrow & T_g \end{array}$

Es fácil ver que este morfismo T es inyectivo:

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

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

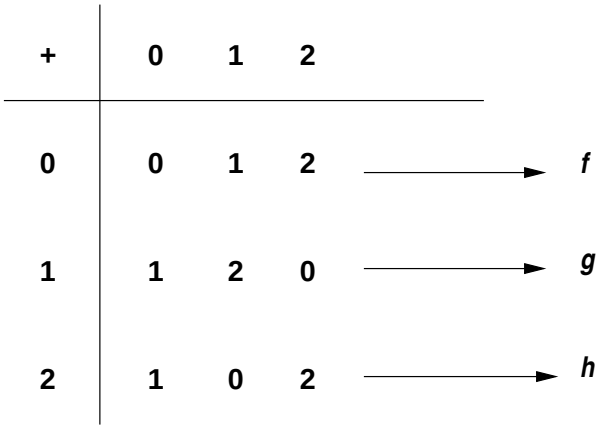
De aquí sale un conocido teorema:

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



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

Ejemplo:

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

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

G actúa por traslaciones sobre G/H mediante $g(x\mathrm{H}) = (gx)\mathrm{H}$.

Definición

Sean (G, X, φ) y (G, Y, ψ) dos G−espacios .Una función $f : X \to Y$ 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

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

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 $(\forall x, y \in X)(\exists g \in \mathrm{G})$ tal que $y = gx$.(G, X, φ) se dice G− espacio homogeneo.

Ejemplo:

G actúa transitivamente sobre cualquier cuociente 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

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

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 homogeneo . Sea $x_o \in X$ un elemento cualquiera. Entonces X es isomorfo a $\mathrm{G}/Est(x_o)$ (como G− espacios) .

Dem.

Sea $f: \begin{array}{ccc} \mathrm{G} & \longrightarrow & X \\ g & \longrightarrow & f(g) = gx_o \end{array}$. Sean $g, h \in \mathrm{G}$ tales que $g \approx_{Est(x_o)} h$ i.e

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

podemos entonces definir $\overline{f}: \begin{array}{ccc} \mathrm{G}/Est(x_o) & \longrightarrow & X \\ [g] & \longrightarrow & \overline{f}([g]) = f(g) = gx_o \end{array}$

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

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

Ejercicio:

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

Definición

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

Observación:

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

$\sim_{\mathrm{G}}$ 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 sóla 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 homogeneo.

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

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 $x_o \in \mathrm{G}$

$Orb(x_o) = \{gx_o g^{-1} / g \in \mathrm{G}\}$

$= \{$ conjugados de $x_o\}$

$= conj(x_o)$ (clase de conjugación de x_o)

$Orb(x_o) \cong \mathrm{G}/Est(x_o)$

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

$= \{g \in \mathrm{G} / g \cdot x_o \cdot g^{-1} = x_o\}$

$= \{g \in \mathrm{G} / g \cdot x_o = x_o \cdot g\}$

$= Z(x_o)$ (centralizador de x_o).

Corolario

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

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

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

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

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

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

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:

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

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

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

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

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

1.6 Teorema de Cauchy

Definición

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

Algunas cosas directas:

Supongamos que g es de orden finito

- Si $g^n = 1 \Rightarrow O(g)/n$
  $< \{g\} > \cong \mathbb{Z}/Kerf = O(g) \cdot \mathbb{Z} \cong \mathbb{Z}_{O(g)}$.
  Mejor aun , $\{n \in \mathbb{Z} / g^n = 1\} = O(g) \cdot \mathbb{Z} = \{$ multiplos de $O(g)\}$
  En particular $O(g) = min\{n > 0 / g^n = 1\}$.

- Si $O(g) = m$ y $x \in < \{g\} >$, 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 $p/ \mid G \mid$. 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 $\mid G \mid$:

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

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

Paso inductivo:

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

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

1. $p/O(g)$
   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 $L = G/ < \{g\} >$ (este cuociente tiene sentido pues, por ser G abeliano , todos sus subgrupos son normales).
   $\mid L \mid = \frac{|G|}{O(g)}$
   como p no divide a $O(g)$, entonces $p/ \mid L \mid$ .Usemos la H.I para L :

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

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:

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

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.

Analicemos 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 $p/$ | $Z(x_\lambda)$ | , 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 $Z(x_\lambda)$

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

$\Rightarrow p/\sum$[G : $Z(x_\lambda)$] y como $p/$ | G |

$\Rightarrow p/$ | 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 $p/ |$ 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
- $g\mathrm{P}g^{-1} = \mathrm{P}$

Entonces $g \in$ P .

Observación:

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

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 cuociente N(P)/P y la clase $[g] \in N(\mathrm{P})/\mathrm{P}$.

Sea K =$< \{[g]\} > \subseteq N(\mathrm{P})/\mathrm{P}$.

Recordando el teorema de correspondencia para subgrupos cuocientes:

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 $O([g]) = O(\mathrm{L/P})$, 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 $g \in \mathrm{L} \Rightarrow g \in \mathrm{P}$.

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

Sea G grupo, H y K subgrupos de G .

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

Podemos poner este problema en el siguiente contexto:

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

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

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

Sabemos lo siguiente:

$Orb(\mathrm{K}) \cong \mathrm{H}/Est(\mathrm{K})$ como H− espacios.

$Est(\mathrm{K}) = \{h \in \mathrm{H}/h\mathrm{K} = \mathrm{K}\}$

$= \{h \in \mathrm{H}/h \cdot \mathrm{K} \cdot h^{-1} = \mathrm{K}\} = N_{\mathrm{H}}(\mathrm{K})$

Normalizador de K en H .

$\Rightarrow Orb(\mathrm{K}) \cong \mathrm{H}/N_{\mathrm{H}}(\mathrm{K})$

(Evidentemente , $N_{\mathrm{H}}(\mathrm{K})$ es subgrupo de H)

Así , si H es finito ,

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

Notar que $N(\mathrm{K}) = N_{\mathrm{G}}(\mathrm{K})$ así

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

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 $\equiv 1(mod p)$
2. El número de p-subgrupos de Sylow de G es un divisor de | G | , mejor aun , este número es $[\mathrm{G} : N(\mathrm{P})]$, 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 :

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

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

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

$$\begin{array}{ccc} \mathrm{G} \times S & \longrightarrow & S \\ (g, \mathrm{H}) & \longrightarrow & g\mathrm{H}g^{-1} \end{array}$$

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

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

$$\mid Orb(\mathrm{P}) \mid = \sum_{\mathrm{P}' \in Orb(\mathrm{P})} \mid Orb_{\mathrm{P}}(\mathrm{P}') \mid$$

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

$$\Rightarrow \mid Orb(\mathrm{P}) \mid = 1 + \sum_{\mathrm{P}' \neq \mathrm{P}} p^{j_{\mathrm{P}'}} \equiv 1 mod(p)$$

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

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

$\mid Orb(\mathrm{H}') \mid = \mid \{g\mathrm{H}'g^{-1}/g \in \mathrm{P}\} \mid = [\mathrm{P} : N_{\mathrm{P}}(\mathrm{H}')] = p^l\, l \geq 1$

por lo tanto $p / \mid Orb(\mathrm{H}') \mid$, $\forall$ H' conjugado de H

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

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 $\mid \mathrm{G} \mid = p^k q$, 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 $\frac{|\mathrm{G}|}{|\mathrm{P}|} = [\mathrm{G} : \mathrm{P}]$, es decir , que $[\mathrm{G} : \mathrm{P}]$ no es divisible por P .

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

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

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

Pero:

$[N(\mathrm{P}) : \mathrm{P}] =\mid N(\mathrm{P})/\mathrm{P} \mid$ (grupo cuociente , pues $\mathrm{P} \lhd N(\mathrm{P})$)

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

Por contradicción , supongamos que el orden de $N(\mathrm{P})/\mathrm{P}$ es divisible por P .

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

$O([g]) = p$

$\Rightarrow [g]^p = [1] = \mathrm{P}$

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

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

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

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

Así p no divide a $\mid N(\mathrm{P})/\mathrm{P} \mid$

Aplicación

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

Sea G un grupo , con $\mid \mathrm{G} \mid = 15$.

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 = Número de 3− subgrupos de Sylow de $\mathrm{G} \equiv 1 mod(3) = [\mathrm{G} : N(\mathrm{P}_3)]$

$[\mathrm{G} : N(\mathrm{P}_3)][N(\mathrm{P}_3) : \mathrm{P}_3] = [\mathrm{G} : \mathrm{P}_3]$

Número de conjugados de P_3 es un divisor de $[\mathrm{G} : \mathrm{P}_3] = \frac{|\mathrm{G}|}{|\mathrm{P}_3|} = \frac{15}{3} = 5$

Hay dos divisores de 5 :

1. $1 \equiv 1 mod(3)$
2. $5 \equiv 2 mod(3)$

Pero sabemos que el número de conjugados de P_3 es $\equiv 1 mod(3)$, por lo tanto ,descartamos 2. y concluimos que P_3 no tiene másconjugados , i.e $\mathrm{P}_3 \triangleleft \mathrm{G}$.

$\mid \mathrm{P}_5 \mid = 5$

Número de conjugados de $\mathrm{P}_5 \equiv 1 mod(5) = [\mathrm{G} : N(\mathrm{P}_3)]$ divisor de $[\mathrm{G} : \mathrm{P}_5] = 3 \Rightarrow$ sólo uno , por lo tanto , $\mathrm{P}_5 \triangleleft \mathrm{G}$.

$\mathrm{P}_3 \cap \mathrm{P}_5$ es subgrupo de P_3 y P_5 , por lo tanto , debe dividir a $\mid \mathrm{P}_3 \mid = 3$ y a $\mid \mathrm{P}_5 \mid = 5$, $\Rightarrow \mathrm{P}_3 \cap \mathrm{P}_5 = \{1\}$.

(Se probará más adelante) $\Rightarrow \mathrm{P}_3\mathrm{P}_5 \cong \mathrm{P}_3 \times \mathrm{P}_5$

$\mathrm{G} = \mathrm{P}_3\mathrm{P}_5 \cong \mathrm{P}_3 \times \mathrm{P}_5$

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

$\Rightarrow$ 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

$\mathrm{G}_o = \{1\} \subset \mathrm{G}_1 \subset \cdots \subset \mathrm{G}_k = \mathrm{G}$, con

$\mid \mathrm{G}_i \mid = p^i \quad i = 0 \ldots k$, $\mathrm{G}_i \triangleleft \mathrm{G}$ $i = 0 \ldots k$

Dem.

Necesitaremos la propiedad ya vista siguiente :

Si H es un $p-$ grupo finito no trivial ($\mid \mathrm{H} \mid > 1$), entonces su centro es no trivial ($\mid Z(\mathrm{H}) \mid > 1$).

Por inducción en i :

Propiedad para i : $\exists$ cadena $\mathrm{G}_o \subset \mathrm{G}_1 \subset \cdots \subset \mathrm{G}_i$,

con $\mid \mathrm{G}_j \mid = p^j$, $\mathrm{G}_j \triangleleft \mathrm{G}$, $\forall j = 0 \ldots i$

$i = 0$:

$\mathrm{G}_o = \{1\} \triangleleft \mathrm{G}$ es cierta.

Pasemos de i a $i + 1$

Sea $\mathrm{L} = \mathrm{G}/\mathrm{G}_i$ grupo no trivial (pues $i+1 \leq k$)

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

$\Rightarrow$ L es $p-$ grupo no trivial

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

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

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

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

Por teorema de correspondencia , $\mathrm{K} = \mathrm{H}/\mathrm{G}_i$, con $\mathrm{H} \triangleleft \mathrm{G}$, $\mathrm{H} \supseteq \mathrm{G}_i$, $| \mathrm{H} | = [\mathrm{H} : \mathrm{G}_i] \mid \mathrm{G}_i |$

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

por lo tanto , podemos definir $\mathrm{G}_{i+1} = \mathrm{H}$ y tenemos

$\mathrm{G}_o \subset \mathrm{G}_1 \subset \cdots \subset \mathrm{G}_i \subset \mathrm{G}_{i+1}$, con $| \mathrm{G}_j | = p^j$

Estudiemos el problema siguiente :

G grupo , H, N subgrupos de G , $\mathrm{N} \triangleleft \mathrm{G}$. Bajo estas condiciones sabemos que
$\mathrm{N}\,\mathrm{H} = \{nh / n \in \mathrm{N}, h \in \mathrm{H}\}$ (subgrupo de G).

Agregemos además la hipótesis de que $\mathrm{N} \cap \mathrm{H} = \{1\}$. Queremos "entender" $\mathrm{N}\,\mathrm{H}$

Sean n_1h_1, $n_2h_2 \in \mathrm{N}\,\mathrm{H}$, $(n_1h_1)(n_2h_2) = [n_1(h_1n_2h_1^{-1})](h_1h_2)$. Podríamos definir en $\mathrm{N} \times \mathrm{H}$ una operación $(n_1h_1)(n_2h_2) = [n_1(h_1n_2h_1^{-1})](h_1h_2)$

Marco general:

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

$$\begin{array}{rccc} \Phi : & \mathrm{H} & \longrightarrow & Aut(\mathrm{N}) \\ & h & \longrightarrow & \Phi_h \end{array}$$

$\Phi_h(n_1n_2) = \Phi_h(n_1)\Phi_h(n_2)$

$\Phi_h(n) = hn$

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

Como conjunto , $\mathrm{N} \times_\Phi \mathrm{H} = \mathrm{N} \times \mathrm{H}$

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 :

$hn = n \ \forall n$

$\Phi_h(n) = id_{\mathrm{N}}(n) = n$

En este caso $\mathrm{N} \times_\Phi \mathrm{H} = \mathrm{N} \times \mathrm{H}$ 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 $\mathrm{N} \times_\Phi \mathrm{H}$, recién definido , es un grupo.

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

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

Volvamos por un momento a la situación original:

G grupo

N, H subgrupos

$\mathrm{N} \triangleleft \mathrm{G}$

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

En este caso , H actúa por conjugación sobre N :

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

Los elementos de $\mathrm{N\,H} \subseteq \mathrm{G}$ 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 $f: \begin{array}{ccc} \mathrm{N} \times_\Phi \mathrm{H} & \longrightarrow & \mathrm{N\,H} \\ (n,h) & \longrightarrow & n \cdot h \end{array}$ es un isomorfismo del grupo $\mathrm{N} \times_\Phi \mathrm{H}$ en el subgrupo de G , N H .

Dem.

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

Que f es sobreyectiva es directo.

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

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

Prop

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

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

y $\mathrm{N\,H} \cong \mathrm{N} \times \mathrm{H}$ ($(n,h) \to (n,h)$).

Dem.

Sólo hay que probar que N y H conmutan :

Sean $n \in \mathrm{N}$, $h \in \mathrm{H}$.

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

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

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

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

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

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

Directamente , $\widetilde{\mathrm{N}}$ y $\widetilde{\mathrm{H}}$ son subgrupos de G .

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

También :

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

¿Cuántos grupos de orden 6 hay ?

$|\ \mathrm{G}\ | = 6 = 2 \cdot 3$

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

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

$\mathrm{P}_2 \cap \mathrm{P}_3 = \{1\}$

Número de conjugados de $\mathrm{P}_2 \equiv 1 mod(2)$, además debe dividir a $3 \Rightarrow 1, 3$

Hay dos posibilidades:

1. Existe un $2-$ subgrupo de Sylow $\Rightarrow \mathrm{P}_2 \triangleleft \mathrm{G}$
2. Existen 3 $2-$ subgrupos de Sylow$\Rightarrow$ no son normales.

Número de conjugados de $\mathrm{P}_3 \equiv 1 mod(3)$, divisor de $2 \Rightarrow 1$, por lo tanto, $\mathrm{P}_3 \triangleleft \mathrm{G}$.

Revisemos las posibilidades para P_2 :

En la situación 1.

$\mathrm{P}_2, \mathrm{P}_3 \triangleleft \mathrm{G}$, $\mathrm{P}_2 \cap \mathrm{P}_3 = \{1\}$

$\Rightarrow \mathrm{P}_2\,\mathrm{P}_3 \cong \mathrm{P}_2 \times \mathrm{P}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ 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.

$\mathrm{G} = \mathrm{P}_3\mathrm{P}_2 \cong \mathrm{P}_3 \times_\Phi \mathrm{P}_2 \cong \mathbb{Z}_3 \times_\Phi \mathbb{Z}_2$

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

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

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

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

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 $\mathbb{Z}_n$.

$$\begin{array}{rccc} f: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & a +_n b & \longrightarrow & f(a +_n b) = f(a) +_n f(b) \end{array}$$

$$\begin{array}{ccc} f(1+1) & = & f(1) + f(1) \\ \vdots & \vdots & \vdots \\ f(k) & = & k \cdot f(1) \end{array}$$

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

$$\forall z \in \mathbb{Z}_n\ , \quad f_z : \begin{array}{ccc} \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ k & \longrightarrow & kz \end{array}$$

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

¿Biyectivos?

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

$(Aut(\mathbb{Z}_n), \circ) \cong (\mathbb{Z}_n^x, \cdot_n)$ ($\mathbb{Z}_n^x$: 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 $\phi : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_3$, 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 :

$(n_1, h_1) \cdot (n_2, h_2) = (n_1 +_3 \phi_{h_1}(n_2), h_1 +_2 h_2) = (n_1 +_3 (-1)^{h_1} n_2, h_1 +_2 h_2)$ Cnclusión: 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:

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

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

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

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

Definición

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

Observación:

No toda permutación es un ciclo . Por ejemplo :

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

σ es producto (composición) de dos ciclos :

$\tau_1 = (1\,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ $\qquad$ $\tau_2 = (3\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

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

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). $\sigma = \sigma_1 \circ \cdots \circ \sigma_l$ σ_j y σ_i disjuntos $\forall j \neq i$.

Dem.

Sea G $=< \{\sigma\} >= \{1, \sigma, \sigma^2, \dots, \sigma^r\}$ 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 $m_j =\mid O_j \mid$(convencerse de que σ es $\sigma_1 \circ \dots \circ \sigma_l$).

La unicidad , (salvo orden de los factores) sale de que si $\sigma = \widetilde{\sigma_1} \circ \dots \circ \widetilde{\sigma_r}$, con los $\widetilde{\sigma_j}$ ciclos disjuntos , entonces las órbitas (de cardinal > 1) de σ , serán los ciclos de los $\widetilde{\sigma_j}$.

Observación:

1. Si $\sigma \in S_n$ es un ciclo de largo k , $O(\sigma) =\mid \{\sigma^i / i \in \mathbb{Z}\} \mid = k$
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 $\sigma = \sigma_1 \circ \dots \circ \sigma_k$ $O(\sigma) = mcm$(largo de susu 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 $\sigma \in S_n$, $\sigma = (i_1\ i_2 \ldots i_k)(j_1 \ldots)$ σ no conmuta con $\tau = (i_k\, j_1)$.
$\tau \circ \sigma \circ \tau = (i_1\, i_2 \ldots j_1)(i_k \ldots) \neq \sigma$,
si no ,$\sigma = (i_2\, i_3 \ldots)$ 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 :

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

Prop

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

Dem.

Por columnas:

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

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 :

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

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

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

Además , $sgn(\sigma) = 1$ si σ se descompone como un número par de traspocisiones y $sgn(\sigma) = -1$ 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 $A_n = \text{Ker}(sgn) \triangleleft S_n$ $A_n = \{\sigma \in S_n / \sigma \text{ es par } \}$.

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 :

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

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

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) $(i\,j)(j\,k) = (i\,j\,k)\ \ i \neq j \neq k$
   (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 , $A_n =< \{\sigma^2/\sigma \in S_n\} >$.

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 :

$f(a,b) = (b,a)$ intercambia H_1 con H_2

$g(a,b) = (a,a+b)$ intercambia H_3 con H_2

Prop

A_n es un subgrupo característico de S_n .

Dem.

$A_n =< \{\sigma^2 / \sigma \in S_n\} >$

Si $f : S_n \to S_n$ es automorfismo$\Rightarrow f(A_n) =< \{f(\sigma^2)/\sigma \in S_n\} >$

$$=< \{f(\sigma)^2/\sigma \in S_n\} >$$
$$=< \{\tau^2/\tau \in S_n\} >$$
$$= A_n$$

Ejercicios

1. Si $f : \mathrm{G} \to \mathrm{K}$ es un morfismo de grupos , y $A \subseteq \mathrm{G}$, entonces $f(< A >) =< f(A) >$.
2. Si $f \in End(S_n)$, entonces $f(A) \subseteq A$.

Corolario

Si $\mathrm{N} \triangleleft A_n$ y $f : S_n \to S_n$ es automorfismo , entonces $f(\mathrm{N}) \triangleleft A_n$.

Prop

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

Dem.

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

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

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

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

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

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

($\tau_1 \neq \tau$ 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 $(k\,l)(j\,m)$ $m \notin \{i,j,k,l\}$ $(n \geq 5) \Rightarrow (i\,j)(k\,l)(k\,l)(j\,m) = (i\,j\,m) \in$ 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 $\sigma = (i,j,k,\ldots)$ (tiene ciclo de largo ≥ 3).

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

$\tau\sigma\tau = (i\,j\,l\ldots)$, σ no conmuta con con $\tau\sigma\tau$. Calculemos:

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

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 .$\Rightarrow N_{S_n}(\mathrm{N}) = A_n$.

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

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

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

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

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

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

Si $\sigma \in \mathrm{N} \Rightarrow \sigma$ conmuta con $\tau\sigma\tau$ $\forall$ trasposición τ . Por el lema anterior $\Rightarrow O(\sigma) = 2 \Rightarrow \forall\sigma \in \mathrm{N}$, $\forall\sigma \in \tau\mathrm{N}\tau$, $O(\sigma) \leq 2 \Rightarrow \forall\sigma \in A_n$, $O(\sigma) \leq 2$
$\rightarrow\leftarrow$ (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 $\cdot$.$(\mathrm{R}, +, \cdot)$ se dice anillo ssi:

1. $(\mathrm{R}, +)$ 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 $(\mathrm{R}, +, \cdot)$ es un anillo , entonces $(\forall a, b \in \mathrm{R})$:

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

Así , 0 no puede tener inverso para $\cdot$.

Definición

Si $(\mathrm{K}, +, \cdot)$ es un anillo conmutativo , se dice cuerpo ssi todo $a \in \mathrm{K} \setminus \{0\}$ 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 $(\mathrm{R} \setminus \{0\}, \cdot)$ es grupo abeliano.

Definición

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

Definición

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

***Ejercicio* :**

- Un anillo R NO tiene divisores del 0 ssi todo $a \in \mathrm{R} \setminus \{0\}$ es cancelable para $\cdot$
- En un anillo R , todo $a \in \mathrm{R}$ 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 $(\mathrm{K}, +, \cdot)$ es dominio de integridad .(por ejemplo : $(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Q}, +, \cdot)$).
- $(\mathbb{Z}_m, +, \cdot)$ es anillo conmutativo ($m \geq 2$).
  $\mathbb{Z}_m = \{[n]_{\equiv_m} / n \in \mathbb{Z}\}$
  $x \equiv_m y \Leftrightarrow x - y \in m \cdot \mathbb{Z}$
  $\left.\begin{array}{c} n_1 \equiv_m n_2 \\ l_{1 \equiv_m} l_2 \end{array}\right\} n_1 \cdot l_{1 \equiv_m} n_2 \cdot l_2$, 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 $\mathrm{R}[x] = \{(a_o, a_1, \ldots, a_n, \ldots) \in \mathrm{R}^{\mathbb{N}} / (\exists n_o)\ tq\ a_n = 0\, \forall n \geq n_o\}$.

Definamos las siguientes operaciones en $\mathrm{R}[x]$:

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

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

Llamamos $x = (0, 1, 0, \ldots, 0, \ldots) \in \mathrm{R}[x]$, de esta forma ,$x^n = \underbrace{x \cdot \ldots \cdot x}_{n\, veces} = (0, \ldots, 0, \underset{\substack{\uparrow \\ i}}{1}, 0, \ldots)$ y , por lo tanto , $(a_o, a_1, \ldots, a_n, 0, \ldots) = \sum_{i=0}^{n} a_i \cdot x^i$, donde identificamos los elementos $a \in \mathrm{R}$ con $(a, 0, \ldots, 0, \ldots) \in \mathrm{R}[x]$. Identificación justificada por el hecho que la función $f : \begin{array}{ccc} \mathrm{R} & \longrightarrow & \mathrm{R}[x] \\ a & \longrightarrow & (a, 0, \ldots, 0, \ldots) \end{array}$ es una inyección que preserva $+$ y $\cdot$: $f(a+b) = f(a) + f(b)$ y $f(a \cdot b) = f(a) \cdot f(b)$.

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

Definición

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

Convenciones:

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

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

Prop

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

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

Observaciones:

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

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

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

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

Es decir , $p(x) = a_o + a_1 \cdot x + \ldots + a_n \cdot x^n \in \mathrm{R}[x]$

$p(a) = a_o + a_1 \cdot a + \ldots + a_n \cdot a^n \in \mathrm{R}$

Definición

$a \in \mathrm{R}$ se dice raíz de $p(x) \in \mathrm{R}[x]$ 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 $a_1, \ldots, a_k \in \mathrm{R}$ son raíces de $p(x)$ distintas entre sí, entonces $(x-a_1)\cdot(x-a_2)\cdots(x-a_k)/p(x)$.

Corolario

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

Corolario

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

Dem.

$\Rightarrow$) $\forall a \in \mathrm{R}\ p(a) = q(a) \Rightarrow p(x) - q(x)$ tiene a todo $a \in \mathrm{R}$ 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 , $\mathrm{R} = \{r_o, \ldots, r_k\}$, entonces $p(x) = (x - r_o) \cdot (x - r_1) \cdots (x - r_k) \in \mathrm{R}[x]$. $\mathrm{gr}(p(x)) = k + 1 \Rightarrow p(x) \neq 0$ .Sin embargo , la función polinomial asociada a $p(x)$ es la función nula $(\forall i \in \{0, \ldots, k\}\, p(r_i) = 0)$. Es decir , $p(x)$ y 0 tienen la misma función polinomal asociada.

Definición

Si R yP son anillos , un morfismo (u homomorfismo) de R a P , será una función $f : \mathrm{R} \longrightarrow \mathrm{P}$ tal que:

1. $(\forall r_1, r_2 \in \mathrm{R})\ f(r_1 + r_2) = f(r_1) + f(r_2)$
2. $(\forall r_1, r_2 \in \mathrm{R})\ f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$
3. $f(1_{\mathrm{R}}) = 1_{\mathrm{P}}$

Observación:

1. y 2. no implican 3. Por ejemplo: $f : \begin{array}{ccc} \mathrm{R} & \longrightarrow & \mathrm{P} \\ r & \longrightarrow & f(r) = 0 \end{array}$ Satisface 1. y 2. pero no 3.

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 $1 \in \mathrm{R}$ y tal que con $+$ y $\cdot$ restringidos es anillo .

Definición

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

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

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

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

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

Observemos que :

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

$x - x' \in \mathrm{I} \Leftrightarrow (\exists z \in \mathrm{I})\, x = x' + z$

$y - y' \in \mathrm{I} \Leftrightarrow (\exists u \in \mathrm{I})\, y = y' + z$

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

Tenemos así en R/I dos leyes:

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

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

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

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

Prop

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

Dem.

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

Sea I un ideal de R , la función $\nu : \begin{array}{ccc} \mathrm{R} & \longrightarrow & \mathrm{R/I} \\ x & \longrightarrow & [x] \end{array}$ es un morfismo de anillos.

$\mathrm{Ker}\nu = \mathrm{I}$, 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:

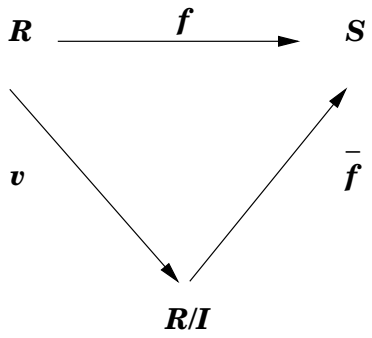
Ideales en $(\mathbb{Z}, +, \cdot)$.

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 $\overline{f} : R/I \longrightarrow S$ tal que el diagrama siguiente conmuta:



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

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

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

Ejemplo:

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

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

Dem:

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

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

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

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

Ideales generados por Subconjuntos

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

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

Ejercicio:

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

Observación:

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

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

Resulta :

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

Ejemplo de anillos no conmutativos:

1. Sea K un cuerpo , $n \geq 2$. $R = \{(a_{ij})_{i,j=1...n} / a_{ij} \in K\}$ 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 $\cdot$:
   $(a, v) \cdot (b, w) = (a \cdot b - < v, w >, a \cdot w + b \cdot v + v \times w)$
   $(a, v)^{-1} = \frac{\overline{(a,v)}}{\|(a,v)\|^2}$ 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 $\varphi : \begin{array}{ccc} R & \longrightarrow & K \\ a & \longrightarrow & [(a, 1)] \end{array}$ es un monomorfismo de anillos y que identificando $a \in R$ con $\varphi(a) = [(a, 1)] \in K$ 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 = "cuerpo de fracciones de R ".

2.4 Algo de Divisibilidad en Anillos

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

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

Definición

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

Notación :

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

Definición

(Divisibilidad) . Sean $a, b \in \mathrm{R}$. Decimos que a "divide" a b ssi $(\exists c \in \mathrm{R})$ 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 $a, b \in \mathrm{R}$. Un elemento $c \in \mathrm{R}$ 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 : $(\forall d \in \mathrm{R})\ d/a \wedge d/b \Rightarrow d/c$

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 $a, b \in \mathrm{R}$, con alguno de los dos distinto de 0 , entonces $\exists c$ m.c.d de a, b .

Dem.

Considerar $\mathrm{I} = (a, b)$, por ser dip , $\mathrm{I} = (c)$, con $c \in \mathrm{R}$.
$a \in (c) \Rightarrow c/a$
$b \in (c) \Rightarrow c/b$
, 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 $(a, b) = \{\alpha \cdot a + \beta \cdot b / \alpha, \beta \in \mathrm{R}$, $(a, b) = (c) = \alpha \cdot a + \beta \cdot b / \alpha, \beta \in \mathrm{R}$ **Igualdad de Bezout**

Ejercicio:

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

Corolario

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

Dem.

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

Definición

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

Prop

Todo dip es dominio de factorización única .

Dem.

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

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

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

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 $\mathrm{I} = \bigcup_{n \in \mathbb{N}} (a_n)$

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

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

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

$\Rightarrow S = \emptyset$

2. Unicidad de la descomposición

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

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

(Si p_k y q_1 son primos relativos , $p_k / q_1 (q_2 \cdots q_l) \Rightarrow p_k / (q_2 \ldots q_l)$, 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 $i = 1 \ldots l$.

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

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

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

$p_{k-j} \sim q_{k-j}$

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"

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

Tal que:

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

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 $\alpha \in \mathbb{Z}, a \in A$,

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

Después de multiples inducciones se concluye que A , "con esta multiplicación por escaler" , resulta un $\mathbb{Z}$ - módulo .

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

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

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

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

$\Rightarrow \alpha m = (-\alpha)(-m) = (-m)+\ldots+(-m)\ -\alpha\, veces$

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$[x]$ $(a \longrightarrow a + 0 \cdot x + \ldots)$. Se puede restringir la "multiplicación por escalar" a escalares de K : $\mathrm{K} \times \mathrm{M} \longrightarrow \mathrm{M}$, con lo que M resulta ser un K - espacio vectorial.

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

$x(m_1 + m_2) = xm_1 + xm_2 \forall m_1, m_2 \in \mathrm{M}$

$x(\alpha m) = \alpha(xm)\ \forall \alpha \in \mathrm{K}, \forall m \in \mathrm{M}$

Así , la función $T:\ \begin{array}{ccc} \mathrm{M} & \longrightarrow & \mathrm{M} \\ m & \longrightarrow & xm \end{array}$

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 $T : V \longrightarrow V$, 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":

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

Facilmente se prueba que si $p(x), q(x) \in \mathrm{K}[x]$ entonces $p \cdot q(T) = p(T) \cdot q(T)$, y de ahí resulta que la "ley de composición externa" $\begin{array}{ccc} \mathrm{K}[x] \times V & \longrightarrow & V \\ (p(x), v) & \longrightarrow & p(x)v \ = p(T)(v) \end{array}$

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 $\mathrm{N} \subseteq \mathrm{M}$ tal que :

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

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: $(\forall r_1, r_2 \in \mathrm{R})(\forall n_1, n_2 \in \mathrm{N})\ r_1 n_1 + r_2 n_2 \in \mathrm{N}$

Ejemplo 1:

Los submódulos de un K - módulo: subespacios vectoriales.

Ejemplo2:

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 $S : V \to V$ 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 . $r \in \mathrm{R}, m \in \mathrm{M}$

$rm = 0$ 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 $\exists r \in \mathrm{R} \setminus \{0\}$ tal que $rm = 0$.

Ejemplo:

Si R es un dominio de integridad , y M es un R - módulo , entonces : $T\mathrm{M} = \{m \in \mathrm{M}/m$ 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 $T : \mathrm{M} \to \mathrm{N}$ tal que:

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

Ejemplo 1:

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

Ejemplo 2:

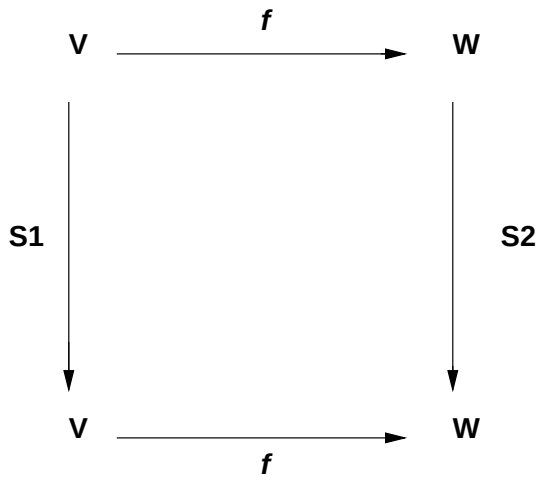
Si $\mathrm{R} = \mathbb{Z}$, como $\mathbb{Z}-$ módulo y grupo abeliano es lo mismo , resulta que las transformaciones lineales entre $\mathbb{Z}$ - módulos simplemente son los morfismos de grupos.

Ejemplo 3:

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

Sea $f : V \longrightarrow W$ 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 $x \in \mathrm{K}[x]$, queremos que $f(xv) = xf(v)$ $(\forall v \in V)$, i.e $f(S_1(v)) = S_2 f(v)$ $\forall v \in V$



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:

$[x] = [y] \wedge v \in \mathrm{R} \Rightarrow [rx] = [ry]$, por lo tanto , queda bien definida en M/$\mathbb{N}$ 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 ν : 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 .

$$\mathrm{N} \subseteq \mathrm{P} \subseteq \mathrm{M} \overset{\nu}{\longrightarrow} \mathrm{P/N}$$

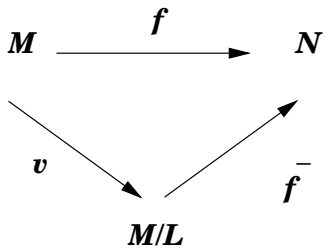
Relevancia de Ker$f$, Imf si f : M $\longrightarrow$ N es R - lineal:

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

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

Teorema del Factor

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



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

f inyectiva $\Leftrightarrow$ L $=$ Ker$f$ (Ker$\overline{f}$ $=$ (Ker$f$)/L

f sobreyectiva $\Leftrightarrow$ $\overline{f}$ sobreyectiva (Im$\overline{f}$ $=$ Imf)

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
   $[n]_{\mathrm{N}\cap\mathrm{L}} \longrightarrow [n]_{\mathrm{L}}$
2. Si M es R - módulo y N $\subseteq$ L $\subseteq$ M submódulo , entonces
   (M/N)/(L/N) $\cong$ M/L
   $[[x]_{\mathrm{N}}]_{\mathrm{L/N}} \longrightarrow [x]_{\mathrm{L}}$

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 :

$$< A >= \bigcap_{\substack{A \subseteq \mathrm{N} \\ \mathrm{N}\, submodulo}} \mathrm{N}$$

$< A >$ es un submódulo , y es el más pequeño de los que contienen a A .

Claramente $< A >= \{\sum_{i=1}^{n} r_i a_i / n \in \mathbb{N}, r_i \in \mathrm{R}, a_i \in A\}$. $< A >$ consiste en las combinaciones lineales finitas de elementos de A .

Suma de Submódulos

Sea M un R - módulo , y $\{\mathrm{M}_\lambda : \lambda \in \Lambda\}$ una familia cualquiera de submódulos de M . La suma de la familia es :

$$+_{\lambda\in\Lambda}\mathrm{M}_\lambda =< \bigcup_{\lambda\in\Lambda} \mathrm{M}_\lambda >$$

$+_{\lambda\in\Lambda}\mathrm{M}_\lambda$ consiste en las sumas finitas de elementos en los distintos M_λ , i.e

$+_{\lambda\in\Lambda}\mathrm{M}_\lambda = \{\sum_{i=1}^{n} m_{\lambda_i} / n \in \mathbb{N}, \lambda_i \in \Lambda, m_{\lambda_i} \in \mathrm{M}_{\lambda_i}\}$

Definición

La suma se dice directa , y se anota $\bigoplus_{\lambda\in\Lambda} \mathrm{M}_\lambda$ $(= +_{\lambda\in\Lambda}\mathrm{M}_\lambda$) ssi :
$(\forall \widetilde{\lambda} \in \Lambda)$ $\mathrm{M}_{\widetilde{\lambda}} \cap (+_{\lambda\in\Lambda\setminus\{\widetilde{\lambda}\}}\mathrm{M}_\lambda) = \{0\}$.

Prop (*Ejercicio*)

Las siguientes proposiciones son equivalentes:

1. La suma $\mathrm{N} = +_{\lambda\in\Lambda}\mathrm{M}_\lambda$ es directa
2. Todo $n \in$ N se escribe de manera única como suma finita de elementos de los M_λ
3. $\forall\{\lambda_1 \ldots \lambda_k\} \subseteq \Lambda$, con $\lambda_i \neq \lambda_j$ si $i \neq j$, se tiene que $m_{\lambda_1} + \ldots + m_{\lambda_k} = 0$, $m_{\lambda_i} \in \mathrm{M}_{\lambda_i} \Rightarrow m_{\lambda_1} = \cdots = m_{\lambda_k} = 0$

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 $\cdot$:

- $(m_\lambda)_{\lambda\in\Lambda} + (\overline{m}_\lambda)_{\lambda\in\Lambda} = (m_\lambda + \overline{m}_\lambda)_{\lambda\in\Lambda} \qquad (m+\overline{m})(\lambda) = m(\lambda) + \overline{m}(\lambda)$
- Multiplicación por escalar en R : $r(m_\lambda)_{\lambda\in\Lambda} = (rm_\lambda)_{\lambda\in\Lambda} \qquad (rm)(\lambda) = rm(\lambda)$

Ejercicio:

M , con las operaciones recién definidas , es un R - módulo.

Prop (*Ejercicio*)

Sea $\lambda_o \in \Lambda$. Definamos

$f_{\lambda_o} : M_{\lambda_o} \longrightarrow M = \prod_{\lambda\in\Lambda} M_\lambda$

$$m_o \longrightarrow (m_\lambda)_{\lambda\in\Lambda} \qquad \text{con } m_\lambda = \begin{cases} 0 & \text{si} \quad \lambda \neq \lambda_o \\ m_o & \text{si} \quad \lambda = \lambda_o \end{cases}$$

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" :

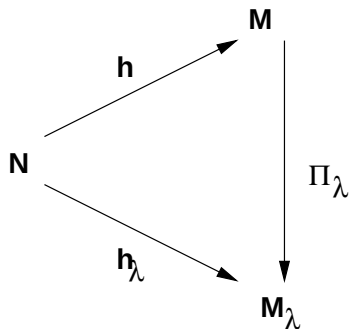
$\pi_{\lambda_o} : M \longrightarrow M_{\lambda_o}$

$(m_\lambda)_{\lambda\in\Lambda} \longrightarrow \pi_{\lambda_o}((m_\lambda)_{\lambda\in\Lambda}) = m_{\lambda_o}$

$m \longrightarrow m(\lambda_o)$ (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 $\{h_\lambda : N \to M_\lambda\}_{\lambda\in\Lambda}$, $\exists!$ morfismo de R - módulos $h : N \to M$, con $M = \prod_{\lambda\in\Lambda} M_\lambda$ tal que , $(\forall\lambda\in\Lambda)$ el diagrama siguiente conmuta :



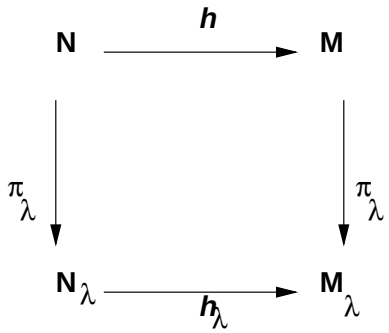
i.e $\pi_\lambda \circ h = h_\lambda$

Dem.

$h(n) = (h_\lambda(n))_{\lambda\in\Lambda}$, la unicidad es directa .

Corolario

Si $\{\mathrm{M}_\lambda\}_{\lambda\in\Lambda}$ y $\{\mathrm{N}_\lambda\}_{\lambda\in\Lambda}$ son familias de R - módulos , indexadas por el mismo Λ , y $\{h_\lambda : \mathrm{N}_\lambda \longrightarrow \mathrm{M}_\lambda\}_{\lambda\in\Lambda}$ una familia de transformaciones R - lineales , entonces $\exists!$ morfismo de R -módulos $h : \mathrm{N} = \prod_{\lambda\in\Lambda} \mathrm{N}_\lambda \longrightarrow \prod_{\lambda\in\Lambda} \mathrm{M}_\lambda = \mathrm{M}$ 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 $\widetilde{M} = \{(m_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda / m_\lambda = 0$ para todos los $\lambda \in \Lambda$ salvo tal vez , un número finito de ellos (para casi todo $\lambda \in \Lambda)\}$.

Es directo que $\widetilde{M}$ es un submódulo de $M = \prod_{\lambda\in\Lambda} M_\lambda$, llamamos a este submódulo $\widetilde{M} \subseteq M$ la "suma directa de los M_λ ".

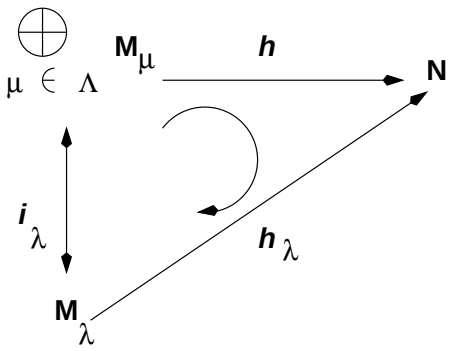
Observaciones:

1. $(\forall\lambda_o \in \Lambda)$ $\mathrm{Im}(f_{\lambda_o}) \subseteq \widetilde{M}$, por lo tanto , podemos considerar esta función llegando a $\widetilde{M}$, anotemosla $i_{\lambda_o} : M_{\lambda_o} \to \widetilde{M}$ (monomorfismo) (inyección canónica). Podemos entonces identificar M_{λ_o} con $i_{\lambda_o}(M_{\lambda_o}) \subseteq \widetilde{M}$.

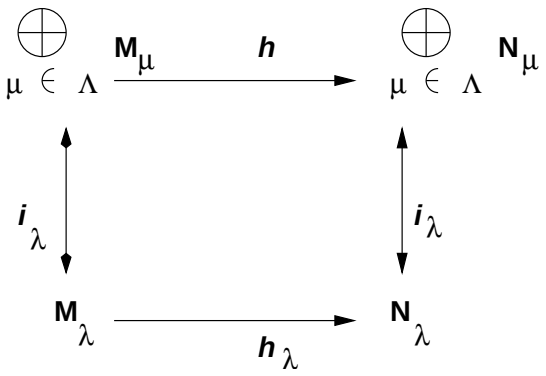
2. Todo $m \in \widetilde{M}$ es suma finita de elementos de los distintos M_λ :
$m = (m_\lambda)_{\lambda\in\Lambda} = \sum_{\lambda\, tq\, m_\lambda \neq 0} m_\lambda$, así $\widetilde{M} =< \bigcup_{\lambda\in\Lambda} M_\lambda >= +_{\lambda\in\Lambda} M_\lambda$, además $\widetilde{M} = \bigoplus_{\lambda\in\Lambda} M_\lambda$.

Ejercicios:

1. Si $\{M_\lambda\}_{\lambda\in\Lambda}$ es una familia de R - módulos , N es otro R - módulo y $\{h_\lambda : M_\lambda \longrightarrow N\}_{\lambda\in\Lambda}$ es una familia de transformaciones R -lineales, entonces $\exists!$ transformación R - lineal $h : \bigoplus_{\lambda\in\Lambda} M_\lambda \to N$ 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 $\{h_\lambda : M_\lambda \to N_\lambda\}_{\lambda\in\Lambda}$ es una familia de transformaciones lineales , $\exists!$ $h : \bigoplus_{\lambda\in\Lambda} M_\lambda \to \bigoplus_{\lambda\in\Lambda} N_\lambda$, R -lineal tal que $(\forall\lambda \in \Lambda)$ el diagrama siguiente conmuta :



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 $r/ \mid$ M $\mid$, 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 $f : M \to N$ 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 $f(\sum_{\lambda\in I} r_\lambda m_\lambda) = \sum_{\lambda\in I} r_\lambda f(m_\lambda)$.

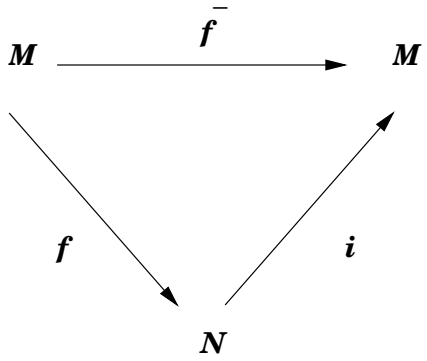
$\Leftarrow$) Supongamos que $\sum_{\lambda\in I} r_\lambda m_\lambda = 0$ .Sea $\lambda_o \in I$, y definamos la sgte función $f : \mathrm{M} \longrightarrow \mathrm{R}$ tal que :

$m_{\lambda_o} \to 1$

$m_\lambda \to 0 \qquad \forall \lambda \neq \lambda_o$, 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 $r_\lambda = 0\ \forall \lambda \in I$, por lo tanto , $\{m_\lambda\}_{\lambda\in I}$ es familia l.i

Veamos ahora que $\{m_\lambda\}_{\lambda\in I} = B$ genera M .

Sea $\mathrm{N} =< B >$ $(\forall \lambda \in \Lambda)$ seleccionemos $n_\lambda = m_\lambda \in \mathrm{N} \Rightarrow \exists!$ una función lineal $f : \mathrm{M} \to \mathrm{N}$ tal que $f(m_\lambda) = m_\lambda$ $(\forall \lambda \in \Lambda)$



Tomemos $\overline{f} : \mathrm{M} \to \mathrm{M}$ como la composición $i \circ f$, donde $i : \mathrm{N} \hookrightarrow \mathrm{M}$ es la inclusión . Como $(\forall \lambda \in \Lambda)\overline{f}(m_\lambda) = i(f(m_\lambda)) = f(m_\lambda) = m_\lambda$. $\overline{f} : \mathrm{M} \to \mathrm{M}$ es la única función lineal tal que $m_\lambda \to m_\lambda$, por lo tanto , $\overline{f} = id_{\mathrm{M}} \Rightarrow \mathrm{Im}\overline{f} = \mathrm{Im}(id_{\mathrm{M}}) = \mathrm{M}$, pero de la construcción de $\overline{f}$, $\mathrm{Im}\overline{f} = \mathrm{Im}(i \circ f) = \mathrm{Im}f \subseteq \mathrm{N} =< B >$, por lo tanto , $\mathrm{M} \subseteq < B > (\subseteq \mathrm{M}) \Rightarrow \mathrm{M} =< B >$.

Módulo libre sobre un conjunto A

Sea R anillo conmutativo. Si a es un elemento , podemos construir $\mathrm{R}_a = \mathrm{R} \times \{a\} = \{(r, a)/r \in \mathrm{R}\}$, 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 $\{1\} \Rightarrow \mathrm{R}_a$ es libre con base $\{(1, a)\}$. Anotaremos $(1, a) = a \in \mathrm{R}_a$, por lo tanto , diremos que R_a es libre con base $\{a\}$. Como $r(1, a) = (r, a)$, se tiene $\mathrm{R}_a = \{ra/r \in \mathrm{R}\} = \mathrm{R}a$.

Si ahora hacemos esto $\forall a \in A$, tenemos una familia de módulos libres $\{\mathrm{R}_a\}_{a\in A}$, con R_a de base $\{a\}$. Anotamos $F_A = \bigoplus_{a\in A} \mathrm{R}_a$.

Prop

F_A es libre con base A .

Dem.

$\forall x \in F_A$, x es suma finita de elementos en los sumandos

$x = \underbrace{x_1}_{\in \mathrm{R}a_1} + \cdots + \underbrace{x_k}_{\in \mathrm{R}a_k} = ra_1 + \cdots + r_k a_k$, $r_i \in \mathrm{R}$, $a_i \in A$, con esto , A genera F_A , por otro lado , si $\sum_{i=1}^{k} r_i a_i = 0$ para $r_i \in \mathrm{R}, a_i \in A$ distintos entre sí.

Recordemos que a_i visto como elemento de F_A es $(0, \ldots, 0, a_i, 0, \ldots, 0)$, por lo tanto , $\sum_{i=1}^{k} r_i a_i = (0 \ldots, r_j a_j, \ldots, 0, \ldots, r_i a_i, 0 \ldots) = 0 \Leftrightarrow r_j a_j = 0$ en $\mathrm{R}a_j \ \forall j \Leftrightarrow r_j = 0 \ \forall j$.

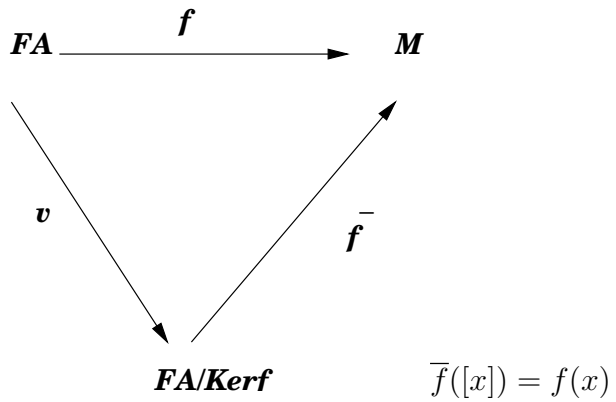
Prop

Todo R -módulo es cuociente de algún R -módulo libre (mas bien isomorfo).

Dem.

Sea M un R -módulo. Sea $A \subseteq \mathrm{M}$ un generador : $< A >= \mathrm{M}$ .Aplicando la construcción anterior , $A \subseteq F_A$.

Por la caracterización de módulo libre con base A , $\exists!$ función lineal $f : F_A \to \mathrm{M}$ tal que $(\forall a \in A)\ f(a) = a$. f es un epimorfismo $\Rightarrow$



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

La función lineal inducida en el cuociente $\overline{f} : F_A/\mathrm{Ker}f \to \mathrm{M}$, es un isomorfismo.

¿Que hay en Ker$f$?

$x \in \mathrm{Ker}f \Leftrightarrow x = r_1 a_1 \oplus \cdots \oplus r_k a_k$, $f(x) = 0$ 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 $\Rightarrow \mathrm{M} \cong \mathrm{N}$.

Dem.

Por la caracterización de módulos libres , $\exists!$ función lineal $f : \mathrm{M} \to \mathbb{N}$ tal que $f(b_\lambda) = c_\lambda \ \forall \lambda \in \Lambda$. Si se prefiere mirar a N como el módulo libre , $\exists!$ función lineal $g : \mathrm{N} \to \mathrm{M}$ tal que $g(c_\lambda) = b_\lambda \ \forall \lambda \in \Lambda$, compongamos :

$$\begin{array}{ccccc} & f & & g & \\ \mathrm{M} & \longrightarrow & \mathrm{N} & \longrightarrow & \mathrm{M} \\ b_\lambda & \longrightarrow & c_\lambda & \longrightarrow & b_\lambda \end{array}$$

$g \circ f : \mathrm{M} \to \mathrm{M}$ es lineal tal que $g \circ f(b_\lambda) = b_\lambda$, por lo tanto , por la caracterización de modulos libres , $g \circ f(b_\lambda) = id_{\mathrm{M}}$. Construyendo $f \circ g$, resulta $f \circ g = id_{\mathrm{N}} \Rightarrow f$ 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 $\mathrm{N} \subseteq \mathrm{M}$ submódulo , entonces N , ni siquiera tiene por que ser libre.

Ejemplo:

$\mathrm{R} = (\mathbb{Z}_6, +, \cdot)$ 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. $\mathrm{I} = (2) = \{0, 2, 4\}$ es un ideal y no es libre.

Hay casos donde estas cosas andan bien , por ejemplo $\mathrm{R} = \mathbb{Z}$ 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 $\mathrm{M} \subseteq \mathrm{L}$ 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 : $\mathrm{L}_{\Lambda'} =< \{b_\lambda\}_{\lambda \in \Lambda} >$. Llamamos $\mathrm{M}_{\lambda'} = \mathrm{M} \cap \mathrm{L}_{\Lambda'}$.

Interesará considerar aquellos casos en que $\mathrm{M}_{\lambda'}$ es libre , con base $\{m_\mu\}_{\mu \in \Gamma}$ y $\mid \Gamma' \mid \leq \mid \Lambda' \mid$.

Trabajaremos con tuplas de la forma $(\Lambda', \mathrm{L}_{\Lambda'}, \mathrm{M}_{\Lambda'}, m' = \{m_\mu\}_{\mu \in \Gamma})$, 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 $\Lambda' = \Lambda$ ($\Rightarrow \mathrm{L}_\Lambda = \mathrm{L}$, $\mathrm{M}_\Lambda = \mathrm{M}$, y por lo tanto , M es submódulo libre de L , con base de cardinal $\leq \mid \Lambda' \mid = \mid \Lambda \mid$).

Usaremos Zorn. Ordenemos A :

Diremos que

$(\Lambda', \mathrm{L}_{\Lambda'}, \mathrm{M}_{\Lambda'}, m' = \{m_\mu\}_{\mu\in\Gamma'}) \leq (\Lambda'', \mathrm{L}_{\Lambda''}, \mathrm{M}_{\Lambda''}, m'' = \{m''_\mu\}_{\mu\in\Gamma''}) \Leftrightarrow \Lambda'' \subseteq \Lambda'$ ($\Rightarrow \mathrm{M}_{\Lambda'} \subseteq \mathrm{M}_{\Lambda''}$) y la base m'' de $\mathrm{M}_{\Lambda''}$ es una extensión de la base m' de $\mathrm{M}_{\Lambda'}$, 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 $(\Lambda' = \emptyset, \mathrm{L}_{\Lambda'} = \{0\}, \mathrm{M}_{\Lambda'} = \{0\}, m' = \emptyset \ \ (\Gamma' = \emptyset)) \in A$.

Veamos que $(A, \leq)$ tiene las hipótesis que requiere el lema de Zorn:

- $A \neq \emptyset$
- Sea $\{(\Lambda'_i, \mathrm{L}_{\Lambda'_i}, \mathrm{M}_{\Lambda'_i}, m'_i = \{m^{(i)}_\mu\}_{\mu\in\Gamma'_i})\}_{i\in I} = \zeta$ 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 $\mathrm{M}_{\Lambda'}$ tendremos la base $m' = \{m_\mu\}_{\mu\in\Gamma'}$, con $\Gamma' = \bigcup_{i\in I} \Gamma'_i$ y $m_\mu = m^{(i)}_\mu$ si $\mu \in \Gamma'_i$ (está bien definido , por que las bases de los distintos $\mathrm{M}_{\Lambda'_i}$ son extensiones de las otras).

P.d m' es l.i y genera $\mathrm{M}_{\Lambda'}$

• Lineal independencia :

Una combinación lineal finita de los m_μ será una combinación lineal en algún $\mathrm{M}_{\Lambda'_i}$, y en ese lugar los $m^{(i)}_\mu$ son l.i

• Generan $\mathrm{M}_{\Lambda'}$:

$x \in \mathrm{M}_{\Lambda'} = \mathrm{L}_{\Lambda'} \cap \mathrm{M} \Leftrightarrow x \in \mathrm{L}_{\Lambda'} = < \{b_\lambda\}_{\lambda\in\Lambda'} > \wedge\ x \in \mathrm{M} \Rightarrow x$ es combinación lineal finita de los b_λ , y los λ que aparezcan estarán todos en algún $\Lambda'_i \Rightarrow x \in \mathrm{L}_{\Lambda'_i} \cap \mathrm{M} = \mathrm{M}_{\Lambda'_i} \Rightarrow x$ es combinación lineal de los $\{m_\mu\}_{\mu\in\Lambda'_i} \subseteq m'$.

Evidentemente , $\mid \Lambda' \mid \geq \mid \Gamma' \mid$ y m' es una extensión de todas las bases m'_i , $\Lambda' \supseteq \Lambda'_i$, por lo tanto , $(\Lambda', \mathrm{L}_{\Lambda'}, \mathrm{M}_{\Lambda'}, m')$ es una cota superior de la cadena ζ .

Por Zorn , A tiene un elemento maximal $(\Lambda', \mathrm{L}_{\Lambda'}, \mathrm{M}_{\Lambda'}, m')$.

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 $(\Lambda', \ldots, m') < (\Lambda'', \ldots, m'')$, 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 $M_{\Lambda''}$?

$x \in M_{\Lambda''} \Leftrightarrow x \in M \wedge x \in L_{\Lambda''}(= L_{\Lambda'} \bigoplus Rb_{\lambda_o})$, 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

Sea $sm_{\lambda_o} + \sum r_\mu \underbrace{m'_\mu}_{\in m'} = 0 \Leftrightarrow sr_o b_{\lambda_o} + \underbrace{sy_o}_{\in L_{\Lambda'}} + \underbrace{\sum r_\mu m'_\mu}_{\in M_{\Lambda'} \subseteq L_{\Lambda'}} = 0$

$$\Rightarrow sy_o + \sum r_\mu m'_\mu \in L_{\Lambda'} \Rightarrow sy_o + \sum r_\mu m'_\mu = \sum_{\substack{\lambda \neq \lambda_o \\ \lambda \in A}} t_\lambda b_\lambda$$

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

$M'' = M \cap (L_{\Lambda'} \bigoplus Rb_{\lambda_o})$. 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 $x - sm_{\lambda_o} = \underbrace{\underbrace{y - sy_o}_{\in L_{\Lambda'} \cap M}}_{M_{\Lambda'}}$, 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 $I\mathrm{M} = \{\sum_{i=1}^{n} s_i m_i / n \in \mathbb{N},\ s_i \in I,\ m_i \in \mathrm{M}\}$. Probar que IM es submódulo de M , y de hecho , $I\mathrm{M} =< \{sm / s \in I, m \in \mathrm{M}\} >$.

2. Sobre M/IM definimos la multiplicación por escalares en el anillo cuociente R/I : $[r] \cdot [m] = [rm]$. Ver que esto da una función bien definida $\mathrm{R}/I \times \mathrm{M}/I\mathrm{M} \to \mathrm{M}/I\mathrm{M}$ y que con esto , M/IM resulta ser un R/I - módulo .

3. Si $\mathrm{M} = \bigoplus_{\lambda \in \Lambda} \mathrm{M}_\lambda$, con los M_λ submódulos de M , entonces $I\mathrm{M} = \bigoplus_{\lambda \in \Lambda} I\mathrm{M}_\lambda$, y de aquí que $\mathrm{M}/I\mathrm{M} \cong \bigoplus_{\lambda \in \Lambda} \mathrm{M}_\lambda / I\mathrm{M}_\lambda$, $[\sum m_\lambda] \leftrightarrow \sum [m_\lambda]$, 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 $I \subset \mathrm{R}$ (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 $J \subset \mathrm{R}$ 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 $\exists A = \{a_1, \ldots, a_k\} \subseteq$ M finito , tal que $\mathrm{M} =< A >= \{\sum_{i=1}^{k} \lambda_i a_i / \lambda_i \in \mathrm{R}\}$.

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 : $M =< \{m_o\} >= Rm_o = \{rm_o / r \in R\}$ 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

$\Rightarrow M \cong R/Ker\varphi$. Pero $Ker\varphi$ es un submódulo de R $\Rightarrow Ker\varphi = I$, un ideal de R (posiblemente todo R).

Notar que $Ker\varphi = \{r \in R / rm_o = 0\} = \{r \in R / (\forall m \in M) rm = 0\}$ = "anulador de M ".

En resumen: un R - módulo cíclico M es isomorfo a (R/anulador de M) $\cong$ M .

Tenemos que $Ker\varphi$ = 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 $B_1 = \{a_1, \ldots, a_n\}$ y $B_2 = \{b_1, \ldots, b_m\}$ respectivamente.

Una función $f : F_1 \to F_2$ queda completamente (y unicamente) determinada si conocemos $f(a_1), \ldots, f(a_n) \in F_2$.

Por su parte , estas imágenes están completamente determinadas por sus coordenadas en la base B_2 :

$f(a_j) = r_{1j}b_1 + \ldots + r_{mj}b_m$, 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

$$[f]_{B_1B_2} = [f] = \begin{bmatrix} r_{11} & r_{12} & \ldots & r_{1n} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{bmatrix}$$

$[f] \in M_{mn}(R)$.

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 $f : F_1 \to F_2$, $g : F_2 \to F_3$ son lineales , entonces $[g \circ f]_{B_1B_2} = [g]_{B_2B_3} \cdot [f]_{B_1B_2}$ (producto usual de matrices).

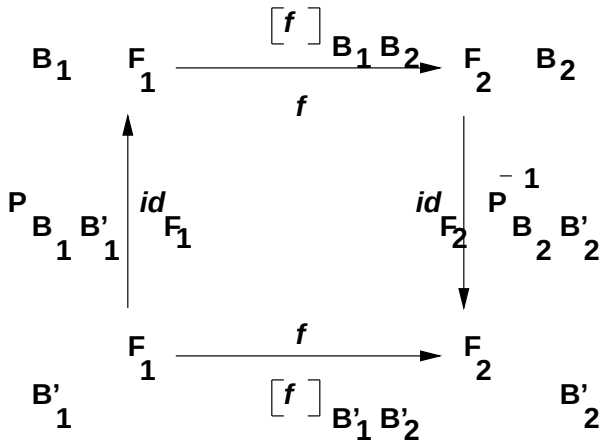
Se tienen los mismos resultados que en álgebra lineal :

•$f : F_1 \to F_2$ es un isomorfismo $\Leftrightarrow [f]_{B_1B_2}$ es invertible en $M_{nn}(R)$, con $[f]^{-1}_{B_1B_2} = [f^{-1}]_{B_1B_2}$.

•Matrices de Pasaje:

Sean B_1 y B_1' bases de F_1

$P_{B_1B_1'} = [id_{F_1}]_{B_1B_1'} \qquad P_{B_1'B_1} = [id_{F_1}]_{B_1'B_1} \qquad P^{-1}_{B_1B_1'} = P_{B_1'B_1} \qquad (\forall x \in F_1)[x]_{B_1} = P_{B_1B_1'}[x]_{B_1'}$



$[f]_{B_1'B_2'} = P^{-1}_{B_2B_2'}[f]_{B_1B_2}P_{B_1B_1'}$

Definición

Dos matrices $A, A' \in M_{mn}(\mathrm{R})$ se dicen equivalentes ssi $\exists P \in M_{mm}(\mathrm{R}), Q \in M_{nn}(\mathrm{R})$ 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:

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

$x \longrightarrow 2x$, su inversa sería $[\frac{1}{2}] \notin M_{11}(\mathbb{Z})$

***Nota*:**

Toda la teoría de determinantes en que las demostraciones NO requieran división , vale para matrices en $M_{nn}(\mathrm{R})$. En particular:

1. $\mid AB \mid = \mid A \mid \cdot \mid B \mid$
2. A es invertible ssi $\mid A \mid$ es invertible en R , y en este caso , $\mid A^{-1} \mid = (\mid A \mid)^{-1}$

Caso general : R - módulos finitamente generados

Sea $\mathrm{M} =< \{m_1, \ldots, m_n\} >= \mathrm{R}m_1 + \ldots + \mathrm{R}m_n$ un módulo finitamente generado sobre el dip R .

Si $F = Ra_1 \oplus \ldots \oplus Ra_n$ es un R-módulo libre finitamente generado, Entonces la función

$\varphi : F \longrightarrow M$

$x = r_1a_1 + \ldots + r_na_n \longrightarrow r_1m_1 + \ldots + r_nm_n$

es un epimorfismo , y por lo tanto , $M \cong F/Ker\varphi$.

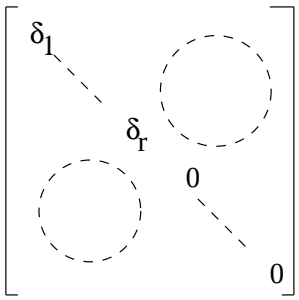
Por un teorema visto con anterioridad , el submódulo $L = Ker\varphi \subseteq F$ es también libre , con base de cardinal k , donde $k \leq n$.

Consideremos el caso general en que $L = Imf$, con $f : F' \to F$, 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/Imf , donde $f : F' \to F$ 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 ?



¿Qué podemos decir del cuociente F/Imf ?

$B' = \{b_1, \ldots, b_m\} \quad B = \{a_1, \ldots, a_n\}$

$f(b_1) = \delta_1a_1$

$f(b_2) = \delta_2a_2$

$\vdots$

$f(b_r) = \delta_ra_r$

$f(b_{r+1}) = \cdots = f(b_m) = 0$

$\Rightarrow Imf = R\delta_1a_1 \oplus \cdots \oplus R\delta_ra_r \oplus 0 \qquad$ Además , $F = Ra_1 \oplus \cdots \oplus Ra_r \oplus \cdots \oplus Ra_n$

$\Rightarrow F/Imf \cong Ra_1/R\delta_1a_1 \oplus \cdots \oplus Ra_r/R\delta_ra_r \oplus Ra_{r+1} \oplus \cdots \oplus Ra_n$ (UN EJERCICIO ANTERIOR)

$\Rightarrow F/Imf \cong (R/R\delta_1)[a_1] \oplus \cdots \oplus (R/R\delta_r)[a_r] \oplus F''$, con F'' libre de base $\{a_{r+1}, \ldots, a_n\}$

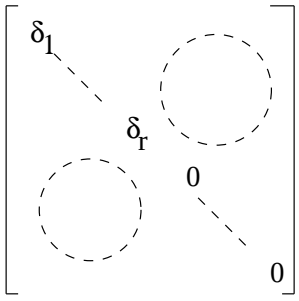
Así , $F/Imf \cong R/(\delta_1) \oplus \cdots \oplus R/(\delta_r) \oplus F''$

Conluiríamos entonces , que el módulo original $M \cong F/L = F/Imf$ 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:

Teorema

Toda matriz $A \in M_{mn}(\mathrm{R})$, con R un dip , es equivalente a una matriz de la forma



con $\delta_1/\delta_2/\cdots/\delta_r \neq 0$.

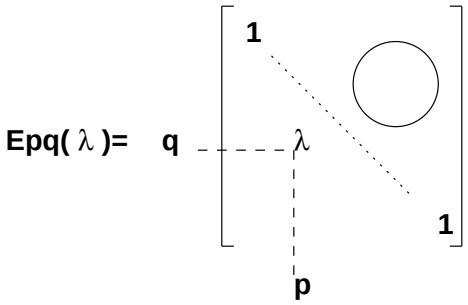
Dem

Aplicaremos operaciones elementales a la matriz A para llevarla a la forma deseada.

Operaciones elementales :

1. Operaciones Primarias

a) Sumar a una fila (o columna) un multiplo de otra

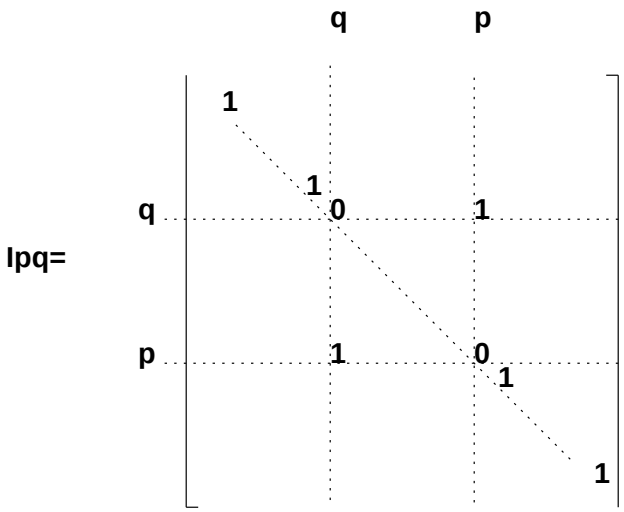


$(E_{pq}(\lambda))^{-1} = E_{pq}(-\lambda)$

$E_{pq}(\lambda) \cdot A$: Suma a la fila q de A , su fila p multiplicada por λ

$A \cdot E_{pq}(\lambda)$: Suma a la columna p de A , su columna q multiplicada por λ

b) Intercambiar filas o columnas

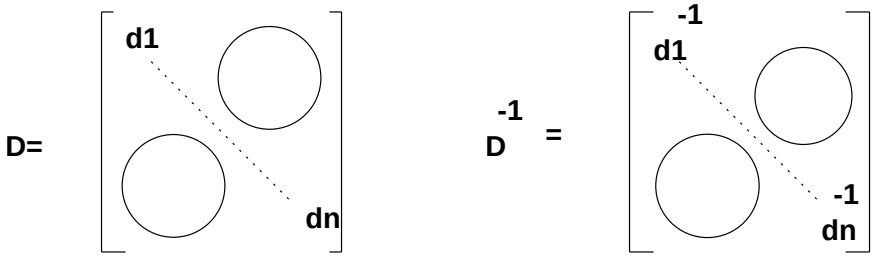


$I_{pq}^{-1} = I_{pq}$

$I_{pq} \cdot A$: intercambia filas p y q

$A \cdot I_{pq}$: intercambia columnas p yq

c) Multiplicar filas ($D \cdot A$) o columnas ($A \cdot D$) por elementos invertibles



$d_1, \ldots, d_n \in \mathrm{R}^x$

2. Además necesitaremos la operación secundaria $S \cdot A$, donde $S = \begin{bmatrix} \alpha & \beta & \\ \gamma & \delta & \bigcirc \\ \bigcirc & & I_{n-2} \end{bmatrix}$ Con determinante de $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ invertible .

Si $A = \begin{bmatrix} a_{11} & \ldots \\ a_{21} & \ldots \\ A' & \end{bmatrix}$, queremos obtener $S \cdot A = \begin{bmatrix} m & \cdots \\ 0 & \cdots \\ A' & \end{bmatrix}$ con $m = \mathrm{mcd}(a_{11}, a_{21})$.

Para esto , debemos escoger de manera apropiada α, β, γ y δ .

$$S \cdot A = \begin{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \cdot \begin{bmatrix} a_{11} & \cdots \\ a_{21} & \cdots \end{bmatrix} \\ A' \end{bmatrix} = \begin{bmatrix} \alpha a_{11} + \beta a_{21} & \cdots \\ \gamma a_{11} + \delta a_{21} & \cdots \\ A' & \end{bmatrix}$$

Como R es dip , sabemos que existen α', $\beta' \in$ 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 $\overline{A}$ de la forma deseada.

Para continuer 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 .

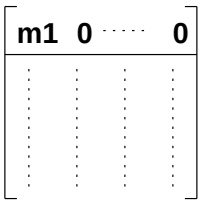
Dem

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:

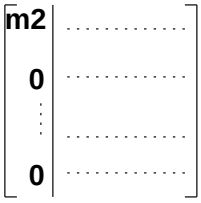
$$\left[\begin{array}{c|c} \mathbf{m} & \cdots \\ \mathbf{0} & \cdots \\ \vdots & \\ \mathbf{0} & \cdots \end{array}\right]$$

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:

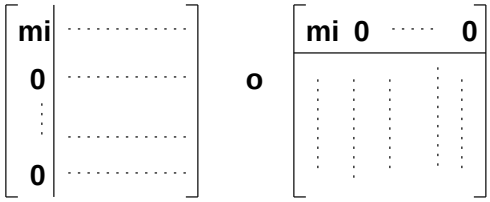


con m_1/m . Al siguiente paso obtenemos:



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

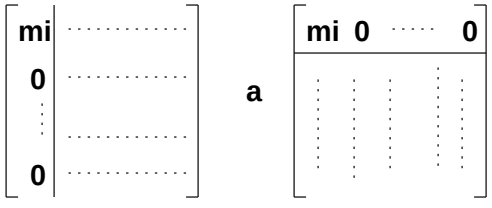


Afirmamos que los m_i se "estabilizan" .

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 , $\exists \overline{m} \in$ R tal que $I = (\overline{m})$. $\overline{m} \in I \Rightarrow \exists i \in \mathbb{N}$ tal que $\overline{m} \in (m_i) \Rightarrow (\overline{m}) \subseteq (m_i) \subseteq (\overline{m}) \Rightarrow I = (\overline{m}) = (m_i)$, 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



(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 pivotear por Gauss y anular el resto de la fila sin alterar los ceros bajo m_i . Hemos llegado a :

$$\left[\begin{array}{c|ccc} \mathbf{m} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & & & \\ \vdots & & \mathbf{B'} & \\ \mathbf{0} & & & \end{array}\right]$$

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

$$\left[\begin{array}{c|ccc} \mathbf{m'} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & & & \\ \vdots & & \mathbf{B''} & \\ \mathbf{0} & & & \end{array}\right]$$

m' divide a $(B')_{ij}$ y a m .

Terminamos cuendo 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 , $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{22}(\mathrm{R})$ se puede transformar en $\begin{bmatrix} m & \cdots \\ 0 & \cdots \end{bmatrix}$ (con $m =$ 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 $\mathrm{R}/(\delta_1)\oplus\cdots\oplus \mathrm{R}/(\delta_k)\oplus \mathrm{F}$, con F un módulo libre finitamente generado , y $1 \nsim \delta_1/\delta_2/\cdots/\delta_k \neq 0$.

Cuando $\mathrm{R}=\mathbb{Z}$, 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 $|A|=24$

$\mathbb{Z}_{24}$	$3\cdot 2^3$
$\mathbb{Z}_{2\oplus\mathbb{Z}_{12}}$	$2\cdot 3\cdot 2^2$
$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_6$	$2\cdot 2\cdot 3\cdot 2$

Corolario

Toda matriz $A\in M_{nn}(\mathrm{R})$ es producto de matrices elementales y secundarias. Sobre $\mathrm{R}=\mathbb{Z}$ o $\mathrm{R}=\mathrm{K}[x]$ (K cuerpo) , A será producto de elementales.

***Ejercicio*1:**

Sea M un R - módulo y TM su módulo de torsión

1. Si $f:\mathrm{M}\to\mathrm{M}'$ es un isomorfismo de R - módulos , entonces $f(T\mathrm{M})=T\mathrm{M}'$.
2. $T(\mathrm{R}/(\delta_1)\oplus\cdots\oplus\mathrm{R}/(\delta_r)\oplus\mathrm{F})=\mathrm{R}/(\delta_1)\oplus\cdots\oplus\mathrm{R}/(\delta_r)$
3. $\mathrm{M}/T\mathrm{M}\cong\mathrm{F}$

Corolario

Si R es un dip y M es un módulo sin torsión (i.e $T\mathrm{M}=\{0\}$) y finitamente generado , entonces M es libre .

***Ejercicio*2 :**

Sea M un R - módulo , $c\in\mathrm{R}$ y $f_c:\mathrm{M}\to\mathrm{M}$ la multiplicación por c ($f_c(x)=cx$) . Anotamos $\mathrm{Im}f_c=c\mathrm{M}$. Notar que $c\mathrm{M}=(c)\mathrm{M}$.

1. Si $\mathrm{M}=\mathrm{M}_1\oplus\mathrm{M}_2$

(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 $R/(\delta_1) \oplus \cdots R/(\delta_r) \oplus F$ con $1 \nsim \delta_1/\cdots/\delta_r \neq 0$ y F libre finitamente generado. El rango de F y los δ_i (salvo multiplos invertibles) son únicos.

Dem

La existencia del isomorfismo se deduce del teorema anterior.

Veamos que sucede con la unicidad de esta descomposición : Supongamos que $M \cong R/(\delta_1) \oplus \cdots R/(\delta_r) \oplus F \cong R/(\delta'_1) \oplus \cdots R/(\delta'_s) \oplus F'$, 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 $L = R/(\delta_1) \oplus \cdots R/(\delta_r) \cong L' = R/(\delta'_1) \oplus \cdots R/(\delta'_s)$ y $F \cong F'$.

Probemos que $r = s$. Por contradicción , supongamos que $r > s$.

Sea p primo tal que $p/\delta_1 \Rightarrow p/\delta_i\ \forall i \in \{1 \ldots r\}$, 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 $\delta_i \nsim \delta'_i$.

Sea j la última vez que $\delta_i \sim No\delta_i'$, i.e $\delta_r' \sim \delta_r, \delta_{r-1}' \sim \delta_{r-1}, \ldots, \delta_{i+1}' \sim \delta_{i+1}, \delta_i' NO \sim \delta_i$.

$\delta_i' NO \sim \delta_i$ 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 , $\delta_i \mathrm{R} \subseteq (\delta_j) \Rightarrow \delta_i \mathrm{R}/(\delta_j) = 0$. Resulta entonces $\mathrm{R}/(\delta_{i+1}/\delta_i) \oplus \cdots \oplus \mathrm{R}/(\delta_r/\delta_i)$

Como $\delta_{i+1} = \delta_{i+1}', \ldots, \delta_r = \delta_r'$

$\mathrm{L}' \cong S \oplus \underbrace{\mathrm{R}/(\delta_i'/\mathrm{mcd}(c, \delta_i))}_{\neq 0} \oplus \mathrm{R}/(\delta_{i+1}/c) \oplus \cdots \oplus \mathrm{R}/(\delta_r/c)$ más largo que L $\rightarrow\leftarrow$, por lo tanto , $\delta_i \sim \delta_i'$ $\forall i = 1 \ldots n$.

Definición

- $\delta_1, \ldots, \delta_r$ 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 $\mathrm{M} \cong \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_r} \oplus \mathbb{Z}^k$, con $1 < q_1/ \ldots /q_r \neq 0$ 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 $I = \{r \in \mathrm{R}/(\forall m \in \mathrm{M})\} rm = 0\}$. I es un ideal , por lo tanto , $\exists e \in \mathrm{R}$ 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 $e = e(\mathrm{M})$, definido unicamente , salvo multiplicación por elementos invertibles.

Si M es finitamente generado : $\mathrm{M} =< \{m_1, \ldots, m_k\} >= \mathrm{R}m_1 + \cdots + \mathrm{R}m_k$.

$r \in$ Anulador de M $\Leftrightarrow rm_i = 0$ $\forall 1 \leq i \leq k$, por lo tanto , $I = \{r \in \mathrm{R}/rm_i = 0 \forall 1 \leq i \leq k\} = (e)$.

Es directo que $e = e(\mathrm{M}) = \mathrm{MCM}\{o(m_1), \ldots, o(m_k)\}$, donde $(a) \cap (b) = (\mathrm{MCM}\{o(m_1), \ldots, o(m_k)\})$.

Sabemos que $\mathrm{M} \cong \mathrm{R}/(\delta_1) \oplus \cdots \oplus \mathrm{R}/(\delta_r) \oplus \mathrm{F}$

$\mathrm{F} \neq \{0\} \Rightarrow e(\mathrm{M}) = 0$

$\mathrm{F} = \{0\} \Leftrightarrow$ M es de torsión

Entonces $m_1 = [1]_{\mathrm{R}/(\delta_1)}, \ldots, m_r = [1]_{\mathrm{R}/(\delta_r)}$ son generadores de (la copia isomorfa de)M y sus respectivos ordenes son $\delta_1, \ldots, \delta_r$, y su MCM es $\delta_r = e(\mathrm{M})$.

Tenemos que si M es finitamente generado , $\mathrm{M} = T\mathrm{M} \oplus \mathrm{F}$, 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 $p \in \mathrm{R}$, la **componente p− primaria** de M es $T_p\mathrm{M} = \{m \in \mathrm{M}/\exists i \geq 0 \text{ tal que } p^i m = 0\}$, para M no necesariamente finitamente generado.

$T_p\mathrm{M}$ es un submódulo de M . En efecto:

- $0 \in T_p\mathrm{M}$
- Si $m_1, m_2 \in T_p\mathrm{M},\ p^i m_1 = 0\,,\ p^j m_2 = 0 \Rightarrow p^{i+j}(rm_1+sm_2) = 0\, r, s \in \mathrm{R} \Rightarrow rm_1+sm_2 \in T_p\mathrm{M}$

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 $\mathrm{M} = \bigoplus_{\lambda\in\Lambda} T_{p_\lambda}\mathrm{M}$.

Dem.

Sea $x \in \mathrm{M} \setminus \{0\}$, y sea $n \in \mathrm{R}$ 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 $x_i \in T_{p_{\lambda_i}}\mathrm{M}\ 1 \leq i \leq k$.

Sea $n_i = \frac{n}{up_{\lambda_i}^{\alpha_i}}$, $1 \leq i \leq k$

Ejercicio: (inducción) $\exists \beta_1, \ldots, \beta_k \in \mathrm{R}$ tal que $\beta_1 n_1 + \cdots + \beta_k n_k = 1$ (puesto que en conjunto , no de a pares , $n_1, \ldots, n_k$ son primos relativos : $\mathrm{mcd}(n_1, \ldots, n_k) = 1$.

$\Rightarrow x = \beta_1 n_1 x + \cdots + \beta_k n_k x$, $x_i = \beta_i n_i x\ 1 \leq i \leq k$, $p_{\lambda_i}^{\alpha_i} x_i = \beta_i p_{\lambda_i}^{\alpha} n_i x = 0 \Rightarrow x_{i\in T_{p_{\lambda_i}}\mathrm{M} \Rightarrow \mathrm{M} = +_{\lambda\in\Lambda} T_{p_\lambda}\mathrm{M}}$.

La suma es directa , esto equivale a : (**Ejercicio**)

Si $x_i \in T_{p_{\lambda_i}}\mathrm{M}$ $\lambda_i \neq \lambda_j$ 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 $\mathrm{M} \neq \{0\}$ es cíclico y de torsión , sabemos que $\mathrm{M} \cong \mathrm{R}/(\delta)$ $\delta = o(\mathrm{M}) = e(\mathrm{M}) \in \mathrm{R}\setminus(\{0\} \cup \mathrm{R}^x)$,$\delta = p_1^{\alpha_1} \cdots p_k^{\alpha_k} u$ $p_1, \ldots, p_k$ primos , $u \in \mathrm{R}^x$, $\alpha_i \in > 0\, \forall 1 \leq i \leq k$. Entonces $\mathrm{R}/(\delta) \cong \mathrm{R}/(p_1^{\alpha_1}) \oplus \cdots \oplus \mathrm{R}/(p_k^{\alpha_k})$.

Aplicando todo esto resulta lo siguiente : Si M es un R - módulo de torsión finitamente generado , entonces $\mathrm{M} \cong \bigoplus_{i=1}^{l} [\mathrm{R}/(p_i^{\alpha_{i,1}}) \oplus \cdots \oplus \mathrm{R}/(p_i^{\alpha_{i,k_i}})]$, con $p_1, \ldots, p_l$ primos que aparecen

en la descomposición de δ_r , con $\delta_1/\cdots/\delta_r$ los factores invariantes . $\alpha_{i,j}$ exponente de p_i en alguno de los δ_j . $\mathrm{R}/(p_i^{\alpha_{i,1}}) \oplus \cdots \oplus \mathrm{R}/(p_i^{\alpha_{i,k_i}}) \cong T_{p_i}\mathrm{M}$. Los $p_i^{\alpha_{i,j}}$ se llaman divisores elementales de M .

Ejemplo:

A grupo abeliano de 24 elementos .

$$\begin{array}{llll} \delta_1 = 3\cdot 2^3 & & & \mathbb{Z}_{24}\ (A_1) \\ \delta_1 = 2 & \delta_2 = 3\cdot 2 & & \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus\ (A_2) \\ \delta_1 = 2 & \delta_2 = 2 & \delta_3 = 3\cdot 2 & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6\ (A_3) \end{array}$$

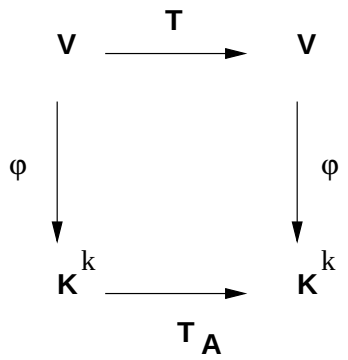
En términos de divisores elementales :

$$A_1 \cong \underbrace{\mathbb{Z}_3}_{T_3A_1} \oplus \underbrace{\mathbb{Z}_8}_{T_2A_1} \quad A_2 \cong \underbrace{\mathbb{Z}_3}_{T_3A_2} \oplus \underbrace{\mathbb{Z}_4 \oplus \mathbb{Z}_2}_{T_2A_2} \quad A_3 \cong \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2}_{T_2A_3} \oplus \underbrace{\mathbb{Z}_3}_{T_3A_3}$$

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 $T : V \to V$ que corresponde a la multiplicación por $x \in \mathrm{K}[x]$ .Si $v \in V$ y $p(x) = a_o + a_1x + \cdots + a_nx^n \in \mathrm{K}[x]$, la multiplicación por escalar está definida por $p(x)v = p(T)(v)$ con $p(T) = a_oid + a_1T + \cdots + a_nT^n$.

Si V es de dimensión finita y $B = \{v_1, \ldots, v_k\}$ es su base , la función $\varphi : V \to \mathrm{K}^k$ tal que a $v = \lambda_1v_1 + \cdots + \lambda_kv_k$ le asigna $\varphi(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix}$, es un isomorfismo de K[x] - módulos : $(V, T) \to (\mathrm{K}^k, T_A)$



con $T_Ax = Ax$, $A = [T]_{BB}$.

Observación:

Si V es e.v de dimensión $n < \infty$ sobre K , sabemos que $\mathrm{L}(V,V) \cong M_{nn}(\mathrm{K})$ (como e.v) , por lo tanto , $\mathrm{L}(V,V)$ es de dimensión n^2 . Entonces , si $T : V \to V$ es una transformación lineal , $\{T^o, T^1, T^2, \ldots, T^k, \ldots\} = \{T^k / k \in \mathbb{N}\}$ es l.d$\Rightarrow \exists a_o, a_1, \ldots, a_k \in \mathrm{K}$ no todos nulos tal que $a_o T^o + a_1 T^1 + \cdots + a_k T^k = 0$. Si $p(x) = a_o + a_1 x + \cdots + a_k x^k \Rightarrow p(x) \in \mathrm{K}[x]/\{0\}$ y $p(T) = 0$.

Sea $I = \{p(x) \in \mathrm{K}[x] / p(T) = 0\}$, I es un ideal en $\mathrm{K}[x]$, por lo tanto , $I = (m(x))$, pues $\mathrm{K}[x]$ es dip . $m(x)$ está únicamente definido , salvo por multiplicación por constantes distintas de cero (i.e , los invertibles en $\mathrm{K}[x]$).

$m(x)$ 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 $m(T) = 0$.

$(\forall p(x) \in \mathrm{K}[x])\, p(T) = 0 \Rightarrow p(x)$ es múltiplo de $m(x)$.

Considerando el par (V,T) como un $\mathrm{K}[x]$ - 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.

$\{p(x) \in \mathrm{K}[x] / p(x) \cdot v = 0 \forall v \in V\}$

$p(x)v = 0 \forall v \in V \Leftrightarrow p(T)v = 0 \forall v \in V \Leftrightarrow p(T) = 0 \in \mathrm{L}(V,V)$

$m(x)$ es anulador minimal entonces.

Notar también que , dado que V es de dimensión finita como K− e.v , tiene base $\{v_1 \ldots v_n\}$, $(\forall v \in V)\ v = \underbrace{\lambda_1}_{\in \mathrm{K}} v_1 + \cdots + \underbrace{\lambda_n}_{\in \mathrm{K}} v_n$, pero $\mathrm{K} \subseteq \mathrm{K}[x]$, por lo tanto , V es generado como $\mathrm{K}[x]-$ módulo por $v_1 \ldots v_n$.

En resumen , si V es e.v sobre el cuerpo K y $T : V \to V$ es lineal :

1. $\exists m(x) \in \mathrm{K}[x] \setminus \{0\}$, 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 $p(x) \in \mathrm{K}[x] \Rightarrow m(x)/p(x)$
2. Considerando V como $\mathrm{K}[x]$ -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 $\mathrm{K}[x]$.

Sabemos que M es un espacio vectorial V sobre K , con una transformación K - lineal $T : V \to V$. Además $\mathrm{M} \cong \mathrm{K}[x]/(\delta_1(x)) \oplus \cdots \oplus \mathrm{K}[x]/(\delta_r(x))$ (como $\mathrm{K}[x]$ - módulos) , con $\delta_1(x)/\cdots/\delta_r(x) \neq 0$ 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 : $\mathrm{M} \cong \mathrm{K}[x]/(\delta(x))$, con $\delta(x)$ el orden de M . Además $\exists v_o \in V (= \mathrm{M})$, tal que $\mathrm{M} = \mathrm{K}[x]v_o$, i.e $(\forall v \in V)(\exists p(x) \in \mathrm{K}[x])\ v = p(T)(v_o) = a_o v_o + a_1 T(v_o) + \cdots + a_k T(v_k) \Rightarrow \{v_o, T(v_o), \ldots, T^k(v_o), T^{k+1}(v_o), \ldots\}$ genera V como espacio vectorial sobre K .

Pero si $p(x) \in \mathrm{K}[x]$, podemos dividirlo por $\delta(x)$: $p(x) = q(x)p(x) + r(x)$, con $\mathrm{gr}(r(x)) < \mathrm{gr}(\delta(x)) = n \Rightarrow v = p(T)(v_o) = q(T)\underbrace{\delta(T)(v_o)}_{\delta(x)v_o=0} + r(T)(v_o) = r(T)(v_o) = b_o + b_1T(v_o) + \cdots +$ $b_{n-1}T^{n-1}(v_o)$,por lo tanto , $\{v_o, T(v_o), \ldots, T^{n-1}(v_o)\}$ generan V como e.v sobre K , i.e V , como e.v sobre K , es de dimensión finita .

Mejor aun : $\{v_o, T(v_o), \ldots, T^{n-1}(v_o)\}$ son l.i , y por lo tanto , constituyen una base del e.v sobre el cuerpo K . En efecto :

Si $\lambda_o v_o + \lambda_1 T(v_o) + \cdots + \lambda_{n-1}T^{n-1}(v_o) = 0$ $\lambda_i \in \mathrm{K}$ $\forall 0 \leq i \leq n-1$, entonces $p(T)(v_o) = 0$, para $p(x) = \lambda_o + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1} \Rightarrow p(x)v_o = 0$ en la estructura de $\mathrm{K}[x]$ -módulo$\Rightarrow p(x)V = 0$, pues V está generado como $\mathrm{K}[x]$ - módulo por $\{v_o\} \Rightarrow p(x)$ es múltiplo de $\delta(x)$, pero $\mathrm{gr}(p(x)) < \mathrm{gr}(\delta(x)) \Rightarrow p(x) = 0 \Rightarrow$ sus coeficientes $\lambda_o = \cdots = \lambda_{n-1} = 0$.

¿Cuál es la matriz de T con respecto a la base $B = \{v_o, T(v_o), \ldots, T^{n-1}(v_o)\}$ del e.v V ?

$$\begin{array}{ccccccccc}
v_1 & = & v_o & Tv_1 & = & Tv_o & = & v_2 \\
v_2 & = & T(v_o) & Tv_2 & = & T^2v_o & = & v_3 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
v_{n-2} & = & T^{n-2}(v_o) & Tv_{n-1} & = & T^{n-1}v_o & = & v_n \\
v_{n-1} & = & T^{n-1}(v_o) & Tv_n & = & T^nv_o & = & ?
\end{array}$$

Sea $\delta(x) = c_o + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$ (el anulador minimal del $\mathrm{K}[x]$ -módulo $\mathrm{M} = (V, T)$).

Calculemos T^nv_o : $\delta(x)v_o = 0 = c_ov_o + c_1Tv_o + \cdots c_{n-1}Tv_o + T^nv_o \Rightarrow T^nv_o = -c_ov_o - c_1Tv_o - \cdots - c_{n-1}T^{n-1}v_o = -c_ov_1 - \cdots - c_{n-1}v_n$.

Por lo tanto ,

$$\mathbf{A = [\,T\,]_B} = \begin{bmatrix}
\mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{-c_1} \\
\mathbf{1} & \mathbf{0} & & & \mathbf{-c_2} \\
\mathbf{0} & \mathbf{1} & \mathbf{0} & & \\
 & \mathbf{0} & \mathbf{1} & \mathbf{0} & \\
 & & \mathbf{0} & \mathbf{1} & \mathbf{0} \\
\mathbf{0} & \cdots & \mathbf{0} & \mathbf{1} & \mathbf{-c_{n-1}}
\end{bmatrix}$$

"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 $T : V \to V$ la multiplicación por x . Sea $\delta(x) \in \mathrm{K}[x] \setminus \{0\}$ 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

$\Leftarrow$) $B = \{v_1, \ldots, v_n\}$, $\delta(x) = c_o + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$. $[T]_B = C_{\delta(x)}$ significa :

$$\begin{array}{rcccrcl} Tv_1 & = & v_2 & \to & xv_1 & = & v_2 \\ Tv_2 & = & v_3 & \to & x^2v_1 & = & v_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ Tv_{n-1} & = & v_n & \to & x^{n-1}v_1 & = & v_n \end{array}$$
$$Tv_n = -c_o v_1 - c_1 v_2 - \cdots - c_{n-1}v_n$$

Como K[x] - módulo , M = V es generado por $\{v_1\}$, i.e M es cíclico.

Además $Tv_n = x^n v_1 = -c_o v_1 - c_1 x v_1 - \cdots - c_{n-1}x^{n-1}v_1 \Leftrightarrow \delta(x)v_1 = 0$, por lo tanto , $\delta(x)$ anula todo M = V .

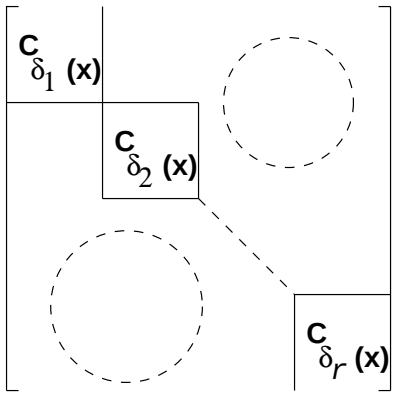
Por ser V = M cíclico , tiene anulador minimal $\delta'(x)$ de grado igual a dim$V = n$, por ser anulador minimal $\delta'(x)/\delta(x)$, pero $\mathrm{gr}(\delta'(x)) = \mathrm{gr}(\delta(x)) = n$ y ambos son mónicos $\Rightarrow \delta'(x) = \delta(x)$.

Generalicemos para el caso en que M es de torsión finitamente generado sobre K[x] : M $\cong$ K[x]/$(\delta_1(x)) \oplus \cdots \oplus$ K[x]/$(\delta_r(x))$, con $\delta_1(x)/\cdots/\delta_r(x) \neq 0$, $\mathrm{gr}(\delta_1(x)) \geq 1$.

$\delta_r(x)$ 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 $V = V_1 \oplus \cdots \oplus V_r$, 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



$\delta_1(x), \ldots, \delta_r(x)$ son los factores invariantes del K$[x]$ - módulo M .

Recordando que todo par (V, T) , con V e.v sobre K de dimensión finita , $T : V \to V$ 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 .

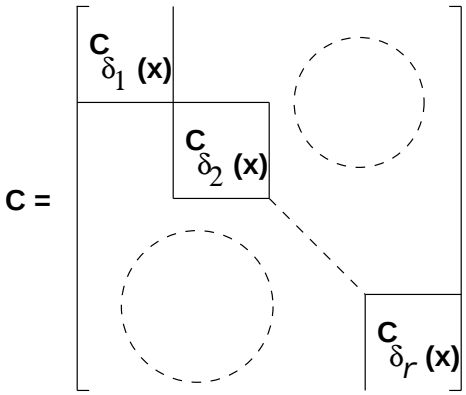
Aplicación a Matrices de $n \times n$ a coeficientes en un Cuerpo

Sea $A \in M_{nn}(\mathrm{K})$. A define una transformación K$-$ lineal

$T_A : \mathrm{K}^n \longrightarrow \mathrm{K}^n$

$x \longrightarrow Ax$

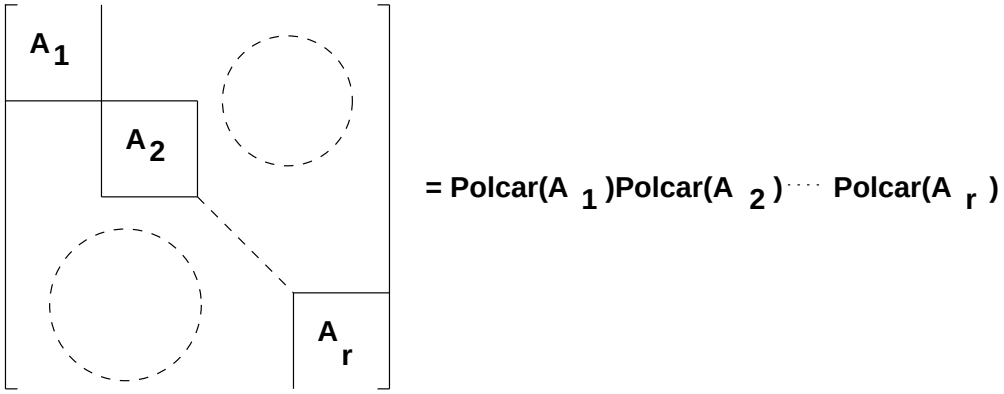
(K^n, T_A) produce un K$[x]$ - módulo finitamente generado y de torsión$\Rightarrow \exists!$ lista de polinomios mónicos $\delta_1(x)/\cdots/\delta_r(x) \neq 0$ $(\mathrm{gr}(\delta_1(x)) \geq 1)$ y una base de K^n , tal que la matriz representante de T_A con respecto a esta base es



"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 $(-1)^{\mathrm{gr}(\delta(x))}\delta(x)$ y que el polinomio característico de una matriz de la forma



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 $A \in M_{nn}(\mathrm{K})$, 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 $A \in M_{nn}(\mathrm{K})$ 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 $A \in M_{nn}(\mathrm{K})$ 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 $\cong \bigoplus_{i=1}^{l} \mathrm{R}/(p_i^{\alpha_{i,1}}) \oplus \cdots \oplus \mathrm{R}/(p_i^{\alpha_{i,k_i}})$ (suma finita).

Tomemos R = K[x] y $p(x) = x - \lambda$, polinomio primo en K[x] (generalmente hay más polinomios primos).Estudiemos K[x]/$(p(x)^k)$:

Sabemos que es cíclico de orden $p(x)^k$, $\mathrm{M} \cong (V,T)$, $\mathrm{M} = \mathrm{K}[x]v_o$.

$$\left.\begin{array}{ccc} v_1 & = & v_o \\ v_2 & = & Tv_o \\ \vdots & \vdots & \vdots \\ v_k & = & T^{k-1}v_o \end{array}\right\} \text{ base de } V = \mathrm{M}$$

$[T]_{Base} = C_{p(x)^k}$. $p(T)v_o = (T-\lambda id)^k v_o = 0$, $(x-\lambda)^k = p(x)^k$ es el anulador minimal de M (polinomio mínimo de T).

Nueva base para $V = \mathrm{M}$:

$$\begin{array}{ccc} (T-\lambda id)^k v_o & = & 0 \\ (T-\lambda id)^{k-1} v_o & = & w_1 \\ (T-\lambda id)^{k-2} v_o & = & w_2 \\ \vdots & \vdots & \vdots \\ (T-\lambda id)v_o & = & w_{k-1} \\ v_o & = & w_k \end{array}$$

$w_i \neq 0 \, \forall 1 \leq i \leq k$. $\{w_1, \ldots, w_k\}$ son una base de V . Calculemos la matriz representante de T con respecto a esta base :

$w_{k-1} = Tw_k - \lambda w_k$

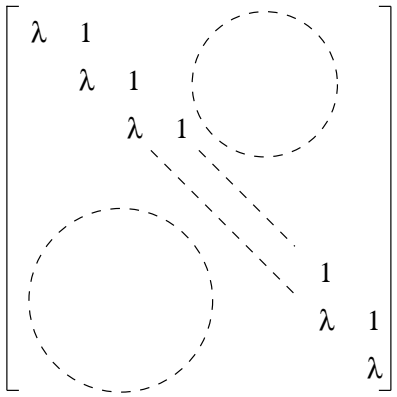
$w_{k-2} = (T-\lambda id)^2 v_o = (T-\lambda id)w_{k-1} = Tw_{k-1} - \lambda w_{k-1}$

$\vdots$

$\Downarrow$

$$\begin{array}{ccc} Tw_k & = & \lambda w_k + w_{k-1} \\ Tw_{k-1} & = & \lambda w_{k-1} + w_{k-2} \\ \vdots & \vdots & \vdots \\ Tw_2 & = & \lambda w_2 + w_1 \\ Tw_1 & = & \lambda w_1 \end{array}$$

Por lo tanto , la matriz de T en esta base es



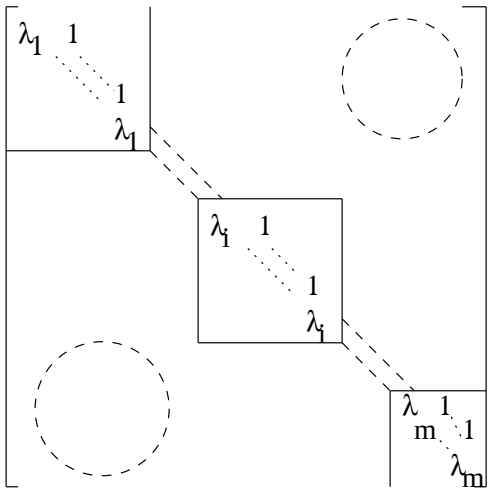
"Bloque de Jordan"

$\{w_1, \ldots, w_k\}$es una base de V por que tiene el número correcto de elementos , y dim$V$ = gr$((x-\lambda)^k) = k$ y además es l.i

$\alpha_1(T-\lambda id)^{k-1}v_o + \cdots + \alpha_k v_o = 0$, multipicando por $(T-\lambda id)^{k-1} \Rightarrow \alpha_k = 0$.

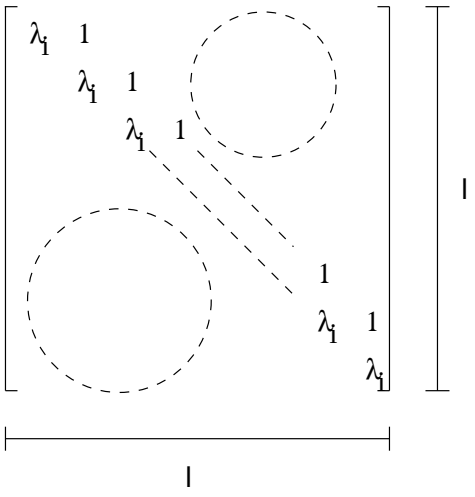
(REVISAR)

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 $\forall T : V \to V$ lineal , existe una base B de V tal que la matriz representante de T con respecto a esta base , es de la forma



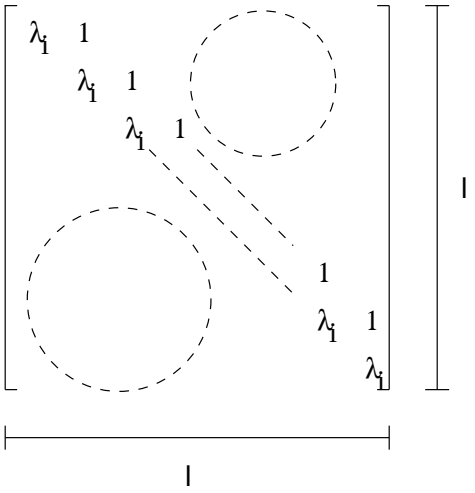
"Forma canónica de Jordan de T"

$\lambda_1, \ldots, \lambda_m$ son los valores propios de T , y los bloques



(en número y tamaño) para cada λ_i están unicamente determinados .

El bloque

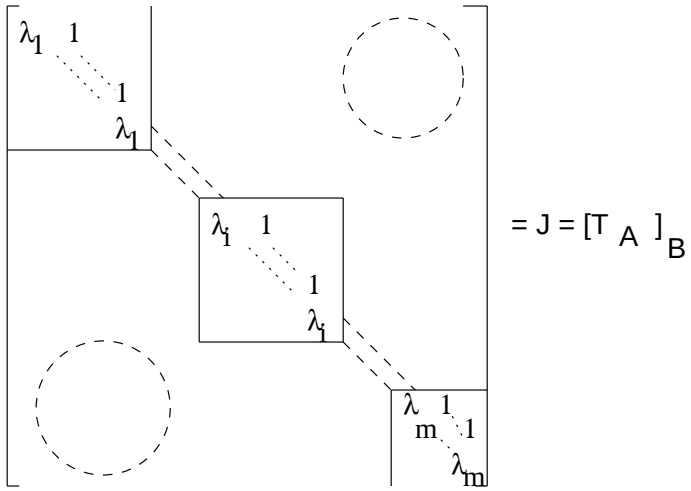


proviene de una parte $\{w_1, \ldots, w_l\}$ de la base B (correspondiente al sumando cíclico primario $\mathrm{K}[x]/((x-\lambda)^l)$ del módulo (V,T)) , que es tal que w_1 es vector propio de T : $Tw_1 = \lambda_i w_1$ (con valor propio asociado λ_i) y $w_2, \ldots, w_l$ son vectores porpios generados de T , "colas" de w_1 que satisfacen

$$\begin{array}{ccccc} Tw_2 & = & \lambda_i w_2 & + & w_1 \\ Tw_3 & = & \lambda_i w_3 & + & w_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ Tw_l & = & \lambda_i w_l & + & w_{l-1} \end{array}$$

(Esta base viene de un generador w_o en $\mathrm{K}[x]/((x-\lambda)^l)$ tal que $(x-\lambda)^l w_o = 0 \rightarrow w_i = (x-\lambda)^{l-i} w_o$ y $(x-\lambda_i)^l w_i = 0$ $i = 1 \ldots l$ $(T - \lambda_i id)^l w_i = 0$)

Si $V = \mathrm{K}^n$, $A \in M_{nn}(\mathrm{K})$, $T = T_A : \mathrm{K}^n \rightarrow \mathrm{K}^n$ 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 $\delta_1(x), \ldots, \delta_r(x)$, 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 $T : V \to V$ lineal) ?

Sea $B = \{v_1, \ldots, v_n\}$ base de V (como e.v sobre K)$\Rightarrow \{v_1, \ldots, v_n\}$ 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 $\{b_1, \ldots, b_n\}$ (F $\cong$ K$[x]^n$) .

Sea φ el único epimorfismo (de K$[x]$ -módulos) de F en V (= M) tal que $\varphi(b_i) = v_i \ \forall i \in \{1, \ldots, n\}$. $\varphi : \mathrm{F} \to V$ epimorfismo $\Rightarrow V \cong \mathrm{F}/\mathrm{Ker}\varphi$. Estudiemos más en detalle Kerφ :

$xv_j = T(v_j) = \sum_{i=1}^n a_{ij} v_i$, 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 $c_j = xb_j - \sum_{i=1}^n a_{ij} b_i \in \mathrm{F}$

$\varphi(c_j) = \varphi(xb_j - \sum_{i=1}^n a_{ij} b_i) = x\varphi(b_j) - \sum_{i=1}^n a_{ij} b_i = xv_j - \sum_{i=1}^n a_{ij} v_i = 0$, por lo tanto , $c_j \in \mathrm{Ker}\varphi$.

Probemos algo mejor : Ker$\varphi =< \{c_1, \ldots, c_n\} >$

Sea L $=< \{c_1, \ldots, c_n\} >$, sabemos que L $\subseteq$ Ker$\varphi \subseteq$ F $=< \{v_1, \ldots, v_n\} >$

¿xb_j módulo L ?

$[xb_j]_{\mathrm{L}} = [\sum_{i=1}^n a_{ij} b_i]$

$[x^2 b_j]_{\mathrm{L}} = [xxb_j] = x[xb_j] = x[\sum_{i=1}^n a_{ij} b_i] = [\sum_{i=1}^n \lambda_i b_i] \ \lambda_i \in \mathrm{K}$. Inductivamente $x^k b_j \equiv_{\mathrm{L}} \sum_{i=1}^n \lambda_i b_i \ \lambda_i \in \mathrm{K}$, por lo tanto , $\forall p(x) \in \mathrm{K}[x]$, $p(x) b_j \equiv_{\mathrm{L}} \sum_{i=1}^n \lambda_i b_i$. así, $\forall z \in \mathrm{F}$ $z \equiv_{\mathrm{L}} \sum_{i=1}^n \lambda_i b_i \quad \lambda_i \in \mathrm{K}$

En particular , si $z \in$ Kerφ :

$z \equiv_{\mathrm{L}} \sum_{i=1}^n \lambda_i b_i \ \lambda_i \in \mathrm{K}$

$\downarrow$

$0 = \sum_{i=1}^n \lambda_i \varphi(b_i) \Rightarrow 0 = \sum_{i=1}^n \lambda_i v_i \Rightarrow \lambda_1 = \cdots = \lambda_n = 0$, es decir ,

$z \in \mathrm{Ker}\varphi \Rightarrow z \equiv_{\mathrm{L}} 0$, $z \in$ L .

En resúmen :

$\varphi : \mathrm{F} \to V$ epimorfismo de K$[x]$ -módulos , F/Ker$\varphi \cong V$ como K$[x]$ -módulos . Ker$\varphi =< \{c_1, \ldots, c_n\} >$.

Sea F$'$ módulo libre de rango n , de base $\{b'_1, \ldots, b'_n\}$ y $f : \mathrm{F}' \to \mathrm{F}$ la única transformación K$[x]$ - lineal que a b'_i le asigna $f(b'_i) = c_i \ \forall i \in \{1, \ldots, n\}$. Resulta Im$f =< \{c_1, \ldots, c_n\} >=$

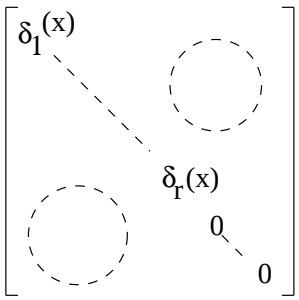
Kerφ , $V \cong \mathrm{F}/\mathrm{Im}f$ como K[x] - módulos . Por lo tanto , la matriz a "diagonalizar" para calcular los factores invariantes de V (como K[x] - módulo) es $[f]_{B'B}$

columna 1 de esta matriz : $[f(b'_1)]_B = [c_1]_B = [xb_1 - \sum_{i=1}^{n} a_{i1}b_i]_B = \begin{pmatrix} x - a_{11} \\ -a_{21} \\ \vdots \\ -a_{n1} \end{pmatrix}$

Columna j : $[f(b'_j)]_B = [c_j]_B = [xb_j - \sum_{i=1}^{n} a_{ij}b_i]_B = \begin{pmatrix} -a_{1j} \\ -a_{2j} \\ \vdots \\ x - a_{jj} \\ \vdots \\ -a_{nj} \end{pmatrix}$, por lo tanto , la matriz es $xI_n - A$.

Prop

Los factores invariantes de $T : V \to V$ son los únicos polinomios mónicos $\delta_1(x)/\cdots/\delta_r(x)$ con $\mathrm{gr}(\delta_1(x)) \geq 1$, tal que al "diagonalizar" $xI_n - A$ resulta .



Ejercicio:

Sea R un dip , $n \in \mathbb{N} \setminus \{0\}$. Miremos los elementos del R - módulo libre R^n como columnas $r = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$. Sean $m_1, \ldots, m_n \in \mathrm{R}^n$ y formemos la matriz $A = [m_1|\cdots|m_n] \in M_{nn}(\mathrm{R})$. Sea $\triangle = \det(A)$. Las siguientes proposiciones son equivalentes:

1. El submódulo $\mathrm{M} =< \{m_1, \ldots, m_n\} > \subseteq \mathrm{R}^n$ es libre

2. $\{m_1, \ldots, m_n\}$ es l.i

3. $\triangle \neq 0$

4. R^n/M es de torsión , finitamente generado . Además :

   (a) Si $\mathrm{R} = \mathbb{Z}$, R^n/M es de torsión finitamente generado $\Leftrightarrow$ R^n/M es finito (grupo abeliano finito) y en este caso $|\mathrm{R}^n/\mathrm{M}| = |\triangle|$

   (b) Si $\mathrm{R} = \mathrm{K}[x]$, K cuerpo , R^n/M es de torsión , finitamente generado $\Leftrightarrow$ $\mathrm{K}[x]^n/\mathrm{M}$ es de dimensión finita como e.v sobre K , y en este caso , $\mathrm{gr}(\triangle) = \dim_{\mathrm{K}} V$.

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 $\alpha : \begin{array}{ccc} \Lambda & \longrightarrow & \mathbb{N} \\ \lambda & \longrightarrow & \alpha(\lambda) = \alpha_\lambda \end{array}$ una función tal que $\forall\lambda \in \Lambda$, salvo un número finito de ellos , $\alpha_\lambda = 0$. Sea $\mathcal{F}$ el conjunto de estas funciones α .

La suma queda bien definida en $\mathcal{F}$:

Sean $\alpha, \beta \in \mathcal{F}$ $\alpha + \beta : \begin{array}{ccc} \Lambda & \longrightarrow & \mathbb{N} \\ \lambda & \longrightarrow & \alpha_\lambda + \beta_\lambda \end{array}$

+ 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 $\{\lambda_1, \ldots, \lambda_k\} = \{\lambda \in \Lambda / \alpha_\lambda \neq 0\}$.

El conjunto de polinomios a coeficientes en R con indeterminada $\mathcal{X} = \{x_\lambda\}_{\lambda\in\Lambda}$ será $\mathrm{R}[\mathcal{X}] = \mathrm{R}[\{x_\lambda\}_{\lambda\in\Lambda}] = \bigoplus_{\alpha\in\mathrm{F}} \mathrm{R}x^\alpha$. Notar que $(\mathrm{R}[\mathcal{X}], +)$ es un R - módulo libre de base $\{x^\alpha\}_{\alpha\in\mathrm{F}}$.

Definimos ahora el producto en $\mathrm{R}[\mathcal{X}]$ como sigue :

Para dos elementos de la base : $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$, y luego se extiende linealmente en cada factor : $(\sum_{i=1}^n r_i x^{\alpha_i})(\sum_{j=1}^m s_j x^{\beta_j}) = \sum_{\substack{i=1\ldots m \\ j=1\ldots n}} r_i s_j x^{\alpha_i+\beta_j}$

Ejercicio:

1. Probar que tenemos un producto bien definido en $\mathrm{R}[\mathcal{X}]$ y que $(\mathrm{R}[\mathcal{X}], +, \cdot)$ es un anillo conmutativo de neutro $x^o \equiv 1$.

2. La función $\varphi : \mathrm{R} \to \mathrm{R}[\mathcal{X}]$ tal que a r le asigna $\varphi(r) = rx^o$ es un monomorfismo de anillos , que permite identificar $r \in \mathrm{R}$ con $rx^o \in \mathrm{R}[\mathcal{X}]$.

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 $\{\lambda_1, \ldots, \lambda_k\} = \{\lambda \in \Lambda / \beta_\lambda \neq\}$, entonces $x^\beta = x_{\lambda_1}^{\beta_{\lambda_1}} \cdots x_{\lambda_k}^{\beta_{\lambda_k}}$

4. Si R no tiene divisores del 0$\Rightarrow$ $\mathrm{R}[\mathcal{X}]$ no tiene divisores del 0.

5. $\mathrm{R}[\mathcal{X}]$ tiene la siguiente "propiedad universal" : Si S es un anillo cualquiera , y $\varphi : \mathrm{R} \to S$ 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 $\widetilde{\varphi} : \mathrm{R}[\mathcal{X}] \to S$ tal que $\widetilde{\varphi}(r) = \varphi(r)\ \forall r \in \mathrm{R}$, y $\widetilde{\varphi}(x_\lambda) = s_\lambda\ \forall \lambda \in \Lambda$. En particular , si $\varphi : \mathrm{R} \to \mathrm{R}$ es la identidad , esto significa que , seleccionando para cada incognita x_λ un valor $s_\lambda \in \mathrm{R}$, cada polinomio $\sum r_i x^{\alpha_i} \in \mathrm{R}[\mathcal{X}]$ da orígen 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 ($\mathrm{K}|_\mathrm{k}$) ssi k es subcuerpo de K .

K es un espacio vectorial sobre k , y su dimensión se anota $[\mathrm{K} : \mathrm{k}] = \dim_\mathrm{k}\mathrm{K}$. La extensión se dice finita si $[\mathrm{K} : \mathrm{k}] = \dim_\mathrm{k}\mathrm{K}$ es finita.

Definición

Sea $\mathrm{K}|_\mathrm{k}$ una extensión . Un elemento $\alpha \in \mathrm{K}$ se dice **algebraico** sobre k ssi $\exists p(x) \in \mathrm{k}[x] \setminus \{0\}$, tal que $p(\alpha) = 0$. La extensión $\mathrm{K}|_\mathrm{k}$ se dice **algebraica** ssi todo $a \in \mathrm{K}$ 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 $\mathrm{K}|_\mathrm{k}$ es finita , entonces es algebraica.

Dem.

Si $a \in$ K , entonces $\{1, a, a^2, \ldots\} \subseteq$ K . Este conjunto no es l.i , pues al ser $\dim_{\mathrm{k}}\mathrm{K} < \infty$,cualquier conjunto l.i será finito $\Rightarrow \exists \lambda_o, \ldots, \lambda_n \in k$, no todos nulos , tal que $\lambda_o 1 + \lambda_1 a + \lambda_2 a^2 + \cdots \lambda_n a^n = 0$. Tomando $p(x) = \lambda_o + \lambda_1 x + \cdots + \lambda_n x^n \in \mathrm{K}[x] \setminus \{0\}$, se tiene $p(a) = 0 \Rightarrow a$ es algebraico.

Definición

Sean $\mathrm{K}|_{\mathrm{k}}$ 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 $\mathrm{k}(A)$.

Este subcuerpo existe y es

$\mathrm{k}(A) = \{\frac{p(a_1 \ldots a_n)}{q(a_1 \ldots a_n)} / n \in \mathbb{N}, p(x_1 \ldots x_n), q(x_1 \ldots x_n) \in \mathrm{k}[x_1 \ldots x_n],\ a_1 \ldots a_n \in A, q(a_1 \ldots a_n) \neq 0\}$

K se dice **finitamente generado** sobre k si A es finito.

Prop

Si $\mathrm{K}|_{\mathrm{k}}$ es una extensión finita , entonces K es finitamente generado como cuerpo sobre k .

Dem.

Si $\{v_1 \ldots v_n\}$ es base de K como espacio vectorial sobre k , entonces $\mathrm{K} = \mathrm{k}(v_1, \ldots, v_n)$.

Nota : La recíproca de esta propiedad no es cierta . Veamos un ejemplo:
Sean k un cuerpo cualquiera y $\mathrm{k}(x)$ el cuerpo cuociente de $\mathrm{k}[x]$:

$\mathrm{k}(x) = \left\{\frac{p(x)}{q(x)} / p(x), q(x) \in \mathrm{k}[x],\ q(x) \neq 0\right\}$.

$\mathrm{k} \subseteq \mathrm{k}[x] \subseteq \mathrm{k}(x)$, por lo tanto , $\mathrm{k}(x)$ es una extensión finitamente generada (generada por x) sobre k y $[\mathrm{k}(x) : \mathrm{k}] = \infty$.

Polinomio mínimo de un elemento algebraico

Sean $\mathrm{K}|_{\mathrm{k}}$ y $a \in$ K algebraico sobre k . Sea $\mathrm{I} = \{p(x) \in \mathrm{k}[x] / p(a) = 0\}$

- $\mathrm{I} \supset \{0\}$ (inclusión estricta) , pues a es algebraico sobre k .
- I es un ideal en $\mathrm{k}[x]$ (no degenerado , pues $1 \notin \mathrm{I}$)

$\mathrm{k}[x]$ es un dip, por lo tanto, $\mathrm{I} = (m(x))$, 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 $\text{gr}(m(x))$.
$\text{I} = (m(x)) \Rightarrow m(a) = p(a)q(a) = 0 \Rightarrow p(a) = 0 \vee q(a) = 0 \Rightarrow p(x) \in \text{I} \vee q(x) \in \text{I}$
$\Rightarrow \text{gr}(p(x)) \geq m(x) \vee \text{gr}(q(x)) \geq m(x) \rightarrow\leftarrow$

Por lo tanto , $\exists! m(x) \in \text{k}[x]$ primo , mónico y de grado mínimo tal que
$\{p(x) \in \text{k}[x] / p(a) = 0\} = m(x) \cdot \text{k}[x]$

$m(x)$ se llama "**polinomio minímo "** o "**polinomio irreducible"** de a con respecto al cuerpo k

Notar que $\text{I} = \text{Ker}\varphi$, con φ el morfismo de anillos $\varphi : \text{k}[x] \rightarrow \text{K}$ tal que a $p(x) \in \text{k}[x]$ le asigna $\varphi(p(x)) = p(a)$. Así , la imagen de φ , que anotaremos $\text{k}[a]$ es un subanillo de K , y es isomorfo , como subanillo de K , a $\text{k}[x]/\text{Ker}\varphi$, de esta forma, $\text{k}[a] \cong \text{k}[x]/(m(x))$ ($p(a) \rightarrow [p(a)]$) .

Notemos que , debido a que $m(x)$ es irreducible , el ideal $\text{I} = (m(x))$ 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 $\Rightarrow \text{k}[x]/(m(x))$ cuerpo$\Rightarrow \text{k}[a] = \{\lambda_o + \lambda_1 a + \cdots + \lambda_n a^n / n \in \mathbb{N}, \lambda_o \ldots \lambda_n \in \text{k}\}$ es un cuerpo , y es el subcuerpo de K generado por k y a . En efecto:
Es claro que $\text{k}[a] \subseteq \text{k}(a)$.
La otra inclusión es cierta , pues a y k están contenidos en $\text{k}[a]$.

Problema Relacionado

Sea k un cuerpo y $p(x) \in \text{k}[x]$ un polinomio primo .

¿Existe algún cuerpo K , extensión de k , tal que $p(x)$ tenga al menos una raíz $a \in \text{K}$?

Existe , y se construye de la siguiente manera :

Consideremos el ideal $\text{I} = (p(x)) \subseteq \text{k}[x]$. Este ideal es maximal (pues $p(x)$ es primo), por lo tanto , $\text{E} = \text{k}[x]/(p(x))$ es cuerpo .

$$\begin{array}{rccc} \text{Sea} \quad \gamma : & \text{k} & \longrightarrow & \text{E} \\ & \alpha & \longrightarrow & \gamma(\alpha) = [\alpha] \end{array}$$

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 $\alpha \in \text{k}$ con $[\alpha] \in \text{E}$).

En E hay una raíz para $p(x)$. En efecto:

$\text{E} = \{[f(x)] / f(x) \in \text{k}[x]\}$, pero si $f(x) = a_o + a_1 x + \cdots + a_n x^n$, entonces $[f(x)] = a_o + a_1[x] + \cdots + a_n[x]^n \Rightarrow \text{E} = \{f([x]) / f(x) \in \text{k}[x]\}$.

$[f(x)] = f([x]) = 0 \Leftrightarrow f(x)$ es un múltiplo de $p(x)$, por lo tanto $p([x]) = 0$. De esta forma , concluímos que $[x] \in \text{E}$ 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 $f(x) = a_o + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x] \Rightarrow [f(x)] = a_o + a_1[x] + \cdots + a_n[x]^n$.

Sabemos que $[x^2+1] = 0 = [x]^2 + 1, \Rightarrow [x]^2 = -1$, por lo tanto , $\forall [f(x)] \in$ E, $[f(x)] = a1 + b[x]$. Así como e.v sobre $\mathbb{R}$, E $=< \{1, [x]\} >$.

$\{1, [x]\}$ son l.i :

Si $\lambda_o + \lambda_1[x] = 0$ en $E \Rightarrow [\lambda_o + \lambda_1 x] = 0 \Rightarrow \underbrace{\lambda_o + \lambda_1 x}_{\text{grado 1}} = q(x)\underbrace{(x^2+1)}_{\text{grado 2}} \Rightarrow \lambda_o = \lambda_1 = 0$

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$|_{\text{k}}$ es una extensión finita , con [E : k] $= \text{gr}(p(x))$:

Sea $p(x) = a_o + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m \quad a_i \in k, \forall i = 1 \ldots m-1$

$p([x]) = a_o + a_1[x] + \cdots + a_{m-1}[x]^{m-1} + [x]^m = 0 \Rightarrow [x]^m = \sum_{i=0}^{m-1}(-a_i)[x]^i$ Por inducción se tiene que $[x]^j =< \{1, [x], \ldots, [x]^{m-1}\} > \forall j \geq m$. Luego , como espacio vectorial sobre k , E está generado por $\{1, [x], \ldots, [x]^{m-1}\}$ .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$[x]$ $\Rightarrow \lambda_i = 0 \ \forall i = 0 \ldots m-1$.

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:

Obsercación : 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$|_{\text{k}}$ es extensión finita $\Leftrightarrow$ E$|_{\text{K}}$ y K$|_{\text{k}}$ son extensiones finitas.

Corolario

Sean $K|_k$ una extensión y $a_1, \ldots, a_n \in K$ algebraicos sobre k , entonces $k(a_1, \ldots, a_n)|_k$ es una extensión algebraica.

Dem.

Consideremos la siguiente cadena de subcuerpos de K :

$k = k_o \hookrightarrow k(a_1) = k_1 \hookrightarrow \cdots \hookrightarrow k(a_1 \ldots a_n) = k_n$. 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 , $[k(a_{i+1}) : k_i] < \infty$, concluímos entonces que $k_n|_{k_o} = k(a_1 \ldots a_n)|_k$ 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 $a \in K = k(a_\lambda : \lambda \in \Lambda) \Rightarrow a = \frac{p(a_{\lambda_1} \ldots a_{\lambda_n})}{q(a_{\lambda_1} \ldots a_{\lambda_n})}$ con $p(x_1 \ldots x_n), q(x_1 \ldots x_n) \in k[x_1 \ldots x_n]$, $q(a_{\lambda_1} \ldots a_{\lambda_n}) \neq 0 \Rightarrow a \in k(a_{\lambda_1} \ldots a_{\lambda_n}) \subseteq K$, y ya probamos que $k(a_{\lambda_1} \ldots a_{\lambda_n})$ 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 $k \subseteq \overline{k} \subseteq K$ cerradura algebraica de k :

Sea $\overline{k} = \{a \in K / a$ es algebraico sobre k$\}$ .Sabemos que :

- $\overline{k}$ es un cuerpo
- $\overline{k}|_k$ es algebraico
- $k \subseteq \overline{k} \subseteq K$

Debemos probar que $\overline{k}$ es algebraicamente cerrado : Sea $f(x) \in \overline{k}[x]$ de grado ≥ 1 .Sabemos que $f(x)$ tiene una raíz $a \in K$.

Sea $E = k(a_o \dots a_n)$, donde $a_o \dots a_n \in \overline{k}$ son tales que $f(x) = a_o + a_1 x + \cdots + a_n x^n$. 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 $\Rightarrow a \in \overline{k}$.

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 $[E_1 : k] = gr(p_1(x))$). $p_2(x) \in k[x] \subseteq E_1[x]$, pero podría no ser primo en $E_1[x]$. Sea $\widetilde{p_2}(x)$ un factor primo de $p_2(x)$ en $E_1[x]$. Sabemos que E_1 se puede extender a $E_2 \cong E_1[x]/(\widetilde{p_2}(x))$ y $E_2 = E_1(a_2)$, con a_2 raíz de $\widetilde{p_2}(x)$, 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 $p_3(x)$ $\cdots E_n = E_{n-1}(a_n) = k(a_1 \dots a_n)$ 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 $f_1(x_1) + x_3 x_4 f_2(x_2)$ 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.

$$\mathrm{k} \overset{i}{\hookrightarrow} \mathrm{k}[\mathcal{X}] \overset{\nu}{\longrightarrow} \mathrm{k}[\mathcal{X}]/\mathrm{J} = \mathrm{E}$$

$\nu \circ i$ es morfismo de cuerpos$\Rightarrow$ es inyectiva , por lo tanto , podemos pensar que $\mathrm{k} \subseteq \mathrm{E}$. Además , los elementos de E son de la forma $\sum \alpha_i [x_{\lambda_1}]^{e_1} \cdots [x_{\lambda_k}]^{e_k}$, $\mathrm{E} = \mathrm{k}[[x_\lambda] : \lambda \in \Lambda]$. E está generado a partir de k por $\{[x_\lambda] : \lambda \in \Lambda\}$ y además en E : $f_\lambda([x_\lambda]) = [\underbrace{f_\lambda(x_\lambda)}_{\in \mathrm{I} \subseteq \mathrm{J}}] = 0$.

Llamando $b_\lambda = [x_\lambda] \in \mathrm{E}$, tenemos $\mathrm{E} = \mathrm{k}(b_\lambda : \lambda \in \Lambda)$,$f_\lambda(b_\lambda) = 0$.

Teorema

Todo cuerpo k tiene clausura algebraica .

Dem.

$\mathrm{E}_o = \mathrm{k}$, E_1 la extensión de E_o del lema anterior , ... En general , E_{n+1} es la extensión de E_n dada por el lema anterior . Tenemos: $\mathrm{k} = \mathrm{E}_o \subseteq \mathrm{E}_1 \subseteq \cdots \subseteq \mathrm{E}_n \subseteq \mathrm{E}_{n+1} \subseteq \cdots$

Sea $\mathrm{K} = \bigcup_{n \in \mathbb{N}} \mathrm{E}_n$, es cuerpo por ser unión creciente de cuerpos .

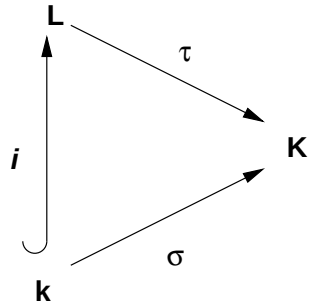
K es algebraico sobre k : Si $a \in \mathrm{K} \Rightarrow \exists n \in \mathbb{N}$ tal que $a \in \mathrm{E}_n$, pero E_n es algebraico sobre k $\Rightarrow$ K es algebraico sobre k .

K es algebraicamente cerrado : Sea $f(x) = a_o + \cdots + a_n x^n \in \mathrm{K}[x] \Rightarrow \exists m_o, \ldots, m_n \in \mathbb{N}$ tales que $a_o, \ldots, a_n$ están en $\mathrm{E}_{m_o}, \ldots, \mathrm{E}_{m_n}$ respectivamente , Si E_m es el mayor (con respecto a la inlcusión) de estos cuerpos , entonces $f(x) \in \mathrm{E}_m[x] \Rightarrow$ tiene raíz en $\mathrm{E}_{m+1} \subseteq \mathrm{K}$.

3.2.2 Inmersiones

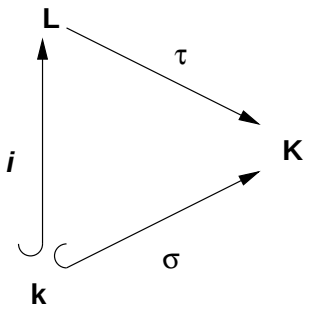
Si k y K son cuerpos , un morfismo de cuerpos $\sigma : \mathrm{k} \to \mathrm{K}$ se suele llamar una **inmersión** de k en K . Recordar que σ es necesariamente inyectivo.

Si ahora $\mathrm{L}|_\mathrm{k}$ es una extensión de cuerpos

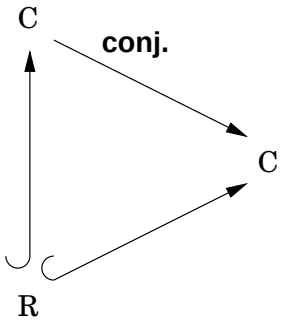


y $\tau : \mathrm{L} \to \mathrm{K}$ es una inmersión que extiende σ , se dice que "τ va sobre σ" .

Caso particular , si σ e una inclusión, se dice que "va sobre k" .

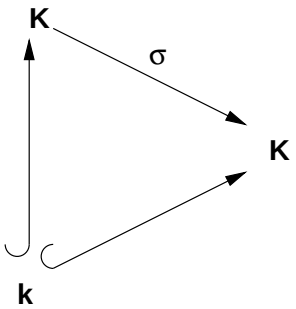


Ejemplo:



Lema

Sea $K|_k$ una extensión algebraica de cuerpos.



Sea σ una inmersión sobre k ($\sigma(x) = x \ \forall x \in k$) , entonces $\sigma : K \to K$ es un automorfismo de cuerpos.

Dem.

Observación1: Si $\sigma : \mathrm{K} \to \mathrm{K}$ 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 $\lambda \in \mathrm{k}$ $\sigma(\lambda) = \lambda$, por lo tanto , σ es k - lineal.

Observación2 : Así, si $[\mathrm{K} : \mathrm{k}] < \infty$, 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 $a \in \mathrm{K}$ y $\mathrm{E} = k(a)$, sabemos que , por ser a algebraico sobre k , $[\mathrm{E} : \mathrm{k}]$ = grado del polinomio mínimo de a en $\mathrm{k}[x] < \infty$.

Probemos que $\sigma(\mathrm{E}) \subseteq \mathrm{E}$.

Sea $p(x) = b_o + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n \in \mathrm{k}[x]$ el polinomio mínimo de $a \Rightarrow p(a) = b_o + b_1 a + \cdots + b_{n-1}a^{n-1} + a^n = 0$. Si aplicamos σ a $p(a)$: $\sigma(p(a)) = 0 = b_o + b_1\sigma(a) + \cdots + b_{n-1}\sigma(a)^{n-1} + \sigma(a)^n \Rightarrow \sigma(a)$ es otra raíz de $p(x)$ en K .

Supongamos que $a_1, \ldots, a_r$ son las raíces de $p(x)$ en K . Tratemos de trabajar con $\mathrm{L} = \mathrm{k}(a_1, \ldots, a_r)$, $\sigma(\mathrm{L}) = \mathrm{k}(\sigma(a_1), \ldots, \sigma(a_r))$, por el argumento anterior , $\sigma(a_i)$ es raíz de $p(x)$ en $\mathrm{K} \Rightarrow \sigma(\mathrm{L}) \subseteq \mathrm{L}$ (en realidad, es directamente igual). como $a_1 = a \in \mathrm{L} \Rightarrow a = \sigma(a_j)$ algún j .

Un poco más de nomenclatura :

Sea $\sigma : \mathrm{k} \to \mathrm{K}$ un morfismo de cuerpos , y sea $p(x) = a_o + a_1 x + \cdots + a_n x^n \in \mathrm{k}[x]$. Anotamos por $p^\sigma(x)$ al polinomio de $\mathrm{K}[x]$ dado por $p^\sigma(x) = \sigma(a_o) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$.

Tenemos un monomorfismo de anillos

$$\begin{array}{ccc} \mathrm{k}[x] & \longrightarrow & \mathrm{K}[x] \\ p(x) & \longrightarrow & p^\sigma(x) \end{array}$$

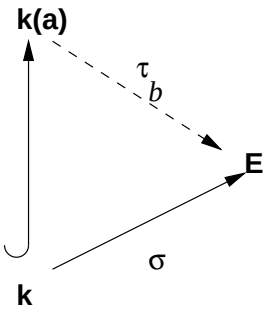
Además , $a \in \mathrm{k}$ raíz de $p(x) \Rightarrow \sigma(a) \in \mathrm{K}$ raíz de $p^\sigma(x)$.

Lema *

Sean $\mathrm{K}|_\mathrm{k}$ una extensión de cuerpos, $\sigma : \mathrm{k} \to \mathrm{E}$ una inmersión y $a \in \mathrm{K}$ algebraico sobre k . Sea $p(x) \in \mathrm{k}[x]$ el polinomio mínimo de a. Entonces , por cada raíz $b \in \mathrm{E}$ del polinomio $p^\sigma(x) \in \mathrm{E}[x]$, existe una única extensión $\tau : \mathrm{k}(a) \to \mathrm{E}$ de σ tal que $\tau(a) = b$. Llamemos τ_b a esta extensión . Además , toda extensión de σ a $\tau : \mathrm{k}(a) \to \mathrm{E}$ es de la forma τ_b , para algún b raíz de $p^\sigma(x)$ en E .

Dem.

Existencia de τ_b :



Sabemos que :

$$\begin{array}{ccc} \mathrm{k}(a) & \cong & \mathrm{k}[x]/(p(x)) \\ \lambda & \leftarrow & \lambda \in \mathrm{k} \\ a & \leftarrow & [x] \end{array}$$

Consideremos la función :

$$\gamma : \begin{array}{ccc} \mathrm{k}[x] & \rightarrow & \mathrm{E} \\ \lambda \in \mathrm{k} & \rightarrow & \sigma(\lambda) \in \mathrm{E} \\ x & \rightarrow & b \end{array} \quad \gamma(c_o + c_1 x + \cdots + c_n x^n) = \sigma(c_o) + \sigma(c_1)x + \cdots + \sigma(c_n)x^n \ .$$

(Es el único morfismo de anillos que extiende σ a todo $\mathrm{k}[x]$ 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

$$\widetilde{\gamma} : \begin{array}{ccc} \mathrm{k}[x[/(p(x)) & \rightarrow & \mathrm{E} \\ \lambda \in \mathrm{k} & \rightarrow & \sigma(\lambda) \\ [x] & \rightarrow & b \end{array} \ .$$

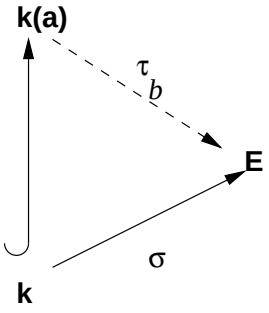
Tenemos entonces que :

$$\begin{array}{ccccc} & f & & \widetilde{\gamma} & \\ \mathrm{k}(a) & \cong & \mathrm{k}[x]/(p(x)) & \longrightarrow & \mathrm{E} \\ \lambda \in \mathrm{k} & \longrightarrow & \lambda \in \mathrm{k} & \longrightarrow & \sigma(\lambda) \\ a & \longrightarrow & [x] & \longrightarrow & b \end{array}$$

$\tau_b = \widetilde{\gamma} \circ f$ es tal que $\begin{cases} \tau_b(\lambda) = \sigma(\lambda) & \text{si } \lambda \in \mathrm{k} \\ \tau_b(a) = b \end{cases}$

La unicidad de τ_b viene del hecho que $\mathrm{k}(a)$ está generado por $\mathrm{k} \cup \{a\}$ 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 $\mathrm{k}(a)$ los elementos son de la forma $y = \alpha_o + \alpha_1 a + \cdots + \alpha_n a^n$ con $\alpha_i \in \mathrm{k}\ \forall i = 1 \ldots n$ ($y = f(a)$, $f(x) \in \mathrm{k}[x]$).

τ_b debiera satisfacer que $\tau_b(\alpha_o) + \tau_b(\alpha_1)\tau_b(a) + \cdots + \tau_b(\alpha_n)\tau_b(a)^n = \sigma(\alpha_o) + \sigma(\alpha_1)b + \cdots + \sigma(\alpha_n)b^n$. Pero y podría escribirse de varias maneras como polinomio evaluado en a . ¿Cómo garantizamos que $\sigma(\alpha_o) + \sigma(\alpha_1)b + \cdots + \sigma(\alpha_n)b^n$ no depende del polinomio que usamos para escribir y ?

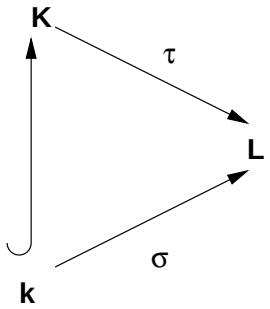
Para resolver este problema , recordemos que $\mathrm{k}(a) \cong \mathrm{k}[x]/(p(x))$ mediante $\alpha \in \mathrm{k} \to \alpha$, $x \to [x]$. Definamos entonces :

$$\left.\begin{array}{ccc} \mathrm{k}[x] & \to & \mathrm{L} \\ \alpha \in \mathrm{k} & \to & \sigma(\alpha) \\ x & \to & b \end{array}\right\} \text{único morfismo de anillos}$$

$q(x) = \alpha_o + \alpha_1 x + \cdots + \alpha_n x^n \to \varphi(q(x)) = \sigma(\alpha_o) + \sigma(\alpha_1)b + \cdots + \sigma(\alpha_n)b^n$ $\varphi(p(x)) = p^\sigma(b) = 0$: φ induce un único $\widetilde{\varphi} : \mathrm{k}[x]/(p(x)) \to \mathrm{L}$ tal que $\alpha_o + \alpha_1[x] + \cdots + \alpha_n[x]^n \to \sigma(\alpha_o) + \sigma(\alpha_1)b + \cdots + \sigma(\alpha_n)b^n$.

Corolario *

Sea $\mathrm{K}|_\mathrm{k}$ extensión algebraica y $\sigma : \mathrm{k} \to \mathrm{L}$ una inmersión de k en un cuerpo algebraicamente cerrado L . Entonces existen inmersiones $\tau : \mathrm{K} \to \mathrm{L}$ sobre σ .

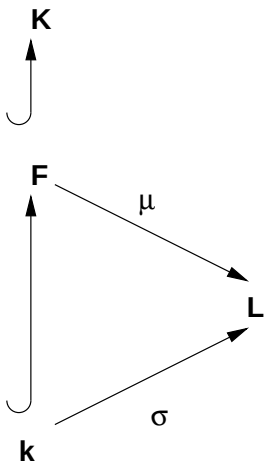


Si además , K es algebraicamente cerrado y L es algebraico sobre $\sigma(\mathrm{k})$, entonces cualquiera de tales τ es un isomorfismo.

Dem.

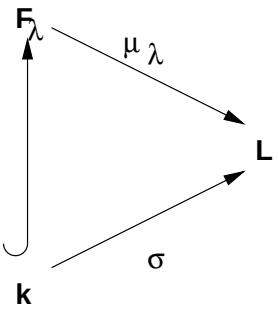
1) Existencia de extensiones $\tau : \mathrm{K} \to \mathrm{L}$:

Por Zorn , sea $A = \{\mu : \mathrm{J} \to \mathrm{L}/\mathrm{k} \subseteq \mathrm{J} \subseteq \mathrm{K},\ \mu|_\mathrm{k} = \sigma\}$

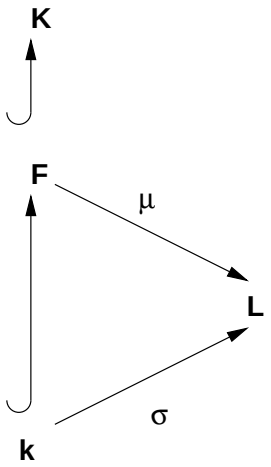


a) A es ordenado : $\mu_1, \mu_2 \in A$, $\mu_1 \preceq \mu_2 \Leftrightarrow \mu_2$ es extensión de μ_1

b) Si $\{\mu_\lambda\}_{\lambda\in\Lambda}$ es una cadena en A

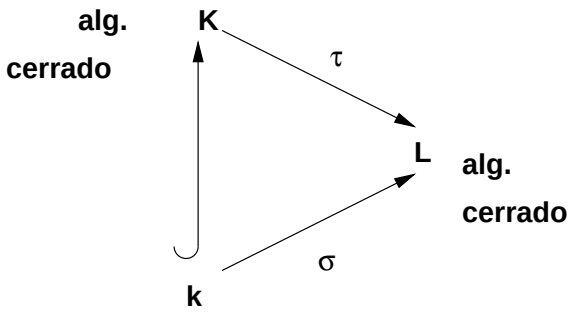


Sea $J = \bigcup_{\lambda\in\Lambda} J_\lambda$. J es un subcuerpo que contiene a k . Definamos $\begin{array}{rccc} \mu: & J & \to & L \\ & y \in J_\lambda & \to & \mu_\lambda(y) \end{array}$, μ está bien definida , y es morfismo de cuerpos sobre σ , por lo tanto , $\mu \in A$, y por definición , es 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 $a \in \mathrm{K} \setminus \mathrm{J}$, 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 $\mathrm{K}^{\tau} = \tau(\mathrm{K}) \subseteq \mathrm{L}$. k^{σ} es isomorfo a k y , por lo tanto , también algebraicamente cerrado , tenemos : $\mathrm{k}^{\sigma} \hookrightarrow \mathrm{K}^{\tau} \hookrightarrow \mathrm{L}$, con $\mathrm{L}|_{\mathrm{k}^{\sigma}}$ algebraica

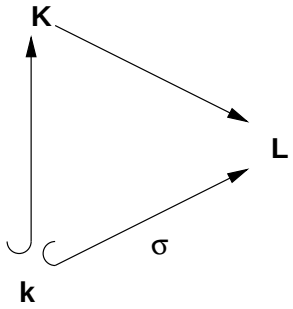
$\Rightarrow \mathrm{L}|_{\mathrm{K}^{\tau}}$ extensión algebraica $\Rightarrow \mathrm{L} = \mathrm{K}^{\tau}$.

Corolario

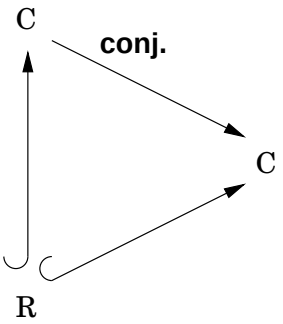
Si $\mathrm{K}|_{\mathrm{k}}$ y $\mathrm{L}|_{\mathrm{k}}$ son dos cerraduras algebraicas del mismo k , entonces existe un isomorfismo $\tau : \mathrm{K} \to \mathrm{L}$ sobre k .

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 $f(x) \in \mathrm{k}[x]$ es un polinomio de grado ≥ 1 , un " cuerpo de descomposición para $f(x)$ es una extensión K de k tal que:

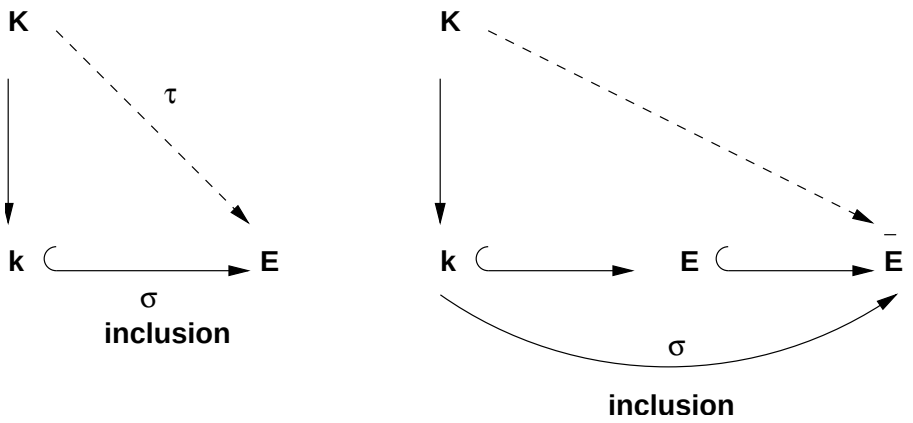
1. $f(x)$ tiene todas sus raíces en K . i.e $f(x)$ se descompone en factores lineales en K$[x]$: $f(x) = \lambda(x - c_1) \cdots (x - c_n)$ con $c_1, \ldots, c_n$ las raíces de $f(x)$.
2. K se genera a partir de k mediante las raíces de $f(x)$, i.e $\mathrm{K} = \mathrm{k}(c_1 \ldots c_n)$.

Prop

Si $f(x)$ es de grado ≥ 1 en k$[x]$, entonces:

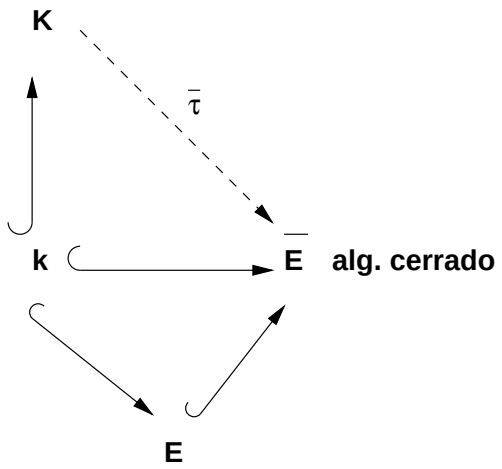
1. Existe un cuerpo de descomposición para $f(x)$.
2. Si $\mathrm{K}|_{\mathrm{k}}$ y $\mathrm{E}|_{\mathrm{k}}$ son dos cuerpos de descomposición de $f(x)$, entonces existen isomorfismos $\tau : \mathrm{K} \to \mathrm{E}$ sobre k (i.e $(\forall x \in \mathrm{k})\ \tau(x) = x$).

Dem.



Sea $\overline{\mathrm{E}}$ cerradura algebraica de E . Notar que , como $\overline{\mathrm{E}}$ es algebraico sobre E y E es algebraico sobre k , entonces $\overline{\mathrm{E}}$ es algebraico sobre k. Además $\overline{\mathrm{E}}$ es algebraicamente cerrado $\Rightarrow$ $\overline{\mathrm{E}}$ es cerradura algebraica de k .

Tenemos el siguiente diagrama :



Por un corolario anterior , la inclusión $\overline{\sigma}$: k $\rightarrow$ $\overline{\mathrm{E}}$ se puede extender a una inmersión $\overline{\tau}$: K $\rightarrow$ $\overline{\mathrm{E}}$ sobre k .

Debemos probar que $\overline{\tau}(\mathrm{K}) = \mathrm{E}$.

Como K y E son cuerpos de descomposición de $f(x) \in \mathrm{k}[x]$, entonces , en $\mathrm{K}[x] = \mathrm{k}(c_1 \dots c_n)$ $f(x) = \lambda(x - c_1) \cdots (x - c_n)$ y en $\mathrm{E}[x] = \mathrm{k}(c'_1 \dots c'_n)$ $f(x) = \lambda(x - c'_1) \cdots (x - c'_n)$.

$$\begin{array}{lccl} (\ )^{\overline{\tau}}: & \mathrm{K}[x] & \longrightarrow & \overline{\mathrm{E}}[x] \quad \text{morfismo de anillos} \\ & g(x) & \longrightarrow & g^{\overline{\tau}}(x) \end{array}$$

Notar que $f(x) = f^{\overline{\tau}}(x)$

$f(x) = \lambda(x - c_1) \cdots (x - c_n) \rightarrow f^{\overline{\tau}}(x) = \lambda(x - \overline{\tau}(c_1)) \cdots (x - \overline{\tau}(c_n))$, Así , en $\overline{\mathrm{E}}$, $f(x)$ se descompone en factores primos como $f(x) = \lambda(x - \overline{\tau}(c_1)) \cdots (x - \overline{\tau}(c_n))$.

Como $\mathrm{E} \subseteq \overline{\mathrm{E}}$, $f(x)$ tiene dos descomposiciones en $\overline{\mathrm{E}}[x]$:

1) $f(x) = \lambda(x - \overline{\tau}(c_1)) \cdots (x - \overline{\tau}(c_n))$

2) $f(x) = \lambda(x - c'_1) \cdots (x - c'_n)$

Por unicidad de descomposición en factores primos, en el dip $\overline{\mathrm{E}}[x]$, 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 $\overline{\tau}(c_i) = c'_j$, $\overline{\tau}(\{c_1, \dots, c_n\}) = \{c'_1, \dots, c'_n\}$ Pero $\mathrm{K} = \mathrm{k}(c_1, \dots, c_n)$ y $\mathrm{E} = \mathrm{k}(c'_1, \dots, c'_n)$, por lo tanto , $\overline{\tau}(\mathrm{k}) = \mathrm{k}(\tau(c_1), \dots, \tau(c_n)) = \mathrm{k}(c'_1, \dots, c'_n) = \mathrm{E}$

Definición

Si $\mathrm{F} = \{f_\lambda(x)\}_{\lambda \in \Lambda}$es una familia cualquiera de polinomios de grado ≥ 1 en $\mathrm{k}[x]$, un cuerpo de descomposición de la familia es una extensión $\mathrm{K}|_\mathrm{k}$ 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 $\mathrm{K}|_\mathrm{k}$ y $\mathrm{E}|_\mathrm{k}$ son cuerpos de descomposición de la familia F , entonces son isomorfos sobre k . Más aun , si $\overline{\tau} : \mathrm{K} \to \overline{\mathrm{E}}$ es una inmersión de K en la clausura algebraica $\overline{\mathrm{E}}$ de E , sobre k , entonces $\overline{\tau}(\mathrm{K}) = \mathrm{E}$, 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 $0, 1, 1+1, 1+1+1, \ldots, n\cdot 1, \ldots$. Sea $\mathrm{P} = \{n \cdot 1 / n \in \mathbb{Z}\}$, este el subanillo más pequeño en R .P se suele llamar el "**subanillo primo** de R"

$(\mathrm{P}, +)$ es un grupo cíclico generado por $\{1\}$, por lo tanto , es isomorfo a $(\mathbb{Z}_{|\mathrm{P}|}, +)$ si es finito o $(\mathbb{Z}, +)$ si no lo es .

Si P es finito , $|\mathrm{P}| = m$ es la primera vez que $\underbrace{1 + \cdots + 1}_{m \text{ veces}} = 0$, en caso contrario , $1 + \cdots + 1$ se anula.

Si $(\mathrm{P}, +) \cong (\mathbb{Z}_m, +)$, el anillo R se dice de **"característica** m**"** ,si $(\mathrm{P}, +) \cong (\mathbb{Z}, +)$, se dice de **"característica** 0**"** .

Notar que , en el caso de característica m , el isomorfismo

$$\begin{array}{ccc} \mathrm{P} & \longrightarrow & \mathbb{Z}_m \\ n\cdot 1 & \longrightarrow & [n] \end{array} \text{ es morfismo de anillos.}$$

Nota:

si $\underbrace{1 + \cdots + 1}_{m \text{ veces}} = 0 \Rightarrow (\forall a \in \mathrm{R})\ \underbrace{a + \cdots + a}_{m \text{ veces}} = a(\underbrace{1 + \cdots + 1}_{m \text{ veces}}) = 0$

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 $(\mathrm{P}, +, \cdot)$ 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 $\mathrm{k}_p \cong (\mathbb{Z}_p, +, \cdot)$. Así, k es una extensión de $\mathrm{k}_p \cong \mathbb{Z}_p$ .k será un e.v vectorial de dimensión finita (no podría tener una base infinita) sobre k_p .Si $\dim_{\mathrm{k}_p}\mathrm{k} = n$, entonces $\mathrm{k} \cong \mathrm{k}_p^n \cong (\mathbb{Z}_p)^n$ como e.v.

2. Caso característica 0 : El subanillo primo P es isomorfo a $(\mathbb{Z}, +, \cdot)$. Si tomamos los cuocientes entre elementos de P , resulta un subcuerpo , el subcuerpo más pequeño en k , llamado subcuerpo primo de k (anotamos $\mathrm{k}_{\mathbb{Q}}$) , que es isomorfo a $(\mathbb{Q}, +, \cdot)$. k es una extensión de $\mathrm{k}_{\mathbb{Q}}$ y , por lo tanto , un e.v sobre $\mathrm{k}_{\mathbb{Q}}$.

Teorema 1

Si k es un cuerpo finito , entonces $|\mathrm{k}| = p^n$, donde $p = \mathrm{car(k)}$ 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 $g(x) \in \mathrm{k}[x]$ 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 $D : \mathrm{k}[x] \to \mathrm{k}[x]$, tal que $D(x^n) = nx^{n-1}$ (ejercicio). Se prueba facilmente que si $f(x), g(x) \in \mathrm{k}[x]$, 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 $g(x) \in \mathrm{k}[x] \Leftrightarrow a$ 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 $\dim_{\mathbb{Z}_p}\mathrm{F} = n$ finito (ext. finita $\Rightarrow$ ext. algebraica).

Comencemos con $\mathrm{K} = \overline{\mathbb{Z}_p}$, la cerradura algebraica de $\mathbb{Z}_p$ (ext. algebraica más grande posible de $\mathbb{Z}_p$) . Llamemos $q = p^n$. Queremos buscar en $\mathrm{K} = \overline{\mathbb{Z}_p}$ un subcuerpo de q elementos .

Para la busqueda : Si F existiera , tomamos $\mathrm{G} = (\mathrm{F} \setminus \{0\}, \cdot)$ grupo multiplicativo con $q-1$ elementos $\Rightarrow (\forall x \in \mathrm{G})\ x^{q-1} = 1 \Rightarrow x^q = x$. Tendríamos entonces : $(\forall x \in \mathrm{F})\, x^q = x$.

Sea ahora $f(x) = x^q - x \in \mathbb{Z}_p[x] \subseteq \mathrm{K}[x]$ .Sea F el cuerpo de descomposición de $x^q - x$ (se puede buscar dentro de K) . Mostremos que $\mathrm{F} = \{\text{raíces de } x^q - x\}$

$\{\text{raíces de } x^q - x\}$ 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 , {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 = {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 $|\mathrm{F}| = p^j$, con j/n
2. $\forall j/n$, $\exists!$ subcuerpo F de F_q con $r = p^j$ elementos .

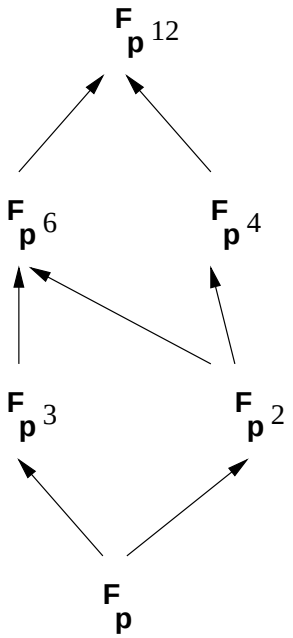
Dem.

La demostración queda de ejercicio, pero se pueden tomar en cuenta las siguientes indicaciones :

1. Si $\mathrm{k} \hookrightarrow \mathrm{K} \hookrightarrow \mathrm{E}$, entonces $[\mathrm{E} : \mathrm{k}] = [\mathrm{E} : \mathrm{K}] \cdot [\mathrm{K} : \mathrm{k}]$.
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 $(\mathrm{G},\cdot) \subseteq (\mathrm{k}^x,\cdot)$ es un subgrupo multiplicativo finito , entonces $(\mathrm{G},\cdot)$ es cíclico.

Dem.

Como $(\mathrm{G},\cdot)$ es finito , $(\mathrm{G},\cdot)$ es cíclico ssi $(\mathrm{G},\cdot) \cong (\mathbb{Z}_n,+)$, con $n = |\mathrm{G}|$.

Sea $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ la descomposición de n en producto de primos distintos entre si.

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1} \cdots p_l^{\alpha_l}} \cong \underbrace{\mathbb{Z}_{p_1^{\alpha_1}}}_{T_{p_1}(\mathbb{Z}_n)} \oplus \cdots \oplus \underbrace{\mathbb{Z}_{p_l^{\alpha_l}}}_{T_{p_l}(\mathbb{Z}_n)}$$

Lo que haremos para la demostración es entonces tomar una componente primaria cualquiera $T_p(\mathrm{G}) = \{a \in \mathrm{G} / a^{p^j} = 1, \text{ algún } j\}$ de G , y probar que es cíclico.

Sea $\mathrm{H} = T_p(\mathrm{G})$ una componente p - primaria , $\mathrm{H} = \{x \in \mathrm{G} / x^{p^j} = 1 \text{ , algún } j\} = \{x \in \mathrm{G} / O(< \{x\} >) = p^j \text{ , algún } j\}$.

Si H fuera cíclico como queremos , entonces $\mathrm{H} =< \{a\} >$, $O(a) = p^l$. p^l será el máximo orden de elementos en H .

Sea $p^l = \mathrm{Max}\{O(x)/x \in \mathrm{H}\}$ y a un elemento de H de orden p^l . Claramente : $p^l = O(a) = | < \{a\} > |/|\mathrm{H}|$. Además , $(\forall x \in \mathrm{H})\, x^{p^l} = 1$, pues $O(x) = p^j \leq p^l$.

Recordar que H es subgrupo de $(\mathrm{k}^x,\cdot)$. 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 $\Rightarrow |\mathrm{H}| \leq p^l$, por lo tanto , $|\mathrm{H}| = p^l$, y como el subgrupo $< \{a\} > \subseteq \mathrm{H}$ tiene también p^l elementos $\Rightarrow < \{a\} > = \mathrm{H}$.

***Ejercicio*:**

1. Sea $\mathrm{K}|_{\mathrm{k}}$ una extensión de cuerpos con $\mathrm{K} = \overline{\mathrm{k}}$ (cerradura algebraica de k) . Sea $a \in \mathrm{K}$, y sea $p(x)$ el polinomio mínimo de a en $\mathrm{k}[x]$. Si r es la multiplicidad de $p(x)$ (i.e , en la descomposición de $p(x)$ en $\mathrm{K}[x]$, $(x-a)$ aparece elevado a r), entonces , todas las raíces de $p(x)$ en K tienen multiplicidad r .

2. $\mathrm{Car}(\mathrm{k}) = 0 \Rightarrow r = 1$

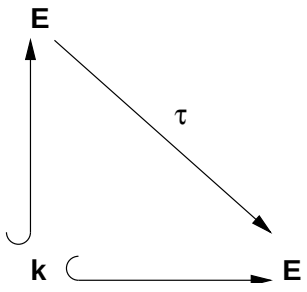
Dem.

1. $p(x) = (x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$ en $\mathrm{K}[x]$, con $a_1 \ldots a_l$ las raíces de $p(x)$ en $\mathrm{K}[x]$ de multiplicidades $r_1 \ldots r_l$ respectivamente . Podemos tomar $a_1 = a$ y , por lo tanto , $r_1 = r$.

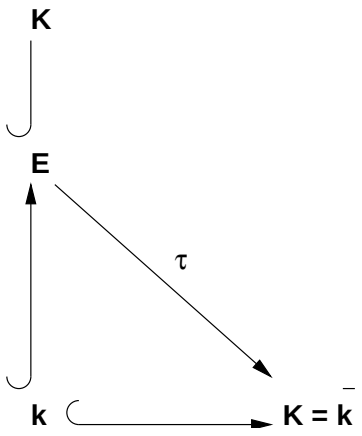
(Esta descomposición de $p(x)$ es válida también en $\mathrm{E} = \mathrm{k}(a_1 \ldots a_l) \subseteq \mathrm{K}$, el cuerpo de descomposición de $p(x)$).

Veamos que ocurre si existe una inmersión sobre k $\tau : \mathrm{E} \to \mathrm{E}$ 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 $\mathrm{E}[x] \Rightarrow$ 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.

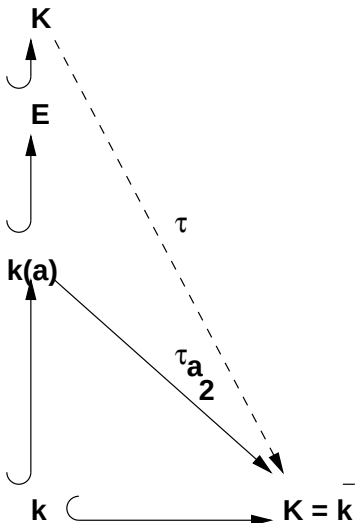
Buscamos



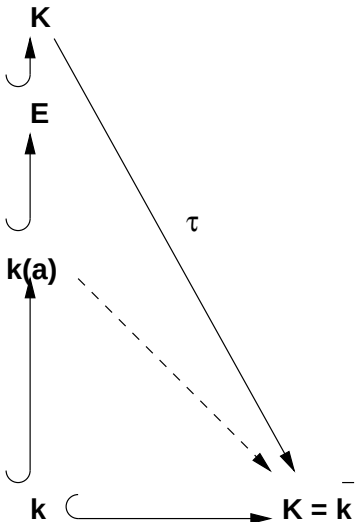
Nuestra situación es:



Primero, extendamos σ (inclusión) a $\tau_{a_2} : \mathrm{k}(a) \to \mathrm{K}$. Obtenemos:



usando el Corolario * , podemos extender la inmersión τ_{a_2} a toda la extensión algebraica E de $\mathrm{k}(a)$. Llegamos a $\tau : \mathrm{E} \to \mathrm{K}$ extensión de τ_{a_2}



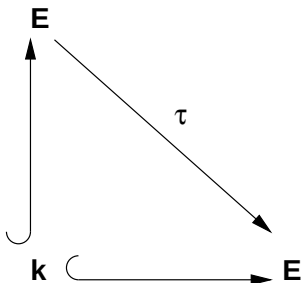
τ extiende la inclusión y además $\tau(a) = \tau(a_2)$. El único problema es como asegurar que $\tau(\mathrm{E}) \subseteq \mathrm{E}$.

$\mathrm{E} = \mathrm{k}(a_1 \dots a_l) \Rightarrow \tau(\mathrm{E}) = \mathrm{k}(\tau(a_1) \dots \tau(a_l))$.

¿Qué valores tienen $\tau(a_1) \dots \tau(a_l)$?

$p(x) = (x - a_1)^{r_1} \cdots (x - a_l)^{r_l}$, $p(x) = p^{\tau}(x) = (x - \tau(a_1))^{r_1} \cdots (x - \tau(a_l))^{r_l}$ en $\mathrm{K}[x]$ $\Rightarrow \tau(a_1) \dots \tau(a_l)$ son las raíces de $p(x)$ en K $\Rightarrow \tau(\mathrm{E}) = \mathrm{k}(\tau(a_1) \dots \tau(a_l)) = \mathrm{k}(a_1 \dots a_l) = \mathrm{E}$.

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 $p(x) \in \mathrm{k}[x]$ es irreducible de grado≥ 1, no tiene raíces repetidas.

$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_o \in \mathrm{k}[x]$ irreducible

$Dp(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in \mathrm{k}[x]$.

Si $a \in \overline{\mathrm{k}}$ es raíz repetida de $p(x)$, entonces también es raíz de $Dp(x) \rightarrow\leftarrow$ pues $\mathrm{gr}(Dp(x)) < \mathrm{gr}(p(x))$, 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 $\mathbb{Z}_2 = \mathrm{F}_2$, y $\mathrm{k} = \mathbb{Z}_2(\alpha)$ (Ejemplo : tomar $\mathrm{k} = \mathbb{Z}_2(x) = \left\{ \frac{p(x)}{q(x)} / p(x), q(x) \in \mathbb{Z}_2[x], q(x) \neq 0 \right\}$ $\alpha = x$) . 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 : Cark $= 2$ (su subcuerpo primo es $\mathbb{Z}_2$) y tiene un elemento α sin raíz cuadrada.

Tomemos el polinomio $p(x) = x^2 - \alpha \in \mathrm{k}[x]$. $p(x)$ es irreducible.

Extendamos k a $\mathrm{E} = \mathrm{k}(b)$ con b raíz de $p(x)$.

$b^2 - \alpha = 0$ en E $\Rightarrow$ $b^2 = \alpha \Rightarrow$ $p(x) = x^2 - b^2$ en $\mathrm{E}[x]$. 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 Cark $= p$, la función $\begin{array}{ccc} \mathrm{k} & \longrightarrow & \mathrm{k} \\ x & \longrightarrow & x^{p^j} \end{array}$ 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 Cark $= p$ $\Rightarrow$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 $\mathrm{K}|_{\mathrm{k}}$ son equivalentes :

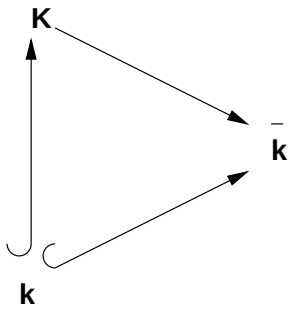
1. K es cuerpo de descomposición sobre k de una familia de polinomios irreducibles a coeficientes en k .
2. Todo polinomio irreducible $p(x) \in \mathrm{k}[x]$ que tiene una raíz $a \in \mathrm{K}$, se descompone completamente en factores lineales en $\mathrm{K}[x]$.
3. Sea $\overline{\mathrm{k}}$ una cerradura algebraica de k que contiene a K (por ejemplo $\overline{\mathrm{k}} = \overline{\mathrm{K}}$), cualquier inmersión $\sigma : \mathrm{K} \to \overline{\mathrm{k}}$ sobre k es un automorfismo de K .

Dem.

$2. \Rightarrow 1.$

Sea $\mathcal{F}$ la familia de todos los polinomios irreducibles $p(x) \in \mathrm{k}[x]$ que tienen una raíz $a \in \mathrm{K}$, 2. dice que cada poinomio de esta familia se descompone en factores lineales en $\mathrm{K}[x]$. Sus raíces generan K sobre k pues todo $a \in \mathrm{K}$ es raíz de algún polinomio irreducible en $\mathrm{k}[x]$: su polinomio mínimo en $\mathrm{k}[x]$.

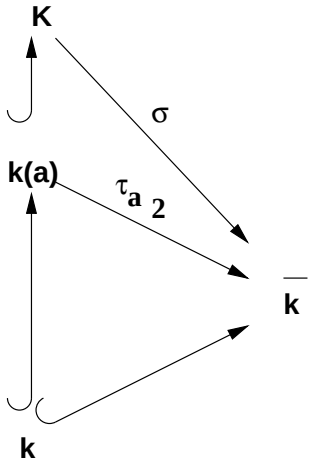
$3. \Rightarrow 2.$



Sea $p(x) \in \mathrm{k}[x]$ irreducible con una raíz $a \in \mathrm{K}$. Sabemos que en $\overline{\mathrm{k}}[x]$, $p(x)$ se descompone en factores lineales : $p(x) = \lambda(x - a_1) \cdots (x - a_n)$.

Necesitamos probar que $a_1 \ldots a_n$, las raíces de $p(x)$, están en $\mathrm{K} \subseteq \overline{\mathrm{k}}$.

Con un argumento ya usado antes , se puede extender la inclusión $\mathrm{k} \hookrightarrow \overline{\mathrm{k}}$ a un morfismo $\tau_{a_2} : \mathrm{k}(a) \to \overline{\mathrm{k}}$ tal que $\tau_{a_2}(a) = a_2$, y luego este , a un morfismo $\sigma : \mathrm{K} \to \overline{\mathrm{k}}$.



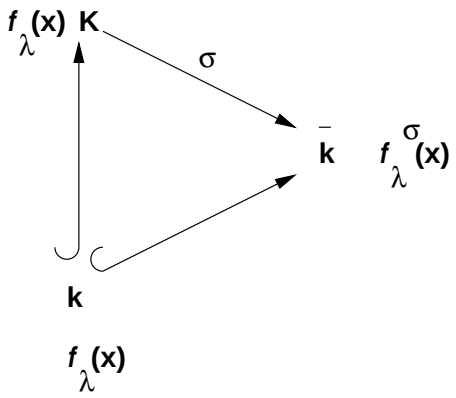
σ es una extensión de $\tau_{a_2} \Rightarrow \sigma(a) = \tau_{a_2}(a) = a_2$, pero 3. dice que $\sigma(\mathrm{K}) = \mathrm{K}$, por lo tanto ,$a_2 \in \mathrm{K}$. (lo mismo para $a_3 \ldots a_n$).

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 $a_1 \ldots a_n$ son las raíces de uno de estos f_λ , entonces $\sigma(a_1) \ldots \sigma(a_n) \in \mathrm{K}$. $f_\lambda(x) = \mu(x - a_1) \cdots (x - a_n)$ en $\mathrm{K}[x]$, $\mu \in \mathrm{k}$.

Consideremos $\begin{array}{ccc} \mathrm{K}[x] & \longrightarrow & \overline{\mathrm{k}}[x] \\ p(x) & \longrightarrow & p^\sigma(x) \end{array}$



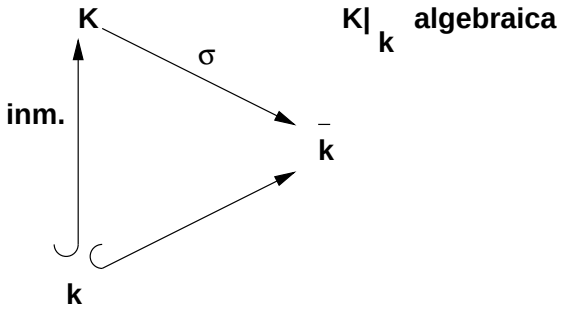
$f_\lambda(x) = \mu(x-a_1)\cdots(x-a_n)$ en $\mathrm{K}[x]$

$\Updownarrow$

$f_\lambda^\sigma(x) = \mu(x-\sigma(a_1))\cdots(x-\sigma(a_n))$ en $\overline{\mathrm{k}}[x]$

Tenemos dos descomposiciones del mismo polinomio en $\overline{\mathrm{k}}[x] \Rightarrow$ son iguales , salvo orden $\Rightarrow$ $\forall i$, $\exists j$ tal que $\sigma(a_i) = a_j \in \mathrm{K} \Rightarrow \sigma(\mathrm{K}) \subseteq \mathrm{K}$.

Tenemos entonces el siguiente diagrama :



σ inmersión sobre k , $\mathrm{K}|_{\mathrm{k}}$ 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 $a \in \mathrm{k}$ y $q(x) \in \mathrm{k}[x]$, tal que este último no tenga raíces en K . Sea $p(x) = (x-a)q(x)$, $p(x) \in \mathrm{k}[x]$ (evidentemente no es irreducible), $p(x)$ tiene una raíz $a \in \mathrm{K}$ y no se descompone en factores lineales en $\mathrm{k}[x]$.

***Ejemplo*:**

Toda extensión $\mathrm{K}|_{\mathrm{k}}$ de grado 2 (i.e $[\mathrm{K} : \mathrm{k}] = 2$) es normal .

Dem.

Sea $p(x) \in \mathrm{k}[x]$ irreducible con alguna raíz $a \in \mathrm{K}$ .Supongamos que $a \notin \mathrm{k}$. Consideremos su polinomio mínimo sobre k.

Afirmamos que $\mathrm{gr}(p(x)) = 2$.

$$\underbrace{\mathrm{k} \hookrightarrow \mathrm{k}(a)}_{\text{grado del pol.min.}} \hookrightarrow \mathrm{K}$$

$\mathrm{k}(a) \cong \mathrm{k}[x]/(p(x))$, además $\mathrm{k}(a) = \mathrm{K}$

$[\mathrm{K} : \mathrm{k}] = \underbrace{[\mathrm{K} : \mathrm{k}(a)]}_{1}[\mathrm{k}(a) : \mathrm{k}] \Rightarrow [\mathrm{k}(a) : \mathrm{k}] = 2$.

***Ejemplo*:**

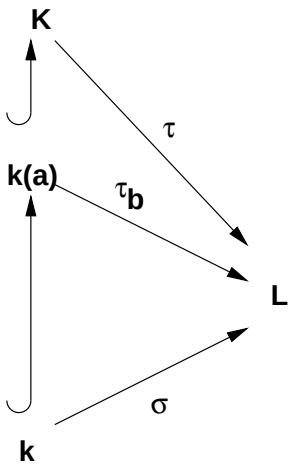
Ejemplo de una extensión que no es normal .

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 $\mathbb{Q}[x]$.

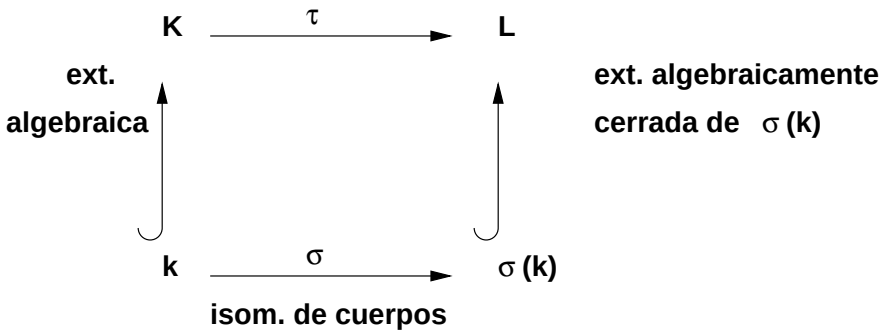
$p(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$ en $\mathbb{C}[x]$. Es fácil ver que ningún producto de estos cuatro factores (excepto de los cuatro juntos) está en $\mathbb{Q}[x] \Rightarrow p(x)$ es el polinomio mínimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}$, sin embargo , $p(x)$ tiene una raíz $\sqrt[4]{2}$ en $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathrm{R}$, 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 :



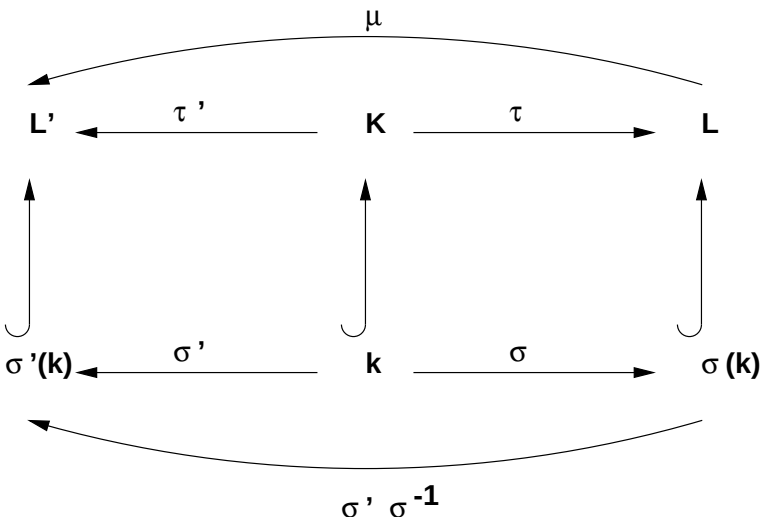
El mismo diagrama :



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 $\sigma' \circ \sigma^{-1} : \sigma(\mathrm{k}) \to \sigma'(\mathrm{k})$ se extiende a un isomorfismo $\mu : \mathrm{L}' \to \mathrm{L}$ (dado que L' , además de ser algebraicamente cerrado es algebraico sobre $\sigma'(\mathrm{k})$, y L , además de ser algebraico sobre $\sigma(\mathrm{k})$a es algebraicamente cerrado).

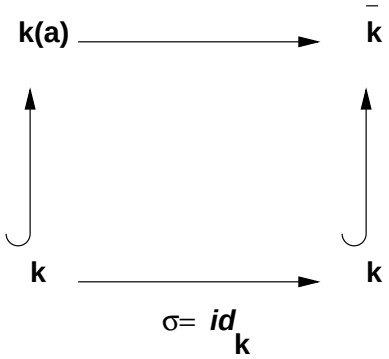
Si definimos los siguientes conjuntos :

$\mathrm{Ext}(\sigma) = \{\tau : \mathrm{K} \to \mathrm{L}/\tau$ es una inmersión extensión de σ $\}$

$\mathrm{Ext}(\sigma') = \{\tau : \mathrm{K} \to \mathrm{L}'/\tau$ es una inmersión extensión de σ' $\}$

Se deduce entonces que la función $\varphi : \begin{array}{ccc} \mathrm{Ext}(\sigma) & \to & \mathrm{Ext}(\sigma') \\ \tau & \to & \mu \circ \tau = \tau' \end{array}$ es una biyección .

En un caso simple : $\mathrm{K} = \mathrm{k}(a)$, 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 $p^{\sigma}(x)$, hay una y sólo una extensión $\tau_b : \mathrm{k}(a) \to \overline{\mathrm{k}}$, 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 , $\mathrm{gr}(p(x)) = r \cdot l = n \Rightarrow$ número de extensiones es $\leq n$.

Definición

Llamamos grado de separabilidad de la extensión $\mathrm{k}(a)|_{\mathrm{k}}$ al número de extensiones de σ . Anotamos $[\mathrm{k}(a):\mathrm{k}]_s \leq [\mathrm{k}(a):\mathrm{k}]$. Notar que $[\mathrm{k}(a):\mathrm{k}]_s/[\mathrm{k}(a):\mathrm{k}]$.

Esta definición se generaliza para cualquier extensión $\mathrm{K}|_{\mathrm{k}}$.

Prop

Sea $\mathrm{k} \hookrightarrow \mathrm{K} \hookrightarrow \mathrm{E}$ una cadena de extensiones algebraicas . Entonces :

1. $[\mathrm{E}:\mathrm{k}]_s = [\mathrm{K}:\mathrm{k}]_s \cdot [\mathrm{E}:\mathrm{K}]_s$.
2. Si K es una extensión finita $[\mathrm{K}:\mathrm{k}]_s \leq [\mathrm{K}:\mathrm{k}]_s$

Dem.

Probemos 2. a partir de 1.

K extensión finita $\Leftrightarrow \mathrm{K} = \mathrm{k}(a_1 \dots a_n)$ con $a_1 \dots a_n$ algebraicos sobre k .

Tenemos la siguiente cadena

$\mathrm{k} \hookrightarrow \mathrm{k}(a_1) \hookrightarrow \cdots \hookrightarrow \mathrm{k}(a_1 \cdots a_{n-1})(a_n) = \mathrm{K}$

En cada uno de estos pasos aplicamos que $[\mathrm{k}(a):\mathrm{k}]_s/[\mathrm{k}(a):\mathrm{k}]$. Obtenemos:

$[\mathrm{k}(a_1):\mathrm{k}]_s \leq_{\text{divisor de}} [\mathrm{k}(a_1):\mathrm{k}]$

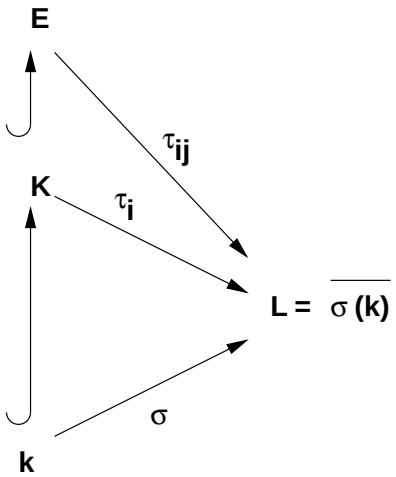
$\vdots$

$[\mathrm{k}(a_1 \dots a_n):\mathrm{k}(a_1 \dots a_{n-1})]_s \leq_{\text{divisor de}} [\mathrm{k}(a_1 \dots a_n):\mathrm{k}(a_1 \dots a_{n-1})]$

multiplicando y usando 1.

$[\mathrm{K}:\mathrm{k}]_s \leq_{\text{divisor de}} [\mathrm{K}:\mathrm{k}]$

Demostremos 1.



Sea $\mathrm{Ext}(\sigma) = \{\tau_i\}_{i\in I}$ la familia de todas las extensiones de σ a morfismos de K en L , $[\mathrm{K} : \mathrm{k}]_s = |\mathrm{Ext}(\sigma)| = |I|$. Para cada $i \in I$, sea $\mathrm{Ext}(\tau_i) = \{\tau_{ij}\}_{j\in J_i}$ la familia de extensiones de τ_i a inmersiones de E en L $(\forall i \in I)\,[\mathrm{E} : \mathrm{K}]_s = |\mathrm{Ext}(\tau_i)| = |J_i|$. Entonces , llamando $\mathrm{Ext}_{\mathrm{E}}(\sigma)$ a la familia de todas las extensiones posibles de σ a un morfismo de E en L , resulta $\mathrm{Ext}_{\mathrm{E}}(\sigma) = \{\tau_{ij} : i \in I, j \in J_i\}$ y $|\mathrm{Ext}_{\mathrm{E}}(\sigma)| = [\mathrm{E} : \mathrm{k}]_s = |\coprod_{i\in I} J_i| = \sum_{i\in I} |J_i| = |I|[\mathrm{E} : \mathrm{K}]_s = [\mathrm{K} : \mathrm{k}]_s[\mathrm{E} : \mathrm{k}]_s$

Definición

Una extensión finita $\mathrm{K}|_{\mathrm{k}}$ se dice **separable** ssi $[\mathrm{K} : \mathrm{k}]_s = [\mathrm{K} : \mathrm{k}]$.

- Si $\mathrm{E}|_{\mathrm{k}}$ es una extensión algebraica de k , un elemento $a \in \mathrm{E}$ se dice separable sobre k ssi $\mathrm{k}(a)|_{\mathrm{k}}$ es una extensión separable (ssi el polinomio mínimo de a en $\mathrm{k}[x]$ no tiene raíces repetidas).
- Un polinomio $f(x) \in \mathrm{k}[x]$ se dice separable ssi $f(x)$ no tiene raíces repetidas en su cuerpo de descomposición.
- Si $\mathrm{K}|_{\mathrm{k}}$ es una extensión algebraica (finita o infinita) , decimos que es separable si toda subextensión finita es separable (i.e , si $\forall$ subcuerpo $\mathrm{k} \subseteq \mathrm{F} \subseteq \mathrm{K}$, $\mathrm{F}|_{\mathrm{k}}$ es separable).

Propiedades simples

1. Si $\mathrm{k} \hookrightarrow \mathrm{K} \hookrightarrow \mathrm{E}$ es una cadena de extensiones finitas , entonces $\mathrm{E}|_{\mathrm{k}}$ es separable $\Leftrightarrow$ $\mathrm{E}|_{\mathrm{K}}$ y $\mathrm{K}|_{\mathrm{k}}$ son separables .
2. Si $\mathrm{k} \hookrightarrow \mathrm{K} \hookrightarrow \mathrm{E}$ es una cadena de extensiones algebraicas , entonces , si $a \in \mathrm{E}$ es separable sobre k , también lo es sobre K .

Dem.

Para demostrar 1. , usar lo siguiente:

$[\mathrm{E} : \mathrm{k}]_s = [\mathrm{E} : \mathrm{K}]_s \cdot [\mathrm{K} : \mathrm{k}]_s \qquad [\mathrm{E} : \mathrm{k}] = [\mathrm{E} : \mathrm{K}] \cdot [\mathrm{K} : \mathrm{k}]$.

Demostremos 2. :

Si $p_{\mathrm{k}}(x)$ es el polinomio mínimo de a en $\mathrm{k}[x]$ y $p_{\mathrm{K}}(x)$ es su polinomio mínimo en $\mathrm{K}[x] \Rightarrow p_{\mathrm{K}}(x)/p_{\mathrm{k}}(x)$ en $\mathrm{K}[x]$, por lo tanto , si $p_{\mathrm{k}}(x)$ no tiene raíces repetidas , entonces $p_{\mathrm{K}}(x)$ tampoco .

Prop

Una extensión algebraica $\mathrm{K}|_{\mathrm{k}}$ es separable ssi toda $a \in \mathrm{K}$ es separable sobre k .

Dem.

$\Rightarrow$)

$k(a)$ es extensión finita siobre 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_λ 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.

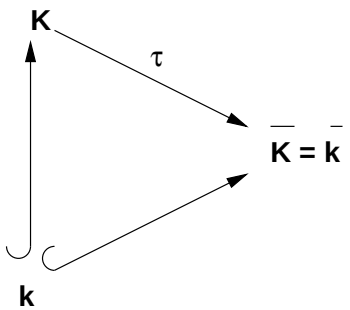
Observación:

En cuerpos de característica 0 , los poinomios irreducibles tienen raíces simples (no repetidas) , por lo tanto , toda extensión algebraica en característica 0 es separable.

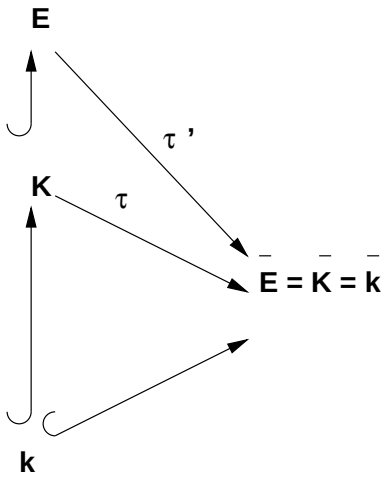
Ejemplo :

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 $\overline{\mathrm{K}}$, generado por $\{\tau(\mathrm{K})/\tau$ inmersión de K en $\overline{\mathrm{K}}$ sobre k$\}$ es una extensión finita de K , normal sobre k , y la menor posible. Tenemos :



Si existe tal E , este debe contener a $\tau(\mathrm{K})$, $\forall\tau : \mathrm{K} \to \overline{\mathrm{K}}$ inmersión sobre k . En efecto : si $\tau : \mathrm{K} \to \overline{\mathrm{K}}$ es inmersión sobre k , debe poder extenderse a $\tau' : \mathrm{E} \to \overline{\mathrm{K}}$ inmersión sobre k , y por la normalidad de $\mathrm{E}|_{\mathrm{k}} \Rightarrow \tau'(\mathrm{E}) = \mathrm{E} \Rightarrow \tau(\mathrm{K}) = \tau'(\mathrm{K}) \subseteq \tau'(\mathrm{E}) = \mathrm{E}$. Notar que tales inmersiones $\tau : \mathrm{K} \to \overline{\mathrm{K}}$ sobre k son un número finito : Hay $[\mathrm{K} : \mathrm{k}]_s \leq [\mathrm{K} : \mathrm{k}] < \infty$. Sean $\tau_1 \ldots \tau_r$ tales inmersiones .Sea E el cuerpo más pequeño que contiene a $\tau_1(\mathrm{K}) \ldots \tau_r(\mathrm{K})$ (subcuerpo de $\overline{\mathrm{K}}$). Si $\mathrm{E}|_{\mathrm{k}}$ es normal , buscamos:

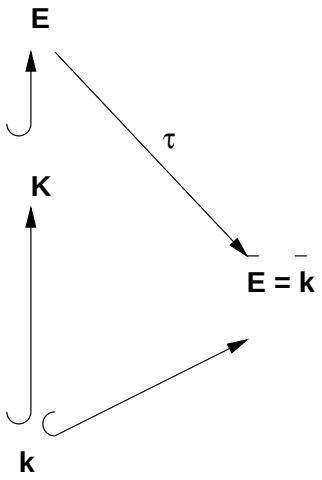
Definición:

Sean $\mathrm{K}_1, \mathrm{K}_2$ dos subcuerpos de un cuerpo L . El compuesto de K_1 y K_2 , que se anota $\mathrm{K}_1\mathrm{K}_2$ (o $\mathrm{K}_1 \vee \mathrm{K}_2$) , es el subcuerpo más pequeño de L que contiene a K_1 y a K_2 . Este subcuerpo es:

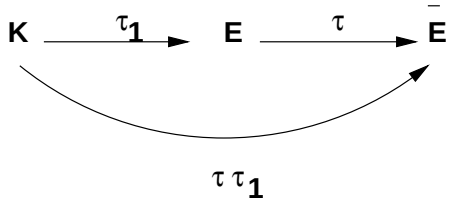
$$\mathrm{K}_1\mathrm{K}_2 = \left\{ \tfrac{\sum x_i y_i}{\sum x'_i y'_i} / x_i, x'_j \in \mathrm{K}_1, y_i, y'_j \in \mathrm{K}_2, \sum x'_i y'_i \neq 0 \right\}$$

$\mathrm{K}_1\mathrm{K}_2 = \mathrm{K}_1(\mathrm{K}_2) = \mathrm{K}_2(\mathrm{K}_1)$ y $\mathrm{K}_1\mathrm{K}_2 \cdots \mathrm{K}_n = \mathrm{K}_n(\cdots \mathrm{K}_3(\mathrm{K}_2\mathrm{K}_1) \cdots)$.

En el caso del ejemplo , $\mathrm{E} = \tau_1(\mathrm{K}) \cdots \tau_r(\mathrm{K})$. Probaremos luego que $\mathrm{E}|_{\mathrm{k}}$ es extensión finita.



Sea $\tau : \mathrm{E} \to \overline{\mathrm{E}}$ una inmersión sobre k .
$\tau(\mathrm{E}) = \tau(\ \tau_1(\mathrm{K}) \cdots \tau_r(\mathrm{K})) = \tau(\tau_1(\mathrm{K}))\tau(\tau_2(\mathrm{K})) \cdots \tau(\tau_r(\mathrm{K})) = \tau \circ \tau_1(\mathrm{K})\tau \circ \tau_2(\mathrm{K}) \cdots \tau \circ \tau_r(\mathrm{K})$.



$\tau \circ \tau_1$

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 , $\{\tau \circ \tau_i / i = 1 \dots r\} = \{\tau_i / i = 1 \dots r\} \Rightarrow \tau \circ \tau_1(\mathrm{K})\tau \circ \tau_2(\mathrm{K}) \cdots \tau \circ \tau_r(\mathrm{K}) = \tau_1(\mathrm{K}) \cdots \tau_r(\mathrm{K}) = \mathrm{E}$

Sólo resta ver que si $\mathrm{K}_1|_\mathrm{k}$ y $\mathrm{K}_2|_\mathrm{k}$ son dos extensiones finitas de k, con $\mathrm{k}, \mathrm{K}_1, \mathrm{K}_2 \subseteq \mathrm{L}$ cuerpo , entonces $\mathrm{K}_1\mathrm{K}_2|_\mathrm{k}$ es extensión finita. $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}] = [\mathrm{K}_1\mathrm{K}_2 : \mathrm{K}_1] \underbrace{[\mathrm{K}_2 : \mathrm{k}]}_{\text{finito}}$. Esperaríamos que

$[\mathrm{K}_1\mathrm{K}_2 : \mathrm{K}_1] \leq [\mathrm{K}_1 : \mathrm{k}]$

1) Si $\mathrm{K}_1 = \mathrm{k}(a)$

$\mathrm{K}_1\mathrm{K}_2 = \mathrm{k}(a)\mathrm{K}_2 = \mathrm{K}_2(\mathrm{k}(a)) = \mathrm{K}_2(a)$, luego

$\underbrace{[\mathrm{K}_2(a) : \mathrm{K}_2]}_{\mathrm{gr}(q(x)),q(x) \in \mathrm{K}_2[x]} \leq \underbrace{[\mathrm{k}(a) : \mathrm{k}]}_{\mathrm{gr}(p(x))} \Rightarrow q(x)/p(x)$

2) $[\mathrm{K}_2(a) : \mathrm{K}_2] \leq [\mathrm{k}(a) : \mathrm{k}]$

$[\mathrm{K}_2(a_1, a_2) : \mathrm{K}_2] = [\mathrm{K}_2(a_1, a_2) : \mathrm{K}_2(a_2)][\mathrm{K}_2(a_2) : \mathrm{K}_2]$

$\leq [\mathrm{k}(a_1a_2) : \mathrm{k}(a_2)][\mathrm{k}(a_2) : \mathrm{k}] = [\mathrm{k}(a_1a_2) : \mathrm{k}]$

Por lo tanto , $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}] \leq [\mathrm{K}_1 : \mathrm{k}][\mathrm{K}_2 : \mathrm{k}]$

Así , por ejemplo , $[\tau_1(\mathrm{K}) \dots \tau_r(\mathrm{K}) : \mathrm{k}] \leq [\mathrm{K} : \mathrm{k}]^r$

Definición

Sea $\mathrm{K}|_{\mathrm{k}}$ extensión de cuerpos . Un elemento $a \in \mathrm{K}$ se dice **primitivo** para $\mathrm{K}|_{\mathrm{k}}$ ssi $\mathrm{K} = \mathrm{k}(a)$. En tal caso , $\mathrm{K}|_{\mathrm{k}}$ se llama extensión primitiva.

Teorema del elemento primitivo

Sea $\mathrm{K}|_{\mathrm{k}}$ extensión algebraica:

1. $\mathrm{K}|_{\mathrm{k}}$ es primitiva ssi existe un número finito de "cuerpos intermedios" para la extensión. Es decir , $|\{\mathrm{Fcuerpo}\ /\mathrm{k} \subseteq \mathrm{F} \subseteq \mathrm{K}\}| < \infty$.
2. Si la extensión $\mathrm{K}|_{\mathrm{k}}$ es finita separable , entonces es primitiva .

Dem.

Caso K finito :

Lo único ha probar , es que toda extensión siempre tiene primitivos.

Consideremos $(\mathrm{K} \setminus \{0\}, \cdot)$, es grupo finito$\Rightarrow$ es cíclico $\Leftrightarrow \exists a \in \mathrm{K} \setminus \{0\}$ tal que $\mathrm{K} \setminus \{0\} = \{a^n : n \in \mathbb{N}\} \Rightarrow \mathrm{K} = \mathrm{k}(a)$.

Caso K no finito:

Demostremos primero 1.

$\Rightarrow$)

a elemento primitivo $\Leftrightarrow \mathrm{K} = \mathrm{k}(a)$. Sea $p(x) \in \mathrm{k}[x]$ el polinomio mínimo de a .

Si F es cuerpo intermedio , entonces $\mathrm{K} = \mathrm{F}(a)$. Sea $p_{\mathrm{F}}(x) \in \mathrm{F}[x]$ el polinomio mínimo de a en F .

$\mathrm{k} \subseteq \mathrm{F}$, entonces , como $p_{\mathrm{F}}(x)$ se anula en $a \Rightarrow p_{\mathrm{F}}(x)/p(x)$.

$p(x)$ tiene un número finito de divisores (en su su cuerpo de descomposición) , por lo tanto , si probamos que : F y F$'$ cuerpos intermedios $\Rightarrow p_{\mathrm{F}}(x) \neq p_{\mathrm{F}'}(x)$, estaríamos demostrando 1.

Veamos que $p_{\mathrm{F}}(x)$ determina F . Sea F$'$ el cuerpo construido a partir de k agregando los coeficientes del polinomio $p_{\mathrm{F}}(x) \in \mathrm{F}[x]$. Obviamente $\mathrm{k} \subseteq \mathrm{F}' \subseteq \mathrm{F}$, probaremos que en realidad $\mathrm{F}' = \mathrm{F}$.

Como F$'$ se construye a partir de los coeficientes de $p_{\mathrm{F}}(x)$, entonces $p_{\mathrm{F}}(x) \in \mathrm{F}'[x]$, además $p_{\mathrm{F}}(a) = 0$. Pero también $p_{\mathrm{F}}(x)$ es irreducible en $\mathrm{F}'[x]$, por lo tanto $p_{\mathrm{F}}(x)$ es el polinomio mínimo de a en $\mathrm{F}'[x]$: $p_{\mathrm{F}}(x) = p_{\mathrm{F}'}(x)$.

Además $\mathrm{F}(a) = \mathrm{K} = \mathrm{F}'(a)$, luego :

$[\mathrm{K} : \mathrm{F}] = \mathrm{gr}(p_{\mathrm{F}}(x)) = \mathrm{gr}(p_{\mathrm{F}'}(x)) = [\mathrm{K} : \mathrm{F}'] \Rightarrow [\mathrm{K} : \mathrm{F}'] = [\mathrm{K} : \mathrm{F}][\mathrm{F} : \mathrm{F}'] \Rightarrow [\mathrm{F} : \mathrm{F}'] = 1 \Rightarrow \mathrm{F} = \mathrm{F}'$

Así , si $p_{\mathrm{F}}(x)$ es el polinomio a coeficientes en $\mathrm{F}[x]$, entonces F está generado sobre k por los coeficientes de $p_{\mathrm{F}}(x)$.

$\Leftarrow$)

Si hay un número finito de cuerpos intermedios$\Rightarrow \mathrm{K} = \mathrm{k}(a)$

algún a . $[\mathrm{K} : \mathrm{k}]$ finito $\Rightarrow \mathrm{K} = \mathrm{k}(a_1 \dots a_n)$.

Probaremos por inducción en n que $(\forall n \in \mathbb{N})$, si $\mathrm{K} = \mathrm{k}(a_1 \dots a_n)$ entonces $\mathrm{K} = \mathrm{k}(a)$, para algún a .

Paso clave es con $n = 2$ ($\Rightarrow$ paso inductivo).

$\mathrm{k}(a_1 \dots a_{n+1}) = \mathrm{k}(a_1 \dots a_n)(a_{n+1})$,

H.I $\Rightarrow \mathrm{k}(a_1 \dots a_n) = \mathrm{k}(a') \Rightarrow$

$\mathrm{k}(a_1 \dots a_{n+1}) = \mathrm{k}(a_1 \dots a_n)(a_{n+1}) = \mathrm{k}(a' a_{n+1}) = \mathrm{k}(a'')$ ($n = 2$).

$n = 2$: Queremos probar que $\mathrm{K} = \mathrm{k}(a_1, a_2) = \mathrm{K} = \mathrm{k}(a)$ algún $a \in \mathrm{K}$.

Aquí usaremos K infinito $\Rightarrow$ k infinito

Para λ en k , sea $a^{\lambda} = a_1 + \lambda a_2$, y sea $\mathrm{F}_{\lambda} = \mathrm{k}(a^{\lambda}) = \mathrm{k}(a_1 + \lambda a_2)$.

Existe un número finito de subcuerpos F_{λ} y un número infinito de elementos $\lambda \Rightarrow \exists \lambda_1, \lambda_2 \in \mathrm{k}$, $\lambda_1 \neq \lambda_2$ tal que $\mathrm{F}_{\lambda_1} = \mathrm{F}_{\lambda_2} = \mathrm{F}$.

$a_1 + \lambda_1 a_2 \in \mathrm{F}$

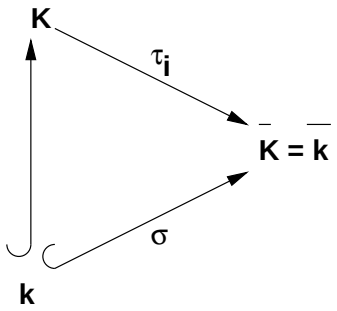
$a_1 + \lambda_2 a_2 \in \mathrm{F}$

restando: $\underbrace{(\lambda_1 - \lambda_2)}_{\neq 0 \in \mathrm{k}} a_2 \in \mathrm{F} \Rightarrow a_2 \in \mathrm{F}$, $a_1 = \underbrace{(a_1 + \lambda_2 a_2)}_{\in \mathrm{F}} - \underbrace{\lambda_1 a_2}_{\in \mathrm{F}} \Rightarrow a_1 \in \mathrm{F}$

$a_1, a_2 \in \mathrm{F} \Rightarrow \mathrm{K} \subseteq \mathrm{F} \subseteq \mathrm{K}$

Probemos 2.

$\mathrm{K}|_{\mathrm{k}}$ finita separable $\Leftrightarrow [\mathrm{K} : \mathrm{k}]_s = [\mathrm{K} : \mathrm{k}] = n$



Hay n inmersiones distintas entre si $\tau_1 \dots \tau_n : \mathrm{K} \to \overline{\mathrm{K}} = \overline{\mathrm{k}}$ sobre k .

Igual que en la demostración anterior , basta probar la propiedad para $\mathrm{K} = \mathrm{k}(a_1, a_2)$ y luego aplicar inducción.

Sea $f(x) \in \mathrm{K}[x]$ el polinomio siguiente:

$f(x) = \prod_{1 \le i \le j \le n} ((a_1 + xa_2)^{\tau_i} - (a_1 + xa_2)^{\tau_j}) \in \overline{\mathrm{K}}[x]$

$f(x) \neq 0$ en $\overline{\mathrm{K}}[x]$.

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 $\overline{\mathrm{K}} \Rightarrow$ como $\mathrm{k} \subseteq \mathrm{K}$ es infinito , habrá al menos un $\lambda \in \mathrm{k}$ 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 $\overline{\mathrm{K}}$.

Si $p(x) \in \mathrm{k}[x]$ es el polinomio mínimo de $a \Rightarrow p^{\tau_i}(x) = p(x)$

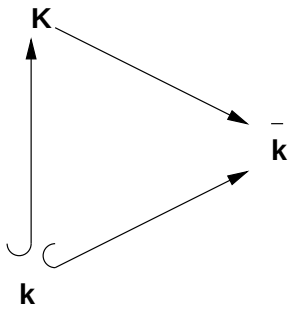
$\Rightarrow$ como $p(a) = 0$, $p(\tau_i(a)) = p^{\tau_i}(\tau_i(a)) = 0$. Luego , $p(x)$ tiene como raíces al menos a los n elementos distintos $\tau_1(a) \ldots \tau_n(a) \Rightarrow \mathrm{gr}(p(x)) \geq n$

$[\mathrm{K} : \mathrm{k}] = n \Rightarrow \mathrm{k}(a) \in \mathrm{K}$.

Ejercicio: Encontrar los cuerpos intermedios de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]|_{\mathbb{Q}}$.

3.4 Teoría de Galois

Sea $\mathrm{K}|_{\mathrm{k}}$ una extensión de cuerpos algebraica . La extensión se dice **de Galois** ssi es normal y separable .



- El **Grupo de Galois** de una extensión $\mathrm{K}|_{\mathrm{k}}$ es por definición $\mathrm{G} = \mathrm{Gal}(\mathrm{K}|_{\mathrm{k}}) = \{\sigma : \mathrm{K} \to \mathrm{K}/\sigma \text{ es automorfismo sobre k}\}$
- Dado un cuerpo K , y G un grupo de automorfismos de K , el **cuerpo fijo** de G es $\mathrm{K}^{\mathrm{G}} = \{x \in \mathrm{K}/\sigma(x) = x, \forall \sigma \in \mathrm{G}\}$

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 $G = Gal(K|_k)$ 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 $Gal(K|_{K^H}) = H$, 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 $H \triangleleft G$

$$\begin{array}{ccc} G/H & \cong & Gal(K^H|_k) \\ [\sigma] & \rightarrow & \sigma|_{K^H} \end{array} .$$

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 $p(x) \in R[x]$ de grado impar , tiene al menos una raíz en $\mathbb{R}$:

$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_o$ mónico , n impar.

Si $x \neq 0$, $p(x) = x^n \left(1 + \frac{a_{n-1}}{x} + \cdots + \frac{a_o}{x^n}\right)$ como función

$$p(x) \underset{x \rightarrow \infty}{\longrightarrow} \infty \qquad p(x) \underset{x \rightarrow -\infty}{\longrightarrow} -\infty$$

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 , $\exists \overline{x} \in \mathbb{R}$ tal que $p(\overline{x}) = 0$.

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 $x + yi = \pm\left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\,\mathrm{sgn}(b)\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\right)$.

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 xtensiones son separables , pero $E|_{\mathbb{R}}$ podría no ser normal , por lo tanto , $E|_R$ 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 $\sigma_1 \ldots \sigma_r$ las inversiones de E en $\overline{E}$ sobre $\mathbb{R}$.

$K|_{\mathbb{R}}$ es de Galois , por lo tanto , podemos aplicar el teorema fundamental . Llamemos $G = Gal(K|_{\mathbb{R}})$.

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 : $K|_F$ es de Galois , $P = Gal(K|_F)$, $|P| = [K : F]$

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 $\mathbb{R}[x]$. $gr(p(x)) = [\mathbb{R}(a) : \mathbb{R}]/[F : \mathbb{R}]$ impar $\Rightarrow$ $gr(p(x))$ 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 $\overline{G} = Gal(K|_{\mathbb{C}})$, $|\overline{G}| = [K : \mathbb{C}] = 2^{r-1}$. $\overline{G}$ es un 2 - grupo , y tendrá subgrupos (normales en $\overline{G}$) de todos los ordenes intermedios . En particular , $\exists H \subseteq G$ tal que $|H| = 2^{r-2}$ (a menos que $r = 1$ y $K = \mathbb{C}$).

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 $G = Gal(K|_k)$.

1. $K^G = k$
2. Si H es subgrupo de G y $F = K^H$, entonces $K|_F$ es extensión de Galois.

Dem.

1.

$G = \{\sigma : K \to K / \sigma$ 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 $k[x]$. $a \in k \Leftrightarrow k(a) = k \Leftrightarrow [k(a) : k] = gr(p(x)) = 1$.

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 $b \in \overline{K}$ de $p(x)$, $\exists!$ extensión de la inclusión $k \hookrightarrow \overline{K}$ a $\tau_b : k(a) \to \overline{K}$.

$\overline{K}|_{k(a)}$ es algebraica , por lo tanto , τ_b se puede extender a $\sigma : K \to \overline{K}$. Obviamente σ también será una extensión de la inclusión $k \hookrightarrow \overline{K}$.

$K|_k$ es normal $\Rightarrow \sigma(K) = K$. Tenemos entonces $\sigma : K \to K$ automorfismo de K sobre k , i.e $\sigma \in G$.

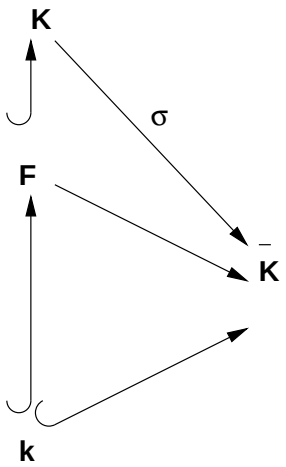
$a \in K^G \Rightarrow \sigma(a) = a$, pero dado que σ extiende a τ_b , $\sigma(a) = \tau_b(a) = b \Rightarrow b = a \Rightarrow$ la única raíz de $p(x)$ es a , y por ser de multipicidad 1 , concluios que $p(x)$ tiene sólo una raíz.

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 $\sigma : K \to \overline{K}$ 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 $G = Gal(K|_k)$. Definamos los siguientes conjuntos y funciones:

$\mathcal{C} = \{F/\ k \subseteq F \subseteq K$ cuerpo intermedio$\}$

$\mathcal{A} = \{H/H$subgrupo de $G\}$

$$\eta: \begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{A} \\ F & \longrightarrow & Gal(K|_F) \end{array} \qquad \gamma: \begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{C} \\ H & \longrightarrow & K^H \end{array}$$

$\gamma \circ \eta : \mathcal{C} \longrightarrow \mathcal{C}$ es $id_{\mathcal{C}}$. 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 $H = Gal(K|_F)$ ($H = \eta(F)$) . 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 $G = Gal(K|_k)$. 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 $F = F_1F_2$.
3. Si $H = H_1H_2 =< H_1 \cup H_2 >$ 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 $r = Max\{\overline{r}/\overline{r} = [k(a) : k]$, 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 $Gal(K|_k) = G$, $[K : k] = |G| = n$.

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 $\leq r \Rightarrow gr(q(x)) \leq r \leq n$ $\Rightarrow [k(a) : k] \leq n$. Por el lema 2 : $K|_k$ es una extensión finita , con $[K : k] \leq n$.

Falta probar $G = Gal(K|_k)$, $[K : k] = |G| = n$

La inclusión $G \subseteq Gal(K|_k)$ es directa .

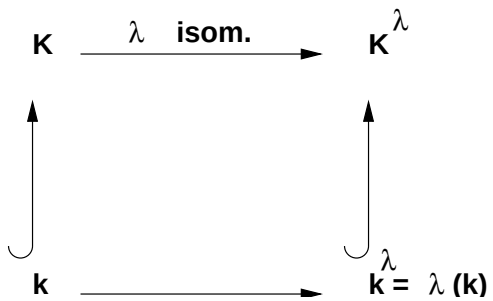
$n = |G| \leq |Gal(K|_k)| = [K : k]_s = [K : k] \leq n$, por lo tanto , $G = Gal(K|_k)$ y $[K : k] = n$.

Corolario

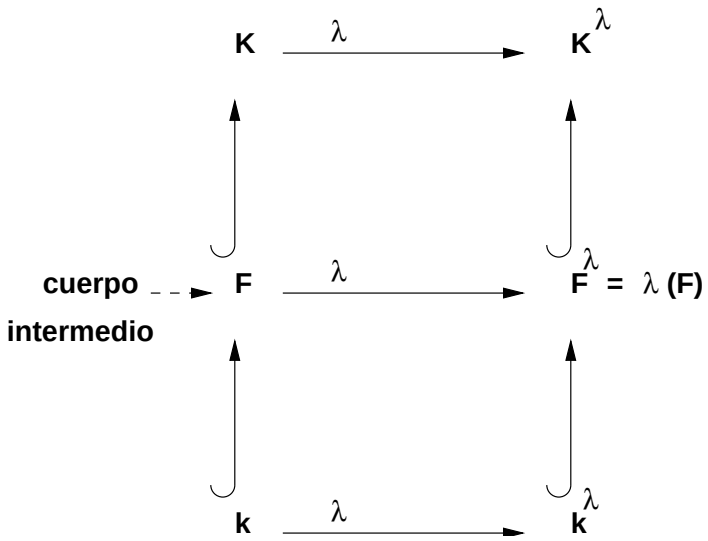
$$\text{id} \left\{ \begin{array}{ccccc} \mathcal{C} & \longrightarrow & \mathcal{A} & \longrightarrow & \mathcal{C} \\ F & \longrightarrow & Gal(K|_F) & & \\ & & H & \longrightarrow & K^H \end{array} \right.$$

Por el teorema de Artin , $Gal(K|_{K^H}) = H$ (la composición que faltaba).

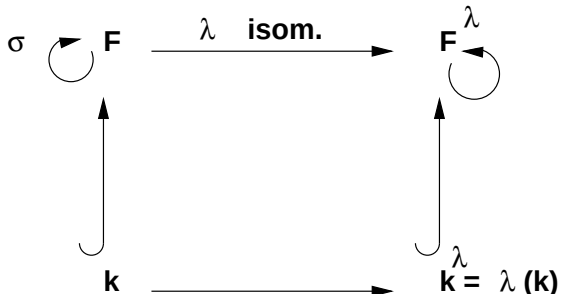
Para terminar de probar el teorema fundamental de la teoría de Galois consideremos la siguiente situación:



$K|_k$ extensión de Galois $\Leftrightarrow$ $K^\lambda|_{k^\lambda}$ es de Galois

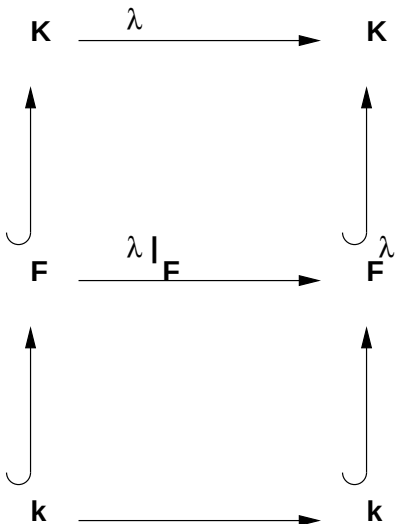


¿Qué relación hay entre $\mathrm{Gal}(F|_k)$ y $\mathrm{Gal}(F^\lambda|_{k^\lambda})$?



$$\mathrm{Gal}(F|_k) \cong \mathrm{Gal}(F^\lambda|_{k^\lambda}) \qquad \begin{array}{ccc} \mathrm{Gal}(K|_F) & \cong & \mathrm{Gal}(K^\lambda|_{F^\lambda}) \\ \sigma & \to & \lambda \circ \sigma \circ \lambda^{-1} \end{array}$$

Caso que nos interesará:



$\lambda \circ \mathrm{Gal}(\mathrm{K}|_{\mathrm{F}}) \circ \lambda^{-1} = \mathrm{Gal}(\mathrm{K}|_{\mathrm{F}^{\lambda}})$

Si $\mathrm{K}|_{\mathrm{k}}$ es de Galois y F cuerpo intermedio , con estas consideraciones se prueba la siguiente propiedad:

Prop

Si $\mathrm{K}|_{\mathrm{k}}$ es de Galois , F cuerpo intermedio , $\mathrm{G} = \mathrm{Gal}(\mathrm{K}|_{\mathrm{k}})$, $\mathrm{H} = \mathrm{Gal}(\mathrm{K}|_{\mathrm{F}})$, entonces $\mathrm{F}|_{\mathrm{k}}$ es de Galois $\Leftrightarrow \mathrm{H} \triangleleft \mathrm{G}$, y en este caso , la restricción $\sigma \in \mathrm{G}$, $\sigma|_{\mathrm{F}} : \mathrm{F} \to \mathrm{F}$ es un epimorfismo de G en $\mathrm{Gal}(\mathrm{F}|_{\mathrm{k}})$, con H su núcleo y $\mathrm{F}|_{\mathrm{k}}$ es de Galois , $\mathrm{G}/\mathrm{H} \cong \mathrm{Gal}(\mathrm{F}|_{\mathrm{k}})$.