R anillo conmutativo con 1.
K cuerpo

<u>Definición</u>. Un álgebra sobre R (ó K) es un R-módulo (ó K-espacio vectorial) con una función $\mu: A\times A \longrightarrow A$ bilineal. ($\mu(a,b)=ab$)

(1) $(ra)b = a(rb) = r(ab)$
(2) $a(b+c) = ab+ac$, $(b+c)a = ba+ca$; $\forall a,b,c\in A$, $r\in R$

- A asociativa ssi $(ab)c = a(bc)$
- A conmutativa ssi $ab=ba$
- A tiene unidad si $\exists 1_A \in A$: $1_A x = x 1_A$, $\forall x\in A$
  - Cuando esto ocurre, $R \hookrightarrow A$.

<u>Ejemplos</u>.

(1) Todo anillo es una $\mathbb{Z}$-álgebra
(2) $M_{n\times n}(R)$ es una R-álgebra asociativa con unidad, y no conmutativa cuando $n>1$.
(3) $R[x]$ es una R-álgebra asociativa, conmutativa y con unidad
(4) $(\mathbb{R}^3, \times)$ es una R-álgebra no asociativa, no conmutativa y sin unidad. Notar que $v\times w = -w\times v$, $v\times v = 0$

<u>Definición</u>.

(1) A R-álgebra ; $M,N \leq$ submódulos. Definimos NM como el submódulo generado por $\{ab \,/\, a\in N, b\in M\}$.
(2) $M\leq A$ es subálgebra si $MM\subseteq M$
(3) $M\leq A$ es ideal de A si $MA+AM\subseteq M$

A soluble $\Leftrightarrow$ $A^{(k)}=0$
A nilpotente $\Leftrightarrow$ $A^{t}=0$

$A^{(1)}=A$
$A^{(n+1)}=(A^{n})^2$

$A^1=A$
$A^n = AA^{n-1}+A^2A^{n-2}+\dots+A^{n-2}A^2$
$+A^{n-1}A$

• El R-módulo A/M es una R-álgebra si M es ideal de A.

Si I es ideal y A no asociativo, puede pasar que I^2 no es un ideal.

Si A es asociativa con unidad, llamamos al centro de A al conjunto

$$Z(A) = \{ x \in A / \ xy = yx \ , \ \forall y \in A \}$$

$Z(A)$ es una subálgebra de A.

<u>Definición</u>. Sean A, B R-álgebras, $\varphi : A \to B$ es homomorfismo si

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(ra) = r\varphi(a)$ $\qquad \forall a,b \in A$, $r \in R$.

(iii) $\varphi(ab) = \varphi(a)\varphi(b)$

Definidos $\ker(\varphi)$, $\mathrm{Im}(\varphi)$ tenemos resultados clásicos: $\ker\varphi \trianglelefteq A$ (ideal), $\mathrm{Im}(\varphi) \leq B$, $A/_{\ker\varphi} \cong \mathrm{Im}\,\varphi$ (averiguar los demás isomorfismos)

Cuando A, B tienen unidad, $\varphi(1_A) = 1_B$ (debe exigirse...)

Si $A = \mathcal{M}_n(R)$, $\varepsilon_{ij} = (x_{rs})_{r,s=1}^{n}$ tal que $x_{rs} = \delta_{ir}\delta_{js}$

$$x = (x_{rs})_{r,s=1}^{n} \implies x = \sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij}\varepsilon_{ij}$$

$$x \cdot y = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n}\sum_{l=1}^{n} x_{ij}\, y_{kl}\, \varepsilon_{ij}\,\varepsilon_{kl}$$

$$\varepsilon_{ij}\,\varepsilon_{kl} = \delta_{jk}\,\varepsilon_{il}$$

$$\begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = \varepsilon_{11} - \varepsilon_{22} \ , \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \varepsilon_{12}$$

Definición.

(1) Sea A una $\mathbb{R}$-álgebra. A es simple si sus únicos ideales son A y $\{0\}$.

(2) Una álgebra D es de división si es asociativa con 1 y $\forall x \in D$, x es invertible.

Teorema. Si D es álgebra de división, entonces $M_n(D)$ es simple $\forall n$.

Teorema. Sea D un álgebra de división, entonces $M_n(D)$ es simple.

$\{\varepsilon_{ij}\}_{i,j=1}^{n}$ D-base : $X = \sum_i \sum_j x_{ij}\varepsilon_{ij}$, $x_{ij} \in D$.

Dem. Sea $I \trianglelefteq M_n(D)$, $I \neq \{0\}$. Sea $Y \in I$, $Y \neq 0$. $\exists (r,s)$ tal que $Y = (y_{ij}) \Rightarrow y_{rs} \neq 0$ en D. $\Rightarrow \exists\, y_{rs}^{-1} \in D$. Sea $X = (x_{ij}) \in M_n(D)$

$X = \sum_{i,j} x_{ij}\varepsilon_{ij}$

[Chequear que se cumple $\varepsilon_{kr} Y \varepsilon_{sl} = y_{rs}\varepsilon_{kl} = \sum x_{ij}\varepsilon_{kr}\varepsilon_{ij}\varepsilon_{sl}$]

$= \sum_{i,j} x_{ij} y_{rs} y_{rs}^{-1} \varepsilon_{ij} = \sum_{i,j} x_{ij}\varepsilon_{ir} Y \varepsilon_{sj} y_{rs}^{-1} \varepsilon_{ij} \in I$

$\therefore I = M_n(D)$

Ejemplo 2. K-cuerpo, A una K-álgebra (A K-espacio vectorial). $\mathrm{Dim}_K(A) = n < \infty$. Existe base ordenada $\underbrace{(e_1, \dots, e_n)}_{=B}$ de A :

$\forall x \in A : \quad x = \sum_{i=1}^{n} x_i e_i$

En particular $e_i \cdot e_j = \sum_{k=1}^{n} \lambda_{ijk} e_k$. Si $y = \sum_{j=1}^{n} y_j e_j$, entonces $x \cdot y = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} x_i y_j \lambda_{ijk} e_k$. El conjunto $\{\lambda_{ijk}\}_{i,j,k=1}^{n}$ son las constantes de estructura de (A, B)

Ejemplo 3. Sea K cuerpo, $\mathrm{char}(K) \neq 2$. Sea $A = K \oplus Ki \oplus Kj \oplus Kij$

1_K es 1_A. Existen $a, b \in K \setminus \{0\}$ tales que $i^2 = a$, $j^2 = b$, $ij = -ji$.

A es asociativa.

$A = \left(\frac{a,b}{K}\right)$; cuando $K = \mathbb{R}$, $\mathbb{H} = \left(\frac{-1,-1}{K}\right)$

Se tiene que $M_2(K) \cong \left(\frac{1,1}{K}\right)$, donde $\{\varepsilon_{11}+\varepsilon_{22}, \varepsilon_{11}-\varepsilon_{22}, \varepsilon_{12}+\varepsilon_{21}, \varepsilon_{12}-\varepsilon_{21}\}$

<u>Lema</u>. Sea K cuerpo, $\mathrm{char}(K) \neq 2$, $A = \left(\frac{a,b}{K}\right) \Rightarrow Z(A) = K$

<u>Dem</u>. Evidente $K \subseteq Z(A)$. Falta demostrar $Z(A) \subseteq K$.
Consideramos $[x,y] = xy - yx$

$$x \in Z(A) \Leftrightarrow [x,y] = 0 \quad \forall y \in A$$

Sea $x = x_0 + x_1 i + x_2 j + x_3 ij$, $x_r \in K$ $(r = 0,1,2,3)$

$[i,x] = 2x_2\, ij + 2a x_3 j = 0$

$[j,x] = -2b x_3 i + 2x_1\, ij = 0$; ya que $x \in Z(A)$

$[ij,x] = 2b x_2 i + 2a x_1 j = 0$

$$\therefore x_1 = x_2 = x_3 = 0.$$

<u>Lema</u>. K cuerpo, $\mathrm{char}(K) \neq 2$, $\left(\frac{a,b}{K}\right)$ es simple.

<u>Dem</u>. Sea $I \trianglelefteq \left(\frac{a,b}{K}\right)$ no nulo. $x \in I$, $x \neq 0$. Se tiene que (por propiedad de ser ideal), $\{[i,x], [j,x], [ij,x]\} \subseteq I$.

$[j,[i,x]] = -4x_2 b i$.

Si $x_2 \neq 0 \Rightarrow i \in I \quad \therefore i a^{-1} i = 1 \in I = \left(\frac{a,b}{K}\right)$

$[ij,[j,x]] = 4ab x_3 j$.

Si $x_3 \neq 0 \Rightarrow j \in I = \left(\frac{a,b}{K}\right)$

$[i,[ij,x]] = -4a x_1 ij$.

Si $x_1 \neq 0 \Rightarrow ij \in I = \left(\frac{a,b}{K}\right)$

$(ij)^2 = -ab$

$\Rightarrow (ij)^{-1} = -a^{-1}b^{-1} ij$

Luego $(x_1,x_2,x_3) \neq (0,0,0) \Rightarrow I = \left(\frac{a,b}{K}\right)$

Para $\left(\frac{a,b}{K}\right) = A = K \oplus Ki \oplus Kj \oplus Kij$, tenemos el "espacio de cuaterniones puros" $A_+ = Ki \oplus Kj \oplus Kij$. Se cumple que $x \in A = \left(\frac{a,b}{K}\right)$ sii $x = c+z$, $c \in K$, $z \in A_+$. También:

$$x \in A_+ \iff x \notin Z(A),\ x^2 \in Z(A)$$

Definimos el conjugado de x como $\bar{x} = c - z$, y la norma como $N(x) = x\bar{x}$

- Propiedades de la norma y el conjugado:
  - $N(x) \in K$
  - $x\bar{x} = \bar{x}x$
  - $\bar{\bar{x}} = x$
  - $N(\bar{x}) = N(x)$
  - $\overline{x+y} = \bar{x} + \bar{y}$
  - $N(xy) = N(x)N(y)$
  - $x \in K \iff x = \bar{x}$ (char $K \neq 2$?)
  - $\forall x \in K : N(x) = x^2$
  - $\overline{xy} = \bar{y}\bar{x}$
  - $\forall (x,y) \in K \times A : N(xy) = x^2 N(y)$

Proposición. Para $A = \left(\frac{a,b}{K}\right)$. Son equivalentes

(i) A es de división

(ii) $\forall x \in A \setminus \{0\} : N(x) \neq 0$

(iii) $\forall (c_0, c_1, c_2) \in K^3 \setminus \{(0,0,0)\} : c_0^2 \neq ac_1^2 + bc_2^2$

Dem. A es de división, $x \in A \setminus \{0\} \Rightarrow \exists x^{-1} \in A : N(xx^{-1}) = N(1) = 1^2 = 1$

$$\therefore N(xx^{-1}) = N(x)N(x^{-1}) = 1$$

$$\therefore N(x) \neq 0.$$

Por demostrar que $N(x) = 0 \Rightarrow x = 0$.

Sea $x \in A$, $x \neq 0$. Se tiene que $N(x) \neq 0$. Sea $y = \frac{\bar{x}}{N(x)}$, se tiene $xy = 1$

Supongamos que existe $(c_0, c_1, c_2) \in K^2 \setminus \{(0,0,0)\}$, $c_0^2 = ac_1^2 + bc_2^2$.

Escogiendo $y = c_0 + c_1 i + c_2 j \neq 0$, $N(y) = c_0^2 - ac_1^2 - bc_2^2 = 0$.

Supongamos que $\forall (c_0, c_1, c_2) \in K^3 \setminus \{(0,0,0)\} \Rightarrow c_0^2 \neq ac_1^2 + bc_2$.

Sea $x = d_0 + d_1 i + d_2 j + d_3 ij$ con $N(x) = d_0^2 - ad_1^2 - bd_2^2 + abd_3 = 0$.

Se obtiene que

$$(d_0^2 - bd_2^2) = a(d_1^2 - bd_3^2) \quad / (d_1^2 - bd_3^2)$$

$$a(d_1^2 - bd_3)^2 = (d_0^2 - bd_2^2)(d_1^2 - bd_3^2)$$
$$= (d_0 d_1 + bd_2 d_3)^2 - b(d_0 d_3 + d_1 d_2)^2$$

Si $c_1 = d_1^2 - bd_3$, $c_0 = d_0 d_1 + bd_2 d_3$, $c_2 = d_0 d_3 + d_1 d_2$

$$c_0^2 = ac_1^2 + bc_2 \Rightarrow c_0 = c_1 = c_2 \Rightarrow \underbrace{d_1^2}_{c_0} - \underbrace{bd_3^2}_{c_2} = \underbrace{0}_{c_1}$$

$\Rightarrow c_0^2 = ac_1^2 + bc_2^2 \Rightarrow c_0 = c_1 = c_2 = 0 \Rightarrow d_1 = d_3 = 0$

Con lo anterior, $\underbrace{d_0^2}_{c_0} - \underbrace{bd_2^2}_{c_2} = \underbrace{0}_{c_1} \Rightarrow c_0^2 = ac_1^2 + bc_2^2$

$\Rightarrow c_0 = c_1 = c_2 = 0 \Rightarrow d_2 = d_3 = 0$

$$\therefore x = 0$$

Observación: $\mathbb{H} \rightsquigarrow c_0^2 = -c_1^2 - c_2^2$, $\mathcal{M}_2(K) \rightsquigarrow c_0^2 = c_1^2 + c_2^2$

$B: K^4 \times K^4 \to K$, $q(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$

La forma bilineal B puede ser definida por:

$B(x,y) = \frac{1}{2}(N(x+y) - N(x) - N(y))$, $N(rx) = r^2 N(x)$

$N(x) = B(x,x)$. B es bilineal simétrica no degenerada.

$B(x,y) = \frac{1}{2}(x\bar{y} + y\bar{x})$

$z, w \in A_+$, $B(z,w) = -\frac{1}{2}(zw + wz)$ ... (ver apuntes para mayor info)

—o—

Lema. Sean $A = \left(\frac{a,b}{K}\right)$, $A' = \left(\frac{a',b'}{K}\right)$ con normas N, N'

$$A \cong A' \Leftrightarrow \exists\, \varphi : A_+ \longrightarrow A'_+ \text{ lineal biyectiva tal que } N'(\varphi(z)) = N(z)$$

Dem. Sea $\varphi: A \to A'$ isomorfismo de álgebras. $\varphi(Z(A)) = Z(A)$

$\varphi(x^2) = \varphi(x)^2$. Si $x \in A_+ \Rightarrow \varphi(x) \in A'_+$ $\therefore$ $\varphi(A_+) = A'_+$.

$\phi = \varphi/_{A_+}$ es un isomorfismo lineal. Dado ~~[illegible]~~

Dado $z \in A_+$: $N'(\phi(z)) = N'(\varphi(z)) = -\varphi(z)^2 = \varphi(-z^2) = \varphi(N(z)) = \varphi(N(z)\cdot 1) = N(z)\varphi(1)$

$$= N(z)\,\varphi(1) = N(z)\cdot 1 = N(z).$$

($\Leftarrow$) Sea $\phi : A_+ \to A'_+$ isomorfismo lineal tal que $N'(\phi(z)) = N(z)$, $\forall z \in A_+$.
Sean B y B' ~~[illegible]~~ a sus funciones bilineales de N y N'.

$$B'(\phi(z), \phi(w)) = B(z,w), \quad \forall z, w \in A_+.$$

Consideramos $\Gamma' = \{1', \phi(i), \phi(j), \phi(ij)\}$. Por demostrar que Γ' es una base de A'. Si $\Gamma = \{1, i, j, k\}$ — Cambiar por $\phi(i)\phi(j)$

$$\varphi : \begin{cases} 1 \longmapsto 1' \\ i \longmapsto \phi(i) \\ j \longmapsto \phi(j) \\ ij \longmapsto \phi(ij) \end{cases}$$

$1'$ ok!. $\phi(i)^2 = -N'(\phi(i)) = -N(i) = i^2 \overset{\varphi(i^2)}{=} a$

$\phi(j)^2 = j^2 = b = \varphi(j^2)$

$\phi(ij)^2 = -N(\phi(ij)) = -N(ij) = (ij)^2 = \varphi((ij)^2)$

$$\varphi(i)\varphi(j)+\varphi(j)\varphi(i)=\phi(i)\phi(j)+\phi(j)\phi(i)=-2B'(\phi(i),\phi(j))$$
$$=-2B(i,j) \qquad (\text{Averiguar!})$$
$$=ij+ji=0.$$

$$(\phi(i)\phi(j))^2=\phi(i)\phi(j)\phi(i)\phi(j)=-\phi(i)^2\phi(j)=-ab\in Z(A)$$

$$\phi(i)\,\phi(i)\phi(j)=-\phi(i)\phi(j)\phi(i)$$

$$\left.\begin{array}{l}\phi(i)\phi(j)\notin Z(A)\\ (\phi(i)\phi(j))^2\in Z(A)\end{array}\right\}\Rightarrow \phi(i)\phi(j)\in A_+ .$$

Falta completar tabla de multiplicación y comprobar que son la misma. ■

Teorema de Frobenius.

Afirmación. Toda álgebra A, asociativa, de dimensión finita sobre $\mathbb{R}$, sin divisores de 0, es isomorfa a otra B, tal que $B\in\{\mathbb{R},\mathbb{C},\mathbb{H}\}$.

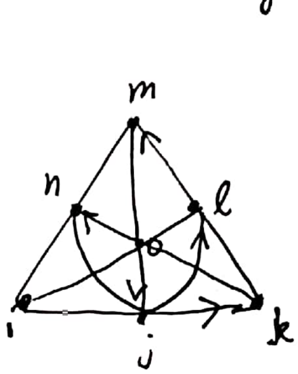
Teorema de Lagrange.

Afirmación. Todo número entero positivo es suma de 4 cuadrados de enteros.

—o—

$\mathcal{C}=\mathbb{H}\times\mathbb{H}$; $(x,y)(z,t)=(xz-\bar{t}y,\ y\bar{z}+tx)$

Octoniones, números de Cayley.



Algebras de Cayley-Dickson

$$\left(\frac{a,b}{K}\right) = Q(a,b)$$

$$x \in Q(a,b) : \quad \bar{x} = x_0 - x_1 i - x_2 j - x_3 ij \quad , \quad N(x) = x\bar{x}$$

$$\mathbb{O} = \mathcal{C}(a,b,c) = \cancel{\mathbb{H}\times\mathbb{H}} = Q \times Q$$

$$(x,y)(x',y') = (xx' + c y' \bar{y} , \ \bar{x} y' + y x')$$

$$\mathcal{C} = \mathcal{C}(-1,-1,-1)_{\mathbb{R}} .$$

Problema. Demostrar que $\left(\frac{a,1}{F}\right) = M_2(F)$

Dem. Elegimos

$$e_{11} = \frac{1}{2}(1-j), \quad e_{22} = \frac{1}{2}(1+j), \quad e_{21} = \frac{1}{2a}(i-k), \quad e_{12} = \frac{1}{2a}(i+k)$$

donde $i^2 = a$, $j^2 = 1$, $k^2 = -a$ y $k = ij$

Se comprueba que:

$$e_{11}^2 = e_{11}, \quad e_{22}^2 = e_{22}, \quad e_{21}^2 = 0, \quad e_{12}^2 = 0, \quad e_{21}e_{11} = e_{21}$$

$e_{11}e_{21} = 0$, $e_{22}e_{21} = \dots$ (para ver que tienen la misma tabla de multiplicación)

Problema. Sea A una F-álgebra de dimensión finita.

A ponderada $\Leftrightarrow \exists \{e_i\}_{i=1}^n$ base de A tal que $e_ie_j = \sum_k \gamma_{ijk} e_k$ con $\sum_k \gamma_{ijk} = 1 \quad \forall i,j$.

Dem. ($\Leftarrow$) Tomar w como $w\left(\sum_k \alpha_k e_k\right) = \sum_k \alpha_k$, $w(e_k) = 1 \ \forall k$

$$w\left(\sum_i \alpha_i e_i \cdot \sum_j \beta_j e_j\right) = w\left(\sum_{i,j} \alpha_i\beta_j e_ie_j\right) = w\left(\sum_{i,j} \alpha_i\beta_j \sum_k \gamma_{ijk} e_k\right)$$

$$= w\left(\sum_k \left(\sum_{i,j} \alpha_i\beta_j\gamma_{ijk}\right) e_k\right) = \sum_{i,j,k} \alpha_i\beta_j\gamma_{ijk} = \sum_{i,j} \alpha_i\beta_j \left(\underbrace{\sum_k \gamma_{ijk}}_{1}\right)$$

$$= \sum_i \alpha_i \sum_j \beta_j = w\left(\sum_i \alpha_i e_i\right) w\left(\sum_j \beta_j e_j\right).$$

($\Rightarrow$) Sea $w: A \to F$ el peso (homo de álgebras no nulo)

Af. Si $\exists \{e_i\}_{i=1}^n$ base tal que $w(e_i) = 1 \ \forall i$, esa sirve

$e_ie_j = \sum_k \gamma_{ijk} e_k \Rightarrow w(e_i)w(e_j) = \sum_k \gamma_{ijk} w(e_k) \quad \therefore 1 = \sum_k \gamma_{ijk}$ ✓

Sea $K = \ker(w)$, con $\{u_1, \dots, u_{n-1}\}$ base de K. $w(u_i) = 0$.

$\exists u_n \in A : A = F u_n \oplus K$, $u = \dfrac{u_n}{w(u_n)}$ $\Rightarrow$ $w(u) = 1$ $\left(w(u_n) \neq 0 \right)$

Ahora tomar ~~que~~ $e_i = u + u_i$, $i \in \{1, \dots, n-1\}$, $e_n = u$

es la base que necesitamos.

R anillo conmutativo con 1

A R-álgebra.

Tenemos funciones
$$L: A \longrightarrow \mathcal{L}(A)$$
$$a \longmapsto L_a : A \longrightarrow A : b \longmapsto ab$$
$$R: A \longrightarrow \mathcal{L}(A)$$
$$a \longmapsto R_a : A \longrightarrow A : b \longmapsto ba$$

A asociativa $\Longleftrightarrow$ (i) L homo de álgebras
(ii) R homo de álgebras
(iii) $R_a \circ L_b = L_b \circ R_a$

$\mathcal{L}(A)$ es un álgebra con unidad.

Definimos $\mathcal{M}(A) = \bigcap_{\substack{B \subset \mathcal{L}(A) \text{, subálgebra} \\ L_a \in B,\ R_a \in B\ \forall a}} B$ $\longleftarrow$ Algebra asociativa

(Ej: $(x^2 y)x = x^2(yx) \Longleftrightarrow$ $R_x \circ L_{x^2} = L_{x^2} \circ R_x$

~~Si~~ $X \subset B$, B R-álgebra asociativa.

$C_B(X) = \{ y \in B \mid yx = xy \ \forall x \in X \}$

$X \subset B$, $X^* = \bigcap_{\substack{S \text{ subálgebra de } \mathcal{L}(B) \\ L_a, R_a \in S\ \forall a \in X}} S \subseteq \mathcal{M}(B)$

$B^* = \mathcal{M}(B)$

Definimos $C' = C_{\mathcal{L}(A)}(\mathcal{M}(A))$ Para un álgebra asociativa A.

~~Tenemos un álgebra asociativa~~

Def. Sea A no asociativa.

$$N(A) = \left\{ x \in A \;\middle|\; \begin{array}{l} (xy)z = x(yz) \\ (yx)z = y(xz) \\ (yz)x = y(zx) \end{array} \quad \forall y, z \in A \right\}$$

$$C(A) = \{ x \in N(A) \mid xy = yx, \forall y \in A \}$$

A álgebra simple sobre cpo F $\Rightarrow C(A) \cong F \vee C(A) \cong \{0\}$

$C' = C(A)^*$ A es una C' álgebra.

$S \leq A$, $T \leq A$ subespacios del álgebra A

$$ST = \langle st \mid s \in S, t \in T \rangle$$

$$A^2 = \langle ab \mid a, b \in A \rangle$$

$$A^n = \sum_{i=1}^{n-1} A^i A^{n-i}$$

$$A^3 = AA^2 + A^2A = \langle a(bc), (ab)c \mid a, b, c \in A$$

A se dice nilpotente ~~⇔~~ si $\exists k \in \mathbb{N}$ tal que $A^k = \{0\}$

$i = \min\{k \in \mathbb{N} / A^k = 0\}$ — índice de Nilpotencia.

$$A' = A^2$$

$$A'' = (A')' = (A^2)^2 = (AA)(AA) = \langle (ab)(cd) \mid a, b, c, d \in A \rangle$$

$$A^{(n)} = (A^{(n-1)})'$$

Resultado: A de Lie, $A/Z(A)$ nilpotente $\Rightarrow$ A nilpotente.

Resultado: $I \trianglelefteq A$, I soluble A/I $\rightarrow$ A soluble.

Sea A algebra. $I \trianglelefteq A$

I es nilpotente $\Leftrightarrow$ I^* es nilpotente

(A nilpotente $\Leftrightarrow$ $\mathfrak{M}(A)$ nilpotente)

Producto Tensorial

M, N son R-módulos.

Un producto tensorial de M y N, es un R-módulo P, con una función $\otimes : M \times N \to P$ R-bilineal, tal que $\forall$ R-módulo Q y toda función R-bilineal B se tiene que $\exists!$ función R-lineal $\tilde{B}$: $(B : M \times N \to Q)$

$$\begin{tikzcd}
P \arrow[r, "\tilde{B}"] & Q \\
M \times N \arrow[u, "\otimes"] \arrow[ur, "B"'] \arrow[ur, phantom, shift left=3, "\circlearrowright"] &
\end{tikzcd}$$

Obs. Tenemos existencia y unicidad del producto tensorial

Notación: $P = M \otimes_R N$

- Si $\{a_i\}_{i \in I}$ base de M, $\{b_j\}_{j \in J}$ base de N, entonces $\{a_i \otimes b_j\}_{(i,j) \in I \times J}$ es base $M \otimes_R N$

- $M \otimes_R N \cong N \otimes_R M$.
$(M \otimes_R N) \otimes_R T \cong M \otimes_R (N \otimes_R T)$

Def/Prop A, B R-álgebras. $A \otimes_R B$ con la multiplicación $(x \otimes y)(r \otimes s) = (xr) \otimes ys$ es una R-álgebra.

A, B R-álgebras $\Rightarrow A\otimes_R B$ R-álgebra

$$\underset{\text{alg.}}{A\otimes_R B \cong B\otimes_R A}, \quad \underset{\text{alg.}}{(A\otimes_R B)\otimes C \cong A\otimes_R (B\otimes_R C)}$$

<u>Definición</u>. G es un grupo, $R[G] = \{ \sum_{i=1}^{n} a_i g_i \,/\, a_i\in R, g_i\in G \}$

R-álgebra de Grupo G. Tiene producto

$$\left(\sum_{i=1}^{n} a_i g_i\right)\left(\sum_{j=1}^{m} b_j h_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j g_i h_j$$

<u>Ejercicio</u> (1) $R[G\times H] \cong R[G]\otimes_R R[H]$ $\forall$ par de grupos (G,H)

(2) F cuerpo : $F[X,Y] \cong F[X]\otimes_F F[Y]$ $\quad (F[X]\subseteq F[\mathbb{Z}])$

(3) Si F es cuerpo : $\mathbb{M}(F)\otimes_F A \cong \mathbb{M}(A)$. A una F-álgebra con 1

<u>Dem</u> (3) $\quad \mathbb{M}(F)\times A \xrightarrow{\phi} \mathbb{M}(A)$

$$((r_{ij}),a) \longmapsto (r_{ij}a) \quad \text{bilineal}$$

$$\exists!\ \tilde{\phi} : \mathbb{M}(F)\otimes_F A \longrightarrow \mathbb{M}(A) \quad \text{tq} \quad \phi((r_{ij}),a) = \tilde{\phi}((r_{ij})\otimes a)$$

$$\therefore \quad \tilde{\phi} : (r_{ij})\otimes a \longmapsto (r_{ij}a)$$

$$\tilde{\phi}\Big(((r_{ij})\otimes a)((s_{kl})\otimes b)\Big) = \tilde{\phi}\big((r_{ij})(s_{kl})\otimes ab\big) = [(r_{ij})(s_{kl})](ab)$$

Queremos que se cumpla : $(r_{ij})(s_{kl})a = (r_{ij})a(s_{kl})$

$$[(r_{ij})a][(s_{kl})b] = \tilde{\phi}((r_{ij})\otimes a)\,\tilde{\phi}((s_{kl})\otimes b)$$

$$(a_{ij}) = \left(\sum_{ij} a_{ij} e_{ij}\right) \overset{\Psi}{\longmapsto} \sum_{ij} e_{ij}\otimes a_{ij}$$

$$\Psi\circ\tilde{\phi}, \quad \tilde{\phi}\circ\Psi \ldots$$

Ejercicio. $\sum_i x_i \otimes b_i = 0 \Rightarrow x_i = 0 \ \forall i$, cuando $\{b_i\}_i$ es LI.

A es F-álgebra, F cuerpo. A se dice central si $Z(A) = F \cdot 1_A$.

Si A es F-álgebra central con 1 (asociativa y simple) y E es una extensión de F

$\Rightarrow A \otimes_F E$ es simple.

Sea $I \trianglelefteq A \otimes_F E$, $I \neq \{0\}$, $u \in I$, $u \neq 0$.

Sea $\{e_i\}_{i \in I}$ F-base de E

$\forall z \in A \otimes_F E$, $\exists \{i_1, \dots, i_n\} \subseteq I$, $a_{i_1}, \dots a_{i_n} \in A$

$$z = \sum_{k=1}^{n} a_{i_k} \otimes e_{i_k} \quad , \quad a_{i_k} \neq 0 \ \forall k$$

sea $l(z) = \min\{n\}$

Podemos elegir $u \in I$, $l(u)$ de longitud mínima.

$\forall r, s \in A$: $(r \otimes 1) u (s \otimes 1) \in I$, $\sum r a_i s \otimes e_i \in I$

asumiendo asociatividad

| $A a A = A$ cuando A es asociativa | $1_A = r a a s$ |

Prop. Sea F cuerpo. A, B F-álgebras. $\{b_i\}_{i=1}^{n} \subseteq B$ linealmente ~~ind~~ independientes sobre F.

P.d: $\sum_{i=1}^{n} x_i \otimes b_i = 0 \Rightarrow x_i = 0 \ \forall i$.

dem. Supongamos que ~~$\exists i_0 \in I$~~ $x_1 \neq 0$. $\exists g: A \to F$, $g(x_1) \neq 0$.
$\exists f: B \to F$ tal que $f(b_1) \neq 0$, $f(b_i) = 0$ $\forall i \in \{2, \dots, n\}$

$$\boxed{\begin{array}{l} g \times f : A \times B \longrightarrow F \\ \qquad (a,b) \longmapsto g(a) f(b) \\ \Rightarrow \exists\, g \otimes f : A \otimes B \to F \end{array}}$$

$$0 = g \otimes f(0) = g \otimes f\left(\sum_{i=1}^{n} x_i \otimes b_i\right)$$
$$= \sum_{i=1}^{n} g(x_i) f(b_i) = g(x_1) f(b_1) \neq 0$$

Def. F cuerpo, A F-álgebra con 1

$$A \text{ central} \Leftrightarrow C(A) = F$$

Ejercicio: $C(A \otimes_F B) = C(A) \otimes_F C(B)$

$$A \text{ central}, B \text{ central} \Rightarrow A \otimes_F B \text{ central}$$

Def. Sea F cuerpo, K/F extensión. A F-álgebra. $A_K = K \otimes_F A$ es una K álgebra y se llama extensión de A por K.

Prop. Sea A álgebra con 1 y K extensión de F.

A es central simple $\Rightarrow K \otimes_F A$ es central simple como K-álgebra.

dem. Sea $\{k_i\}_{i \in I}$ una base de K sobre F.

$\forall x \in K \otimes A$, $\exists \{i_1, \dots, i_n\}$, $x = \sum_{l=1}^{n} k_{i_l} \otimes x_{i_l}$, $x_{i_l} \neq 0$, $x_{i_l} \in A$

El mínimo de tales $n = \ell(x)$ (largo de x)

Dado $U \trianglelefteq K\otimes_F A$, $U \neq \{0\}$, $\exists x \in U$ de largo minimal.

Se identifica A con $1_K \otimes A$ $\quad (x \mapsto 1_K \otimes x)$

$A^* = \mathcal{M}(K\otimes A) = \langle L_a, R_b \mid a,b \in A \rangle \leq \{ T : K\otimes_F A \to K \otimes_F A \}$

$W \in A^*$; $W\left(\sum_i k_i \otimes x_i\right) = \sum_i k_i \otimes W(x_i)$

$a \in A$: $(a) = \bigcap_{\substack{I \trianglelefteq A \\ a \in I}} I = \mathcal{M}(A)a$

A simple $\Rightarrow 1_A \in \mathcal{M}(A)a$.

$x \in U$, $x \neq 0$, $x = \sum_{i=0}^{n} k_i \otimes x_i$, $\ell(x) = n+1$

$\exists W \in A^*$, $W(k_0 \otimes x_0) = k_0 \otimes 1_A$, $W(x) \in U$

$W(x) = k_0 \otimes 1_A + \sum_{i=1}^{n} k_i \otimes x_i'$, $x_i' = W(x_i)$

$a \in A$: $[1_K \otimes a, W(x)] \in U$

$$\begin{aligned}
[1_K \otimes a, W(x)] &= \left[1_K \otimes a, k_0 \otimes 1_A + \sum_{i=1}^{n} k_i \otimes x_i'\right] \\
&= [1_K \otimes a, k_0 \otimes 1_A] + \left[1_K \otimes a, \sum_{i=1}^{n} k_i \otimes x_i'\right] \\
&= \underbrace{[1_K \otimes a, k_0 \otimes 1_A]}_{=0} + \sum_{i=1}^{n} [1_K \otimes a, k_i \otimes x_i']
\end{aligned}$$

$$\begin{aligned}
[1_K \otimes a, k_i \otimes x_i'] &= (1_K \otimes a)(k_i \otimes x_i') - (k_i \otimes x_i')(1_K \otimes a) \\
&= k_i \otimes a x_i' - k_i \otimes x_i' a = k_i \otimes [a, x_i']
\end{aligned}$$

$U \ni \sum_{i=1}^{n} k_i \otimes [a, x_i'] = y$, $\ell(y) \leq n$ $\quad \therefore y = 0 \Rightarrow [a, x_i'] = 0$
$\forall i \in \{1, \dots, n\}$

$$(a,b,w(x)) = (ab)w(x) - a(bw(x))$$

$$\Rightarrow \Big(1_K\otimes a,\, 1_K\otimes b,\, k_0\otimes 1_A + \sum_{i=1}^{n}{}' k_i\otimes x_i'\Big) = \sum_{i=1}^{n}{}' k_i\otimes(a,b,x_i') \in U$$

$$\overset{\shortparallel}{z}\quad,\ \ell(z)\le n$$

$x_i'\in F\ \forall i$, $x_i' = \alpha_i$

$$W(x) = k_0\otimes 1_A + \sum_{i=1}^{n}{}' k_i\otimes\alpha_i = \Big(\sum_{i=0}^{n}{}'\alpha_i k_i\Big)\otimes 1_A = k\otimes 1_A\ ,\ k\in K$$

$$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \cap\ U$$

$\therefore\ k\neq 0$ $\quad\therefore\ k\otimes 1_A$ es invertible y $U = K\otimes_F A$

Por demostrar: $C(K\otimes_F A) = K$.

Por ejercicio anterior, $C(K\otimes_F A) = C(K)\otimes_F C(A)$
$= K\otimes_F F = K$

<u>Proposición</u>. A, B F-álgebras con 1 y A central simple y B simple, $A\otimes_F B$ es simple.

<u>Proposición</u>. Si ambas son centrales simples $\Rightarrow A\otimes_F B$ central simple.

<u>Cap II</u>. <u>Semi-Simplicidad</u>

Resultado "cumbre"

Teorema de Wedderburn: Sea A una F-álgebra semi-simple, entonces existen $n_1,\dots,n_t$ y álgebras de división $D_1,\dots,D_t$ tales que

$$A\cong M_{n_1}(D_1)\oplus\cdots\oplus M_{n_t}(D_t)$$

Los pares (n_i, D_i) son únicos salvo isomorfismos

De ahora en adelante, una F-álgebra será:
Asociativa, con 1, no necesariamente conmutativa.

Habrá A-módulos por la izquierda y por la derecha.
Usaremos A-módulos por la izquierda y los llamaremos A-módulos

Nota: Se define A^o = álgebra opuesta a A: como espacio vectorial se trata de A y la multiplicación es

$$x \cdot y = yx \quad \forall x, y \in A^o.$$

Obs. Toda F-álgebra A, es un A-módulo. Como son A-módulos por la izquierda, lo denotaremos por A_i y sus submódulos serán los ideales por la izquierda. Similarmente existe A_d.

Obs. Sea $\phi: A \to B$ homo de R-álgebras. M un B-módulo, entonces M es un A-módulo con $a \cdot m = \phi(a)m \quad \forall a \in A, \forall m \in M$ y se denota por M_ϕ.

Ejemplo. Sea A una R-álgebra, I ideal de A, $\pi: A \to A/I$ epimorfismo canónico. Entonces todo A/I-módulo es un A-módulo con $a \cdot m = am + I \quad \forall a \in A, \forall m \in A$.

Definición. Sean A un M-módulo, X subconjunto de M. Se define $Anul(X) = \{\alpha \in A \mid \alpha x = 0 \ \forall x \in X\}$

Lema. Sean M, M' dos A-módulos, $X \subseteq M$, $Y \subseteq M$, entonces

(1) $Anul(X)$ es un ideal por la izquierda de A, y si X submódulo de M, entonces $Anul(X) \trianglelefteq A$

(2) $X \subset Y \Rightarrow Anul(Y) \subseteq Anul(X)$

(3) $M \cong M' \Rightarrow Anul(M) = Anul(M')$

(4) Sea J ideal izquierda de A, entonces $K = Anul(A/J)$ es el mayor ideal de A tal que $K \subseteq J$.

Dem. (1) Es claro que $Anul(X)$ es ideal por la izquierda de A, si X es subconjunto de M.

Sea X submódulo de M. Probemos que $Anul(X)$ es ideal por la derecha de A. Pd: $\alpha \cdot a \in Anul(X)$ $\forall a \in A$. $\forall \alpha \in Anul(X)$

$(\alpha \cdot a) X = \alpha(\underbrace{aX}_{\in X}) = 0$, pués $\alpha \in Anul(X)$.

$\therefore$ $Anul(X)$ es ideal por la derecha de A y como ya es ideal por la izquierda, entonces es un ideal de A.

(2) (Ejercicio)

(3) Sea $M \cong M'$. $\phi: M \to M'$ isomorfismo de A-módulos. Sea $\alpha \in Anul(M)$

$\therefore$ $\alpha m = 0$ $\forall m \in M$.

P.d: $\alpha m' = 0$ $\forall m' \in M' = \phi(M)$. pero $\alpha m' = \alpha \phi(m_1) = \phi(\underbrace{\alpha m_1}_{=0}) = \phi(0)$

$\therefore$ $Anul(M) \subseteq Anul(M')$

Sea $\beta \in Anul(M')$ $\therefore$ $\beta m' = 0$ $\forall m' \in M'$. Pero $m' = \phi(m)$, $m \in M$

$\therefore$ $\beta m \in \ker(\phi) = \{0\}$

$\therefore$ $\beta m = 0$ $(\forall m \in M)$

$\therefore$ $\beta \in Anul(M)$

$\therefore$ $Anul(M') \subseteq Anul(M)$ (2)

(1), (2) implica (3).

(4) (i) $K = anul(A/J)$ es ideal de A. Pd: $a\, Anul(A/J) \subseteq Anul(A/J)$ $\forall a \in A$.

y $Anul(A/J) \cdot a \subseteq Anul(A/J)$ $\forall a \in A$.

$A/J = \{a_1 + J \,/\, a_1 \in A\}$

$Anul(A/J) = \{\alpha \in A \,/\, \alpha a_1 + J = J \ \forall a_1 \in A\} = \{\alpha \in A \,/\, \alpha a_1 \in J \ \forall a_1 \in A\}$

Tenemos de inmediato que $\text{Anul}(A/J)$ es ideal izquierdo de A.
Veamos que $\text{Anul}(A/J)\beta \subseteq \text{Anul}(A/J) \quad \forall \beta \in A$.
Sea $\alpha \in \text{Anul}(A/J) \therefore \alpha \in A$ y $\alpha a_1 \in J \quad \forall a_1 \in A$.

Pd: $(\alpha\beta)a_1 \in J \quad \forall a_1 \in A$

$$(\alpha\beta)a_1 = \alpha(\underbrace{\beta a_1}_{\in A}) \in J \quad \text{pués } \alpha \in \text{Anul}(A/J)$$

Sea $K = \text{Anul}(A/J) = \{\alpha \in A \mid \alpha a_1 \in J, \forall a_1 \in A\}$
Sea $I \trianglelefteq A$, $I \subseteq J$. Por demostrar que $I \subseteq K$.

Sea $y \in I$. Por demostrar $y a_1 \in J \quad \forall a_1 \in A$
como $I \trianglelefteq A$, $y a_1 \in I \quad \forall a_1 \in A$ y $I \subseteq J$

$$\therefore y a_1 \in J \quad \forall a_1 \in A$$
$$\therefore I \subseteq K$$

Definición (1) Sea M un A-módulo, $M \neq \{0\}$. M se dice irreducible o simple ssi sus únicos submódulos son los triviales
(2) M se dice completamente irreducible o semisimple ssi M es suma directa de módulos simples.

Obs. Simple $\Rightarrow$ semi-simple
No vale el recíproco. Para ello consideremos F cuerpo, $A = M_n(A)$ entonces A_i es A-módulo semi-simple que no es simple.
(Obs. Los submódulos son los ideales por la izquierda de A)

En efecto, definamos

$$I_1 = \left\{ \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{n1} & 0 & & 0 \end{pmatrix} \middle/ a_{i1} \in F \ \forall i \right\}$$

$$I_2 = \left\{ \begin{pmatrix} 0 & a_{12} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{n2} & 0 & \cdots & 0 \end{pmatrix} \middle/ a_{i2} \in F \ \forall i \right\}$$

$$\vdots$$

$$I_n = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1n} \\ \vdots & & & \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix} \middle/ a_{in} \in F \ \forall i \right\}$$

$A = I_1 \oplus \cdots \oplus I_n$, I_i son simples $\forall i$

I_j son ideales propios de A_i.

<u>Lema de Schur</u>. Sean M, N dos A-módulos, $\phi: M \to N$ homo no nulo, entonces

(1) M simple $\Rightarrow \phi$ inyectiva

(2) N simple $\Rightarrow \phi$ epiyectiva

<u>Dem</u>. (1) $\ker(\phi)$ submódulo de M y $\phi \neq 0$, M simple $\Rightarrow \ker\phi = \{0\}$

(2) Consideremos $\operatorname{Im}(\phi)$ submódulo de N. Como $\phi \neq 0 \Rightarrow \operatorname{Im}\phi = N$

$\therefore \phi$ epiyectiva

<u>Corolario</u>. Sean M, N A-módulos simples, entonces $\operatorname{Hom}_A(M,N) = \{0\}$ o $M \cong N$.

__Corolario__. Sea M un A-módulo simple, entonces $End_A(M)$ es un álgebra de división.

En efecto, sea $f: M \to M$ homomorfismo, $f \neq 0$. Como M es simple $\Rightarrow$ f es isomorfismo. Luego f es invertible.

__Definición__. Sea M un A-módulo y P submódulo de M. Se dice que P es maximal si $P \neq M$ y si $P \subset M_1$, entonces $M_1 = M$.

Se dice que P es minimal ssi $P \neq \{0\}$ y si $M_1 \subset M$, entonces $M_1 = \{0\}$

__Obs__: (1) J ideal izquierdo, entonces J es submódulo simple de A minimal ($A = A_i$)

(2) Sea M un A-módulo y N submódulo de M. Entonces M/N es simple ssi N es submódulo maximal de M.

__Lema__. Sea M un A-módulo, $M \neq \{0\}$. Son equivalentes.

(1) M simple

(2) $M = Ax \quad \forall x \in M,\ x \neq 0$.

(3) $M \cong A_i/J$ para algún ideal izquierdo maximal J de A.

__dem__. (3) $\Rightarrow$ (1) se obtiene de la observación 2, pues A_i/J es simple $\therefore$ M es simple.

(1) $\Rightarrow$ (2) Sea M simple. Como $x \neq 0$, $Ax \neq \{0\}$ y es submódulo de M. $\therefore$ $Ax = M$

(2) $\Rightarrow$ (3) Sea ~~xxx~~ $t \neq 0$ $\therefore$ $M = At$. Definamos

De la clase pasada. Son equivalentes

(1) M simple

(2) $M = Ax$, para todo $x \in M$, $x \neq 0$

($\Rightarrow$) Probado

($\Leftarrow$) P.d: M simple. Sea N submódulo de M, $N \neq \{0\}$

$$\therefore \exists n \in N,\ n \neq 0$$

Por (2), $M = An$; pero N submódulo de M y $n \in N \Rightarrow An \subseteq N$

$$\therefore M \subseteq N$$
$$\therefore M = N$$

Se tiene así que M es simple.

Con esto quedan demostradas las tres equivalencias del lema (ver apuntes. Lema 2.1.3).

<u>Ejercicio (2.1.4)</u>: Sea $M = M_1 \oplus M_2$ (M_i submódulo de M). Sea P submódulo de M, $M_1 \subset P$. Entonces $P = M_1 \oplus (M_2 \cap P)$.

<u>Teorema</u>. Sea M un A-módulo. Son equivalentes:

(1) M es semi-simple.

(2) M es suma (no necesariamente directa) de submódulos simples N_j, $j \in J$ ($N_j \leq M$)

(3) Todo submódulo de M es sumando directo de M, más precisamente, para cada submódulo T de M, existe submódulo S de M tal que $M = T \oplus S$ (También se dice que cada submódulo de M tiene complementario en M)

Dem.

(1) ⇒ (2) Inmediato

(2) ⇒ (3) Sea $M = \sum_{j\in J}' N_j$, N_j simple $\forall j \in J$. Sea T submódulo de M, $T \neq \{0\}$. Por encontrar S submódulo de M tal que $M = T \oplus S$.

Construiremos una sucesión de índices $j_1, \dots, j_q$ ($j_i \in J$), en forma recursiva. Sea j_1 el menor índice tal que $N_{j_1} \not\subset T$, j_2 el menor índice tal que $N_{j_2} \not\subset T + N_{j_1}$; así sucesivamente, hasta que j_q el menor índice tal que $N_{j_q} \not\subset T + N_{j_1} + \dots + N_{j_{q-1}}$.

El proceso termina cuando ya no se puede definir un nuevo índice.

Primero probemos que $T + N_{j_1} + \dots + N_{j_{q-1}} + N_{j_q}$ es directa usando inducción sobre q.

$q = 1$: P.d : $T \cap N_{j_1} = \{0\}$ $\therefore T \oplus N_{j_1}$

$T \cap N_j$ es submódulo N_{j_1} y $N_{j_1} \not\subset T$

$\therefore T \cap N_j = \{0\}$ (N_{j_1} simple)

Hipótesis de inducción: $T + N_{j_1} + \dots + N_{j_{q-1}}$ directa. Sea

$H = T \oplus N_{j_1} \oplus \dots \oplus N_{j_{q-1}}$

Tesis: Pd: $T + N_{j_1} + \dots + N_{j_q}$ directa

$H + N_{j_q} = T \oplus N_{j_1} \oplus \dots \oplus N_{j_{q-1}} + N_{j_q}$

Pd: $H \cap N_{j_q} = \{0\}$

Como $H \cap N_{jq}$ es submódulo de N_{jq}, N_{jq} simple y $N_{jq} \not\subset H$, entonces se tiene que $H \cap N_{jq} = \{0\}$

$$\therefore T \oplus N_{j_1} \oplus \dots \oplus N_{jq}$$

$\therefore$ Por inducción, se tiene que $T \oplus N_{j_1} \oplus \dots \oplus N_{j_t} \quad \forall t \geq 1$.

Falta probar que $M = T \oplus \underbrace{N_{j_1} \oplus \dots \oplus N_{jq}}_{S}$

Tenemos $M = \sum'_{j \in J} N_j$, N_j simple. Como jq es el último de los índices $j_1, \dots, j_k$, entonces todos los N_i tal que $M = \sum'_{i \in I} N_i$ están contenidos en $T + N_{j_1} + \dots + N_{jq}$ $\therefore M \subset T + N_{j_1} + \dots + N_{jq}$

$$\therefore M = T + N_{j_1} + \dots + N_{jq}$$

(3) $\Rightarrow$ (1) Para todo T submódulo de M, $\exists S$ tal que $M = T \oplus S$.

Por demostrar que $M = \bigoplus_{i \in I} N_i$, N_i simples.

Primero mostremos que M tiene submódulos simples. Usemos lema de Zorn. Sea $x \in M$, $x \neq 0$, formemos $S(x) = \{T \subset M \mid T$ submódulo de M, $x \notin T\}$. $S(x) \neq \emptyset$ ya que $\{0\} \in S(x)$.

Sea $\{T_i\}_{i \in I}$ cadena de submódulos en $S(x)$, entonces $\bigcup_{i \in I} T_i$ es cota superior en la cadena. Por lema de Zorn, $S(x)$ tiene un elemento maximal T_0 ($\therefore x \notin T_0$ y maximal c/respecto a esta propiedad).

Por (3), T_0 tiene complemento en M

$\therefore \exists N$ submódulo de M tal que $M = T_0 \oplus N$

Veamos que N es simple. Supongamos que hay submódulo propio N_1 de N por (3), $M = N_1 \oplus N_2$. Como $N_1 \subset N$, por ejercicio anterior al teorema,

$$N = N_1 \oplus (N_2 \cap N)$$

Ahora bien, $x \in T_0 \oplus N_1$ y $x \in T_0 \oplus (N_2 \cap N)$ (pues T_0 es maximal c/r a $x \notin T_0$, $N_1 \neq \{0\}$, $N_2 \cap N \neq \{0\}$)

Por lo tanto: $\begin{array}{l} x = t_0 + n_1 \\ x = t_0' + n_2 \end{array}$, $\begin{array}{l} t_0, t_0' \in T_0 \\ n_1 \in N_1, \; n_2 \in N_2 \cap N \end{array}$

$\therefore \; n_1 + t_0 = n_2 + t_0'$. Así

$$n_1 - n_2 = t_0' - t_0$$

por otro lado, $n_1, n_2 \in N$

$\therefore \; n_1 - n_2 \in T_0 \cap N = \{0\}$

$\therefore \; n_1 = n_2$. Además $N_1 \cap (N_2 \cap N) = \{0\}$

$\therefore \; n_1 = 0 = n_2$

$\therefore \; x = t_0 \in T_0$ $(\Rightarrow\!\Leftarrow)$.

Así se tiene que N es simple.

Consideremos la familia

M un A-módulo finitamente generado
A Noetheriano
Entonces M es noetheriano.

—∘—

Sea n = cant. de generadores de M.

$f: A^n \to M$, $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i e_i$

f bien definida, homomorfismo, epiyectiva.

$\therefore A^n / \ker(f) \cong M$

Como A es noetheriano, A^n lo es $\therefore A^n/\ker(f)$ es noetheriano.

Sea T submódulo de M

$$0 \to T \xrightarrow{\varphi} M \xrightarrow{\pi} M/T \to 0 \quad \text{exacta}$$

Recordatorio:
$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0 \quad \text{exacta}$$

M, P noetherianos (artinianos) $\Leftrightarrow$ N noetheriano (artiniano)

Lo complicado es: M y P noetherianos $\Rightarrow$ N noetheriano.

Sea $N_1 \subset N_2 \subset \ldots$ cadena de submódulos de N.

$\therefore$ (1) $f^{-1}(N_1) \subset f^{-1}(N_2) \subset \ldots$ cadena de submódulos de M

M noetheriano $\Rightarrow f^{-1}(N_n) = f^{-1}(N_{k_1}) \quad \forall n \geq k_1$

(2) $g(N_1) \subset g(N_2) \subset \ldots$ cadena de submódulos de P

P noetheriano $\Rightarrow g(N_n) = g(N_{k_2}) \quad \forall n \geq k_2$

f inyectiva $\Rightarrow$ (3) $N_n \cap f(M) = f(f^{-1}(N_n))$ $\forall n \in \mathbb{N}$

g epiyectiva $\Rightarrow$ (4) $N_n + \ker(g) = g^{-1}(g(N_n))$ $\forall n \in \mathbb{N}$.

Sea $k = \max\{k_1, k_2\}$. Pd: $N_n = N_k$ $\forall n \geq k$

Sabemos que $\forall n \geq k$, $N_k \subset N_n$

Pd: $N_n \subseteq N_k$

de (3) y M noetheriano $\Rightarrow$ $\forall n \geq k$

$$(5)\quad N_n \cap f(M) = f(f^{-1}(N_n)) = f(f^{-1}(N_k)) \underset{(3)}{=} N_k \cap f(M)$$

de (4) y P noetheriano $\Rightarrow$

$$(6)\quad N_n + \ker(g) = N_k + \ker(g) \quad \forall n \geq k$$

Además $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ exacta $\Rightarrow f(M) = \ker(g)$

$$\therefore (7)\quad N_n + f(M) \underset{(6)}{=} N_k + \ker(g) \quad \forall n \geq k.$$

Sea $x \in N_n$ $\quad \therefore x \in N_k + f(M)$

$\therefore x = z + f(m)$, ciertos $z \in N_k$, $m \in M$

$\therefore x - z \in f(M)$

Por demostrar: $x - z \in N_k$

Por (*): $N_k \subset N_n$ $\quad \therefore x - z \in N_n$

$\therefore x - z \in N_n \cap f(M) \underset{(5)}{=} N_k \cap f(M)$

$\therefore x - z \in N_k \cap f(M) \subseteq N_k$

$\therefore \underbrace{x - z}_{\in N_k} \in N_k \cap f(M) \subseteq N_k$

$\therefore x \in N_k$

Vimos: Sea A una R-álgebra

(1) A semi simple $\Leftrightarrow$ Todo A-módulo es semi simple

(2) A semi simple $\Rightarrow$ Todo A-módulo simple es un ideal por la izquierda minimal.

(3) lema: I, J ideales por la izquierda minimales $\Rightarrow IJ = \{0\}$ ó $I \cong J$ (isomorfismo de A-módulos).

Proposición. Sea A semisimple, $A = I_1 \oplus \dots \oplus I_m$ descomposición de A en ideales por la izquierda minimales de A. Entonces todo ideal por la izquierda minimal de A es isomorfo a algún I_i, $i = 1, \dots, m$

dem. Sea T un ideal por la izquierda minimal de A. Afirmamos que $I_j T \neq \{0\}$ para algún $j = 1, \dots, m$, y con esto $I_j \cong T$.

En efecto, si $I_j T = \{0\}$ $\forall j = 1, \dots, m$, se tiene que $AT = \{0\}$

$\therefore T = \{0\}$ $(\Rightarrow\Leftarrow)$

Proposición. Sea A álgebra simple. Entonces son equivalentes

(1) A semi simple

(2) A artiniana

(3) A posee un ideal por la izquierda minimal.

dem. (1) $\Rightarrow$ (2): A s.s y f.g, por proposición 2.26, A es artiniana.

(2) $\Rightarrow$ (3): Es inmediato.

$(3) \Rightarrow (1)$: Sea N un ideal por la izquierda minimal de A.

Entonces $NA = \sum\limits_{x \in A}' Nx$. Además, cada Nx no nulo es un ideal por la izquierda minimal de A_i, luego es un A-módulo simple

$\therefore A$ es semi-simple,

pués NA es ideal de A, $NA \neq \{0\}$

$\therefore NA = A$ (pués A es simple).

<u>Proposición</u>. Sea A s.s. Son equivalentes:

(1) A es simple

(2) Todos los ideales por la izquierda minimales de A son isomorfos.

(3) Todos los A-módulos simples son isomorfos.

<u>dem</u>. Ver apuntes.

<u>Ejercicio 2.3.2</u>. Sean D álgebra de división. Para cada $i = 1, \dots, n$, se define $N_i = A e_{ii}$, donde e_{ii} son elementos de la base canónica, donde $A = \mathbb{M}_{nn}(D)$. Entonces

(1) N_i es ideal izquierdo minimal de A, $\forall i = 1, \dots, n$.

(2) $A = \bigoplus\limits_{i=1}^{n} N_i$

(3) $N_i \cong N_j$, $\forall i,j = 1, \dots, n$

(4) A es simple y semi-simple.

(5) $\mathrm{End}_A(N_i) \cong D$ $\forall i = 1, \dots, n$.

Sección : Teorema de Wedderburn.

• Matrices de endomorfismos.

Sean A una R-álgebra ; $M_1, \dots, M_n$ A-módulos. Consideremos el conjunto de matrices

$$M_{n\times n}(\mathrm{Hom}_A(M_j, M_i)) = \left\{ \begin{pmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2n} \\ \vdots & \vdots & & \vdots \\ \phi_{2n} & \phi_{n2} & & \phi_{nn} \end{pmatrix} \;\middle|\; \begin{array}{c} \phi_{ij} \in \mathrm{Hom}_A(M_j, M_i) \\ \forall i,j = 1,\dots,n \end{array} \right\}$$

Entonces $(\mathrm{Hom}_A(M_j, M_i))$ es una R-álgebra con suma y multiplicación usual, y producto:

$$(\phi_{ij})_{i,j} \cdot (\psi_{r,s})_{r,s} = (x_{tm})_{t,m} \,, \text{ con}$$

$$x_{tm} = \sum_{j=1}^{n}{}' \phi_{ij} \circ \psi_{jm} \in \mathrm{Hom}_A(M_m, M_j)$$

Proposición Sea A una R-álgebra ; $M_1, \dots, M_n$ A-módulos, entonces $M_{n\times n}(\mathrm{Hom}_A(M_j, M_i)) \cong \mathrm{End}_A(M_1 \oplus \dots \oplus M_n)$ (isomorfismo de álgebras) dem. Consideremos las inyecciones y las proyecciones inducidas por la suma directa $\bigoplus_{i=1}^{n} M_i$

$$\varphi_j : M_j \longrightarrow \bigoplus_{i=1}^{n} M_i$$
$$\pi_j : \bigoplus_{i=1}^{n} M_i \longrightarrow M_j \qquad \forall j = 1, \dots, n$$

que cumplen (a) $\sum_{j=1}^{n} \varphi_j \circ \pi_j = id_{\bigoplus_{i=1}^{n} M_i}$

(b) $\pi_j \circ \varphi_k = 0$ si $k \neq j$, $\pi_j \circ \varphi_j = id_{M_j}$ $\forall j$.

Sea $F : End_A\left(\bigoplus_{i=1}^{n} M_i\right) \longrightarrow M_{n\times n}\left(Hom_A(M_j, M_i)\right)$

definida por $F(f) = (\pi_i \circ f \circ \varphi_j)_{i,j}$. Y

$G : M_{n\times n}\left(Hom_A(M_j, M_i)\right) \longrightarrow End_A\left(\bigoplus_{i=1}^{n} M_i\right)$, definida por

$$G\left((\phi_{ij})_{i,j}\right) = \sum_{i,j=1}^{n} \varphi_i \circ \phi_{ij} \circ \pi_j$$

entonces F, G lineales y cumplen que una es la inversa de la otra (y vice-versa). Además F es homomorfismo de álgebras.
$\left(F(f \circ g) = F(f) F(g) \right)$

$$F(f\circ g) = (\pi_i \circ f \circ g \circ \varphi_k)_{i,k}$$

$$= \left(\pi_i \circ f \circ \sum_{j=1}^{n} \varphi_j \circ \pi_j \circ g \circ \varphi_k\right)_{i,k}$$

$$= \left(\sum_{j=1}^{n} (\pi_i \circ f \circ \varphi_j)(\pi_j \circ g \circ \varphi_k)\right)_{i,k}$$

$$= F(f)\,F(g)$$

$\therefore$ F es homomorfismo de álgebras y es biyectivo

$$\therefore \quad End_A\left(\bigoplus_{i=1}^{n} M_i\right) \cong M_{n\times n}(Hom_A(M_j, M_i))$$

Fecha / Date:

pd: $C(K\otimes A) = K$

$C(K) = K \quad C(A) = F \quad K \otimes_F F = K$

Proposición A, B F-álgebras con 1, A central simple y B simple. Entonces $A\otimes_F B$ es simple.

Proposición Si A, B son centrales simples $A\otimes_F B$ es central simple

Prueba ↑

CAPÍTULO 2: Semi-simplicidad

- Resultado "cumbre": teo de Wedderburn

Sea A una F-álgebra semi-simple. Entonces existen naturales $n_1, \dots, n_t$ y álgebras de división $D_1, \dots, D_t$ tales que $A \cong M_{n_1}(D_1) \oplus \dots \oplus M_{n_t}(D_t)$. Los pares (n_i, D_i) son únicos salvo isomorfía.

De ahora en adelante, una F-álgebra será asociativa, con unidad, no necesariamente conmutativa. Habrá A-módulos por la izquierda, o por la derecha. Usaremos A-módulos por la izquierda y los llamaremos simplemente A-módulos.

Nota: se define A^{o} = álgebra opuesta de A; como espacio vectorial, se trata de A y la multiplicación es $x\cdot y = yx \quad \forall x, y \in A^{o}$

Obs: toda F-álgebra de A es un A-módulo. Como son A-módulos por la izquierda, lo denotaremos A_i y sus submódulos serán los ideales por la izquierda. Similarmente, existe A_d.

Notas / Notes:

2/10

Obs: Sea $\phi: A \to B$ homomorfismo de R-álgebras, M es un B-módulo. Entonces M es un A-módulo con $a \cdot m = \phi(a)m$ $\forall a \in M$, y se anota M_ϕ.

Ejercicio: Sea A un R-álgebra, I ideal de A, $\pi: A \to A/I$ epimorfismo canónico. Entonces todo A/I-módulo es un A-módulo con $a \cdot m = am + I$ $\forall a \in A$ $\forall m \in M$. ✓ chequeable

Definición: Sean M un A-módulo, X subconjunto de M. Se define
$$Anl(X) = \{a \in A / ax = 0 \ \forall x \in X\}$$

Lema: Sean M, M' dos A-módulos. $X \subseteq M$, $Y \subseteq M$ (subconjuntos). Entonces:

1) $Anl(X)$ es un ideal por la izquierda de A. Si X es submódulo de M, entonces $Anl(X) \trianglelefteq A$.

2) $X \subseteq Y \Rightarrow Anl(Y) \subseteq Anl(X)$

3) $M \simeq M' \Rightarrow Anl(M) = Anl(M')$

4) Sea J ideal izquierdo de A, entonces $K = Anl(A/J)$ es el mayor ideal de A tq $K \subseteq J$.

Dem:

1) Es claro que $Anl(X)$ es ideal izq de A si X es subconjunto de M. Sea X submódulo de M. Probemos que $Anl(X)$ es ideal por la derecha de A.

pd: $\alpha \cdot a \in Anl(X)$ $\forall a \in A$ $\forall \alpha \in Anl(X)$

$(\alpha a) \cdot x \overset{\text{prop módulo}}{=} \alpha(a \cdot x) = 0$ pues $\alpha \in Anl(X)$ y $ax \in A$

$\therefore$ $Anl(X) \trianglelefteq A$.

2) Tarea. Sea $a \in Anl(Y)$. Luego $ay = 0$ $\forall y \in Y \supseteq X$.

$\Rightarrow ax = 0$ $\forall x \in X$

$\Rightarrow a \in Anl(X)$

3) Sea $M \simeq M'$ y $\phi : M \to M'$ isomorfismo de A-módulos.
Sea $\alpha \in Anul(M)$. Luego $\alpha m = 0 \ \forall m \in M$.
pd: $\alpha m' = 0 \ \forall m' \in M' = \phi(M)$. Pero $\alpha m' = \alpha \phi(m) = \phi(\alpha m) = \phi(0) = 0 \ \forall m \in M$
$\therefore Anul(M) \subseteq Anul(M')$
Otro caso: análogo. Sea $\beta \in Anul(M')$ $\therefore \beta m' = 0 \ \forall m' \in M'$.
$\therefore \beta \phi(m) = 0 \ \forall m \in M$ $\therefore \phi(\beta m) = 0 \ \forall m \in M$.
$\therefore \beta m \in Ker\,\phi = \{0\} \ \forall m \in M$ $\therefore \beta m = 0 \ \forall m \in M$
$\therefore Anul(M') \subseteq Anul(M)$

(1) y (2) implican (3). El recíproco no es cierto. Veamos un ej:
$M = X = A = \mathbb{Z}$, $M' = \mathbb{Q}$ $Anul(\mathbb{Z}) = Anul(\mathbb{Q}) = \{0\}$, pero $M \not\simeq M'$

4) J ideal izq de A.
Sea $K = Anul(A/J)$
pd: $a \cdot Anul(A/J) \subseteq Anul(A/J) \ \forall a \in A$ ✓, y $Anul(A/J) \cdot a \subseteq Anul(A/J) \ \forall a \in A$
$A/J = \{a_1 + J \mid a_1 \in A\}$
$Anul(A/J) = \{\alpha \in A \mid \alpha a_1 + J = J \ \forall a_1 \in A\}$
$= \{\alpha \in A \mid \alpha a_1 \in J \ \forall a_1 \in A\}$
Tenemos de inmediato que $Anul(A/J)$ es ideal por la izq de A.
Veamos que $Anul(A/J)\beta \subseteq Anul(A/J) \ \forall \beta \in A$.
Sea $\alpha \in Anul(A/J)$, $\beta \in A$. Luego $\alpha \in A$ y $\alpha a_1 \in J \ \forall a_1 \in A$
pd: $\alpha\beta a_1 \in J \ \forall a_1 \in A$
$(\alpha\beta)a_1 = \alpha(\beta a_1) \in J$ ✓ pues $\alpha \in Anul(A/J)$
$\therefore Anul(A/J) \trianglelefteq A$
Sea $K = Anul(A/J) = \{\alpha \in A \mid \alpha a_1 \in J \ \forall a_1 \in A\}$
Sea I ideal de A, $I \subseteq J$ pd: $I \subseteq K$.
Sea $y \in I$. pd: $y a_1 \in J \ \forall a_1 \in A$.
Pero $y a_1 \in I \subseteq J$, pues I es ideal $\Rightarrow y \in Anul(A/J) = K$
$\therefore I \subseteq K$.

Notas / Notes:

Fecha / Date:

Definición Sea M un A-módulo, $M \neq \{0\}$

1) M se dice <u>irreducible</u> o <u>simple</u> ssi sus únicos submódulos son los triviales.

2) M se dice <u>completamente reducible</u> o <u>semi-simple</u> ssi M es suma directa de módulos simples.

<u>Obs:</u> simple $\Rightarrow$ semisimple.

El recíproco no es cierto. Consideremos F cuerpo, $A = M_n(F)$

Entonces A_i es A-módulo semi-simple que no es simple.

Dijo! los sub-módulos son los ideales por la izq de A.

Definamos $A_K = \{(a_{ij})_{ij} \in A \,/\, a_{ij} = 0 \ \forall\, i \neq K\} \quad \forall\, K \in \{1, \dots, n\}$

$A = A_1 \oplus A_2 \oplus \dots \oplus A_n$

A_K no es simple pues:

Sea I ideal en A_K, $I \neq \{0\}$. pd: $I = A_K$.

Sea $y \in I \setminus \{0\} \subseteq A_K$, $y = (a_{ij})_{ij}$ con $a_{ij} = 0 \quad \forall\, j \neq K$

Existe $a_{iK} \neq 0 \quad \forall\, i \in \{1, \dots, n\}$

Sea $x = (b_{ij})_{ij} \in A_K$ con $b_{ij} = 0 \ \forall\, j \neq K$ y $\forall$

$$\begin{pmatrix} 0 & a_{2K}^{-1} & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} 0 & \dots & 0 & a_{iK} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2K+1} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & & \vdots \\ 0 & \dots & 0 & a_{nK} & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Lema de Schur Sean M, N dos A-módulos, $\phi : M \to N$ homom no nulo. Entonces:

1) M simple $\Rightarrow \phi$ inyect

2) N simple $\Rightarrow \phi$ epiyect.

<u>Dm:</u> 1) $Ker\, \phi$ submódulo de M, y $\phi \neq 0$ y M simple $\Rightarrow Ker\, \phi = \{0\}$

$\Rightarrow \phi$ inyectiva

2) Consideremos $Im(\phi)$ submódulo de N.

Como $\phi \neq 0$, $Im(\phi) = N \Rightarrow \phi$ epiyectiva

Fecha / Date:

$End_A(M) = \{f: M \to M / f$ homom$\}$ ↳ con composición de funciones

Corolario Sean M, N A-módulos, ambos simples.
Entonces $Hom_A(M,N) = \{0\}$ ó $M \simeq N$

Corolario Sea M un A-módulo simple. Entonces $End_A(M)$ es un álgebra de división.
En efecto, sea $f: M \to M$ homom, $f \neq 0$ y M simple $\Rightarrow$ f isom
$\therefore$ f invertible.

(16:15 hrs)

(Exposición Claudio)

Aplicaciones aritméticas de los cuaterniones $\mathbb{H}$.

Se trabajará sobre $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ y se define el anillo
$A_1 = \{a+bi+cj+dk \,/\, a,b,c,d \in \mathbb{Z}\}$
. A_1 es anillo ✓
Motivación: Teo de Lagrange. Todo nº positivo es suma de 4 cuadrados. Caso trivial: $0 = 0^2+0^2+0^2+0^2$. Veremos 5 lemas para finalmente probar el teo
(lema 1 antes)
Lema 2. Sea p primo impar. Entonces existen $a,b \in \mathbb{Z}$ tq $p \mid a^2+b^2+1$.
Dem: observe que en $\mathbb{Z}/p\mathbb{Z}$ hay $\frac{p+1}{2}$ cuadrados, pues $a^2 = (-a)^2$, pero además si $a^2 = b^2$, $b \neq 0$, $\left(\frac{a}{b}\right)^2 = 1 \Rightarrow \frac{a}{b} = 1$ ó $\frac{a}{b} = -1$
$\Rightarrow a = b$ ó $a = -b$.
$\therefore$ hay $\frac{p+1}{2}$ cuadrados en $\mathbb{F}_p$.
Sean $A = \{a^2 / a \in \mathbb{F}_p\}$, $B = \{-1-b^2 / b \in \mathbb{F}_p\}$ $\Big\}$ $|A| = |B| = \frac{p+1}{2}$.
Entonces $a^2 = -1-b^2$ ciertos $a,b \in \mathbb{F}_p$ $\therefore$ $a^2+b^2+1 = 0$ (p)
$\therefore$ $p \mid (a^2+b^2+1)$

Notas / Notes:

Comentario: todo número F_p es suma de dos cuadrados, pues en la dem podría haber puesto n en vez de -1.

Lema 1. Para todos $(x_i)_{i=1}^{4}$, $(y_i)_{i=1}^{4}$ se tiene que

$(x_1^2+\dots+x_4^2)(y_1^2+\dots+y_4^2) = z_1^2+z_2^2+z_3^2+z_4^2$

donde $z_1+z_2 i+z_3 j+z_4 k = (x_1+\dots+x_4 k)(y_1+\dots+y_4 k)$

Lema 3. Sea $R\subseteq H$ definido por $R=\{a+bi+cj+dk \,/\, a,b,c,d\in \mathbb{Z} \text{ ó } a,b,c,d\in \mathbb{Z}+\frac{1}{2}\}$

R es un anillo.

Dem:

Claramente R es cerrado bajo la suma. Sea $x,y\in R$, $x=x^*+e$, con $x^*\in A_1$, $e=\frac{1}{2}(i+j+k)$, $y=y^*+e$.

Por casos:

(1) Si $x,y\in A_1 \Rightarrow xy\in A_1\subseteq R$.

(2) Si $x\in A_1$, $y\in R\setminus A_1$, $xy=xy^*+xe$. Basta demostrar que $ie, je, ke, ei, ej, ek\in R$.

(3) $x\in R\setminus A_1$, $y\in R\setminus A_1$, hay que demostrar que $e^2\in R$:

$e^2=\frac{1}{4}(1-1-1-1+2i+2j+2k) = -\frac{1}{2}+\frac{i+j+k}{2} = y+e$

07/10

Definición Sea M un A-módulo y P un submódulo de M. Se dice que P es maximal ssi $P\neq M$ y si $P\subseteq M_1$ entonces $M_1=M$.

Se dice que P es minimal si $P\neq\{0\}$ y si $M_1\subseteq P$ entonces $M_1=\{0\}$.

Obs:

J ideal izq de A (como A-módulo), entonces J es submódulo simple de A ($A=A_1$) minimal.

Obs:

Sea M un A-módulo y N un submódulo de M. Entonces M/N es simple $\Leftrightarrow$ N es submódulo maximal de M.

Fecha / Date:

n° 2.7.3 de los apuntes

Lema Sea M un A-módulo, $M \neq \{0\}$. Entonces son equivalentes

(1) M es simple

(2) $M = Ax$, $\forall x \in M$, $x \neq 0$

(3) $M \cong A/J$, $\forall J$ ideal izq maximal de A.

Dem:

(3) $\Rightarrow$ (1): se obtiene de la observac 2, pues A/J es simple, y luego M es simple.

(1) $\Rightarrow$ (2): Sea M simple. Como $x \neq 0$, $Ax \neq \{0\}$ y es submódulo de M $\therefore$ $Ax = M$.

(2) $\Rightarrow$ (3): sea $t \neq 0$. $\therefore$ $M = At$ Definamos $\phi : A \to M$ por $\phi(a) = at$ Entonces ϕ es lineal, epiyectiva $\therefore$ $A/\mathrm{Ker}\,\phi \cong M$

09/10

(2) $\Rightarrow$ (1): Sea N submódulo de M, $N \neq \{0\}$ $\therefore$ $\exists\, n \in N$, $n \neq 0$. Por (2), $M = An$, pero N submódulo de M y $n \in N \Rightarrow$ $An \subseteq N$, $\therefore$ $M \subseteq N$, $\therefore$ $N = M$, $\therefore$ M simple.

Ejercicio (2.14): sea $M = M_1 \oplus M_2$, M_i submódulos de M. Sea P submódulo de M tq $M_1 \subseteq P$. Entonces $P = M_1 \oplus (M_2 \cap P)$

Teorema Sea M un A-módulo. Son equivalentes:

(1) M es semi-simple

(2) M es suma (no necesariam. directa) de submódulos simples N_j de M, $j \in J$.

(3) Todo submódulo de M es sumando directo de M, más precisamente para cada submódulo T de M, existe submódulo S de M tq $M = T \oplus S$ (tb se dice que cada submódulo de M tiene complementario en M)

Dem:

(1) $\Rightarrow$ (2): inmediato.

Notas / Notes:

RHEIN.

Fecha / Date:

(2) ⇒ (3): Sea $M = \sum_{j \in J} N_j$, N_j simple $\forall j \in J$.
Sea T submódulo de M, $T \neq \{0\}$. Para encontrar S submódulo de M tq $M = T \oplus S$ construiremos una sucesión de subíndices $j_1, j_2, \dots, j_q$ ($j_i \in J$) en forma recursiva.

Sea j_1 el menor índice tq $N_{j_1} \not\subseteq T$

j_2 el menor índice tq $N_{j_2} \not\subseteq T + N_{j_1}$

$\vdots$

j_q el menor índice tq $N_{j_q} \not\subseteq T + N_{j_1} + \dots + N_{j_{q-1}}$

El proceso termina cuando ya no se puede definir un nuevo índice.

Probemos que $T + N_{j_1} + \dots + N_{j_q}$ es directa usando inducción sobre q.

Para $q = 1$. pd: $T \cap N_{j_1} = \{0\}$. Tenemos que $T \cap N_{j_1}$ es submódulo de N_{j_1} y $N_{j_1} \not\subseteq T$. $\therefore T \cap N_{j_1} = \{0\}$. (pues N_{j_1} es simple)

Hipótesis inductiva: $T + N_{j_1} + \dots + N_{j_{q-1}}$ es directa. Sea $H = T \oplus N_{j_1} \oplus \dots \oplus N_{j_{q-1}}$.

Tesis inductiva: $T + N_{j_1} + \dots + N_{j_q}$ es directa, y entonces $H + N_{j_q} = T \oplus N_{j_1} \oplus \dots \oplus N_{j_{q-1}} + N_{j_q}$.

pd: $H \cap N_{j_q} = \{0\}$.

Como $H \cap N_{j_q}$ es submódulo de N_{j_q}, N_{j_q} simple y $N_{j_q} \not\subseteq H$, entonces se tiene que $H \cap N_{j_q} = \{0\}$. $\therefore T \oplus N_{j_1} \oplus \dots \oplus N_{j_q}$.

$\therefore$ por ppio de inducción, $T \oplus N_{j_1} \oplus \dots \oplus N_{j_t}$, $\forall t \geq 1$.

Falta probar que $M = T \oplus \underbrace{N_{j_1} \oplus \dots \oplus N_{j_q}}_{S}$.

Tenemos $M = \sum_{j \in J} N_j$, N_j simple. Como j_q es el último de los índices $j_1, \dots, j_q$ entonces todos los N_i tq $M = \sum_{i \in I} N_i$ están contenidos en $T + N_{j_1} + \dots + N_{j_q}$

$\therefore M \subseteq T + N_{j_1} + \dots + N_{j_q}$, $\therefore M = T + N_{j_1} + \dots + N_{j_q}$

RHEIN. Notas / Notes:

Scanned with CamScanner

(3) $\Rightarrow$ (2): $\forall$ T submódulo de M, $\exists$ S, tq $M = T \oplus S$.

pd: $M = \bigoplus_{i \in I} N_i$ con N_i simples.

Primero, mostremos que M tiene submódulos simples. Usemos lema de Zorn. Sea $x \in M$, $x \neq 0$. Formemos $S(x) = \{T \subseteq M \,/\, T$ submódulo de M, $x \notin T\}$

$S(x) \neq \emptyset$, pues $\{0\} \in S(x)$. Sea $\{T_i\}_{i \in I}$ cadena de submódulos en $S(x)$, entonces $\bigcup_{i \in I} T_i$ es cota superior de la cadena.

Por Zorn, $S(x)$ tiene elemento maximal T_0 ($\therefore$ $x \notin T_0$ y maximal con respecto a esta propiedad). Por (3), T_0 tiene un complemento en M, $\therefore$ $\exists$ N submódulo de M tq $M = T_0 \oplus N$.

Veremos que N es simple.

Supongamos que hay submódulo propio N_1 de N, por (3), $M = N_1 \oplus N_2$. Como $N_1 \subseteq N$, por ejercicio anterior al teorema, $N = N_1 \oplus (N_2 \cap N)$. Ahora bien, $x \in T_0 \oplus N_1$ y $x \in T_0 \oplus (N_2 \cap N)$ (pues T_0 es maximal con respecto a $x \notin T_0$, $N_1 \neq \{0\}$, $N_2 \cap N \neq \{0\}$).

Por lo tanto, $x = t_0 + n_1$, $x = t_0' + n_2$ con $t_0, t_0' \in T_0$, $n_1 \in N_1$, $n_2 \in N_2 \cap N$.

$\therefore$ $n_1 + t_0 = n_2 + t_0'$

$\therefore$ $n_1 - n_2 = t_0' - t_0 \in T_0$

Por otro lado, $n_1, n_2 \in N$. $\therefore$ $n_1 - n_2 \in T_0 \cap N = \{0\}$.

$\therefore$ $n_1 = n_2$. Además $N_1 \cap (N_2 \cap N) = \{0\}$, $\therefore$ $n_1 = 0 = n_2$.

$\therefore$ $x = t_0 \in T_0 \Rightarrow \Leftarrow$

$\therefore$ N es simple.

(16:15 hrs)

(continuación expo' Claudio)

$R = \{a + bi + cj + dk \,/\, \substack{a,b,c,d \in \mathbb{Z} \\ a,b,c,d \in \mathbb{Z} + \frac{1}{2}}\}$

Subanillo $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ no conmutativo. $(i, j \in \mathbb{H} : ij = -ji)$

Dados $u, v \in R$, $\exists$ $q', r' \in R$ tq: $u = vq' + r'$ $N(r') < N(v)$ (eucl por der)

$u = q''v + r''$ $N(r'') < N(v)$ (eucl por izq). Luego todo ideal I de R es de la forma $I = Rv$ (o análoga/: vR)

Notas / Notes:

Fecha / Date:

Lema 4. R es un dominio euclidiano (por derecha e izquierda).

Dem:

Sea $s \in \mathbb{H}$. $s = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$; $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$

Por casos, encontremos $t \in R$ tq $N(s-t) < 1$. (se puede hacer de mejor manera)

(i) si al menos dos 'coordenadas' tienen distancia menor a $\frac{1}{4}$ de su entero + próximo.

Simbólica/.: $\exists\, \alpha_i, \alpha_j \in (\alpha_i)_{i=1}^{4}$: $\exists\, a_i, a_j \in \mathbb{Z}$: $|\alpha_i - a_i| \leq \frac{1}{4}$, $|\alpha_j - a_j| \leq \frac{1}{4}$

entero + próximo, no necesaria/. parte entera

Sea $t = [\alpha_0] + [\alpha_1] i + [\alpha_2] j + [\alpha_3] k \in A \subsetneq R$

Y se cumple que:

$N(s-t) = (\alpha_0 - [\alpha_0])^2 + \dots + (\alpha_3 - [\alpha_3])^2 \leq \frac{2}{16} + \frac{2}{4} = \frac{5}{8}$

(ii) En caso contrario, consideremos: (aquí es la parte entera)

$t = ([\alpha_0] + \frac{1}{2}) + \dots + ([\alpha_3] + \frac{1}{2}) k \in R$ tq

$N(s-t) \leq \frac{2}{16} + \frac{2}{4} = \frac{5}{8}$

Ahora: sean $u, v \in R$. Consideremos $uv^{-1} \in \mathbb{H}$. Por lo anterior,

$\exists\, q'' \in R$ tq $N(uv^{-1} - q'') \leq \frac{5}{8}$.

Luego $u = q''v + r'$ $\quad r' = u - q''v$ y cumple con

$N(r') = N(u - q''v) = N((uv^{-1} - q'')v) = N(uv^{-1} - q'')N(v) \leq \frac{5}{8} N(v) < N(v)$

Sólo queda verificar que es un DIP.

Sea J ideal, $J \neq \{0\}$ (si $J = (0)$, $J = R(0)$).

$J \subseteq R$ (por la izq)

$\exists\, v \in J$ tq $v \neq 0 \Rightarrow N(v) \neq 0$ → porque aunque tenemos $\mathbb{Z} + \frac{1}{2}$, tendremos $\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$

Sea así $\emptyset \neq A = \{N(z) / z \in J\} \subseteq \mathbb{Z}_0$

Por axioma del buen orden, tiene elemento mínimo.

Tomemos v tq $N(v) = \min A$.

Siempre es cierto que $Rv \subseteq J$ (pues J es ideal por izq)

Sea $x \in J$. Entonces, por lo anterior, existen $r'', q'' \in R$ tq

$x = q''v + r''$ $\quad N(r'') < N(v)$ $\Rightarrow$ $r'' = 0$. Entonces $r'' = \underset{\in J}{x} - \underbrace{q''v}_{\in J} \in J$

∴ $r'' = 0$. Luego $x = q''v \in Rv$

∴ $J = Rv$

dominio de integridad → sin div de cero
" " " ppal → todo ideal es ppal (generado por 1 elem)

RHEIN. Notas / Notes:

Obs:

$J = Rv \quad \forall v$ con norma mínima (de J)

Lema 5.- Para todo primo impar p, se tiene que $\exists\, q \in R$ tq $N(q) = p$.

Dem:

Sea p primo impar. Por lema 2 $\exists\, a, b \in \mathbb{Z}$ tq $p \mid (1 + a^2 + b^2)$

Luego, consideremos el sgte ideal por la izq.

$J = (p) + (1 + ai + bj) = (q)$ Nos gustaría $N(q) = p$.

Obs: $p \in (p) + (1 + ai + bj) \Rightarrow p = t \cdot q$

Luego $p^2 = N(tq) = N(t) N(q) \Rightarrow N(q) \mid p^2$

Debemos probar: $1 \neq N(q) \neq p^2$.

(i) Si $N(q) = 1 \Rightarrow q\bar{q} = 1 \Rightarrow J = R$ ¡falso!

Si fuese esto cierto, tendríamos $1 = \tilde{t} p + s(1 + ai + bj)$

$1 = t\bar{t} p^2 + p\tilde{t}\bar{s}(1 - ai - bj) + p\bar{t}s(1 + ai + bj) + s\bar{s}(1 + a^2 + b^2)$

$\therefore\ p \mid 1 \Rightarrow \Leftarrow$

(ii) $N(q) = p^2 = N(p) \Rightarrow (p) = (p) + (1 + ai + bj)$

$\therefore\ 1 + ai + bj \in (p)$

$\therefore\ 1 + ai + bj = tp$

$\therefore\ p \mid 1 \Rightarrow \Leftarrow$

Luego $N(q) = p$

Teorema (Lagrange) todo entero positivo es suma de cuatro cuadrados enteros (no nulos).

Dem:

Sea p primo impar. Por lema 5, $\exists\, q \in R$ tq $N(q) = p$.

Luego, si $q \in A_1$, se tiene lo pedido.

Si no: $q = 2(y_0 + y_1 i + y_2 j + y_3 k) + \dfrac{\pm 1 \pm i \pm j \pm k}{2}$

Sea $q_1 = q - 2(y_0 + y_1 i + y_2 j + y_3 k)$

Entonces, $q\bar{q}_1 \in A_1$ pues $\left(2(y_0 + y_1 i + y_2 j + y_3 k) + \dfrac{\pm 1 \pm 1 \pm 1 \pm 1}{2}\right)\left(\dfrac{\pm 1 \pm 1 \pm 1 \pm 1}{2}\right) \in A$

Notas / Notes:

Fecha / Date:

$N\left(\frac{1 \pm i \pm j \pm k}{2}\right) = 4 \cdot \frac{1}{4} = 1$ y $N(q\bar{q}) = N(q)\,N(\bar{q}) = N(q) = p$

Ahora bien, si $p = 2$, $N(1+i) = 2$ $\quad i+1 \in A$.
Se concluye, pues $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ para p_i $\exists\, q_i \in A$, tq.
$N(q_i) = p_i$
Así $n = N(q_1)^{\alpha_1} \cdots N(q_r)^{\alpha_r} = N(\underbrace{q_1^{\alpha_1} \cdots q_r^{\alpha_r}}_{\in A}) = z_1^2 + z_2^2 + z_3^2 + z_4^2$

con $z_i \in \mathbb{Z}$

(Expó Boris)

Álgebra de multiplicación de un álgebra A

Definición Sea A un F-álgebra (no necesariamente tiene 1), y sea $a \in A$. Se define:
$R_a : A \to A$, $x \mapsto xa$ $\quad L_a : A \to A$, $x \mapsto ax$. Son operadores lineales.

$M(A) = \langle R(A) \cup L(A) \rangle \subseteq End(A)$

Obs:

- $M(A)$ es asociativo (a pesar que A no lo sea) pero no conmutativo.
- $M(A)$ es la intersecc. de todas las subalg de $End(A)$ que contienen a $R(A) \cup L(A)$.
- $f \in M(A) \iff f = \sum_{\text{finita}} S_1 \cdots S_t$ $\quad S_i \in R(A) \cup L(A)$

Definición $\phi \neq B \subset A$, se denota por B^* al subalgebra de $M(A)$ generado por $R(B) \cup L(B)$. Notemos que $f \in R(B) \Leftrightarrow f = R_b : A \to A$ $\forall b \in B$.
(NO: $f : B \to B$)

Obs:

- $A^* = M(A)$ y $\{0\}^* = \{f = 0\}$
- $I \trianglelefteq A$ (bilatero) $\Rightarrow I^*$ subalg de $M(A)$ (no nec ideal)

Definición Sea A álgebra asociativa con 1, y sea $\emptyset \neq X \subseteq A$. Se define como centralizador $C_A(X) = \{a \in A \mid [x, a] = 0 \ \forall x \in X\}$

14/10

Teorema Sea M un A-módulo. Las sgtes son equivalentes.

(i) M es semi-simple

(ii) M es suma no necesariamente directa de submódulos simples N_j

(iii) Para todo T submódulo de M, existe $S \leq M$ tal que $M = T \oplus S$ (se dice que T tiene complementario en M).

Dem:

(i) $\Rightarrow$ (ii): inmediato.

(ii) $\Rightarrow$ (iii): listo por la clase anterior.

(iii) $\Rightarrow$ (i). Habíamos visto que si se cumple (iii), M tiene un submódulo simple. Consideremos la familia $\{N_i\}_{i \in I}$ de submódulos simples de M de manera que $\sum_{i \in I} N_i$ sea directa, con $\# I$ maximal.

pd: $M = \sum_{i \in I} N_i$. Si no, $M = (\sum_{i \in I} N_i) \oplus Q$ con Q submódulo de M. Entonces Q tiene un submódulo simple N_k, con $k \notin I$. (similar a lo probado antes) $\therefore \sum_{i \in I \cup \{k\}} N_i$ es directa $\Rightarrow \Leftarrow$ (contradice $\# I$ máximo).

$\therefore M = \bigoplus_{i \in I} N_i$.

$\therefore M$ es semi-simple.

Corolario Sea M un A-módulo semi-simple. Entonces todo submódulo P de M, con $P \neq \{0\}$, tiene un submódulo simple.

Definición Un A-módulo M se dice indescomponible si: $M \neq \{0\}$ y no puede escribirse como suma directa de dos submódulos no nulos.

Fecha / Date:

Proposición Sea M un A-módulo semi-simple. Entonces son equivalentes:

(i) M es simple

(ii) $End_A(M)$ es un álgebra de división

(iii) M es indescomponible.

$$\begin{tikzcd} f: N_1 \oplus N_2 \arrow[r] & N_1 \oplus N_2 \\ f|_{N_1}: N_1 \arrow[r] \arrow[dr, dotted] & N_1 \oplus N_2 \arrow[d, "p_1"] \\ & N_1 \end{tikzcd}$$

$p_1 \circ f|_{N_1} \in End_A(N_1)$

$End_A(N_1 \oplus N_2) = End_A N_1 \oplus End_A N_2$

Dem:

(i) $\Rightarrow$ (ii): sale de corolario de lema de Schur.

(ii) $\Rightarrow$ (iii): Supongamos $M = N_1 \oplus N_2$, N_i submódulos de M.

$End_A(M)$ de división $\Rightarrow$ $id_M \neq \{0\}$ y $M \neq \{0\}$.

Consideremos la proyección $p_1: M \to M$ $\quad p_1(n_1, n_2) = n_1$

$\therefore$ $Im(p_1) = p(M) = N_1$, $p_1^2 = p_1$ ... luego $p_1^2 - p_1 = 0$

$\therefore$ $p_1(p_1 - id_M) = 0 \Rightarrow p_1 = 0$ ó $p_1 = id_M$ porque $End_A(M)$ es de div.

$\therefore$ $N_1 = \{0\}$ ó $N_2 = \{0\}$.

$\therefore$ M es indescomponible.

(iii) $\Rightarrow$ (i): Sea M indescomponible. Supongamos M no es simple.

Sea $T \leq M$ T submódulo propio. Por ser M semi-simple, T tiene complementario $\{0\} \neq S$ en M, es decir, existe $S \leq M$ tal que $M = T \oplus S$.

Esto contradice que M sea indescomponible.

$\therefore$ M es simple.

Ejercicio: sea T submódulo de M. Entonces T tiene complementario en M $\Leftrightarrow$ $\exists\, f: M \to T$ lineal, tal que $f(t) = t$ $\forall t \in T$. Es decir, $f|_T = id_T$. $\to$ parecido N° 3, guía 5 con $g: M \to M$, $m \mapsto f^?(m)$ $\quad g^2 = g$

Módulos noetherianos y artinianos:

Definición Sea M un A-módulo. Se dice que M es noetheriano ssi toda sucesión de submódulos estrictamente creciente de submódulos es estacionaria.

Si $S_1 \subset S_2 \subset S_3 \subset \ldots$, $\exists\, t$ tal que $S_t = S_{t+1} = S_k$ $\forall k \geq t$

Notas / Notes:

Definición. Sea M un A-módulo. Se dice que M es artiniano si toda sucesión decreciente de submódulos de M es estacionaria.

Proposición. Sea M un A-módulo. Son equivalentes:
(i) M es noetheriano.
(ii) Todo submódulo de M es finitamente generado.
(iii) Todo conjunto no vacío de submódulos de M tiene elemento maximal.

Dem:
(i) $\Rightarrow$ (ii): Sea $P \leq M$ submódulo. Supongamos $P \neq \{0\}$, pues si no es inmediato. Supongamos además P no es finitamente generado.
Sea $0 \neq a_1 \in P$. $A a_1 = (a_1) \subset P$.
Sea $0 \neq a_2 \in P \setminus \{a_1\}$. Luego $(a_1, a_2) \subset P$.
Tenemos así una sucesión de submódulos $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$ la cual no es estacionaria. Contradicción.
(ii) $\Rightarrow$ (iii): Sea $\mathcal{T}$ conjunto no vacío de submódulos de M, sin elemento maximal. Sea $T_1 \in \mathcal{T}$. Como $\mathcal{T}$ no tiene maximal, sea $T_2 \in \mathcal{T}$ con $T_1 \subset T_2$. Así sucesivamente, tenemos una sucesión de submódulos $T_1 \subset T_2 \subset T_3 \subset \ldots$
Sea $P = \bigcup_{i \in I} T_i$. P es submódulo de M, y no es finitamente generado. Contradicción.
(iii) $\Rightarrow$ (i): Supongamos existe una sucesión estrictamente creciente de submódulos de M no estacionaria $S_1 \subset S_2 \subset S_3 \subset \ldots$
Entonces $\mathcal{H} = \{S_1, S_2, S_3, \ldots\}$ no tiene elemento maximal. Contradicción.

Notas / Notes:

RHEIN.

Proposición Sea M un A-módulo. Son equivalentes:

(i) M es artiniano.

(ii) Todo cjto no vacío de submódulos de M tiene elemento minimal.

(ii) $\Rightarrow$ (i):

~~(i) $\Rightarrow$ (ii)~~: tomar $\cap$

Corolario Sea M un A-módulo simple. Entonces M es noetheriano y artiniano.

Ej: $\mathbb{Z}$ es un $\mathbb{Z}$-módulo noetheriano (porque todo ideal es finitam. generado) pero no artiniano, pues por ejemplo:

$(2) \supset (2^2) \supset (2^3) \supset \dots$

Definición Sean M_1, M_2, M_3 tres A-módulos. Se dice que $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ es sucesión exacta de módulos ssi $\operatorname{Im}(f) = \operatorname{Ker}(g)$.

Proposición Si M_i, $i \in \{1,2,3\}$, son A-módulos, entonces

(i) $0 \longrightarrow M_1 \xrightarrow{f} M_2$ exacta $\Leftrightarrow$ f es inyectiva

(ii) $M_2 \xrightarrow{g} M_3 \longrightarrow 0$ exacta $\Leftrightarrow$ g es epiyectiva

Cada pedazo de a 2 y exacta

Definición Sean M_i, con $i \in \{1,2,3\}$, A-módulos. Se dice que $0 \xrightarrow{h} M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \xrightarrow{k} 0$ es exacta corta ssi:

(i) f inyectiva

(ii) g epiyectiva

(iii) $\operatorname{Im}(f) = \operatorname{Ker}(g)$

Ej: $M_1 \xhookrightarrow{i} M_1 \oplus M_2 \xrightarrow{p_2} M_2$

$i(m_1) = (m_1, 0)$ $\quad$ $p_2(m_1, m_2) = m_2$ $\quad$ Además, i es inyectiva

$\operatorname{Im}(i) = M_1 = \operatorname{Ker} p_2$ $\quad$ (i, p_2 son lineales) $\quad$ y p_2 es epiyectiva

Ej: Sea $n \in \mathbb{N}$. $\mathbb{Z} \xrightarrow{L_n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z}$ $\quad$ $\operatorname{Im}(L_n) = n\mathbb{Z} = \operatorname{Ker}(\pi)$

$x \longmapsto nx$

L_n, π lineales, L_n inyect, π epiy.

Notas / Notes:

Fecha / Date:

Ej: $M_1 \leq M_2$ submódulo. $Im(i) = M_1 = Ker(p)$

$0 \to M_1 \xrightarrow{i} M_2 \xrightarrow{p} M_2/M_1$ i, p lineales

$m_1 \mapsto m_1$

$m_2 \longmapsto m_2 + M_1$ i inyectiva, p epiyectiva

16/10

• $H \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$

Sea ϕ: $i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ $\mathbb{R}$-lineal (se extiende por linealidad)

$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

$1 \mapsto id$

Sea $\psi: H \times \mathbb{C} \longrightarrow M_2(\mathbb{C})$ $\mathbb{R}$-bilineal

$(q, c) \mapsto \phi(q)\phi(c)$

Por prop univ del pdto tens: $\exists ! \, f: H \otimes \mathbb{C} \longrightarrow M_2(\mathbb{C})$ $\mathbb{R}$-lineal

$q \otimes c \mapsto \phi(q)\phi(c)$

$q \otimes c \in Ker(f) \Rightarrow \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}\begin{pmatrix} u+iv & 0 \\ 0 & u-iv \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\begin{pmatrix} (a+ib)(u+iv) & (c+id)(u-iv) \\ (-c+d)(u+iv) & (a-ib)(u-iv) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$(a+ib)(u+iv) = (-c+id)(u+iv) = (c+id)(u-iv)(a-ib)(u-iv) = 0$

$\Rightarrow q = 0$ ó $c = 0 \Rightarrow q \otimes c = 0$

Sea $z \in Ker(f) \Rightarrow z = \sum_{\text{finita}} q_i \otimes c_i \Rightarrow f(z) = \sum_{\text{finita}} f(q_i \otimes c_i) = 0$

$H \xhookrightarrow{l} End_{\mathbb{C}}(H) \cong M_2(\mathbb{C})$ Otra idea: $z = \lambda_1 1\otimes 1 + \lambda_2 i \otimes 1 + \lambda_3 j \otimes 1 + \lambda_4 k \otimes 1$

$+ \lambda_5 i \otimes 1 + \lambda_6 i \otimes i + \lambda_7 i \otimes j + \lambda_8 i \otimes k$

$i \mapsto l_i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

$j \mapsto l_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$f(z) = \lambda_1 f(1 \otimes 1) + \lambda_2 f(i \otimes 1) + \lambda_3 f(j \otimes 1) + \lambda_4 f(k \otimes 1)$

$+ \lambda_5 f(i \otimes 1) + \lambda_6 f(i \otimes i) + \lambda_7 f(i \otimes j) + \lambda_8 f(i \otimes k)$

$f(z) = \lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + \lambda_5 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \lambda_6 \underbrace{\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}_{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}} + \lambda_7 \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}_{\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}}$

$+ \lambda_8 \underbrace{\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}_{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}} = \begin{pmatrix} \lambda_1 + \lambda_2 i + \lambda_5 i - \lambda_6 & \lambda_3 + \lambda_4 i - \lambda_7 i + \lambda_8 \\ -\lambda_3 + \lambda_4 i - \lambda_7 i - \lambda_8 & \lambda_1 - \lambda_2 i - \lambda_5 i - \lambda_6 \end{pmatrix}$

Notas / Notes:

$z \in \operatorname{Ker} f \Rightarrow (\alpha_1-\alpha_6)+(\alpha_2+\alpha_5)i=0 \qquad (\alpha_3+\alpha_8)+(\alpha_4-\alpha_7)i=0$

$-(\alpha_3+\alpha_8)+(\alpha_4-\alpha_7)i=0 \qquad (\alpha_1-\alpha_6)+-(\alpha_2+\alpha_5)i=0$

$\Rightarrow \left.\begin{array}{ll} \alpha_1=\alpha_6 & \alpha_3=-\alpha_8 \\ \alpha_2=-\alpha_5 & \alpha_4=\alpha_7 \end{array}\right\}$ f no es inyectiva !!

Idea de Gandriel: $u,v \in \mathbb{C}$

$f(q\otimes c) = f(u+vj\otimes c) = \phi(u+vj)\,\phi(c)$

$= \begin{pmatrix} u & v \\ -\bar v & \bar u \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & \bar c \end{pmatrix} = \begin{pmatrix} uc & v\bar c \\ -c\bar v & \bar u \bar c \end{pmatrix}$

$g: M_2(\mathbb{C}) \longrightarrow (\mathbb{C}\oplus\mathbb{C}j)\otimes_{\mathbb{R}}\mathbb{C}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a+bj \otimes ad-bc$

$g\begin{pmatrix} uc & v\bar c \\ -c\bar v & \bar u\bar c \end{pmatrix} = (uc+v\bar c j)\otimes(uc\bar u\bar c)+(v\bar c c\bar v) = (uc+v\bar c j)\otimes(uc\bar u\bar c)+N(c)N(v)$

21/10

Ej: Sean $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ sucesión corta de A-módulos. Entonces: (i) N noetheriano $\Leftrightarrow$ M y P noetherianos

(ii) N artiniano $\Leftrightarrow$ M y P artinianos

Proposición Sean $M_1,\dots,M_n$ A-módulos. Entonces $\bigoplus_{i=1}^{n} M_i$ noetheriano (respectivamente artiniano) $\Leftrightarrow$ M_i noetheriano (respectivamente artiniano) cada $i=1,\dots,n$.

Dem:

Ver apuntes.

Proposición (Teorema de la base de Hilbert) Si R es un anillo noetheriano, entonces el anillo de polinomios $R[x]$ es noetherino.

Obs: Si R es artiniano, $R[x]$ no lo es necesariamente.

Dem Teo' de la base de Hilbert:

Sea J un ideal de $R[x]$. pd: J es finitamente generado.
Si $J=\{0\}$: ✓
Sea $J\neq\{0\}$. Sea $f(x)\in J$, $f(x)\neq 0$. Escribamos $f(x)=\sum_{i=0}^{n(f)} a_i(f)\cdot x^i$, donde $n(f)$ es el grado de f. Luego $a_{n(f)}(f)\neq 0$.
Denotemos por $s(f)=a_{n(f)}(f)=$ coef. supremo (o lider) de f.
Formemos el conjunto $I=\{s(f)\,/\,f\in J\}\cup\{0\}$. Entonces I es ideal de R; en efecto, para todo $r\in R$ y para todo $f\in J$, $r\cdot s(f)=s(r\cdot f)\in I$.
Sean ahora $f(x)=a_0(f)+a_1(f)\cdot x+\dots+a_{n(f)}(f)\cdot x^{n(f)}$ y $g(x)=b_0(g)+\dots+b_{n(g)}\cdot x^{n(g)}$,
Queremos demostrar que hay $h(x)\in J$ tal que $s(h)=s(f)+s(g)$, es decir, $s(h)=a_{n(f)}(f)+b_{n(g)}(g)$.
Sea $N=\max\{n(f),n(g)\}$. Tomemos $h(x)=x^{N-n(f)}f+x^{N-n(g)}g$
Así, $s(h)=a_{n(f)}(f)+a_{n(g)}(g)$, pues:
$h(x)=a_0(f)\,x^{N-n(f)}+\dots+a_{n(f)}(f)\,x^N+b_0(g)\cdot x^{N-n(g)}+\dots+b_{n(g)}(g)\cdot x^N$
$\therefore$ I es ideal de R. Como R es noetheriano, I es finitamente generado.
Sean $h_1(x),\dots,h_n(x)\in J$ tales que $s(h_1),\dots,s(h_n)$ generan I.
Sea $N=\max\{n(h_1),n(h_2),\dots,n(h_n)\}$, y sean $h_i'(x)=x^{N-n(h_i)}\cdot h_i(x)$ para todo $i\in\{1,\dots,n\}$. Así, $N=n(h_i')$ y $s(h_i)=s(h_i')$ $\forall i$.
Sea J_N el conjunto de polinomios de J de grado $\leq N$, unión el polinomio 0.
Probemos que $J=J_N+\sum_{i=1}^{n}R[x]h_i'(x)$. Así J estaría finitamente generado. Ya sabemos $J_N+\sum_{i=1}^{n}R[x]\cdot h_i'(x)\subseteq J$.
Sea $f(x)\in J$. Usemos inducción sobre $n(f)$.
Si $n(f)\leq N$, entonces $f(x)\in J_N$. Luego $f(x)\in J_N+\sum_{i=1}^{n}R[x]h_i'(x)$.
Si $n(f)>N$: supongamos (hipótesis de inducción) que $J\subseteq J_N+\sum_{i=1}^{n}R[x]h_i'(x)$ vale para polinomios de grado $<n(f)$.

Notas / Notes:

Todo módulo simple no nulo es monogénico.

Como $s(h_i) = s(h_i')$ y $\{s(h_1), \ldots, s(h_n)\}$ genera I, tenemos $\{s(h_1'), \ldots, s(h_n')\}$ genera I. Por lo tanto, $s(f) = \sum_{i=1}^{n} a_i s(h_i)$ ciertos $a_i \in R$. Consideremos entonces el sgte polinomio en J: $g(x) = f(x) - x^{n(f)-n} \sum_{i=1}^{n} a_i h_i'(x)$. Tiene grado $< n(f)$.

$\therefore g(x) \in J_n + \sum_{i=1}^{n} R[x] \cdot h_i'(x)$ por hipótesis de inducción, y $f(x) \in J_n + \sum_{i=1}^{n} R[x] \cdot h_i'(x)$.

$\therefore J = J_n + \sum_{i=1}^{n} R[x]\, h_i'(x)$.

Obs:

¿Qué pasa si R es artiniano?

Sea $R = \mathbb{R}$ (cuerpo) es artiniano (y noetheriano). Luego $\mathbb{R}[x]$ es noetheriano, pero no es artiniano: $(x) \supset (x^2) \supset (x^3) \supset \ldots$

Ejercicio:

Todo módulo M finitamente generado, sobre A anillo noetheriano, es noetheriano.

Sugerencia: M es isomorfo a un cuociente de A^n, para algún n. Pruebe que A^n es noetheriano.

Proposición: Sea M un A-módulo semi-simple. Entonces son equiv:

(i) M es finitamente generado.

(ii) $M = N_1 \oplus N_2 \oplus \ldots \oplus N_t$ con N_i simples $\forall i$

(iii) M es artiniano

(iv) M es noetheriano

A f.g. pues $A = \langle 1_A \rangle$

Dem:

(ii) $\Leftrightarrow$ (iii), (ii) $\Leftrightarrow$ (iv): inmediato.

(i) $\Rightarrow$ (ii): Sea M finitamente generado. Si $M = \bigoplus_{i \in I} N_i$, con N_i simples e I infinito, entonces M no es finitam/. generado.

(ii) $\Rightarrow$ (i): $M = N_1 \oplus \ldots \oplus N_t$ con $N_i = A \cdot x_i$, $x_i \neq 0$ $\forall i = 1, \ldots, t$.

Luego $\{x_i\}_{i=1}^{t}$ genera M.

Álgebras semi-simples:

Definición Un álgebra A se dice semi-simple ssi A es semi-simple como A-módulo por la izquierda.

Obs:

- Los submódulos de A son los ideales por la izquierda.
- Los submódulos simples de A son los ideales por la izquierda de A, minimales.
- A semi-simple $\Rightarrow A = \bigoplus_{i \in J} N_i$ con N_i ideales por la izq, minimales y J finito.

23/10

(continuamos expo' Boris)

$$C' = C_{End(A)}(\underbrace{M(A)}_{\text{es asoc.}}) = \{T \in End(A) \,/\, TR_y = R_y T,\ L_x T = T L_x \quad \forall x, y \in A\}$$

Obs:

$\forall S, T \in C'$ se cumple:

a) $T(xy) = T(x)y = xT(y)$ pues $T(xy) = T(R_y(x)) = TR_y(x) = R_y T(x) = T(x)y$

$T(xy) = T(L_x(y)) = L_x(T(y)) = x\,T(y)$

b) $ST(xy) = S(T(xy)) = S(x)T(y) = T(S(x)y) = T(S(xy)) = TS(xy) \quad \forall x, y \in A$

Luego, si $A^2 = A$, $ST = TS$

Esto porque $S(T(xy)) = S(x\,T(y)) = S(x)\,T(y) = T(S(x)\,y) = T(S(xy))$

Definición Sea A álgebra, sean $x, y, z \in A$. Se define el Asociador de x, y, z como $(x, y, z) = (xy)z - x(yz)$

$N(A) = \{g \in A \,/\, 0 = (g, x, y) = (x, g, y) = (y, x, g) \quad \forall x, y \in A\}$

$N(A)$ se llama núcleo de A

$C(A) = \{g \in N(A) \,/\, [g, x] = 0 \quad \forall x \in A\}$ = centro de A

Notas / Notes:

Fecha / Date:

Obs:

$c \in C(A) \Rightarrow R_c \overset{\text{conm}}{=} L_c$, $[R_c, R_y] = R_cR_y - R_yR_c \overset{\text{asoc}}{=} R_cR_y - R_{cy}$
$= R_yR_c - R_{yc} = 0 \quad \forall y \in A$

Teorema (Jacobson) El centro $C(A)$ de cualquier álgebra simple A sobre F es 0, o es un cuerpo. En este último caso, A contiene la unidad,

$C' = C(A)^* = alg\{R_c / c \in C(A)\}$, y A es álgebra sobre $C(A)$

Recordemos que $B^* = alg\{L_b, R_b / b \in B\}$

Dem:

Primero demostraremos que $T(c) \in C(A)$ $\forall c \in C(A)$ $\forall T \in C'$

(Queremos que $T(c)$ asocie y conmute)

$R_y T = TR_y = R_{T(y)}$ $\forall y \in A$ pues:

$R_y T(x) = T(x)y = T(R_y(x)) = TR_y(x) = T(xy) = TL_x(y) = L_x T(y) = xT(y)$

$= L_{T(y)}(x)$

$L_y T = TL_y = L_{T(y)}$

Si tomamos $y = c \in C(A)$ $R_{T(c)} = TR_c = TL_c = L_{T(c)}$

Además, $R_{T(c)} R_y = R_c TR_y = R_c R_{T(y)} = R_{cT(y)} = R_{T(c)y}$

$R_y R_{T(c)} = R_y R_c T = R_c R_y T = R_c TR_y = R_{T(c)} R_y$

$\therefore$ se verifican las condiciones de la obs, y $\therefore$ $T(c) \in C(A)$ $\forall T \in C'$ $\forall c \in C(A)$ 1.42

$C(A)^* \leq_{subalg} \mathcal{M}(A)$ porque (*) $\boxed{L_x R_c = R_c L_x \ \forall x \in C(A) \ x \in A}$ $R_{c_1} R_{c_2} = R_{c_1 c_2}$

$C(A)^* = alg\{R_c / c \in C(A)\}$ (pues $R_c = L_c$)

$f: C(A) \longrightarrow C(A)^*$ es monomorfismo

$c \mapsto R_c$

pd: $C(A) = C'$

Por (*) y como R_c conmuta $C(A)^* \subseteq C'$

C' es un cuerpo conmut $C' = C_{End(A)}(\mathcal{M}(A))$ $f \in C'$

$f: A \to A$ homom A es simple Por lema de Schur f es iso ($f \neq 0$)

Notas / Notes: *

Fecha / Date:

$C(A)^* \trianglelefteq C'$

$TR_c = R_{T(c)}$

$\Rightarrow C(A)^* = C'$

Como A es simple, $C(A)^* = 0$ v $C(A)^* = C'$

Si $C(A)^* = 0$, $R_c = 0$ $\forall c \in C(A)$

Si hubiera $c \neq 0$ tq $R_c = 0$ $(c \in C(A))$, entonces $B = F \cdot c \neq 0$

es un ideal de A pues $AB = BA = 0 \subseteq B$ pero $B = A$ $A^2 = 0 \Rightarrow \not\!E$

$\therefore C(A)^* = C'$.

$Id_A \in C(A)^*$ (vamos a probar $f^{-1} \in C'$)

$\exists$ $e \in C(A)$ tq $R_e = L_e = Id_A$ ☆

$C(A)^* = alg\{R_c / c \in C(A)\} = \{TR_c / c \in C(A)\}$ pues $R_{c_1} R_{c_2} \cdots = R_{c_1 c_2 \cdots}$

☆ $\Rightarrow ae = ea = a$ $\forall a \in A$

$\Rightarrow e = 1_A$

$\therefore$ $c \mapsto R_c$ es un isomorfismo

Vamos a demostrar $g = R_c^{-1} \in C'$.

$f \in C'$ $g = f^{-1}$ pd. $g \in C'$

$L_x(f^{-1}(y)) = x \underbrace{f^{-1}(y)}_{a}$

$xa = L_x(a)$

$f\, L_x(a) = L_x(f(a)) = xy$

$L_x(a) = f^{-1}(xy)$

$L_x f^{-1}(y) = f^{-1} L_x(y)$

(Profe^{π.})

distinto a los apuntes

Teorema Sea B ideal de A. B nilpotente $\iff$ B^* es nilpotente

Obs:

A álg $\quad A^1 = A \quad A^n = \sum_{k=1}^{n-1} A^{n-k} A^k \quad \forall n \geq 2$

A nilpotente $\iff A^r = 0 \; \forall r$

B subálgebra $\Rightarrow B^n$ subálg $\forall n$

Vamos a probar: (i) $(B^*)^{n+1} A \subseteq B^n \quad \forall n \in \mathbb{N} \qquad B^{*\,n+1} A \subseteq B^{*\,n} B$

(ii) $B^{n+1} \subseteq (B^*)^n B \quad \forall n \in \mathbb{N}$

Obs: como B^* es asoc, $B^{*\,n} = \underbrace{B^* B^* \cdots B^*}_{n\ veces}$

Veamos quien es $B^* B$. Afirmacion: $B^* B = B^2$.

$T \in B^*$, $b \in B$. Entonces $T = \sum \pi S_1 \ldots S_n \quad S_i \in \{L_x, R_x\} \; \forall x \in B$

$S_n(b) \in B^2 \qquad S_1 \ldots S_n \in B^2 = B^2 \Rightarrow T(b) \in B^2$

$x \in B^2 \Rightarrow x = \sum y_i b_i \quad y_i, b_i \in B \Rightarrow x \in \sum L_{y_i} b_i \quad y_i \in B \Rightarrow x \in B^* B$

23/10

- M un A-modulo finitam/ gen, A noeth $\Rightarrow M$ noeth

$f: A^n \to M \qquad A$ noeth $\Rightarrow A^n$ noeth $\Rightarrow A^n/\ker(f)$ noeth

$(a_1, \ldots, a_n) \mapsto \sum_{i=1} a_i e_i \qquad A^n/\ker(f) \cong M$

T submod de $M \Rightarrow 0 \to T \xrightarrow{i} M \xrightarrow{\pi} M/T \to 0$ exacta

$T, M/T$ noeth $\iff M$ noeth

- $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ exacta $\quad M, P$ noeth $\iff N$ noeth

Parte complicada: M, P noeth $\Rightarrow N$ noeth

Sea $N_1 \subset N_2 \subset \ldots$ cadena submodulos de N

$\therefore f^{-1}(N_1) \subset f^{-1}(N_2) \subset \ldots$ cadena de submodulos de M

M noeth $\Rightarrow f^{-1}(N_n) = f^{-1}(N_{n+1}) \; \forall n \geq k_1 \quad (1)$

$g(N_1) \subset g(N_2) \subset \cdots$ cadena de submódulos de P

P noeth $\Rightarrow g(N_n) = g(N_{k_2})\ \forall n \geq k_2$ (2)

f inyectiva $\Rightarrow N_n \cap f(M) = f(f^{-1}(N_n))\ \forall n \in \mathbb{N}$ (3)

g epiyectiva $\Rightarrow N_n + Ker(g) = g^{-1}(g(N_n))\ \forall n \in \mathbb{N}$ (4)

Sea $k = \max\{k_1, k_2\}$. pd: $N_n = N_k\ \forall n \geq k$

Sabemos que $\forall n \geq k$ $N_k \subset N_n$ (*) pd: $N_n \subset N_k\ \forall n \geq k$.

De (3) y M noeth $\Rightarrow N_n \cap f(M) = f(f^{-1}(N_n)) = f(f^{-1}(N_k))$

$\therefore N_n \cap f(M) = N_k \cap f(M)$ (5)

De (4) y P noeth $\Rightarrow N_n + Ker(g) = N_k + Ker(g)$ (6)

Además, la sucesión es exacta por lo que $f(M) = Ker(g)$

Entonces $N_n + f(M) \overset{(6)}{=} N_k + Ker(g)$ (7)

Sea $x \in N_n$. Luego $x \in N_k + f(M)$, y $x = z + f(m)$ $\exists z \in N_k$, $m \in M$

$x - z \in f(M) = Ker(g)$ pd: $x - z \in N_k$

Por (*) $N_k \subset N_n \Rightarrow x - z \in N_n$. $\therefore x - z \in N_n \cap f(M) \overset{(5)}{=} N_k \cap f(M)$

$\therefore x - z \in N_k \Rightarrow x \in N_k$ (pues $z \in N_k$)

$\therefore N_n \subset N_k$.

Notas / Notes: