Universidad de Valladolid

FACULTAD DE CIENCIAS
DEPARTAMENTO DE ÁLGEBRA, ANÁLISIS MATEMÁTICO,
GEOMETRÍA Y TOPOLOGÍA

TESIS DOCTORAL:

ÁLGEBRAS FINITAS SOBRE UN CUERPO. LA RECTA PROYECTIVA.

Tesis presentada por CLAUDIA INÉS GRANADOS PINZÓN
para optar al grado de
Doctora por la Universidad de Valladolid

Dirigida por:
José Manuel Aroca Hernández-Ros

Noviembre de 2014

Introducción

S. Lie propone una geometría de la circunferencia donde elimina la diferencia entre puntos, rectas y circunferencias del plano euclídeo. Un punto es para Lie una circunferencia de radio cero y una recta es una circunferencia de radio infinito, además considera las rectas y las circunferencias dotadas de una orientación.

La razón de la orientación es que permite establecer una dualidad punto-línea. Si tomamos tres puntos no alineados, por éstos pasa una única circunferencia no orientada pero para la figura dual, los tres lados de un triángulo, hay cuatro circunferencias tangentes, se puede corregir esta situación con la orientación, asignando al contacto una condición de compatibilidad que hace que solo una de las cuatro circunferencias sea tangente orientada a las tres rectas añadiendo un punto del infinito común a todas las rectas del plano.

El plano de Lie se sumerge en una cuádrica de $\mathbb{P}^4_{\mathbb{R}}$ asociando a cada "punto" las coordenadas pentacíclicas, las coordenadas pentacíclicas de la circunferencia Γ de centro (a, b) y radio r (con signo) son

$$[\frac{1+p}{2}, \frac{1-p}{2}, a, b, -r]$$

donde p es la potencia del punto origen respecto de Γ, las de un punto (a, b) son sus coordenadas como circunferencia de radio cero $[\frac{1+d^2}{2}, \frac{1-d^2}{2}, a, b, 0]$ con d distancia del punto al origen y las de la recta de ecuación $ax + by + c = 0$ es $[-c, c, a, b, 1]$. La orientación es la del vector $(-b, a)$ que determina el signo de la ecuación.

Observe que la recta se obtiene como límite de la circunferencia de centro $(\lambda a, \lambda b)$ y radio $\lambda - c$ (supuesto (a, b) unitario) y que el límite de las coordenadas de las circunferencias dan las coordenadas de la recta.

Es inmediato que a la imagen de la aplicación que asocia a cada elemento sus coordenadas pentacíclicas es la cuádrica de ecuación $-x_0^2 + x_1^2 + x_2^2 + x_3^2 - x_4^2 = 0$ y que la

condición de contacto es la polaridad respecto de esta cuádrica.

Como alternativa a la geometría de Lie, Moebius propone una geometría en la que aparece por una parte puntos, los de $\mathbb{R}^2$, y por otra ciclos, es decir rectas y circunferencias no orientadas. Ahora, vía la proyección estereográfica, los puntos se representan como puntos de la esfera S^2, o de la cuádrica de $\mathbb{P}^3_{\mathbb{R}}$, $-x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ y los ciclos corresponden a las secciones planas de la cuádrica, las rectas corresponden a las secciones por planos que pasan por el centro de la proyección.

La geometría de Laguerre considera las "lanzas" (rectas orientadas) y las circunferencias orientadas como Lie (incluyendo los puntos) una cadena de base un punto es el conjunto de lanzas por el punto y una cadena de base una circunferencia las tangentes orientadas a ella. De esta forma los puntos son las "lanzas" y los ciclos, o bien la cadena de lanzas por un punto, o bien la familia de cadena de lanzas tangentes a una circunferencia. Ésta geometría admite una representación sobre un cilindro por proyección estereográfica.

Las dos geometrías planas, Moebius y Laguerre, derivadas de las de Lie admiten un planteamiento común mediante el uso de la recta proyectiva.

La recta proyectiva compleja se puede interpretar como la compatificación por un punto de $\mathbb{R}^2$ y los ciclos se reproducen en ella por medio de la razón doble, dados tres puntos A, B, C de $\mathbb{P}^1_{\mathbb{C}}$, el ciclo que los tiene por base es el conjunto

$$[ABC] = \{X \in \mathbb{P}^1_{\mathbb{C}} : [A, B; C, X] \in \mathbb{R}\}.$$

Es inmediato que si $A, B, C \in \mathbb{R}^2 \equiv \mathbb{C} \subset \mathbb{P}^1_{\mathbb{C}}$ están alineados en $\mathbb{R}^2$ entonces $[ABC]$ es la recta que pasa por ellos, y si no están alineados y son distintos dos a dos entonces $[ABC]$ es la circunferencia que definen. Entonces la geometría de Moebius es la de $\mathbb{P}^1_{\mathbb{C}}$ con los ciclos y se representan en la esfera. Pues la proyección estereográfica identifica $\mathbb{P}^1_{\mathbb{C}}$ con S^2 y los ciclos con las secciones planas de S^2.

Para la geometría de Laguerre no sirve la recta proyectiva sobre un cuerpo, luego construimos el anillo de los números duales $\mathbb{D} = \frac{\mathbb{R}[x]}{(x^2)}$ y la recta proyectiva sobre $\mathbb{D}$, $\mathbb{P}^1_{\mathbb{D}}$, que consiste en el cociente $\mathcal{L}^2_{\mathbb{D}}/\sim$ donde $\mathcal{L}^2_{\mathbb{D}}$ es el conjunto de pares "complementables" de elementos de $\mathbb{D}$, es decir pares $(\alpha, \beta) \in \mathbb{D}^2$ tales que existen $a, b \in \mathbb{D}$ con $a\alpha + b\beta$ inversible, y $\sim$ es la relación $(a, b) \sim (c, d)$ si y sólo si existe $\lambda \in \mathbb{D}^*$ tal que $(a, b) = \lambda(c, d)$ entonces $\mathbb{P}^1_{\mathbb{D}} \supset \mathbb{D} \simeq \mathbb{R}^2$ identificando $\alpha \in \mathbb{D}$ con $[1\ \alpha] \in \mathbb{P}^1_{\mathbb{D}}$ y los ciclos

$$[ABC] = \{D \in \mathbb{P}^1_{\mathbb{D}} : [A, B; C, D] \in \mathbb{R}\}$$

corresponden a parábolas con eje paralelo a una línea fija y $\mathbb{P}^1_{\mathbb{D}}$ se proyecta estereográficamente en el cilindro y los ciclos en las secciones planas de éste.

Si buscamos un modelo común a ambas geometrías podemos tomar el plano afín real $\mathbb{A} = (X, \mathbb{R}^2, +)$, y considerar en $\mathbb{P}^1_{\mathbb{R}} = \mathbb{A}_\infty$ cada una de las cónicas no nulas reales, los tres tipos son los de matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. La primera cónica corresponde a los puntos cíclicos del plano $[0\ 1\ i]$, $[0\ 1\ -i]$ en la inmersión $\mathbb{A} \subset \mathbb{P}^2_{\mathbb{R}}$ y la tercera al punto $[0\ 0\ 1]$. Las cónicas de $\mathbb{A}$ que intersecan en el infinito, las cónicas dadas por la métrica son exactamente los ciclos de Moebius en el primer caso y de Laguerre en el tercero.

Para el segundo la cónica de la métrica consta de un par de puntos reales y la cónica que interseca al infinito en ella son las rectas (recta + recta del infinito) y las hipérbolas con asíntotas en la dirección de dichos puntos. La geometría correspondiente se conoce habitualmente como geometría de Minkowski y corresponde a la tercera álgebra de dimensión dos sobre $\mathbb{R}$, los de los números paracomplejos $\mathbb{M} = \frac{\mathbb{R}[x]}{(x^2-1)}$.

Así las geometrías clásicas del plano corresponden a las tres extensiones bidimensionales de $\mathbb{R}$, $\mathbb{R}[x]/(x^2-1)$, $\mathbb{R}[x]/(x^2+1)$ y $\mathbb{R}[x]/(x^2)$.

Hay trabajos recientes sobre la geometría correspondiente a algunas algebras tridimensionales, y una teoría general muy incompleta. En esta memoria hemos hecho un estudio sistemático de las $K-$álgebras finitas, es decir que son espacios vectoriales de dimensión finita sobre K. Todas ellas son suma directa de $K-$álgebras locales finitas y por tanto identificando éstas las conocemos todas. Así hemos clasificado las $\mathbb{R}-$álgebras locales finitas de dimensión real menor que seis ya que probamos que hay infinitas de dimensión seis. Poonen en [24] clasifica las $\mathbb{C}-$álgebras locales finitas hasta dimensión siete, y encuentra que es en ésta dimensión donde hay infinitos modelos, nuestro ejemplo vale también en dimensión seis compleja, por lo cual, en nuestra opinión, el trabajo de Poonen contiene un error en este caso.

Una vez estudiado los tipos de $K-$álgebras finitas, estudiamos la geometría de las rectas proyectivas sobre anillos, con un interés especial en la razón doble y las cuaternas armónicas probando un teorema de Staudt para rectas proyectivas sobre anillos totales de cocientes, estructura ésta más general que la de $K-$álgebras finitas.

Resulta misterioso como la aplicación

$$\begin{array}{rccl} \varphi: & \mathbb{P}^1_A & \to & \mathbb{P}^3_{\mathbb{R}} \\ & [\boldsymbol{a}, \boldsymbol{b}] & \mapsto & [\boldsymbol{a}\overline{\boldsymbol{a}} + \boldsymbol{b}\overline{\boldsymbol{b}}, \overline{\boldsymbol{a}}\boldsymbol{b} + \overline{\boldsymbol{b}}\boldsymbol{a}, \delta(\overline{\boldsymbol{a}}\boldsymbol{b} - \overline{\boldsymbol{b}}\boldsymbol{a}), \boldsymbol{a}\overline{\boldsymbol{a}} - \overline{\boldsymbol{b}}\boldsymbol{b}] \end{array}$$

donde A es una $\mathbb{R}-$álgebra de dimensión dos, $\overline{\boldsymbol{a}}$ es el conjugado de $\boldsymbol{a} \in A$ y δ es i, j o ϵ según se trate de los complejos, paracomplejos o duales, verifique que
(i) $\varphi(\mathbb{P}^1_A)$ es la cuádrica $-x_0^2+x_1^2+x_2^2+x_3^2 = 0$ en el caso complejo, $-x_0^2+x_1^2-x_2^2+x_3^2 = 0$ en el paracomplejo y $-x_0^2 + x_1^2 + x_3^2 = 0$ para el álgebra de los números duales, es decir

la cuádrica que se obtiene sumando a la métrica un plano hiperbólico.
(ii) φ lleva ciclos a secciones planas de la cuádrica.
Esperamos que si A es una $\mathbb{R}-$álgebra $n-$dimensional se pueda encontrar una aplicación similar $\varphi : \mathbb{P}^1_A \to \mathbb{P}^{2n-1}_{\mathbb{R}}$ que identifique $\mathbb{P}^1_A$ en este espacio. Tenemos la certeza de que no será posible para todas las álgebras ya que el número de todas las álgebras de dimensión n es muy superior al de cuádricas en $\mathbb{P}^{2n-1}_{\mathbb{R}}$, y nos planteamos para un trabajo futuro caracterizar las álgebras con ésta propiedad.

Índice general

Capítulo 1

Generalidades

En este primer capítulo consideramos y comparamos tres tipos de anillos sobre los cuales el álgebra lineal funciona de modo razonable. Estos son los anillos totales de cocientes, los $\beta-$anillos y los anillos de Hermite. En esta memoria, un anillo R siempre hará referencia a un anillo conmutativo con unidad. Denotaremos por R^* los elementos inversibles de R.

1.1. Anillos totales de cocientes.

Definición 1.1.1 *Un anillo R es un* anillo total de cocientes *si sus elementos son inversibles o divisores de cero.*

Ejemplo 1.1.2 *(1) Un cuerpo es un anillo total de cocientes y un dominio que no es un cuerpo no es anillo total de cocientes.*

(2) Si R es un dominio euclídeo y $f \in R$, $f \neq 0$, entonces $R/(f)$ es un anillo total de cocientes.
En efecto, Sea $g + (f) \in R/(f)$ y supongamos que $d = \text{mcd}(f, g)$. Por el teorema de Bézout, existen $\lambda, \mu \in R$ tales que $\lambda f + \mu g = d$. Por tanto,

$$(g + (f))(\mu + (f)) = g\mu + (f) = g\mu + \lambda f + (f) = d + (f).$$

Consideremos los casos siguientes:
(i) si d es inversible en R, entonces $d + (f)$ es inversible en $R/(f)$ y por tanto $g + (f)$ también lo es.
(ii) si d no es inversible, como $d|f$ y $d|g$, existen $c_1, c_2 \in R$ tales que $f = c_1 d$, $g = c_2 d$. Luego $c_1 + (f) \neq 0$ ya que f no divide a c_1 pues d no es inversible. Ahora,

como $(g+(f))(c_1+(f)) = gc_1+(f) = c_2dc_1+(f) = 0+(f)$, *entonces* $g+(f)$ *es divisor de cero.*

Como ejemplos particulares de este caso se tienen los siguientes anillos totales de cocientes.

(a) Sean $\mathbb{Z}$ *el anillo de números enteros y* $n \in \mathbb{Z}$. *Entonces el anillo* $\mathbb{Z}/(n)$ *es un anillo total de cocientes.*

(b) Sea $K[x]$ *el anillo de polinomios en la variable* x, *con coeficientes en el cuerpo* K. *Entonces los anillos* $K[x]/(f(x))$ *con* $f(x) \neq 0$ *son anillos totales de cocientes, en particular, el cuerpo complejo*

$$\mathbb{C} = \frac{\mathbb{R}[x]}{(x^2+1)} = \{a+bi : a,b \in \mathbb{R},\ i^2 = -1\},$$

el anillo de los paracomplejos

$$\mathbb{P} = \frac{\mathbb{R}[x]}{(x^2-1)} = \{a+bj : a,b \in \mathbb{R},\ j^2 = 1\}$$

y el anillo de los números duales

$$\mathbb{D} = \frac{\mathbb{R}[x]}{(x^2)} = \{a+b\varepsilon : a,b \in \mathbb{R},\ \varepsilon^2 = 0\}$$

son anillos totales de cocientes.

(3) En general el anillo de polinomios $R[x]$ *no es un anillo total de cocientes, pues* x *no es ni inversible ni divisor de cero en* $R[x]$.

Lema 1.1.3 *Sea* $S \subset R$ *un subconjunto multiplicativamente cerrado. Consideremos el homomorfismo canónico*

$$\begin{array}{rccc} \varphi: & R & \to & S^{-1}R \\ & a & \mapsto & \frac{a}{1} \end{array}.$$

Entonces

(1) $\frac{a}{s} \in S^{-1}R$ *es inversible si y sólo si existen* $b \in R$ *y* $u \in S$ *con* $abu \in S$.

(2) $\frac{a}{s} \in S^{-1}R$ *es divisor de cero si y sólo si existe* $b \in R$ *tal que*

(i) $bt \neq 0$ *para todo* $t \in S$.

(ii) existe $u \in S$ *con* $abu = 0$.

(3) $a \in \mathrm{Ker}(\varphi)$ *si y sólo si existe* $s \in S$ *con* $as = 0$.

Demostración. *(1)* $\frac{a}{s} \in S^{-1}R$ es inversible si y sólo si existe $\frac{b}{t} \in S^{-1}R$ tal que $\frac{a}{s}\frac{b}{t} = 1$ y esto equivale a que existe $u \in S$ tal que $(ab - st)u = 0$ luego $abu = stu \in S$. Recíprocamente, si $v = abu \in S$ entonces $\frac{a}{s}\frac{bus}{v} = \frac{vs}{sv} = 1$.
(2) $\frac{a}{s} \in S^{-1}R$ es divisor de cero si y sólo si existe $\frac{b}{t} \neq 0$ tal que $\frac{a}{s}\frac{b}{t} = 0$ y esto equivale a que existe $u \in S$ tal que $abu = 0$ y $bs \neq 0$ para todo $s \in S$.
(3) Inmediato. ■

Observación 1.1.4 *Si a es inversible en R lo es en $S^{-1}R$ porque $aa^{-1}(1) = 1 \in S$. Pero si a es divisor de cero en R no necesariamente lo es en $S^{-1}R$ e incluso puede ser inversible en este anillo. Por ejemplo, en $R = \mathbb{Z}/(6)$, $2 + (6)$ es divisor de cero pero si $S = \{\overline{1}, \overline{2}, \overline{4}\}$, S es multiplicativamente cerrado y $\overline{2} \in S$ luego $\overline{2}$ es inversible en $S^{-1}R$. Recíprocamente, a puede ser inversible en $S^{-1}R$ sin serlo en R y si a es divisor de cero en $S^{-1}R$ entonces a es divisor de cero en R.*

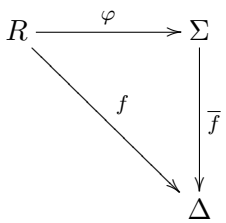
Proposición 1.1.5 *Sean R un anillo y $S \subset R$ el subconjunto multiplicativo de los no divisores de cero de R. Consideremos el anillo $\Sigma = S^{-1}R = \{\frac{a}{b} : a \in R,\ b \in S\}$ entonces*

(1) Σ es un anillo total de cocientes.

(2) Existe un homomorfismo

$$\begin{array}{rccc} \varphi: & R & \to & \Sigma \\ & a & \mapsto & \frac{a}{1} \end{array}$$

tal que para todo anillo total de cocientes Δ y todo homomorfismo $f : R \to \Delta$ existe un único homomorfismo $\overline{f} : \Sigma \to \Delta$ con el cual el diagrama



es conmutativo.

Demostración. *(1)* Sea $z = \frac{a}{b} \in \Sigma$. Si $a \in S$ entonces $a(1)(1) \in S$ luego, por el Lema 1.1.3, z es inversible. Si $a \notin S$ entonces a es divisor de cero, luego existe $0 \neq c \in R$ tal que $ac = 0$. Así, $ac1 = 0$ y $cs \neq 0$ para todo $s \in S$ pues los elementos de S no son divisores de cero luego, por el Lema 1.1.3, z es divisor de cero.
(2) Es consecuencia de la propiedad universal de los anillos de cocientes ya que todo homomorfismo unitario de anillos transforma elementos inversibles en inversibles. ■

El homomorfismo φ, de la Proposición 1.1.5, es inyectivo.
En efecto, si $\varphi(a) = \frac{a}{1} = 0$, existe $b \in S$ tal que $ab = 0$ pero como S está formado por

los elementos no divisores de cero entonces $a = 0$.

El anillo $\Sigma = S^{-1}R = \{\frac{a}{b} : a \in R,\ b \in S\}$, dado en la Proposición 1.1.5, se llama *el anillo total de cocientes* de R.

Proposición 1.1.6 *Un anillo Σ es un anillo total de cocientes si y sólo si existe R, no necesariamente único, tal que Σ es el anillo total de cocientes de R.*

Demostración. Si Σ es un anillo total de cocientes entonces Σ es el anillo total de cocientes de Σ. Recíprocamente, si Σ es el anillo total de cocientes de un anillo R, por la Proposición 1.1.5, Σ es un anillo total de cocientes. El anillo R no es único pues si Σ es el anillo total de cocientes de un anillo $R \neq \Sigma$, se tiene que Σ también es el anillo total de cocientes de Σ. ■

Teorema 1.1.7 *(Arapovic) Si R es un anillo las siguientes son equivalentes*

(1) R es $0-$dimensional.

(2) R es un anillo total de cocientes y para todo $a \in R$ existe $b \in R$ con $a+b$ inversible y ab nilpotente.

(3) R es un anillo total de cocientes y para todo $a \in R$ existe un entero positivo n tal que $a^n = re$ con r inversible de R y e nilpotente de R.

Demostración. *(1) $\Rightarrow$ (2)* : Si $a \in R$ es no inversible entonces existe $\mathfrak{m} \in \mathrm{Max}(R)$ tal que $a \in \mathfrak{m}$. Como R es $0-$dimensional $\mathfrak{m}$ no contiene a ningún ideal primo y en consecuencia $R_{\mathfrak{m}}$ es también $0-$dimensional con ideal maximal $\mathfrak{m}$, luego el nilradical de $R_{\mathfrak{m}}$ es $\mathfrak{m}$ y todos los elementos de $\mathfrak{m}$ son nilpotentes. Entonces existe un entero positivo n tal que $a^n = 0$ en $R_{\mathfrak{m}}$. Tomamos n mínimo, es decir $a^{n-1} \neq 0$ y $a^n = 0$ en $R_{\mathfrak{m}}$ luego existe $s \notin \mathfrak{m}$ tal que $a^n s = 0$ y $a^{n-1}s \neq 0$ por tanto $a(a^{n-1}s) = 0$ y $a^{n-1}s \neq 0$ luego a es divisor de cero de R. En consecuencia R es anillo total de cocientes.
Sean N el nilradical de R y $0 \neq a \in R$, tenemos dos opciones:
(i) Si $a \in N$, existe n mínimo tal que $a^n = 0$ y por tanto existe $1 - a \in R$ tal que $a + (1 - a)$ es inversible y $(a(1 - a))^n = 0$.
(ii) Si $a \notin N$, tomamos $A = R/N$, el nilradical de A es cero luego no tiene elementos nilpotentes y A es 0-dimensional pues R lo es, y si $\mathrm{Max}(A) = \{\mathfrak{m}_t\}_{t\in T}$ entonces

$$\begin{array}{rccc} \varphi: & A & \to & B = \prod_{t\in T} R/\mathfrak{m}_t \\ & a & \mapsto & (a + \mathfrak{m}_t)_{t\in T} \end{array}$$

es inyectiva. Llamamos $\overline{A} = \varphi(A) \subset B$, luego $\overline{A} \simeq A$. Consideramos $\boldsymbol{e} \in B$ dado por $e_t = \begin{cases} 0 & \text{si } a \in \mathfrak{m}_t \\ 1 & \text{si } a \notin \mathfrak{m}_t \end{cases}$. Note que

1. $\boldsymbol{e}^2 = \boldsymbol{e}$.

2. $\boldsymbol{e} \cdot \varphi(a) = \varphi(a)$.

3. Sea $S = \overline{A}[\boldsymbol{e}]$, como $\boldsymbol{e}$ es raíz de $x^2 - x = 0$, S es entero sobre $\overline{A}$ y S es $0-$dimensional. Luego S es anillo total de cocientes.

Tomamos $\boldsymbol{b} = (b_t)_{t\in T} = \mathbf{1} - \boldsymbol{e} + \varphi(a)$, note que $b_t = \begin{cases} 1 & \text{si } \ a \in \mathfrak{m}_t \\ a + \mathfrak{m}_t \neq 0 & \text{si } \ a \notin \mathfrak{m}_t \end{cases}$. Luego $\boldsymbol{b}$ es inversible en S.

Como $\frac{\mathbf{1}}{\boldsymbol{b}} \in S$, $\frac{\mathbf{1}}{\boldsymbol{b}} = \gamma_1\mathbf{1} + \gamma_2\boldsymbol{e}$ con $\gamma_1, \gamma_2 \in \overline{A}$ y por otra parte $\boldsymbol{b}\cdot\boldsymbol{e} = \boldsymbol{e} - \boldsymbol{e}^2 + \boldsymbol{e}\cdot\varphi(a) = \varphi(a)$ es decir $\boldsymbol{e} = \frac{\varphi(a)}{\mathbf{1}-\boldsymbol{e}+\varphi(a)} = (\gamma_1\mathbf{1} + \gamma_2\boldsymbol{e}) \cdot \varphi(a) = \gamma_1\varphi(a) + \gamma_2\boldsymbol{e} \cdot \varphi(a) = (\gamma_1 + \gamma_2)\varphi(a) = \varphi((c_1 + c_2)a) \in \overline{A}$ donde $\gamma_1 = \varphi(c_1)$ y $\gamma_2 = \varphi(c_2)$ para $c_1, c_2 \in A$.

Sea $h = (c_1 + c_2)a$ entonces $\varphi(ha) = \varphi(h) \cdot \varphi(a) = \boldsymbol{e} \cdot \varphi(a) = \varphi(a)$ y $ha = a$ pues φ es inyectiva.

Por tanto $(1 - h)a = a - ha = 0$ y $1 - h + a$ es inversible pues φ es isomorfismo y $\varphi(1 - h + a) = \mathbf{1} - \boldsymbol{e} + \varphi(a)$ es inversible.

Retomando que $0 \neq a \notin N$, $a + N \in A$ y existe $l \in R$ tal que $l + N = h$, como $(1 - (l + N))(a + N) = 0$ entonces $(1 - l)a \in N$ y por tanto es nilpotente, y puesto que $1 - (l + N) + (a + N)$ es inversible, $1 - l + a + N$ es inversible y por tanto $1 - l + a$ es inversible.

(2) ⇒ (3) : Sea $a \in R$, como existe $b \in R$ y existe un entero positivo n tales que $a + b$ es inversible y $(ab)^n = 0$ entonces $a^n + b^n$ es inversible de R pues en caso contrario para algún $\mathfrak{p} \in \operatorname{Spec}(R)$, $a^n + b^n \in \mathfrak{p}$ y como $a^n b^n = 0$ entonces $a^n \in \mathfrak{p}$ y $b^n \in \mathfrak{p}$ pero $\mathfrak{p}$ es primo luego $a \in \mathfrak{p}$ y $b \in \mathfrak{p}$. Así, $a + b \in \mathfrak{p}$ lo cual es absurdo.

Además, $\frac{a^n}{a^n+b^n}$ es un elemento idempotente de R ya que $a^n(a^{2n} + b^{2n}) = a^{2n}(a^n + b^n) = a^{3n}$ y $(\frac{a^n}{a^n+b^n})^2 = \frac{a^{2n}}{a^{2n}+b^{2n}} = \frac{a^n}{a^n+b^n}$. Entonces $a^n = (a^n + b^n)(\frac{a^n}{a^n+b^n})$ es la descomposición buscada.

(3) ⇒ (1) : Sean $\mathfrak{p}_1$ y $\mathfrak{p}_2$ ideales primos de R con $\mathfrak{p}_1 \subset \mathfrak{p}_2$ y tomemos $a \in \mathfrak{p}_2$. Como existe un entero positivo n tal que $a^n = re$ con r inversible y e idempotente, entonces $r \notin \mathfrak{p}_2$ y como $\mathfrak{p}_2$ es primo, $e \in \mathfrak{p}_2$. Luego, $1 - e \notin \mathfrak{p}_2$ y como $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $1 - e \notin \mathfrak{p}_1$. Pero $e(1 - e) = 0 \in \mathfrak{p}_1$ entonces $e \in \mathfrak{p}_1$ por tanto $a \in \mathfrak{p}_1$ y $\mathfrak{p}_1 = \mathfrak{p}_2$. ■

Ejemplo 1.1.8 *Sean K un cuerpo y $R = K[x, y]_{(x,y)}/(xy, y^2)$.*

(1) $K[x, y]_{(x,y)}$ es un anillo local con ideal maximal $\mathfrak{m} = (x, y)$ donde identificamos $\frac{x}{1} = x$ y $\frac{y}{1} = y$. Note que R es un anillo local con ideal maximal $\mathfrak{m} = (\overline{x}, \overline{y})$, donde $\overline{x} = x + (xy, y^2)$ y $\overline{y} = y + (xy, y^2)$.

(2) R es un anillo total de cocientes ya que los elementos que no están en el maximal $\mathfrak{m}$ son inversibles por ser R anillo local y los elementos de $\mathfrak{m}$ son divisores de cero pues existe $0 \neq \overline{y} \in \mathfrak{m}$ tal que $(\alpha\overline{x} + \beta\overline{y})\overline{y} = 0$ para todos $\alpha, \beta \in R$.

(3) Los elementos de R admiten una escritura única como $\frac{a+\overline{x}A(\overline{x})+c\overline{y}}{b+\overline{x}B(\overline{x})+d\overline{y}}$ con $a, b, c, d \in$

K, $b \neq 0$ y $A, B \in K[\overline{x}]$. Además los elementos de $R/(\overline{y})$ admiten una escritura única como $\frac{a+\overline{x}A(\overline{x})}{b+\overline{x}B(\overline{x})}$ con $a, b \in K$, $b \neq 0$ y $A, B \in K[\overline{x}]$. Note que $R/(\overline{y}) \simeq K[\overline{x}]_{(\overline{x})}$ y como $K[\overline{x}]_{(\overline{x})}$ es un dominio, el ideal $(\overline{y})$ es primo. Por otra parte, $(\overline{y}) \subset \mathfrak{m}$ entonces R no es $0-$dimensional.

Observación 1.1.9 *(1) Si R es un anillo total de cocientes y S es un subanillo de R, S no es necesariamente un anillo total de cocientes. Por ejemplo, si R es un dominio que no es un cuerpo y K es su cuerpo de fracciones entonces $R \subset K$, K es un anillo total de cocientes y R no lo es.*

(2) Si R es un anillo total de cocientes y $R \simeq A \times B$ con A y B subanillos de R entonces A es necesariamente un anillo total de cocientes.
En efecto, si $a \in A$ entonces $(a, 1) \in R$ y tenemos dos casos:

(i) Si $(a, 1)$ es inversible entonces existe (b, c) tal que $(a, 1)(b, c) = (ab, c) = (1, 1)$ luego $ab = 1$ y a es inversible.

(ii) Si a es divisor de cero, existe $(b, c) \neq (0, 0)$ tal que $(a, 1)(b, c) = (ab, c) = (0, 0)$ luego $ab = 0$ y $c = 0$. Así, $b \neq 0$ y en consecuencia a es divisor de cero.

(3) Si R es un anillo total de cocientes y $\mathfrak{a}$ es un ideal de R, entonces $R/\mathfrak{a}$ no es en general un anillo total de cocientes, por ejemplo, sea R el anillo total de cocientes del Ejemplo 1.1.8. Como $(\overline{y})$ es un ideal primo no maximal de R entonces $R/(\overline{y})$ es un dominio y no es cuerpo. En consecuencia, $R/(\overline{y})$ no es anillo total de cocientes.

1.2. Producto de anillos.

Sean I un conjunto arbitrario y $\{R_i\}_{i \in I}$ una familia de anillos. Consideremos el anillo producto $R = \prod_{i \in I} R_i$ con las operaciones suma y producto componente a componente. Sea $\pi_i : R \to R_i$ la proyección i-ésima, es decir para $\boldsymbol{f} = (f(i))_{i \in I} \in R$, $\pi_i(\boldsymbol{f}) = f(i)$.

Proposición 1.2.1 *Sean $R = \prod_{i \in I} R_i$ y $\boldsymbol{f} = (f(i))_{i \in I} \in R$. Entonces*

(1) $\boldsymbol{f}$ es inversible si y sólo si, para todo $i \in I$, $\pi_i(\boldsymbol{f}) = f(i)$ es inversible.

(2) $\boldsymbol{f}$ es un divisor de cero si y sólo si existe $i \in I$ tal que $\pi_i(\boldsymbol{f}) = f(i)$ es divisor de cero.

(3) $\boldsymbol{f}$ es idempotente si y sólo si, para todo $i \in I$, $\pi_i(\boldsymbol{f}) = f(i)$ es idempotente.

Demostración. *(1)* Si para todo $i \in I$ se tiene que $f(i)$ es inversible, entonces para cada $i \in I$ sea $f^*(i) = \frac{1}{f(i)}$. Definimos $\boldsymbol{f}^* = (f^*(i))_{i \in I} \in R$. En consecuencia, $\boldsymbol{f}^* = \boldsymbol{f}^{-1}$.

El recíproco es inmediato.
(2) Si existe $i \in I$ tal que $f(i)$ es divisor de cero entonces existe $0 \neq a_i \in R_i$ tal que $f(i)a_i = 0$. Definimos $\boldsymbol{g} = (g(i))_{i\in I} \in R$ como $g(i) = a_i$ y $g(j) = 0$ para todo $j \neq i$. Luego, $\boldsymbol{g} \neq \boldsymbol{0}$ y $\boldsymbol{f} \cdot \boldsymbol{g} = \boldsymbol{0}$. El recíproco es inmediato.
(3) $\boldsymbol{f}^2 = \boldsymbol{f}$ si y sólo si $f(i)^2 = f(i)$ para todo $i \in I$, es decir $f(i) \in R_i$ es idempotente para todo $i \in I$. ■

Corolario 1.2.2 *Si para todo $i \in I$ se tiene que R_i es un anillo total de cocientes, entonces $R = \prod_{i\in I} R_i$ es también un anillo total de cocientes.*

Demostración. Por hipótesis, para todo $i \in I$, R_i es un anillo total de cocientes y como los items *(1)* y *(2)* de la Proposición 1.2.1 son mutuamente excluyentes, entonces para cada $\boldsymbol{f} \in R$ se tiene que $\boldsymbol{f}$ es divisor de cero o inversible. ■

Corolario 1.2.3 *Sean $R = \prod_{i\in I} R_i$ y $\boldsymbol{f} = (f(i))_{i\in I} \in R$. Si para todo $i \in I$ se tiene que R_i es un cuerpo, entonces*

(1) $\boldsymbol{f}$ es inversible si y sólo si $f(i) \neq 0$ para todo $i \in I$.

(2) $\boldsymbol{f}$ es un divisor de cero si y sólo si existe $i \in I$ tal que $f(i) = 0$.

(3) $\boldsymbol{f}$ es idempotente si y sólo si $f(i) = 0$ o $f(i) = 1$ para todo $i \in I$.

Demostración. Como R_i es un cuerpo, para todo $i \in I$, los inversibles de R_i son los $f(i) \neq 0$, los idempotente son $\{0, 1_{R_i}\}$ y el único divisor de cero es 0. Así, las tres afirmaciones se deducen respectivamente de los items *(1)-(3)* de la Proposición 1.2.1. ■

Para cada $j \in I$ definimos $\boldsymbol{e}_j \in R = \prod_{i\in I} R_i$ como

$$\pi_i(\boldsymbol{e}_j) = \delta_{ij} 1_{R_i} = \begin{cases} 1_{R_i} & \text{si } j = i \\ 0 & \text{si } j \neq i \end{cases}$$

donde δ_{ij} es la función delta de Kronecker. Como consecuencia directa de la definición de $\boldsymbol{e}_j$ se tienen las siguientes propiedades elementales de los elementos $\boldsymbol{e}_j \in R = \prod_{i\in I} R_i$.

Propiedades:

(1) $\boldsymbol{e}_i^2 = \boldsymbol{e}_i$.

(2) $\boldsymbol{e}_i \cdot \boldsymbol{e}_j = \boldsymbol{0}$ para todo $j \neq i$.

(3) $\boldsymbol{f} \cdot \boldsymbol{e}_i = f(i)\boldsymbol{e}_i$ para todo $\boldsymbol{f} \in R$.

(4) $(\boldsymbol{f} - f(i)\boldsymbol{e}_i) \cdot \boldsymbol{e}_i = \mathbf{0}$ para todo $\boldsymbol{f} \in R$.

Lema 1.2.4 *Sea R un anillo. R es producto de una familia finita de anillos si y sólo si existen $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in R$ idempotentes tales que*

(i) $\boldsymbol{u}_i \cdot \boldsymbol{u}_j = \delta_{ij}\boldsymbol{u}_i$.

(ii) $\sum_{i=1}^n \boldsymbol{u}_i = \boldsymbol{1}_R$.

Demostración. $\Rightarrow$: Como $R = \prod_{i=1}^n R_i$, tomemos los $\mathbf{e}_j \in R$, $j = 1, \ldots, n$, dados por $\pi_i(\mathbf{e}_j) = \delta_{ij} 1_{R_i}$. Note que $\{\mathbf{e}_j\}_{1 \leq j \leq n}$ satisface los items (i) y (ii).
$\Leftarrow$: Por hipótesis, existen $\boldsymbol{u}_i \in R$, $1 \leq i \leq n$, que satisfacen (i) y (ii). Definimos $R_i = \boldsymbol{u}_i R = \{\boldsymbol{a} \cdot \boldsymbol{u}_i : \boldsymbol{a} \in R\} = \{\boldsymbol{a} \in R : \boldsymbol{a} \cdot \boldsymbol{u}_i = \boldsymbol{a}\}$.
Observe que, para todo i, R_i es un anillo y veamos que $R \simeq \prod_{i=1}^n R_i$.
En efecto, consideremos $\varphi : R \to \prod_{i=1}^n R_i$ definida por $\varphi(\boldsymbol{a}) = (\boldsymbol{a} \cdot \boldsymbol{u}_1, \ldots, \boldsymbol{a} \cdot \boldsymbol{u}_n)$ y $\phi : \prod_{i=1}^n R_i \to R$ definida por $\phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = \sum_{i=1}^n \boldsymbol{a}_i \cdot \boldsymbol{u}_i$. Estas aplicaciones son homomorfismos de anillos e inversas una de la otra puesto que $\varphi(\phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)) = \varphi(\sum_{i=1}^n \boldsymbol{a}_i \cdot \boldsymbol{u}_i) = (\sum_{i=1}^n \boldsymbol{a}_i \cdot \boldsymbol{u}_i \cdot \boldsymbol{u}_1, \ldots, \sum_{i=1}^n \boldsymbol{a}_i \cdot \boldsymbol{u}_i \cdot \boldsymbol{u}_n) = (\boldsymbol{a}_1 \cdot \boldsymbol{u}_1, \ldots, \boldsymbol{a}_n \cdot \boldsymbol{u}_n) = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ y $\phi(\varphi(\boldsymbol{a})) = \phi(\boldsymbol{a} \cdot \boldsymbol{u}_1, \ldots, \boldsymbol{a} \cdot \boldsymbol{u}_n) = \sum_{i=1}^n \boldsymbol{a} \cdot \boldsymbol{u}_i \cdot \boldsymbol{u}_i = \sum_{i=1}^n \boldsymbol{a} \cdot \boldsymbol{u}_i = \boldsymbol{a} \cdot \sum_{i=1}^n \boldsymbol{u}_i = \boldsymbol{a}$. ■

Lema 1.2.5 *Sea R un anillo.*

(1) Para todos $f, g \in R$ idempotentes se tiene que $f \cdot g$ es idempotente. Más aún, si $f \cdot g = 0$, entonces $f + g$ es idempotente.

(2) Para todo $f \in \mathbb{R}$ idempotente se tiene que $1 - f$ es idempotente.

Demostración. *(1)* $(f \cdot g)^2 = f^2 \cdot g^2 = f \cdot g$ y $(f + g)^2 = f^2 + g^2 + 2f \cdot g = f + g$.
(2) $(1 - f)^2 = 1 + f^2 - 2f = 1 - f$. ■

Lema 1.2.6 *Sea $R = \prod_{i \in I} R_i$.*

(1) Si para cada $\mathfrak{p} \in \operatorname{Spec}(R_i)$ consideramos $M_{\mathfrak{p},i} = \pi_i^{-1}(\mathfrak{p})$, entonces $M_{\mathfrak{p},i}$ es un ideal primo de R y

$$M_{\mathfrak{p},i} = \prod_{j \in I} m_j \text{ con } m_j = R_j \text{ para todo } j \neq i, \quad y \quad m_i = \mathfrak{p}.$$

(2) Si para cada $\mathfrak{m} \in \operatorname{Max}(R_i)$ consideramos $M_{\mathfrak{m},i} = \pi_i^{-1}(\mathfrak{m})$, entonces $M_{\mathfrak{m},i}$ es un ideal maximal de R y

$$M_{\mathfrak{m},i} = \prod_{j \in I} m_j \text{ con } m_j = R_j \text{ para todo } j \neq i, \quad y \quad m_i = \mathfrak{m}.$$

(3) Si P es un ideal primo de R y existe $i \in I$ tal que $\boldsymbol{e}_i \notin P$ entonces $\boldsymbol{e}_j \in P$ para todo $j \neq i$ y en consecuencia i es único. Además si I es finito, entonces existe $i \in I$ tal que $\boldsymbol{e}_i \notin P$.

(4) Sea P un ideal. Entonces $\boldsymbol{e}_i \in P$ si y sólo si $\pi_i(P) = R_i$.

(5) Si I es finito, entonces los ideales primos de R son los $M_{\mathfrak{p},i}$ con $\mathfrak{p} \in \operatorname{Spec}(R_i)$.

(6) Si I es finito, entonces los ideales maximales de R son los $M_{\mathfrak{m},i}$ con $\mathfrak{m} \in \operatorname{Max}(R_i)$.

(7) Si I es finito, entonces

$$\operatorname{Spec}(R) \simeq \coprod_{i \in I} \operatorname{Spec}(R_i).$$

(8) Si I es finito, entonces

$$\operatorname{Max}(R) \simeq \coprod_{i \in I} \operatorname{Max}(R_i).$$

(9) Si I es infinito, entonces existen ideales maximales y por tanto primos de R que no son de la forma $M_{\mathfrak{m},i}$.

Demostración. *(1)* Puesto que π_i es un homomorfismo de anillos y $\mathfrak{p} \in \operatorname{Spec}(R_i)$, entonces $\pi_i^{-1}(\mathfrak{p}) = M_{\mathfrak{p},i}$ es un ideal primo de R.
(2) Como π_i es sobreyectiva y $\mathfrak{m} \in \operatorname{Max}(R_i)$, entonces $\pi_i^{-1}(\mathfrak{m}) = M_{\mathfrak{m},i}$ es un ideal maximal de R.
(3) Como $\mathbf{e}_i \cdot \mathbf{e}_j = 0$ para todo $i \neq j$, $\mathbf{e}_i \cdot \mathbf{e}_j \in P$ y si existe $i \in I$ tal que $\mathbf{e}_i \notin P$ entonces $\mathbf{e}_j \in P$ para todo $j \neq i$ luego $\mathbf{e}_i$ es único. Además, si I es finito y $\mathbf{e}_i \in P$ para todo $i \in I$ entonces $\sum_{i \in I} \mathbf{e}_i = \mathbf{1} \in P$ y $P = R$. Luego existe $i \in I$ tal que $\mathbf{e}_i \notin P$.
(4) Sea P un ideal. Si $\mathbf{e}_i \in P$, entonces $1 = \pi_i(\mathbf{e}_i) \in \pi_i(P)$ y como π_i es sobreyectiva, $\pi_i(P)$ es un ideal luego $\pi_i(P) = R_i$. Recíprocamente, si $\pi_i(P) = R_i$, entonces existe $\boldsymbol{a} \in P$ tal que $\pi_i(\boldsymbol{a}) = 1$ luego $\pi_i(\mathbf{e}_i \cdot \boldsymbol{a}) = 1$ y $\pi_j(\mathbf{e}_i \cdot \boldsymbol{a}) = 0$ para todo $j \neq i$ por tanto $\mathbf{e}_i \cdot \boldsymbol{a} = \mathbf{e}_i$. Como $\boldsymbol{a} \in P$ se tiene que $\mathbf{e}_i \in P$.
(5) Si P es un ideal primo de R se tienen dos casos:
(a) existe $i \in I$ tal que $\pi_i(P) \neq R_i$.
(b) $\pi_i(P) = R_i$, para todo $i \in I$.
Si se verifica (a), existe $i \in I$ tal que $\pi_i(P) \neq R_i$, entonces $P = \pi_i^{-1}(\pi_i(P))$.
En efecto, $P \subset \pi_i^{-1}(\pi_i(P))$ y si $\boldsymbol{a} \in \pi_i^{-1}(\pi_i(P))$ entonces $\pi_i(\boldsymbol{a}) \in \pi_i(P)$ luego existe $\boldsymbol{b} \in P$ tal que $\pi_i(\boldsymbol{a}) = \pi_i(\boldsymbol{b})$ por tanto $(\boldsymbol{a} - \boldsymbol{b}) \cdot \boldsymbol{e}_i = 0 \in P$. Como $\boldsymbol{e}_i \notin P$, $\boldsymbol{a} - \boldsymbol{b} \in P$ y en consecuencia $\boldsymbol{a} \in P$ ya que $\boldsymbol{b} \in P$.
Por el item (3), el caso (b) no puede darse si I es finito.
(6) Si M es un ideal maximal de R entonces M es primo y por el item (5), $M = M_{\mathfrak{p},i}$ con $\mathfrak{p} \in \operatorname{Spec}(R_i)$. Si $\mathfrak{p}$ no es maximal entonces existe $\mathfrak{m} \in \operatorname{Max}(R_i)$ tal que $\mathfrak{p} \subset \mathfrak{m}$ por

tanto $M \subsetneq \pi_i^{-1}(\mathfrak{m})$ lo cual es absurdo pues M es maximal de R. Entonces $\mathfrak{p}$ es maximal.
(7) Consideremos en $R = \prod_{i=1}^n R_i$ los ideales primos, $M_{\mathfrak{p},i}$. Por el item (2),

$$\operatorname{Spec}(R) = \coprod_{i=1}^{n} \{M_{\mathfrak{p},i} : \mathfrak{p} \in \operatorname{Spec}(R_i)\}.$$

Para todo i definimos $X_i = \{M_{\mathfrak{p},i} : \mathfrak{p} \in \operatorname{Spec}(R_i)\}$ y consideramos la aplicación

$$\phi_i : X_i \to \operatorname{Spec}(R_i)$$

definida por $\phi_i(M_{\mathfrak{p},i}) = \pi_i(M_{\mathfrak{p},i}) = \mathfrak{p}$. Así, ϕ_i es inyectiva pues si $\mathfrak{p} = \mathfrak{q}$ entonces $M_{\mathfrak{p},i} = M_{\mathfrak{q},i}$ y ϕ_i es sobreyectiva pues π_i es sobreyectiva, y ϕ_i es continua ya que

$$\phi_i^{-1}(V(\mathfrak{p})) = \{M_{\mathfrak{q},i} \in \operatorname{Spec}(R) : \mathfrak{p} \subset \mathfrak{q}\} = V(M_{\mathfrak{p},i}),$$

donde $V(\mathfrak{p})$ denota el cerrado de Zariski del ideal $\mathfrak{p}$. De igual forma, ϕ_i^{-1} es continua y por tanto X_i es homeomorfo a $\operatorname{Spec}(R_i)$. En consecuencia,

$$\operatorname{Spec}(\prod_{i=1}^{n} R_i) \simeq \coprod_{i=1}^{n} \operatorname{Spec}(R_i).$$

(8) La demostración es similar a la del item (7), solo cambiamos $\mathfrak{p} \in \operatorname{Spec}(R_i)$ por $\mathfrak{m} \in \operatorname{Max}(R_i)$ y $\operatorname{Spec}(R)$ por $\operatorname{Max}(R)$.
(9) Sea I infinito y consideremos

$$Q = \{\boldsymbol{a} \in R : \ \exists\ J \subset I,\ J \ \text{ finito con } \pi_i(\boldsymbol{a}) = 0\ \forall i \notin J\}$$

es decir, $Q = \bigoplus_{i \in I} R_i$. Entonces Q es un ideal de R. En efecto, sean $\boldsymbol{a}, \boldsymbol{b} \in Q$ entonces existen $J_1, J_2 \subset I$ finitos tales que $\pi_i(\boldsymbol{a}) = 0$ para todo $i \notin J_1$ y $\pi_i(\boldsymbol{b}) = 0$ para todo $i \notin J_2$. Luego para todo $i \notin J_1 \cup J_2$, $\pi_i(\boldsymbol{a} + \boldsymbol{b}) = 0$ y $J_1 \cup J_2$ es finito. Así, $\boldsymbol{a} + \boldsymbol{b} \in Q$. Además, si $\boldsymbol{\lambda} \in R$, entonces $\pi_i(\boldsymbol{\lambda} \cdot \boldsymbol{a}) = 0$ para todo $i \notin J_1$ y como J_1 es finito entonces $\boldsymbol{\lambda} \cdot \boldsymbol{a} \in Q$. Por otra parte, como todo ideal está contenido en un ideal maximal entonces existe un ideal maximal M y por tanto un ideal primo de R que contiene a Q y que cumple que $\pi_i(M) = \pi_i(Q) = R_i$ para todo $i \in I$. ■

Observación 1.2.7 *En el Lema 1.2.6(9) Q no es primo, por ejemplo, sea $R = A^{\mathbb{N}}$ con A un anillo. Sean a y b divisores de cero de A tales que $ab = 0$. Si definimos $\pi_i(\boldsymbol{a}) = a$ y $\pi_i(\boldsymbol{b}) = b$ para todo $i = 1, \ldots, n$ entonces $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{0} \in Q$ pero $\boldsymbol{a} \notin Q$ y $\boldsymbol{b} \notin Q$.*

Lema 1.2.8 *Si I es finito, entonces los ideales primos minimales de R son de la forma*

$$M_{\mathfrak{p},i} = \prod_{j\in I} m_j \quad con \quad m_j = R_j \text{ para todo } j \neq i, \ y \ \ m_i = \mathfrak{p} \tag{1.1}$$

donde $\mathfrak{p}$ un ideal primo minimal de R_i.

Demostración. Es consecuencia del Lema 1.2.6(5). ■

1.3. Producto de cuerpos.

Sean I un conjunto arbitrario y $\{R_i\}_{i\in I}$ una familia de cuerpos. En toda esta sección consideramos el anillo producto $R = \prod_{i\in I} R_i$.

Proposición 1.3.1 *Para todo $\boldsymbol{f} \in R$, existen $\boldsymbol{u}_f$ inversible y $\boldsymbol{\alpha}_f$ idempotente tal que $\boldsymbol{f} = \boldsymbol{\alpha}_f \cdot \boldsymbol{u}_f$. Además, $\boldsymbol{\alpha}_f$ es único y $\boldsymbol{\alpha}_f = \mathbf{1}$ si y sólo si $\boldsymbol{f}$ es inversible.*

Demostración. Definimos la aplicación $u_f(i) = f(i)$ si $f(i) \neq 0$ y $u_f(i) = 1$ si $f(i) = 0$ y la aplicación $\alpha_f(i) = 1$ si $f(i) \neq 0$ y $\alpha_f(i) = 0$ si $f(i) = 0$. Así, $\boldsymbol{u}_f$ es inversible, $\boldsymbol{\alpha}_f$ es idempotente y $\boldsymbol{f} = \boldsymbol{u}_f \cdot \boldsymbol{\alpha}_f$. Note que $\boldsymbol{u}_f$ no es único pues la construcción es válida con $u_f(i) \neq 0$ si $f(i) = 0$. Además, $\boldsymbol{\alpha}_f$ está unívocamente determinado por $\boldsymbol{f}$. En efecto, $f(i) = u_f(i)\alpha_f(i)$ y $u_f(i) \neq 0$ para todo i pues $\boldsymbol{u}_f$ es inversible. Luego si $f(i) = 0$, entonces $\alpha_f(i) = 0$ y si $f(i) \neq 0$ entonces $\alpha_f(i) \neq 0$ y por tanto $\alpha_f(i) = 1$ ya que $\boldsymbol{\alpha}_f$ es idempotente. En particular, $\boldsymbol{\alpha}_f = \mathbf{1}$ si y sólo si $\boldsymbol{f}$ es inversible. ■

Para cada ideal $\mathfrak{a}$ de R definimos el conjunto de idempotentes de $\mathfrak{a}$ como

$$\mathrm{id}(\mathfrak{a}) = \{\boldsymbol{f} \in \mathfrak{a} : \boldsymbol{f} \text{ es idempotente}\}.$$

En particular $\mathrm{id}(R) = \{\boldsymbol{f} \in R : \boldsymbol{f}$ es idempotente $\}$.

Observación 1.3.2 *En la Proposición 1.3.1, como $\boldsymbol{\alpha}_f \in \mathrm{id}(R)$ es único, se llama a $\boldsymbol{\alpha}_f$* el idempotente asociado a $\boldsymbol{f}$ *y es denotado por* $\mathrm{id}(\boldsymbol{f})$. *Definimos así la aplicación*

$$\begin{array}{rccc} \mathrm{id}: & R & \to & R \\ & \boldsymbol{f} & \mapsto & \mathrm{id}(\boldsymbol{f}) \end{array}.$$

Se satisfacen las siguientes propiedades:

(1) $\mathrm{id}(\boldsymbol{f} \cdot \boldsymbol{g}) = \mathrm{id}(\boldsymbol{f}) \cdot \mathrm{id}(\boldsymbol{g})$.

En efecto, por la Proposición 1.3.1, $\boldsymbol{f} \cdot \boldsymbol{g} = \mathrm{id}(\boldsymbol{f}) \cdot \boldsymbol{u}_f \cdot \mathrm{id}(\boldsymbol{g}) \cdot \boldsymbol{u}_g$ *además el producto*

de idempotentes es idempotente y el de inversibles es inversible luego

$$\boldsymbol{f}\cdot\boldsymbol{g} = (\mathrm{id}(\boldsymbol{f})\cdot\mathrm{id}(\boldsymbol{g}))\cdot(\boldsymbol{u}_f\cdot\boldsymbol{u}_g) = \mathrm{id}(\boldsymbol{f}\cdot\boldsymbol{g})\cdot\boldsymbol{u}_{f.g}.$$

Pero el idempotente es único entonces $\mathrm{id}(\boldsymbol{f}\cdot\boldsymbol{g}) = \mathrm{id}(\boldsymbol{f})\cdot\mathrm{id}(\boldsymbol{g})$.

(2) Para todo ideal $\mathfrak{a}$ *se tiene que* $\mathrm{id}(\mathfrak{a})\subset\mathfrak{a}$.
En efecto, para todo $\boldsymbol{f}\in R$, $\boldsymbol{f}=\boldsymbol{\alpha}_f\cdot\boldsymbol{u}_f$. *Luego, si* $\boldsymbol{f}\in\mathfrak{a}$ *entonces* $\boldsymbol{\alpha}_f=\boldsymbol{f}\cdot\boldsymbol{u}_f^{-1}\in\mathfrak{a}$.

(3) Para todo $\boldsymbol{f}\in R$, $\boldsymbol{f}\in\mathfrak{a}$ *si y sólo si* $\mathrm{id}(\boldsymbol{f})\in\mathrm{id}(\mathfrak{a})$.

(4) Sean $\mathfrak{a},\mathfrak{b}$ *ideales de* R. *Por el item (3),* $\mathfrak{a}=\mathfrak{b}$ *si y sólo si* $\mathrm{id}(\mathfrak{a})=\mathrm{id}(\mathfrak{b})$.

Proposición 1.3.3 *Sea* $\boldsymbol{f}\in R$, $\boldsymbol{f}$ *no es inversible si y sólo si existe* $\boldsymbol{g}\neq\boldsymbol{0}$ *tal que* $\boldsymbol{f}\cdot\boldsymbol{g}=\boldsymbol{0}$ *y* $\boldsymbol{f}+\boldsymbol{g}$ *es inversible.*

Demostración. Si $\boldsymbol{f}$ no es inversible, por la Proposición 1.3.1, $\boldsymbol{f}=\mathrm{id}(\boldsymbol{f})\cdot\boldsymbol{u}_f$ y $\boldsymbol{1}-\mathrm{id}(\boldsymbol{f})\neq\boldsymbol{0}$. Entonces definimos $\boldsymbol{g}=\boldsymbol{u}_f\cdot(\boldsymbol{1}-\mathrm{id}(\boldsymbol{f}))$ y de esta forma, $\boldsymbol{g}\neq\boldsymbol{0}$,

$$\boldsymbol{f}\cdot\boldsymbol{g}=\boldsymbol{u}_f^2\cdot\mathrm{id}(\boldsymbol{f})\cdot(\boldsymbol{1}-\mathrm{id}(\boldsymbol{f}))=\boldsymbol{0}\qquad\text{y}\qquad\boldsymbol{f}+\boldsymbol{g}=\boldsymbol{u}_f$$

es inversible. Recíprocamente como $\boldsymbol{f}\cdot\boldsymbol{g}=\boldsymbol{0}$ y $\boldsymbol{g}\neq\boldsymbol{0}$, $\boldsymbol{f}$ es no inversible. ■

El resultado anterior no es cierto en los anillos totales de cocientes, por ejemplo, $\mathbb{Z}/(4)$ es anillo total de cocientes, $\overline{2}$ no es inversible y $\overline{2}$ es el único elemento tal que $\overline{2}\cdot\overline{2}=\overline{0}$ pero $\overline{2}+\overline{2}=\overline{0}$.

Proposición 1.3.4 *Sean* $\mathfrak{m}\in\mathrm{Max}(R)$ *y* $\boldsymbol{f}\in R$. *Entonces* $\boldsymbol{f}\in\mathfrak{m}$ *si y sólo si existe* $\boldsymbol{h}\notin\mathfrak{m}$ *tal que* $\boldsymbol{f}\cdot\boldsymbol{h}=\boldsymbol{0}$.

Demostración. Si existe $\boldsymbol{h}\notin\mathfrak{m}$ tal que $\boldsymbol{f}\cdot\boldsymbol{h}=\boldsymbol{0}$ entonces $\boldsymbol{f}\in\mathfrak{m}$ pues $\mathfrak{m}$ es primo. Recíprocamente, si $\boldsymbol{f}\in\mathfrak{m}$, $\boldsymbol{f}$ no es inversible y por la Proposición 1.3.3, existe $\boldsymbol{h}\neq\boldsymbol{0}$ tal que $\boldsymbol{f}\cdot\boldsymbol{h}=\boldsymbol{0}$ y $\boldsymbol{f}+\boldsymbol{h}$ es inversible entonces $\boldsymbol{h}\notin\mathfrak{m}$ ya que $\boldsymbol{f}\in\mathfrak{m}$ y $\boldsymbol{f}+\boldsymbol{h}\notin\mathfrak{m}$. ■

Proposición 1.3.5 *Para todo* $\mathfrak{m}\in\mathrm{Max}(R)$, *los cuerpos* $R/\mathfrak{m}$ *y* $R_{\mathfrak{m}}$ *son canónicamente isomorfos.*

Demostración. Consideremos el homomorfismo canónico

$$\begin{array}{rccc}\varphi: & R & \to & R_{\mathfrak{m}}\\ & \boldsymbol{f} & \mapsto & \frac{\boldsymbol{f}}{\boldsymbol{1}}.\end{array}$$

Veamos que para todo $\boldsymbol{f}\in R$, $\boldsymbol{f}\in\mathfrak{m}$ si y sólo si $\frac{\boldsymbol{f}}{\boldsymbol{1}}=\boldsymbol{0}$. En efecto, si $\boldsymbol{f}\in\mathfrak{m}$ entonces $\boldsymbol{f}$ no es inversible y por la Proposición 1.3.3, existe $\boldsymbol{g}\neq\boldsymbol{0}$ tal que $\boldsymbol{f}\cdot\boldsymbol{g}=\boldsymbol{0}$ y $\boldsymbol{f}+\boldsymbol{g}=\boldsymbol{1}$.

Por tanto $\boldsymbol{g} \notin \mathfrak{m}$ y $\frac{\boldsymbol{f}}{\boldsymbol{1}} = \boldsymbol{0}$. Recíprocamente, si $\frac{\boldsymbol{f}}{\boldsymbol{1}} = \boldsymbol{0}$, entonces existe $\boldsymbol{g} \notin \mathfrak{m}$ tal que $\boldsymbol{f} \cdot \boldsymbol{g} = \boldsymbol{0}$. Luego $\boldsymbol{f} \cdot \boldsymbol{g} \in \mathfrak{m}$ y por tanto $\boldsymbol{f} \in \mathfrak{m}$.
En consecuencia, φ induce un homomorfismo inyectivo

$$\begin{array}{rccc} \psi: & R/\mathfrak{m} & \to & R_{\mathfrak{m}} \\ & \boldsymbol{f}+\mathfrak{m} & \mapsto & \frac{\boldsymbol{f}}{\boldsymbol{1}} \end{array}.$$

Veamos ahora que ψ es sobreyectivo. Es decir, si para todo $\boldsymbol{f} \in R$ y para todo $\boldsymbol{g} \notin \mathfrak{m}$ existe $\boldsymbol{h} \in R$ tal que $\frac{\boldsymbol{f}}{\boldsymbol{g}} = \frac{\boldsymbol{h}}{\boldsymbol{1}}$ y esto es equivalente a que existe $\boldsymbol{t} \notin \mathfrak{m}$ tal que $(\boldsymbol{f}-\boldsymbol{g}\cdot\boldsymbol{h})\cdot\boldsymbol{t} = \boldsymbol{0}$ pero por la Proposición 1.3.4, $\boldsymbol{f} - \boldsymbol{g} \cdot \boldsymbol{h} \in \mathfrak{m}$. Por tanto, hay que demostrar que para todo $\boldsymbol{f} \in R$ y para todo $\boldsymbol{g} \notin \mathfrak{m}$ existe $\boldsymbol{h} \in R$ tal que $\boldsymbol{f}-\boldsymbol{g}\cdot\boldsymbol{h} \in \mathfrak{m}$. Como $\boldsymbol{g} \notin \mathfrak{m}$, entonces $\boldsymbol{g}+\mathfrak{m} \neq \boldsymbol{0}$ en el cuerpo $R/\mathfrak{m}$ luego existe $\boldsymbol{s}+\mathfrak{m} \in R/\mathfrak{m}$ tal que $(\boldsymbol{g}+\mathfrak{m})\cdot(\boldsymbol{s}+\mathfrak{m}) = \boldsymbol{1}+\mathfrak{m}$ y esto es equivalente a que $\boldsymbol{1} - \boldsymbol{g} \cdot \boldsymbol{s} \in \mathfrak{m}$. Por tanto, $\boldsymbol{f} - \boldsymbol{g} \cdot (\boldsymbol{f} \cdot \boldsymbol{s}) \in \mathfrak{m}$. ■

El resultado anterior no es válido en el caso en que R sea un anillo total de cocientes. Por ejemplo, si R es anillo total de cocientes y anillo local pero no cuerpo, entonces $R_{\mathfrak{m}} = R$ y $R/\mathfrak{m}$ es un cuerpo.

La siguiente proposición muestra que si I es un conjunto arbitrario, $\{R_i\}_{i\in I}$ es una familia de cuerpos y $R = \prod_{i\in I} R_i$ entonces R es $0-$dimensional. Este resultado es inmediato por el Teorema 1.1.7 y observando que R es un anillo total de cocientes con la propiedad de la Proposición 1.3.1. Pero mostramos a continuación una demostración distinta.

Proposición 1.3.6 *Si $\mathfrak{p}$ es un ideal primo de R entonces $\mathfrak{p}$ es maximal. Es decir R es $0-$dimensional.*

Demostración. Supongamos que $\mathfrak{p}$ es un ideal primo contenido estrictamente en un ideal maximal $\mathfrak{m}$, entonces existe $\boldsymbol{f} \in \mathfrak{m}$ tal que $\boldsymbol{f} \notin \mathfrak{p}$. Como $\boldsymbol{f}$ no es inversible, por la Proposición 1.3.3, existe $\boldsymbol{g} \neq \boldsymbol{0}$ tal que $\boldsymbol{f} \cdot \boldsymbol{g} = \boldsymbol{0}$ y $\boldsymbol{f} + \boldsymbol{g}$ es inversible. Por tanto, $\boldsymbol{f} \cdot \boldsymbol{g} \in \mathfrak{p}$ y como $\boldsymbol{f} \notin \mathfrak{p}$, $\boldsymbol{g} \in \mathfrak{p}$. Pero $\mathfrak{p} \subset \mathfrak{m}$ entonces $\boldsymbol{f} + \boldsymbol{g} \in \mathfrak{m}$ y $\boldsymbol{f} + \boldsymbol{g}$ es inversible, entonces $\mathfrak{m} = R$. ■

En consecuencia, si R es un producto arbitrario de cuerpos, entonces

$$\mathrm{Max}(R) = \mathrm{Spec}(R).$$

Corolario 1.3.7 *Sean K un cuerpo, I un conjunto finito y $R = K^I$. Entonces*

(1) $\mathrm{Spec}(R) = \mathrm{Max}(R) = \{\mathfrak{m}_i\}_{i\in I}$ *donde* $\mathfrak{m}_i = \{\boldsymbol{f} \in R : f(i) = 0\}$.

(2) $R/\mathfrak{m} \simeq R_{\mathfrak{m}} \simeq K$.

Demostración. *(1)* Es inmediato ya que, por el Lema 1.2.6(6), todos los ideales maximales de R son de la forma $\{\mathfrak{m}_i\}_{i\in I}$ donde $\mathfrak{m}_i = \{\boldsymbol{f} \in R : f(i) = 0\}$.
(2) Por la Proposición 1.3.5, basta mostrar que para todo $\mathfrak{m} \in \mathrm{Max}(R)$, $R/\mathfrak{m} \simeq K$. Pero para todo $i \in I$ el homomorfismo $\psi : R \to K$ definido por $\psi(\boldsymbol{f}) = f(i)$ es sobreyectivo y $\mathrm{Ker}(\psi) = \mathfrak{m}_i$ entonces

$$\begin{array}{rccc} \varphi: & R/\mathfrak{m}_i & \to & K \\ & \boldsymbol{f} + \mathfrak{m}_i & \mapsto & f(i) \end{array}$$

es un isomorfismo. ■

Proposición 1.3.8 *Sean K un cuerpo finito, I un conjunto arbitrario y $R = K^I$. Para todo $\mathfrak{m} \in \mathrm{Max}(R)$,*

$$R_{\mathfrak{m}} \simeq R/\mathfrak{m} \simeq K.$$

Demostración. Por la Proposición 1.3.5, basta demostrar que $R/\mathfrak{m} \simeq K$ para todo $\mathfrak{m} \in \mathrm{Max}(R)$. Sean $K = \{\alpha_0, \ldots, \alpha_n\}$ y consideremos la aplicación

$$\begin{array}{rccc} \phi: & K & \to & R/\mathfrak{m} \\ & \alpha & \mapsto & \alpha\mathbf{1} + \mathfrak{m} \end{array}.$$

ϕ es inyectiva ya que si $\alpha \in K$ y $\alpha\mathbf{1} \in \mathfrak{m}$ entonces $\alpha = 0$ pues si $\alpha \neq 0$, por la Proposición 1.2.1, $\alpha\mathbf{1}$ es inversible en R. Veamos que ϕ es sobreyectiva. Sea $\boldsymbol{f} \in R$, para todo $i \in I$, $f(i) \in \{\alpha_0, \ldots, \alpha_n\}$ y

$$(\boldsymbol{f} - \alpha_0\mathbf{1}) \cdot \cdots \cdot (\boldsymbol{f} - \alpha_n\mathbf{1}) = \mathbf{0}$$

ya que para todo $i \in I$ existe $j \in \{0, 1, \ldots, n\}$ tal que $f(i) = \alpha_j$, es decir $(\boldsymbol{f} - \alpha_j\mathbf{1})(i) = 0$. Entonces

$$(\boldsymbol{f} - \alpha_0\mathbf{1}) \cdot \cdots \cdot (\boldsymbol{f} - \alpha_n\mathbf{1}) \in \mathfrak{m}$$

y por tanto existe $j \in \{1, \ldots, n\}$ tal que $\boldsymbol{f} - \alpha_j\mathbf{1} \in \mathfrak{m}$. Así ϕ es sobreyectiva. ■

Veremos más adelante que el resultado anterior no es cierto si K es un cuerpo infinito, I un conjunto infinito y $R = K^I$.

Lema 1.3.9 *Si $\boldsymbol{f} \in R$ es idempotente entonces $D(\boldsymbol{f}) = \{\mathfrak{p} \in \mathrm{Max}(R) : \boldsymbol{f} \notin \mathfrak{p}\}$ es abierto cerrado en* $\mathrm{Max}(R)$.

Demostración. Para todo $\boldsymbol{f} \in R$, $V(\boldsymbol{f}) \cap V(\mathbf{1} - \boldsymbol{f}) \subset V(\boldsymbol{f} + (\mathbf{1} - \boldsymbol{f})) = V(\mathbf{1}) = \emptyset$ y puesto que $\boldsymbol{f} \in \mathrm{id}(R)$ entonces $V(\boldsymbol{f}) \cup V(\mathbf{1} - \boldsymbol{f}) = V(\boldsymbol{f} \cdot (\mathbf{1} - \boldsymbol{f})) = V(\mathbf{0}) = \mathrm{Max}(R)$. Así, $D(\boldsymbol{f}) = \mathrm{Max}(R) - V(\boldsymbol{f}) = V(\mathbf{1} - \boldsymbol{f})$ y $D(\boldsymbol{f})$ es abierto cerrado de $\mathrm{Max}(R)$. ■

Lema 1.3.10 *Si en R todo elemento es inversible o producto de un inversible por un idempotente, como sucede en el caso de que R sea un producto de cuerpos, entonces*

todos los conjuntos $D(\boldsymbol{f}) = \{\mathfrak{p} \in \mathrm{Max}(R) : \boldsymbol{f} \notin \mathfrak{p}\}$*, para* $\boldsymbol{f} \in R$*, son abiertos cerrados de* $\mathrm{Max}(R)$*.*

Demostración. Para todo $\boldsymbol{f} \in R$ se tiene que $\boldsymbol{f} = \boldsymbol{u}_f \cdot \boldsymbol{\alpha}_f$ donde $\boldsymbol{u}_f$ es inversible y $\boldsymbol{\alpha}_f$ es idempotente. Note que $V(\boldsymbol{f}) = V(\boldsymbol{\alpha}_f)$ y por tanto $D(\boldsymbol{f}) = D(\boldsymbol{\alpha}_f)$. Además, por el Lema 1.3.9, $D(\boldsymbol{\alpha}_f)$ es abierto cerrado de $\mathrm{Max}(R)$. ■

1.3.1. Filtros y ultrafiltros de I.

Hemos visto en el Lema 1.2.6(9) que hay ideales maximales de K^I, con I arbitrario, que no son de la forma $\mathfrak{m}_i$. Sobre estos ideales hay mucha literatura, pero aquí nos limitaremos a estimar el cardinal del conjunto que forman usando filtros y ultrafiltros.

Sean I un conjunto arbitrario, K un cuerpo y $R = K^I$. Para todo $C \subset I$, definimos la aplicación

$$\begin{array}{rccl} \mathbf{e}_C : & I & \to & K \\ & i & \mapsto & e_C(i) = \left\{ \begin{array}{ll} 0, & \text{si } \ i \in C \\ 1, & \text{si } \ i \notin C \end{array} \right. . \end{array}$$

Propiedades: Sean $B, C \subset I$. Entonces se tiene que:

(1) $\mathbf{e}_I = 0, \ \ \mathbf{e}_\emptyset = 1.$

(2) $\mathbf{e}_B + \mathbf{e}_C = \mathbf{e}_{B\cap C} + \mathbf{e}_{B\cup C}.$

(3) $\mathbf{e}_B \cdot \mathbf{e}_C = \mathbf{e}_{B\cap C}.$

(4) $\mathbf{e}_C^2 = \mathbf{e}_C.$

Veamos que existe una correspondencia biunívoca entre el conjunto de partes de I, $\mathcal{P}(I)$, y el conjunto de los elementos idempotentes de R, $\mathrm{id}(R)$.

Proposición 1.3.11 *Sean* I *un conjunto arbitrario y* $R = K^I$*. Entonces la aplicación*

$$\begin{array}{rccc} \gamma : & \mathcal{P}(I) & \to & \mathrm{id}(R) \\ & C & \mapsto & \boldsymbol{e}_C \end{array}$$

es una biyección.

Demostración. γ es inyectiva pues si $\mathbf{e}_B = \mathbf{e}_C$ entonces $e_B(i) = e_C(i)$, para todo $i \in I$. Luego $e_B(j) = 0$ con $j \in B$ si y sólo si $e_C(j) = 0$ con $j \in C$. Por tanto $B = C$. Por último, γ es sobreyectiva pues si $\boldsymbol{f} \in \mathrm{id}(R)$, $f(i) = 0 \ \ \text{o} \ \ f(i) = 1$, para todo $i \in I$, entonces $C = \{i \in I : f(i) = 0\}$ cumple que $\gamma(C) = \boldsymbol{f}$. ■

Definición 1.3.12 *Un filtro $\mathfrak{F}$ sobre un conjunto I es una familia no vacía de subconjuntos no vacíos de I, que satisfacen:*

(i) si $B, C \in \mathfrak{F}$ entonces $B \cap C \in \mathfrak{F}$,

(ii) si $C \in \mathfrak{F}$ y $C \subset D$ entonces $D \in \mathfrak{F}$.

Proposición 1.3.13 *Si $\mathfrak{a}$ es un ideal propio de R, entonces*

$$\mathfrak{F}(\mathfrak{a}) = \{C \subset I : \boldsymbol{e}_C \in \mathfrak{a}\} = \gamma^{-1}(\mathrm{id}(\mathfrak{a}))$$

es un filtro en I.

Demostración. Veamos que $\mathfrak{F}(\mathfrak{a})$ cumple las condiciones de filtro. Puesto que $\mathbf{e}_I = \mathbf{0} \in \mathfrak{a}$, entonces $I \in \mathfrak{F}(\mathfrak{a})$ y por tanto $\mathfrak{F}(\mathfrak{a})$ es no vacío. Ahora si B, $C \in \mathfrak{F}(\mathfrak{a})$ entonces $\mathbf{e}_B$, $\mathbf{e}_C \in \mathfrak{a}$ y como $\mathfrak{a}$ es ideal, $\mathbf{e}_B + \mathbf{e}_C - \mathbf{e}_B \cdot \mathbf{e}_C = \mathbf{e}_{B\cap C} \in \mathfrak{a}$, por tanto $B \cap C \in \mathfrak{F}(\mathfrak{a})$. Por último, si $C \in \mathfrak{F}(\mathfrak{a})$ y $C \subset D$ entonces $\mathbf{e}_C \cdot \mathbf{e}_D = \mathbf{e}_{C\cup D} = \mathbf{e}_D \in \mathfrak{a}$. Luego $D \in \mathfrak{F}(\mathfrak{a})$. La segunda igualdad es inmediata por la Proposición 1.3.11. ■

Lema 1.3.14 *Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de R. Entonces $\mathfrak{a} \subset \mathfrak{b}$ si y sólo si $\mathfrak{F}(\mathfrak{a}) \subset \mathfrak{F}(\mathfrak{b})$.*

Demostración. Sea $C \subset I$ tal que $C \in \mathfrak{F}(\mathfrak{a})$ entonces $\mathbf{e}_C \in \mathfrak{a} \subset \mathfrak{b}$, luego $\mathbf{e}_C \in \mathfrak{b}$ por tanto $C \in \mathfrak{F}(\mathfrak{b})$. Recíprocamente, si $\mathbf{e}_C \in \mathfrak{a}$ entonces $C \in \mathfrak{F}(\mathfrak{a}) \subset \mathfrak{F}(\mathfrak{b})$, luego $C \in \mathfrak{F}(\mathfrak{b})$ y por tanto $\mathbf{e}_C \in \mathfrak{b}$. ■

Ahora mostraremos que existe una correspondencia biunívoca entre el conjunto de ideales de R, $\mathrm{ideal}(R)$, y el de los filtros en I, $\mathrm{fil}(I)$.

Proposición 1.3.15 *Sean I un conjunto arbitrario y $R = K^I$. Entonces la aplicación*

$$\begin{array}{rccc} \mu: & \mathrm{ideal}(R) & \to & \mathrm{fil}(I) \\ & \mathfrak{a} & \mapsto & \mathfrak{F}(\mathfrak{a}) \end{array}$$

es una biyección.

Demostración. Por el Lema 1.3.14, $\mathfrak{a} = \mathfrak{b}$ si y sólo si $\mathfrak{F}(\mathfrak{a}) = \mathfrak{F}(\mathfrak{b})$. Por tanto, μ está bien definida y es inyectiva. Veamos que μ es sobreyectiva. Dado un filtro $\mathfrak{F}$ de I, el ideal propio de R asociado a $\mathfrak{F}$ es $\mathfrak{a}(\mathfrak{F}) = (\{\mathbf{e}_C\}_{C\in\mathfrak{F}})R$ pues $\mathfrak{a}(\mathfrak{F}(\mathfrak{a})) = (\{\mathbf{e}_C\}_{C\in\mathfrak{F}(\mathfrak{a})})R = (\{\mathbf{e}_C\}_{\mathbf{e}_C\in\mathfrak{a}})R = (\{\mathfrak{a}\})R = \mathfrak{a}$. ■

Definición 1.3.16 *Un ultrafiltro es un filtro maximal con respecto a la relación de contenido.*

Proposición 1.3.17 *La correspondencia* $\mu : \text{ideal}(R) \to \text{fil}(I)$ *relaciona biunívocamente los ideales maximales de* R *con los ultrafiltros de* I*.*

Demostración. Por la Proposición 1.3.6, todo ideal primo de R es maximal. Además, por el Lema 1.3.14 y la Proposición 1.3.15, μ es una aplicación biyectiva que preserva la relación de contenido, por tanto los ideales maximales de R son enviados en los ultrafiltros de I. ■

Lema 1.3.18 *(1) Si* $\{\mathfrak{F}_\alpha\}_{\alpha\in T}$ *es una familia no vacía de filtros de* I*, entonces* $\bigcap_{\alpha\in T}\mathfrak{F}_\alpha$ *es un filtro de* I*.*

(2) Si $\mathcal{C} = \{\mathfrak{F}_i\}_{i\in\mathbb{N}}$ *es una cadena, es decir,* $\{\mathfrak{F}_i\}_{i\in\mathbb{N}}$ *es una familia no vacía de filtros de* I *tal que* $\mathfrak{F}_i \subset \mathfrak{F}_{i+1}$*, entonces* $\bigcup \mathcal{C} = \bigcup_{i\in\mathbb{N}}\mathfrak{F}_i$ *es un filtro de* I*.*

Demostración.
(1) Se deduce de la Proposición 1.3.15 y el hecho que la intersección de ideales es un ideal. *(2)* Veamos que $\bigcup_{i\in\mathbb{N}}\mathfrak{F}_i$ cumple las condiciones de un filtro de I. $\bigcup_{i\in\mathbb{N}}\mathfrak{F}_i \neq \emptyset$ ya que $\{\mathfrak{F}_i\}_{i\in\mathbb{N}}$ es una familia no vacía. Además si $B, C \in \bigcup_{i\in\mathbb{N}}\mathfrak{F}_i$, como $\mathfrak{F}_i \subset \mathfrak{F}_{i+1}$, existe i tal que $B, C \in \mathfrak{F}_i$ y por tanto $B \cap C \in \mathfrak{F}_i$, luego $B \cap C \in \bigcup_{i\in\mathbb{N}}\mathfrak{F}_i$. Por último, si $C \in \bigcup_{i\in\mathbb{N}}\mathfrak{F}_i$ y $C \subset D$, existe i tal que $C \in \mathfrak{F}_i$ y $C \subset D$, luego $D \in \mathfrak{F}_i$ y por tanto $D \in \bigcup_{i\in\mathbb{N}}\mathfrak{F}_i$. ■

Lema 1.3.19 *Todo filtro puede extenderse a un ultrafiltro.*

Demostración. Sea $\mathfrak{F}_0$ un filtro en I. Supongamos $\mathbf{P}$ el conjunto de todos los filtros $\mathfrak{F}$ en I tales que $\mathfrak{F} \supset \mathfrak{F}_0$ y consideremos el conjunto parcialmente ordenado $(\mathbf{P}, \subset)$. Si $\mathcal{C}$ es una cadena en $\mathbf{P}$, por el Lema 1.3.18(2), $\bigcup \mathcal{C}$ es un filtro y por tanto una cota superior de $\mathcal{C}$ en $\mathbf{P}$. Por el lema de Zorn existe un elemento maximal $\mathfrak{U}$ en $\mathbf{P}$ y por definición, $\mathfrak{U}$ es un ultrafiltro. ■

Proposición 1.3.20 *Existen exactamente* $2^{2^{\#(I)}}$ *ultrafiltros de* I*.*

Demostración. Ver por ejemplo [8, Theorem 7.6, pág 75]. ■

Ejemplo 1.3.21 *Si* $I = \mathbb{N}$ *y* $K = \mathbb{Z}/(2)$*, por las Proposiciones 1.3.17 y 1.3.20,*

$$\#(\text{Max}(K^I)) = 2^{2^{\#(\mathbb{N})}}.$$

Como $2^{2^{\aleph_0}} > \aleph_1$*, hay una cantidad de ideales maximales de* K^I *que no se pueden describir pero hay una cantidad numerable de la forma* $\mathfrak{m}_i$*.*

1.3.2. Inmersión de un anillo en un producto de cuerpos.

Sea R un anillo y consideremos el producto de cuerpos

$$\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}.$$

Por la propiedad universal del producto existe un homomorfismo de anillos

$$\begin{array}{rccc} \varphi: & R & \to & \prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m} \\ & \boldsymbol{a} & \mapsto & (\boldsymbol{a}+\mathfrak{m})_{\mathfrak{m}\in \mathrm{Max}(R)} \end{array}.$$

En general φ es no inyectiva pues $\mathrm{Ker}(\varphi) = \mathcal{J}(R)$, donde $\mathcal{J}(R)$ es el radical de Jacobson de R. En efecto,

$$\begin{array}{rcl} \boldsymbol{a} \in \mathrm{Ker}(\varphi) & \Leftrightarrow & \varphi(\boldsymbol{a}) = \boldsymbol{0} \Leftrightarrow \ \boldsymbol{a} \in \mathfrak{m},\ \forall\ \mathfrak{m} \in \mathrm{Max}(R) \\ & \Leftrightarrow & \boldsymbol{a} \in \bigcap_{\mathfrak{m}\in \mathrm{Max}(R)} \mathfrak{m} = \mathcal{J}(R). \end{array}$$

Definimos los conjuntos

$$O(R) = \{\boldsymbol{f} \in R : \exists \boldsymbol{g} \neq \boldsymbol{0} \text{ tal que } \boldsymbol{f}\cdot\boldsymbol{g} = \boldsymbol{0}\}$$

y

$$I(R) = \{\boldsymbol{f} \in R : \exists \boldsymbol{g} \in R \text{ tal que } \boldsymbol{f}\cdot\boldsymbol{g} = \boldsymbol{1}\}$$

Proposición 1.3.22 *(1)* $\varphi(I(R)) = I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$.

(2) Para todo $\boldsymbol{a} \in R$, $\varphi(\boldsymbol{a}) \in O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$ *si y sólo si existe* $\mathfrak{m} \in \mathrm{Max}(R)$ *tal que* $\boldsymbol{a} \in \mathfrak{m}$.

(3) $\varphi(O(R)) \subset O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$.

(4) Si R *es anillo total de cocientes entonces* $\varphi(O(R)) = O\left(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}\right) \bigcap \varphi(R)$. *Además, el recíproco se verifica si* $\mathcal{J}(R) = \{0\}$.

Demostración. *(1)* Si $\boldsymbol{a} \in R$ es inversible entonces $\boldsymbol{a} \notin \mathfrak{m}$ para todo $\mathfrak{m} \in \mathrm{Max}(R)$ luego $\boldsymbol{a}+\mathfrak{m} \neq \boldsymbol{0}$ en $R/\mathfrak{m}$ para todo $\mathfrak{m}$, por tanto $\varphi(\boldsymbol{a})$ es inversible en $\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}$. Recíprocamente, sea $\boldsymbol{b} \in I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$, existe $\boldsymbol{a} \in R$ tal que $\boldsymbol{b} = \varphi(\boldsymbol{a})$ y $\varphi(\boldsymbol{a})$ es inversible en $\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}$ entonces $\boldsymbol{a}+\mathfrak{m} \neq \boldsymbol{0}$ en $R/\mathfrak{m}$ para todo $\mathfrak{m} \in \mathrm{Max}(R)$ por tanto $\boldsymbol{a} \notin \mathfrak{m}$ para todo $\mathfrak{m}$, luego $\boldsymbol{a}$ es inversible y $\boldsymbol{b} \in \varphi(I(R))$.
(2) Inmediato porque un elemento de un producto de cuerpos es cero o divisor de cero si y sólo si tiene una componente nula.

(3) Un elemento que es cero o divisor de cero está contenido en algún maximal y por tanto aplicamos el item *(2)*.
(4) Por el Corolario 1.2.3, $\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}$ es un anillo total de cocientes, entonces
$O\left(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}\right) \bigcup I\left(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}\right) = \prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}$ y
$O\left(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}\right) \bigcap I\left(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}\right) = \emptyset$.
Por tanto, se tiene que:
(i) $\varphi(R) = \left(O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcup I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m})\right) \bigcap \varphi(R) =$

$$= \left(O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)\right) \bigcup \left(I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)\right)$$

y (ii) $\left(O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)\right) \bigcap \left(I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)\right) \subset$

$$\subset O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) = \emptyset.$$

Además, por el item (1), $\varphi(I(R)) = I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$ y por el item (3), $\varphi(O(R)) \subset O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$.
$\Rightarrow$: Por hipótesis, R es un anillo total de cocientes, entonces $R = O(R) \cup I(R)$ y $O(R) \cap I(R) = \emptyset$. En consecuencia,

$$\varphi(O(R)) = O\left(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}\right) \bigcap \varphi(R).$$

$\Leftarrow$: Sea $\boldsymbol{a} \in R$. Vamos a ver que R es anillo total de cocientes para esto vemos primero que si $\boldsymbol{a} \notin I(R)$ entonces $\varphi(\boldsymbol{a}) \notin I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$.
En efecto, si $\varphi(\boldsymbol{a}) \in I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$ entonces, por el item (1), existe $\boldsymbol{b} \in R$ tal que $\varphi(\boldsymbol{b}) = \varphi(\boldsymbol{a})$ y $\boldsymbol{b} \in I(R)$ por tanto $\varphi(\boldsymbol{b} - \boldsymbol{a}) = \boldsymbol{0}$. Como φ es inyectiva ya que $\mathcal{J}(R) = \{\boldsymbol{0}\}$ entonces $\boldsymbol{b} = \boldsymbol{a}$ y $\boldsymbol{a} \in I(R)$.
Ahora, si $a \notin I(R)$, entonces $\varphi(\boldsymbol{a}) \notin I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R)$ pero $\varphi(\boldsymbol{a}) \in \varphi(R)$ luego $\varphi(\boldsymbol{a}) \notin I(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m})$. Por lo tanto $\varphi(\boldsymbol{a}) \in O(\prod_{\mathfrak{m}\in \mathrm{Max}(R)} R/\mathfrak{m}) \bigcap \varphi(R) = \varphi(O(R))$. Luego existe $\boldsymbol{b} \in O(R)$ tal que $\varphi(\boldsymbol{a}) = \varphi(\boldsymbol{b})$ esto es $\varphi(\boldsymbol{a} - \boldsymbol{b}) = \boldsymbol{0}$ y como φ es inyectiva, $\boldsymbol{a} = \boldsymbol{b}$ y $\boldsymbol{a} \in O(R)$.
En consecuencia, R es un anillo total de cocientes. ■

En general, el recíproco del item (4) de la Proposición 1.3.22 no es cierto, por ejemplo, si R es un anillo local que es dominio y no es cuerpo, entonces $O(R) = \{0\}$, $O(R/\mathfrak{m}) = \{0\}$ y sin embargo R no es un anillo total de cocientes.

Ejemplo 1.3.23 (Un anillo total de cocientes que no es producto de cuerpos) *Sea* $R = \frac{\mathbb{R}[x]}{(x^3)}$. *Entonces*

(i) R es un anillo total de cocientes porque $\mathbb{R}[x]$ es un dominio euclídeo.

(ii) R *es un anillo local porque el único ideal maximal de* $\mathbb{R}[x]$ *que contiene al ideal* (x^3) *es* (x).

(iii) Si $R \simeq \mathbb{R}^r$ *entonces* $r = 1$ *pues* R *tiene un único ideal maximal y* $\mathbb{R}^r$ *tiene* r *ideales maximales. Pero* R *no es isomorfo a* $\mathbb{R}$ *pues* R *no es un cuerpo.*

Proposición 1.3.24 *R es un anillo con* $\mathrm{Max}(R) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ *y* $\mathcal{J}(R) = \{\mathbf{0}\}$ *si y sólo si* $R = K_1 \times \cdots \times K_r$ *donde* K_i *es un cuerpo para todo* $i = 1, \ldots, r$.

Demostración. $\Rightarrow$: Sea

$$\begin{array}{rccl} \varphi: & R & \to & R/\mathfrak{m}_1 \times \cdots \times R/\mathfrak{m}_r \\ & \boldsymbol{a} & \mapsto & (\boldsymbol{a}+\mathfrak{m}_1, \ldots, \boldsymbol{a}+\mathfrak{m}_r) \end{array}$$

Como $\mathcal{J}(R) = \{\mathbf{0}\}$, φ es inyectiva. Vamos a ver que φ es sobreyectiva para ello se debe probar que para todo $(\boldsymbol{a}_1, ..., \boldsymbol{a}_r) \in R^r$ existe $\boldsymbol{a} \in R$ con $\boldsymbol{a}_i + \mathfrak{m}_i = \boldsymbol{a} + \mathfrak{m}_i$ para todo i. Por otra parte, para todo $i \in \{1, \ldots, r\}$, $\mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r \neq \{\mathbf{0}\}$ donde $\widehat{\mathfrak{m}}_i$ denota que $\mathfrak{m}_i$ no hace parte de la intersección. Ya que si $\mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r = \{\mathbf{0}\}$ entonces $\mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r \subset \mathfrak{m}_i$. Por [3, Proposición 1.11], existe k, $1 \leq k \leq r$, con $k \neq i$ tal que $\mathfrak{m}_k \subset \mathfrak{m}_i$. Pero $\mathfrak{m}_k$ y $\mathfrak{m}_i$ son maximales luego $\mathfrak{m}_k = \mathfrak{m}_i$ y esto es absurdo. En consecuencia, $\mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r \neq \{\mathbf{0}\}$ y

$$\mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r \nsubseteq \mathfrak{m}_i.$$

De esta forma, existe $\mathbf{x}_i \notin \mathfrak{m}_i$ y $\mathbf{x}_i \in \mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r$ luego $\mathbf{x}_i + \mathfrak{m}_i \neq \mathbf{0}$ en el cuerpo $R/\mathfrak{m}_i$ y existe $\mathbf{y}_i + \mathfrak{m}_i$ tal que $(\mathbf{x}_i + \mathfrak{m}_i)(\mathbf{y}_i + \mathfrak{m}_i) = \mathbf{1} + \mathfrak{m}_i$. Entonces $\mathbf{x}_i\mathbf{y}_i - \mathbf{1} \in \mathfrak{m}_i$ y $\mathbf{x}_i\mathbf{y}_i \in \mathfrak{m}_1 \cap \cdots \cap \widehat{\mathfrak{m}}_i \cap \cdots \cap \mathfrak{m}_r$. Llamamos $\mathbf{e}_i = \mathbf{x}_i\mathbf{y}_i$ para $i = 1, \ldots, r$.
Por consiguiente para todo i, $1 \leq i \leq r$, $\mathbf{e}_i - \mathbf{1} \in \mathfrak{m}_i$ y $\mathbf{e}_i \in \mathfrak{m}_j$ para todo $j \neq i$ además si $\boldsymbol{a} = \sum_{i=1}^{r} \boldsymbol{a}_i\mathbf{e}_i$ entonces

$$\boldsymbol{a} + \mathfrak{m}_j = \sum_{i=1}^{r} \boldsymbol{a}_i\mathbf{e}_i + \mathfrak{m}_j = \boldsymbol{a}_j\mathbf{e}_j + \mathfrak{m}_j = \boldsymbol{a}_j + \mathfrak{m}_j.$$

En consecuencia, φ es sobreyectiva y R es un producto de cuerpos.
$\Leftarrow$: Si $R = K_1 \times \cdots \times K_r$, entonces por el Lema 1.2.6, $\mathrm{Max}(R) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ donde $\mathfrak{m}_i = \{\boldsymbol{a} \in R : a(i) = 0\}$. Luego, $\mathcal{J}(R) = \{\mathbf{0}\}$. ■

Ejemplo 1.3.25 *Sea* $R = \mathcal{C}([0,1], \mathbb{R})$ *y consideremos* $x \in [0,1]$. *En consecuencia,* $\mathfrak{m}_x = \{f \in R : f(x) = 0\}$ *es un ideal maximal,* $\bigcap_{x\in[0,1]} \mathfrak{m}_x = \{0\}$ *y como* $\mathcal{J}(R) \subset \bigcap_{x\in[0,1]} \mathfrak{m}_x$ *entonces* $\mathcal{J}(R) = \{0\}$. *Pero* R *no es un producto de cuerpos.*

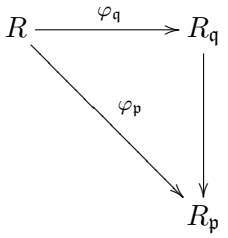
1.4. $\beta-$Anillos.

Si $R = K^I$ con K un cuerpo e I un conjunto finito entonces, por el Corolario 1.3.7, R es producto de sus localizados. Para un anillo general R no es cierto este resultado. Podemos plantearnos generalizar la noción de anillo producto directo de anillos locales, por anillo que es límite proyectivo de sus localizados.

Sea R un anillo. Para todo $\mathfrak{p} \in \mathrm{Spec}(R)$ consideramos el morfismo

$$\begin{array}{rccc} \varphi_{\mathfrak{p}}: & R & \to & R_{\mathfrak{p}} \\ & a & \mapsto & \frac{a}{1} \end{array}.$$

Si $\mathfrak{p} \subset \mathfrak{q}$, el diagrama



es conmutativo. En consecuencia, si construimos el límite proyectivo

$$\varprojlim_{\mathfrak{p}\subset\mathfrak{q}} (R_{\mathfrak{p}}, f_{\mathfrak{q}\mathfrak{p}})_{\mathfrak{p},\mathfrak{q}\in\mathrm{Spec}(R)}$$

existe un homomorfismo canónico

$$\varphi : R \to \varprojlim_{\mathfrak{p}\subset\mathfrak{q}} (R_{\mathfrak{p}}, f_{\mathfrak{q}\mathfrak{p}})_{\mathfrak{p},\mathfrak{q}\in\mathrm{Spec}(R)}$$

donde $\varphi(a) = (\frac{a}{1})_{\mathfrak{p}\in\mathrm{Spec}(R)}$.

Lema 1.4.1 $\mathrm{Ker}(\varphi) \subset \bigcap_{\mathfrak{p}\in\mathrm{Spec}(R)} \mathfrak{p}$ *y en consecuencia si R es reducido, es decir R no tiene elementos nilpotentes, entonces φ es inyectiva.*

Demostración. Sea $a \in \mathrm{Ker}(\varphi)$, $\frac{a}{1} = 0$ en $R_{\mathfrak{p}}$, para todo $\mathfrak{p} \in \mathrm{Spec}(R)$. Esto equivale a que para todo $\mathfrak{p}$, existe $\lambda_{\mathfrak{p}} \notin \mathfrak{p}$ tal que $\lambda_{\mathfrak{p}} a = 0$. Luego $a \in \mathfrak{p}$, para todo $\mathfrak{p} \in \mathrm{Spec}(R)$. Por tanto $a \in \bigcap_{\mathfrak{p}\in\mathrm{Spec}(R)} \mathfrak{p}$. Por otra parte, la intersección de todos los ideales primos de R es el nilradical de R y R no tiene elementos nilpotentes entonces $a = 0$ y φ es inyectiva. ■

El recíproco del Lema 1.4.1, no es cierto y lo veremos en el Ejemplo 1.4.4.

Definición 1.4.2 *R es un $\beta-$anillo si y sólo si φ es un isomorfismo.*

En la tesis doctoral de E. Fernández Bermejo, [7], se utiliza la propiedad característica de los $\beta-$anillos para extender resultados de grupos clásicos en módulos libres sobre anillos locales a propiedades de módulos libres sobre $\beta-$anillos.

Lema 1.4.3 *Si R es un anillo local entonces*

$$R = \varprojlim (R_{\mathfrak{p}}, f_{\mathfrak{q}\mathfrak{p}})_{\substack{\mathfrak{p},\mathfrak{q}\in \mathrm{Spec}(R) \\ \mathfrak{p}\subset\mathfrak{q}}}$$

y R es $\beta-$anillo.

Demostración. Sea $\mathfrak{m}$ el ideal maximal del anillo R. Entonces para todo $\mathfrak{p} \in \mathrm{Spec}(R)$, $\mathfrak{p} \subset \mathfrak{m}$ pues todo ideal primo de R está contenido en el maximal $\mathfrak{m}$. Por tanto

$$\varprojlim (R_{\mathfrak{p}})_{\mathfrak{p}\in \mathrm{Spec}(R)} = R_{\mathfrak{m}}.$$

Pero $R_{\mathfrak{m}} = R$ ya que $R_{\mathfrak{m}} = S^{-1}R$ donde S es el complementario del ideal maximal, que en el anillo local R coinciden con los elementos inversibles.
En consecuencia,

$$R = R_{\mathfrak{m}} = \varprojlim (R_{\mathfrak{p}})_{\mathfrak{p}\in \mathrm{Spec}(R)},$$

φ es el homomorfismo identidad y R es $\beta-$anillo. ■

Ejemplo 1.4.4 (Un $\beta-$anillo con elementos nilpotentes)
Consideremos el anillo local $R = \mathbb{Z}/(4)$ con ideal maximal $\mathfrak{m} = (2)$ y con conjunto de elementos inversibles $S = \{1, 3\}$. Entonces, por el Lema 1.4.3, R es $\beta-$anillo.
Por otra parte, este ejemplo muestra que el recíproco del Lema 1.4.1 no se cumple pues

$$\varphi : R \to \varprojlim (R_{\mathfrak{p}})_{\mathfrak{p}\in \mathrm{Spec}(R)}$$

es inyectiva ya que φ es el homomorfismo identidad y R tiene elementos nilpotentes.

Proposición 1.4.5 (Significado de la definición de $\beta-$anillo) *R es un $\beta-$anillo si y sólo si para toda familia de elementos $\left\{ \frac{f_{\mathfrak{p}}}{g_{\mathfrak{p}}} \in R_{\mathfrak{p}} \right\}_{\mathfrak{p}\in \mathrm{Spec}(R)}$ tal que si $\mathfrak{p} \subset \mathfrak{q}$, $\frac{f_{\mathfrak{p}}}{g_{\mathfrak{p}}} = \frac{f_{\mathfrak{q}}}{g_{\mathfrak{q}}}$ en $R_{\mathfrak{p}}$, existe un único $a \in R$ con $\frac{a}{1} = \frac{f_{\mathfrak{p}}}{g_{\mathfrak{p}}}$ para todo $\mathfrak{p} \in \mathrm{Spec}(R)$.*

Demostración. Se sigue de la definición de límite proyectivo. ■

La idea intuitiva de la definición de $\beta-$anillo es la siguiente: los elementos de $R_{\mathfrak{p}}$ son "funciones que pertenecen localmente a R en el punto $\mathfrak{p}$", los elementos de $\varprojlim R_{\mathfrak{p}}$ son funciones que "localmente" están en R para todo $\mathfrak{p} \in \mathrm{Spec}(R)$. Entonces R es un $\beta-$anillo si toda función que localmente está en R, para todo $\mathfrak{p} \in \mathrm{Spec}(R)$, es un elemento de R.

Vamos a mostrar que si R es un dominio entonces R es un $\beta-$anillo pero necesitamos de la proposición siguiente.

Proposición 1.4.6 *Sea R un dominio. Si identificamos R y sus anillos cocientes con sus imágenes en el cuerpo de fracciones entonces*

$$R = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}}.$$

Demostración. $R \subset \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}}$ ya que si $a \in R$, $\frac{a}{1} \in R_{\mathfrak{p}}$, para todo $\mathfrak{p} \in \mathrm{Spec}(R)$. Para la otra contención sea $a \in \bigcap_{\mathfrak{p}\in \mathrm{Spec}\ R} R_{\mathfrak{p}}$. Definimos

$$I_a = \{x \in R : ax \in R\}.$$

Es claro que I_a es un ideal de R y note que $a \in R$ si y sólo si $1 \in I_a$. Veamos que $1 \in I_a$ si y sólo si I_a no es un ideal propio de R. En efecto, si $1 \in I_a$ entonces $I_a = R$ y recíprocamente, si I_a es propio, existe $\mathfrak{p} \in \mathrm{Spec}(R)$ tal que $I_a \subset \mathfrak{p}$, como $a \in R_{\mathfrak{p}}$ entonces $a = \frac{x}{y}$ con $y \notin \mathfrak{p}$ luego $ay = x$ y en consecuencia $y \in I_a \subset \mathfrak{p}$ lo cual es absurdo. Así, $a \in R$ y $R = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}}$. ■

Proposición 1.4.7 *Si R es un dominio, entonces R es un $\beta-$anillo.*

Demostración. Por la Proposición 1.4.6,

$$R = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}}.$$

Por otra parte, para todo $\mathfrak{p} \in \mathrm{Spec}(R)$, $R_{\mathfrak{p}}$ es subconjunto de $K(R)$, el cuerpo de fracciones de R. Además, $K(R)$ es el localizado de R en el ideal primo (0) y $\{f_{\mathfrak{q}\mathfrak{p}} : R_{\mathfrak{q}} \to R_{\mathfrak{p}}\}$ son las inclusiones entonces el límite proyectivo es

$$\varprojlim (R_{\mathfrak{p}}, f_{\mathfrak{q}\mathfrak{p}})_{\mathfrak{p},\mathfrak{q}\in \mathrm{Spec}(R)}^{\mathfrak{p}\subset\mathfrak{q}} = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}} = R.$$

En consecuencia, φ es el homomorfismo identidad y R es un $\beta-$anillo. ■

Ejemplo 1.4.8 *De acuerdo a la Proposición 1.4.7, si K es un cuerpo entonces el anillo de polinomios $K[x_1, \ldots, x_n]$ es un $\beta-$anillo pues $K[x_1, \ldots, x_n]$ es un dominio.*

Teorema 1.4.9 *Si K es un cuerpo e I es finito, entonces $R = K^I$ es un $\beta-$anillo.*

Demostración. Por el Corolario 1.3.7, $R = K^I$ es un anillo en el que todos sus ideales primos son maximales, por tanto no hay morfismos entre los localizados, luego el límite

proyectivo es el producto de éstos. Es decir

$$\varprojlim(R_{\mathfrak{p}})_{\mathfrak{p}\in \mathrm{Spec}(R)} = \prod_{\mathfrak{m}\in \mathrm{Max}(R)} R_{\mathfrak{m}}.$$

Además, también por el Corolario 1.3.7, para todo $\mathfrak{m} \in \mathrm{Max}(R)$ se tiene que $R_{\mathfrak{m}} \simeq K$ entonces

$$\varprojlim(R_{\mathfrak{p}})_{\mathfrak{p}\in \mathrm{Spec}(R)} = \prod_{\mathfrak{m}\in \mathrm{Max}(R)} R_{\mathfrak{m}} \simeq R.$$

Por tanto, φ es el homomorfismo identidad y R es $\beta-$anillo. ■

Note que si I es infinito, la aplicación $\delta : I \to \mathrm{Max}(R)$ dada por $\delta(i) = \mathfrak{m}_i$ es inyectiva pero no sobre ya que $\#(I) << \#(\mathrm{Max}(R)) = 2^{2^{\#(I)}}$. Luego el cardinal del conjunto de los ideales maximales de $R = K^I$ con I finito y de $\overline{R} = K^J$ con J infinito se comparan como $\#(\mathrm{Max}(R)) << \#(\mathrm{Max}(\overline{R}))$. Por tanto, en el caso en el que J es infinito, $\overline{R} = K^J$ no puede ser un $\beta-$anillo. En la siguiente sección vamos a generalizar este resultado.

1.4.1. Componentes grafoconexas.

Sean I un conjunto arbitrario y $\Delta \subset I \times I$. En lo que sigue diremos que $\{C_j, f_{ij}\}_{\substack{j\in I \\ (i,j)\in\Delta}}$ es un diagrama en una categoría $\mathcal{C}$ si está compuesto por

(i) una familia de objetos $\{C_j\}_{j\in I}$ de $\mathcal{C}$ y

(ii) una familia de morfismos de $\mathcal{C}$, $\{f_{ij} : C_i \to C_j\}_{(i,j)\in\Delta}$.

Sea X un conjunto. Todo subconjunto Δ de $X \times X$ induce una relación de equivalencia en X mediante el proceso siguiente de construcción de relaciones

$$\begin{aligned}
R_1 :&\quad aR_1b \;\Leftrightarrow\; (a,b) \in \Delta \text{ o } a = b\\
R_2 :&\quad aR_2b \;\Leftrightarrow\; aR_1b \text{ o } bR_1a\\
R :&\quad aRb \;\Leftrightarrow\; \exists a_1, \ldots, a_t \in X \text{ tales que } aR_2a_1R_2 \ldots R_2a_tR_2b.
\end{aligned}$$

La relación R_1 es reflexiva, R_2 es reflexiva y simétrica, y R es una relación de equivalencia llamada *relación de equivalencia asociada a* Δ. Además R es la mínima relación de equivalencia en X que contiene a Δ es decir para toda Q relación de equivalencia de X tal que $\Delta \subset Q$, se tiene que $R \subset Q$.

Definición 1.4.10 *Si* $D = \{C_j, f_{ij}\}_{\substack{j\in I \\ (i,j)\in\Delta}}$ *es un diagrama en* $\mathcal{C}$ *entonces*

(1) Llamamos componente grafoconexa de I *a cada elemento de* $I/R = \{I_\alpha\}_{\alpha\in T}$ *donde* R *es la relación de equivalencia asociada a* Δ.

(2) Para toda I_α componente grafoconexa de I, llamamos componente grafoconexa del diagrama D a $D_\alpha = \{C_j, f_{ij}\}_{\substack{j\in I_\alpha \\ (i,j)\in\Delta_\alpha}}$ con $\Delta_\alpha = \Delta \cap (I_\alpha \times I_\alpha)$.

Observe que si $\Delta_\alpha = \Delta \cap (I_\alpha \times I_\alpha)$ entonces

(i) Para todos $\alpha, \beta \in T$, $\alpha \neq \beta$, $\Delta_\alpha \cap \Delta_\beta = \emptyset$.

(ii) $\Delta = \amalg_{\alpha\in T}\Delta_\alpha$.

(iii) Como $\Delta = \amalg_{\alpha\in T}\Delta_\alpha$, $(i,j) \in \Delta$ si y sólo si existe α único tal que $i, j \in I_\alpha$.

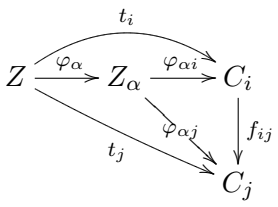
Proposición 1.4.11 *Sean $I = \amalg_{\alpha\in T} I_\alpha$ una partición de I y $\Delta \subset I \times I$ un subconjunto tal que $\Delta = \amalg_{\alpha\in T}\Delta\cap(I_\alpha \times I_\alpha)$. En la categoría $\mathcal{C}$ dado un diagrama $D = \{C_j, f_{ij}\}_{\substack{j\in I \\ (i,j)\in\Delta}}$, si $D_\alpha = \{C_j, f_{ij}\}_{\substack{j\in I_\alpha \\ (i,j)\in\Delta_\alpha}}$ con $\Delta_\alpha = \Delta \cap (I_\alpha \times I_\alpha)$ entonces*

$$\varprojlim D = \prod_{\alpha\in T} \varprojlim D_\alpha.$$

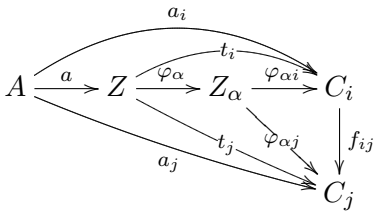
Demostración. Para todo $\alpha \in T$, llamamos

$$(Z_\alpha, \varphi_{\alpha j}) := \varprojlim D_\alpha, \quad \varphi_{\alpha j} : Z_\alpha \to C_j, \ \forall j \in I_\alpha$$

Entonces, para todo A y toda familia de morfismos $a_j : A \to C_j$, $j \in I_\alpha$, tales que para todo $(i,j) \in \Delta_\alpha$, $f_{ij} \circ a_i = a_j$, existe $\delta_\alpha : A \to Z_\alpha$ único tal que $a_j = \varphi_{\alpha j} \circ \delta_\alpha$.
Definimos $Z = \prod_{\alpha\in T} Z_\alpha$ y $\varphi_\alpha : Z \to Z_\alpha$ a la proyección. Entonces para todo A y para toda familia de morfismos $\delta_\alpha : A \to Z_\alpha$, $\alpha \in T$, existe $a : A \to Z$ único tal que $\varphi_\alpha \circ a = \delta_\alpha$, para todo $\alpha \in T$.
Vamos a probar que Z cumple la propiedad universal del límite proyectivo.
(1) Existen los morfismos $t_j : Z \to C_j$, para todo $j \in I$, ya que existe $\alpha \in T$ único con $j \in I_\alpha$ y existe el morfismo proyección sobre la componente α, $\varphi_\alpha : Z \to Z_\alpha$ y puesto que $j \in I_\alpha$ existe el morfismo del límite $\varphi_{\alpha j} : Z_\alpha \to C_j$. Por tanto, podemos construir $t_j : Z \to C_j$ por $t_j = \varphi_{\alpha j} \circ \varphi_\alpha$ para todo $j \in I_\alpha$.
(2) Para todo $(i,j) \in \Delta$, $f_{ij} \circ t_i = t_j$. En efecto, si $(i,j) \in \Delta$, existe α único tal que $(i,j) \in \Delta_\alpha$ y si consideramos el diagrama



Entonces, $f_{ij} \circ t_i = f_{ij} \circ (\varphi_{\alpha i} \circ \varphi_\alpha) = (f_{ij} \circ \varphi_{\alpha i}) \circ \varphi_\alpha = \varphi_{\alpha j} \circ \varphi_\alpha = t_j$.
(3) Para todo A y toda familia de morfismos $a_j : A \to C_j$ de manera que para todo $(i,j) \in \Delta$, $f_{ij} \circ a_i = a_j$ existe un único morfismo a de A en Z tal que $t_j \circ a = a_j$, para todo $j \in I_\alpha$.
En efecto, fijamos $\alpha \in T$. Tomando la familia de morfismos $a_j : A \to C_j$, para todo $j \in I_\alpha$ y puesto que para todo $(i,j) \in \Delta \cap (I_\alpha \times I_\alpha)$, $f_{ij} \circ a_i = a_j$ entonces existe $\delta_\alpha : A \to Z_\alpha$ con $\varphi_{\alpha j} \circ \delta_\alpha = a_j$, para todo $j \in I_\alpha$. Teniendo la familia de morfismos $\delta_\alpha : A \to Z_\alpha$, para todo $\alpha \in T$, existe $a : A \to Z$ tal que $\varphi_\alpha \circ a = \delta_\alpha$, para todo $\alpha \in T$. Además,



Entonces, $t_j \circ a = (\varphi_{\alpha j} \circ \varphi_\alpha) \circ a = \varphi_{\alpha j} \circ (\varphi_\alpha \circ a) = \varphi_{\alpha j} \circ \delta_\alpha = a_j,\ \forall j \in I_\alpha$.
Veamos que a es único con esta propiedad. Supongamos que b verifica la misma condición, es decir para todo $j \in I$, $t_j \circ a = a_j$ y $t_j \circ b = a_j$. Como $j \in I_\alpha$, para algún $\alpha \in T$, entonces $t_j \circ a = \varphi_{\alpha j} \circ \varphi_\alpha \circ a$ y $t_j \circ b = \varphi_{\alpha j} \circ \varphi_\alpha \circ b$. Luego

$$\varphi_{\alpha j} \circ \varphi_\alpha \circ a = \varphi_{\alpha j} \circ \varphi_\alpha \circ b,\ \forall j \in I_\alpha.$$

Por la unicidad de δ_α tal que $a_j = \varphi_{\alpha j} \circ \delta_\alpha$, para todo $j \in I_\alpha$, tenemos que $\varphi_\alpha \circ a = \varphi_\alpha \circ b$ para todo $\alpha \in T$, y por tanto, $a = b$. ■

En consecuencia, si $D = \{C_j, f_{ij}\}_{\substack{j \in I \\ (i,j) \in \Delta}}$ es un diagrama y $\{D_\alpha\}_{\alpha \in T}$ es la familia de componentes grafoconexas asociadas a Δ entonces

$$\varprojlim D = \prod_{\alpha \in T} \varprojlim D_\alpha.$$

Observación 1.4.12 *Podemos pensar que al tomar una descomposición del conjunto de índices, que no verifique la hipótesis de la Proposición 1.4.11 se obtiene el mismo resultado. Esto no es cierto en general, por ejemplo sean A, B, C conjuntos, y $f : A \to B$ y $g : C \to B$ dos aplicaciones con el mismo rango. Además consideremos el diagrama $A \xrightarrow{f} B \xleftarrow{g} C$. El límite proyectivo del primero es A, el límite del segundo es C y el límite de $\{A, C\}$ es $A \times C$. Pero el límite del diagrama $A \xrightarrow{f} B \xleftarrow{g} C$ es el producto fibrado*

$$A \times_B C = \{(a,c) \in A \times C : f(a) = g(c)\} \neq A \times C.$$

Si R es un anillo, trasladando a $\mathrm{Spec}(R)$ las notaciones iniciales de esta sección tomamos en $\mathrm{Spec}(R)\times\mathrm{Spec}(R)$ a $\Delta = \{(\mathfrak{p},\mathfrak{q}) \in \mathrm{Spec}(R)\times\mathrm{Spec}(R) : \mathfrak{p}\subset\mathfrak{q}\}$ y la relación de equivalencia asociada a Δ. Sea $\{G_\alpha\}_{\alpha\in T}$ el conjunto de componentes grafoconexas de $\mathrm{Spec}(R)$. El diagrama $D = \{R_\mathfrak{q}, f_{\mathfrak{pq}}\}_{\mathfrak{p},\mathfrak{q}\in\mathrm{Spec}(R)}$ se descompone en sus componentes grafoconexas $\{D_\alpha\}_{\alpha\in T}$ donde $D_\alpha = \{R_\mathfrak{q}, f_{\mathfrak{pq}}\}_{\substack{\mathfrak{p},\mathfrak{q}\in G_\alpha\\ \mathfrak{p}\subset\mathfrak{q}}}$.

Por la Proposición 1.4.11,

$$\text{si}\quad R_\alpha = \varprojlim D_\alpha \quad \text{entonces} \quad \varprojlim D = \prod_{\alpha\in T} R_\alpha.$$

Los morfismos

$$\left\{ \begin{array}{ccc} R & \to & R_\mathfrak{q} \\ a & \mapsto & \frac{a}{1} \end{array} \right\}_{\mathfrak{q}\in G_\alpha}$$

inducen homomorfismos $\varphi_\alpha : R \to R_\alpha$ para todo $\alpha\in T$. Entonces, R es un $\beta-$anillo si el morfismo $\varphi : R \to \prod_{\alpha\in T} R_\alpha$ inducido por los φ_α es un isomorfismo.

Lema 1.4.13 *Si $R_1,\ldots,R_n$ son $\beta-$anillos, entonces $R = R_1\times\cdots\times R_n$ es un $\beta-$anillo. En particular el producto finito de anillos locales y el producto finito de dominios enteros son $\beta-$anillos.*

Demostración. Por el Lema 1.2.6(7),

$$\mathrm{Spec}(R) \simeq \coprod_{i=1}^{n} \mathrm{Spec}(R_i).$$

Por tanto, si $M_\mathfrak{p}$ y $M_\mathfrak{q}$ son ideales primos de R tales que $M_\mathfrak{p}\subset M_\mathfrak{q}$ entonces existe i único tal que $\mathfrak{p},\mathfrak{q}\in \mathit{Spec}(R_i)$ y $\mathfrak{p}\subset\mathfrak{q}$. Luego, por la Proposición 1.4.11 y como $R_1,\ldots,R_n$ son $\beta-$anillos, entonces

$$\varprojlim\{R_{M_\mathfrak{q}}\}_{M_\mathfrak{q}\in\mathrm{Spec}(R)} = \prod_{i=1}^{n} \varprojlim\{(R_i)_\mathfrak{q}\}_{\mathfrak{q}\in\mathrm{Spec}(R_i)} = \prod_{i=1}^{n} R_i = R.$$

En consecuencia, φ es el morfismo identidad y $R = R_1\times\cdots\times R_n$ es un $\beta-$anillo. ■

Observe que el Lema 1.4.13 no se cumple si cambiamos el producto finito por infinito pues en este caso aparecen ideales primos descritos en el Lema 1.2.6(9).

Proposición 1.4.14 *Si R es $\beta-$anillo entonces* $\mathrm{Spec}(R)$ *tiene un número finito de componentes grafoconexas.*

Para la demostración de la Proposición 1.4.14 necesitamos el siguiente lema.

Lema 1.4.15 *Si R es un $\beta-$anillo y $\mathfrak{m}$ es un ideal maximal de R, entonces existe α único con $\mathfrak{m} \in G_\alpha$ tal que*

$$\varphi_\alpha(\mathfrak{m}) = \{(\frac{a}{1})_{\mathfrak{p}\in G_\alpha} : a \in \mathfrak{m}\}$$

es un ideal propio de R_α.

Demostración. Como φ_α es el morfismo proyección, $\varphi_\alpha(\mathfrak{m}) = \{(\frac{a}{1})_{\mathfrak{p}\in G_\alpha} : a \in \mathfrak{m}\}$ es ideal de R_α. Además, $\varphi_\alpha(\mathfrak{m})$ es un ideal propio porque si $(1)_{\mathfrak{p}\in G_\alpha} \in \varphi_\alpha(\mathfrak{m})$ entonces existe $a \in \mathfrak{m}$ tal que

$$(1)_{\mathfrak{p}\in G_\alpha} = (\frac{a}{1})_{\mathfrak{p}\in G_\alpha}$$

y como $\mathfrak{m} \in G_\alpha$, en particular, $1 = \frac{a}{1}$ en $R_\mathfrak{m}$. Luego existe $\lambda \notin \mathfrak{m}$ tal que $\lambda(1-a) = 0$, pero $0 \in \mathfrak{m}$ entonces $(1-a) \in \mathfrak{m}$ y por tanto $1 \in \mathfrak{m}$ ya que $a \in \mathfrak{m}$ y esto es absurdo. ■

Demostración. (de la Proposición 1.4.14) Sea T infinito, por el Lema 1.2.6(9), existe M ideal maximal de $\prod_{\alpha\in T} R_\alpha$ tal que $\varphi_\alpha(M) = R_\alpha$ para todo $\alpha \in T$. Pero esto es absurdo pues en el Lema 1.4.15 se probó que existe un α tal que $\varphi_\alpha(M)$ es un ideal propio de R_α. En consecuencia si R es $\beta-$anillo, entonces $\mathrm{Spec}(R)$ tiene un número finito de componentes grafoconexas. ■

Como consecuencia de la Proposición 1.4.14 los anillos de funciones continuas $\mathcal{C}(X, \mathbb{R})$ con X abierto de $\mathbb{R}^n$ no son $\beta-$anillos.

1.4.2. Relación entre las componentes grafoconexas, irreducibles y conexas de $\mathrm{Spec}(R)$.

Recordemos que

Definición 1.4.16 *Si X es un espacio topológico,*

(1) una componente conexa de X es un subconjunto conexo maximal de X.

(2) una componente irreducible de X es un subconjunto irreducible maximal de X.

Es conocido que las componentes irreducibles de $\mathrm{Spec}(R)$ se corresponden con los ideales primos minimales.

Proposición 1.4.17 *Si R es un anillo reducido y $\mathrm{Spec}(R)$ tiene un número finito de componentes irreducibles, entonces son equivalentes:*

(1) Las componentes irreducibles de $\mathrm{Spec}(R)$ son abiertas.

(2) Las componentes conexas, grafoconexas e irreducibles de $\mathrm{Spec}(R)$ coinciden.

(3) Las componentes irreducibles de $\mathrm{Spec}(R)$ *coinciden con las componentes grafoconexas.*

(4) $R = \prod_{i=1}^{r} R_i$*, con* R_i *dominio, para todo* i*.*

En consecuencia, un anillo R *que satisface una de estas propiedades es un* $\beta-$*anillo por la Proposición 1.4.13.*

Demostración. Para todo $\mathfrak{p} \in \mathrm{Spec}(R)$, llamamos $I_\mathfrak{p}$, $G_\mathfrak{p}$ y $C_\mathfrak{p}$ a las componentes irreducibles, grafoconexas y conexas respectivamente de $\mathfrak{p}$.
(1) $\Rightarrow$ (2): Veamos primero que $I_\mathfrak{p} = C_\mathfrak{p}$ para todo $\mathfrak{p} \in \mathrm{Spec}(R)$. Si $I_\mathfrak{p}$ es no conexo, entonces existen abiertos U y V de $X = \mathrm{Spec}(R)$ tales que

$$(U \cap I_\mathfrak{p}) \cup (V \cap I_\mathfrak{p}) = I_\mathfrak{p} \text{ y } (U \cap I_\mathfrak{p}) \cap (V \cap I_\mathfrak{p}) = \emptyset.$$

Además, como $I_\mathfrak{p}$ es abierto de X, $U' = U \cap I_\mathfrak{p}$ y $V' = V \cap I_\mathfrak{p}$ son abiertos de X. Por tanto, $X - U'$ y $X - V'$ son cerrados además como $I_\mathfrak{p}$ es cerrado, $(X - U') \cap I_\mathfrak{p}$ y $(X - V') \cap I_\mathfrak{p}$ son cerrados de X tales que

$$((X - U') \cap I_\mathfrak{p}) \cup ((X - V') \cap I_\mathfrak{p}) = (X - (U' \cap V')) \cap I_\mathfrak{p} = X \cap I_\mathfrak{p} = I_\mathfrak{p}$$

y

$$((X - U') \cap I_\mathfrak{p}) \cap ((X - V') \cap I_\mathfrak{p}) = (X - (U' \cup V')) \cap I_\mathfrak{p} = \emptyset.$$

Esto contradice la irreducibilidad de $I_\mathfrak{p}$. Luego $I_\mathfrak{p}$ es conexo y $I_\mathfrak{p} \subset C_\mathfrak{p}$.
Antes de probar que $C_\mathfrak{p}$ es irreducible para todo $\mathfrak{p} \in \mathrm{Spec}(R)$, veamos que

$$I_\mathfrak{p} \cap I_\mathfrak{q} = \emptyset \text{ si } I_\mathfrak{p} \neq I_\mathfrak{q}.$$

En efecto, supongamos que $I_\mathfrak{p} \cap I_\mathfrak{q} \neq \emptyset$ con $I_\mathfrak{p} \neq I_\mathfrak{q}$. Puesto que $I_\mathfrak{q}$ es abierto entonces $I_\mathfrak{p} - I_\mathfrak{q}$ es cerrado y como $I_\mathfrak{p} \neq I_\mathfrak{q}$, $I_\mathfrak{p} - I_\mathfrak{q}$ es no vacío. Además, $I_\mathfrak{p} \cap I_\mathfrak{q}$ es cerrado, luego $I_\mathfrak{p} = (I_\mathfrak{p} \cap I_\mathfrak{q}) \cup (I_\mathfrak{p} - I_\mathfrak{q})$ es la unión de los cerrados propios. Esto contradice la irreducibilidad de $I_\mathfrak{p}$.
Si $I_\mathfrak{p} \subsetneq C_\mathfrak{p}$ entonces $C_\mathfrak{p}$ es la unión de abiertos disjuntos $I_\mathfrak{q} \cap C_\mathfrak{p}$, $\mathfrak{q} \in \mathrm{Spec}(R)$. Es decir,

$$C_\mathfrak{p} = \bigcup_{\mathfrak{q} \in \mathrm{Spec}(R)} (I_\mathfrak{q} \cap C_\mathfrak{p}) \tag{1.2}$$

donde ninguno de los conjuntos $I_\mathfrak{q} \cap C_\mathfrak{p}$ coincide con $C_\mathfrak{p}$ porque $I_\mathfrak{p} \cap C_\mathfrak{p} \neq C_\mathfrak{p}$ y $I_\mathfrak{q} \cap C_\mathfrak{p} \neq C_\mathfrak{p}$ ya que si $I_\mathfrak{q} \cap C_\mathfrak{p} = C_\mathfrak{p}$ entonces $C_\mathfrak{p} \subset I_\mathfrak{q}$ y como $I_\mathfrak{p} \subset C_\mathfrak{p}$ entonces $I_\mathfrak{p} \subset I_\mathfrak{q}$ es decir $I_\mathfrak{p} \cap I_\mathfrak{q} \neq \emptyset$ lo cual es absurdo. Pero la Ecuación (1.2) contradice la conexidad de $C_\mathfrak{p}$,

por tanto $I_{\mathfrak{p}} = C_{\mathfrak{p}}$ para todo $\mathfrak{p} \in \operatorname{Spec}(R)$.
Por último veamos que $I_{\mathfrak{p}} = G_{\mathfrak{p}}$ para todo $\mathfrak{p} \in \operatorname{Spec}(R)$. En efecto, puesto que las componentes irreducibles de $\operatorname{Spec}(R)$ son los cierres de primos minimales entonces sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ los primos minimales y $I_{\mathfrak{p}_1}, \ldots, I_{\mathfrak{p}_r}$ sus componentes irreducibles. Note que $I_{\mathfrak{p}_i}$, para $i = 1, \ldots, r$, es una componente grafoconexa ya que $I_{\mathfrak{p}} \cap I_{\mathfrak{q}} = \emptyset$ si $I_{\mathfrak{p}} \neq I_{\mathfrak{q}}$ y si $\mathfrak{p}, \mathfrak{q} \in I_{\mathfrak{p}_i}$ entonces $\mathfrak{p}_i \subset \mathfrak{p}$ o $\mathfrak{p}_i \subset \mathfrak{q}$. Además, $I_{\mathfrak{p}_i} = G_{\mathfrak{p}_i}$ porque de lo contrario existe $\mathfrak{p} \in G_{\mathfrak{p}_i}$ y $\mathfrak{p} \notin I_{\mathfrak{p}_i}$. Como $\mathfrak{p} \notin I_{\mathfrak{p}_i}$, existe j tal que $\mathfrak{p} \in I_{\mathfrak{p}_j}$ y $I_{\mathfrak{p}_j} \subset G_{\mathfrak{p}_j}$ entonces $\mathfrak{p} \in G_{\mathfrak{p}_i} \cap G_{\mathfrak{p}_j}$ y esto es absurdo pues las componentes grafoconexas son disjuntas.
(2) ⇒ (3) Es inmediata.
(3) ⇒ (1) Por hipótesis, $I_{\mathfrak{p}} = G_{\mathfrak{p}}$ para todo $\mathfrak{p} \in \operatorname{Spec}(R)$ y como las componentes grafoconexas son disjuntas $G_{\mathfrak{p}} \neq G_{\mathfrak{q}}$, entonces $I_{\mathfrak{p}} \cap I_{\mathfrak{q}} = \emptyset$ si $I_{\mathfrak{p}} \neq I_{\mathfrak{q}}$ y

$$I_{\mathfrak{p}} \bigcap \left(\bigcup_{\mathfrak{q} \in \operatorname{Spec}(R),\ \mathfrak{q} \neq \mathfrak{p}} I_{\mathfrak{q}} \right) = \emptyset.$$

Por tanto, $I_{\mathfrak{p}}$ es abierto pues sólo hay un número finito de componentes irreducibles.
(1) ⇒ (4) Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ los ideales primos minimales de $\operatorname{Spec}(R)$ y $I_{\mathfrak{p}_1}, \ldots, I_{\mathfrak{p}_r}$ las componentes irreducibles. Existe un isomorfismo entre R y el producto de dominios $R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_r$. En efecto,

$$\begin{array}{rccc} \psi: & R & \to & R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_r \\ & a & \mapsto & (a + \mathfrak{p}_1, \ldots, a + \mathfrak{p}_r) \end{array}.$$

Veamos que ψ es inyectiva. Si $a + \mathfrak{p}_i = b + \mathfrak{p}_i$, para todo $i = 1, \ldots, r$, entonces $a - b \in \bigcap_{i=1}^{r} \mathfrak{p}_i$. Puesto que R es reducido, esto es, $\bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p} = \{0\}$ y como $\bigcap_{i=1}^{r} \mathfrak{p}_i = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$ entonces $\bigcap_{i=1}^{r} \mathfrak{p}_i = \{0\}$ luego $a = b$. Para ver que ψ es sobreyectiva basta ver que $(0 + \mathfrak{p}_1, \ldots, 1 + \mathfrak{p}_s, \ldots, 0 + \mathfrak{p}_r) \in \psi(R)$ para todo $s = 1, \ldots, r$. Veamos primero que $\mathfrak{p}_i + \mathfrak{p}_j = R$ para todos i, j. Si $\mathfrak{p}_i + \mathfrak{p}_j \neq R$ entonces existe un maximal $\mathfrak{m}$ tal que $\mathfrak{p}_i + \mathfrak{p}_j \subset \mathfrak{m}$ luego $\mathfrak{p}_i \subset \mathfrak{m}$ y $\mathfrak{p}_j \subset \mathfrak{m}$, es decir $\mathfrak{m} \in I_{\mathfrak{p}_i} \cap I_{\mathfrak{p}_j}$ y esto es absurdo si $\mathfrak{p}_i \neq \mathfrak{p}_j$ porque $I_{\mathfrak{p}_i} \cap I_{\mathfrak{p}_j} = G_{\mathfrak{p}_i} \cap G_{\mathfrak{p}_j} = \emptyset$.
Ahora, como $\mathfrak{p}_i + \mathfrak{p}_j = R$ para todos i, j, con $i < j$, entonces existen α_{ij}, β_{ij} tales que $\alpha_{ij} + \beta_{ij} = 1$, $\alpha_{ij} \in \mathfrak{p}_i$, $\beta_{ij} \notin \mathfrak{p}_i$, $\alpha_{ij} \notin \mathfrak{p}_j$ y $\beta_{ij} \in \mathfrak{p}_j$. Sea $e_s = \alpha_{1s} \ldots \alpha_{(s-1)s} \beta_{s(s+1)} \ldots \beta_{sr}$ entonces $e_s \in \mathfrak{p}_i$ para todo $i \neq s$ ya que $\alpha_{1s} \in \mathfrak{p}_1, \ldots, \alpha_{(s-1)s} \in \mathfrak{p}_{s-1}, \beta_{s(s+1)} \in \mathfrak{p}_{s+1}, \ldots, \beta_{sr} \in \mathfrak{p}_r$. De esta forma, $\psi(e_s) = (0, \ldots, e_s + \mathfrak{p}_s, \ldots, 0)$. Ahora veamos que $e_s + \mathfrak{p}_s = 1 + \mathfrak{p}_s$. En efecto,

$$e_s = (1 - \beta_{1s}) \cdots (1 - \beta_{(s-1)s})(1 - \alpha_{s(s+1)}) \cdots (1 - \alpha_{sr}) = 1 - f_s$$

donde $f_s \in \mathfrak{p}_s$ ya que en cada término de f_s hay por lo menos un $\beta_{1s}, \ldots, \beta_{(s-1)s}$, $\alpha_{s(s+1)}, \ldots, \alpha_{sr}$ que pertenecen a $\mathfrak{p}_s$. Por tanto, si $a = a_1e_1 + \cdots + a_re_r$ entonces

$$\psi(a) = (a + \mathfrak{p}_1, \ldots, a + \mathfrak{p}_r) = (a_1 + \mathfrak{p}_1, \ldots, a_r + \mathfrak{p}_r)$$

ya que para todo $s = 1, \ldots, r$, $a + \mathfrak{p}_s = a_1e_1 + \cdots + a_re_r + \mathfrak{p}_s = a_se_s + \mathfrak{p}_s = a_s(e_s + \mathfrak{p}_s) = a_s(1 + \mathfrak{p}_s) = a_s + \mathfrak{p}_s$.
(4) ⇒ (1) Puesto que las componentes irreducibles de $\mathrm{Spec}(R)$ son los cierres de ideales primos minimales y por el Lema 1.2.8, los primos minimales de R son de la forma $\mathfrak{m} = \prod_{i=1,\ i\neq j}^{n} \mathfrak{p}_i$ con $\mathfrak{p}_i = R_i$ y $\mathfrak{p}_j = (0)$. Entonces solo falta ver que son abiertas pero esto se tiene pues las componentes irreducibles son cerradas y disjuntas. ■

En la Proposición 1.4.17, la hipótesis de que el anillo R sea reducido es necesaria solo para demostrar *(1) ⇒ (4)*. Por ejemplo si K es un cuerpo, el anillo

$$R = K[[t]]/(t^2) = \{a + bt : a, b \in K\}$$

tiene un único ideal primo minimal y maximal, el ideal generado por (t). En consecuencia R cumple (1) pero no es producto finito de dominios.

1.5. Anillos de Hermite.

Si M es un $R-$módulo libre, toda base $\mathcal{B} = \{\mathbf{u}_i\}_{i\in I}$ de M induce un isomorfismo $M \simeq R^{(I)}$ que asocia a cada $\boldsymbol{a} \in M$ sus coordenadas $(a_i)_{i\in I}$ en la base $\mathcal{B}$.

Definición 1.5.1 *Sean M un $R-$módulo libre y $\mathcal{B} = \{\mathbf{u}_i\}_{i\in I}$ una base de M. Definimos a $I(\boldsymbol{a})$ como el ideal de R generado por las "coordenadas" de $\boldsymbol{a}$ en $\mathcal{B}$. Es decir, si $\boldsymbol{a} = \sum_{i\in I} a_i\mathbf{u}_i$, entonces $I(\boldsymbol{a}) = (\{a_i\}_{i\in I})R = (\{a_i\}_{i\in I})$.*

Proposición 1.5.2 *$I(\boldsymbol{a})$ es independiente de la base $\mathcal{B}$ elegida.*

Demostración. Sea $\mathcal{B}' = \{\mathbf{v}_i\}_{i\in I}$ otra base de M. Entonces $\mathbf{v}_i = \sum_{j\in I} c_{ij}\mathbf{u}_j$ donde $\#(j : c_{ij} \neq 0) < \infty$ para todo i. Luego

$$\boldsymbol{a} = \sum_{i\in I} b_i\mathbf{v}_i = \sum_{i\in I} b_i \sum_{j\in I} c_{ij}\mathbf{u}_j = \sum_{j\in I} \left(\sum_{i\in I} c_{ij}b_i \right) \mathbf{u}_j.$$

Además, como $\boldsymbol{a} = \sum_{j\in I} a_j\mathbf{u}_j$, entonces $a_j = \sum_{i\in I} c_{ij}b_i$ y $(\{a_j\}_{j\in I}) \subset (\{b_i\}_{i\in I})$. Por simetría en la prueba tenemos que $(\{b_i\}_{i\in I}) \subset (\{a_j\}_{j\in I})$ y por tanto $(\{a_j\}_{j\in I}) = (\{b_i\}_{i\in I})$. ■

Definición 1.5.3 *Sea M un $R-$módulo libre de rango finito.*

(1) *Un elemento* $\boldsymbol{a} \in M$ *se dice unimodular si* $I(\boldsymbol{a}) = R$.

(2) *Un elemento* $\boldsymbol{a} \in M$ *se llama complementable si existe una base de* M *que contiene a* $\boldsymbol{a}$.

(3) *Un anillo* R *se llama anillo de Hermite si para todo* M, $R-$*módulo libre de rango finito, todo elemento unimodular es complementable.*

Observación 1.5.4 *Sea* $M = R^n$.

(1) *Un vector fila* $(a_1, \ldots, a_n) \in R^n$ *es unimodular si y sólo si existen* $\lambda_1, \ldots, \lambda_n \in R$ *tales que* $\lambda_1 a_1 + \cdots + \lambda_n a_n = 1$.

(2) *Un elemento* $(a_1, \ldots, a_n) \in R^n$ *es complementable si y sólo si existe una matriz* A *de* $n \times n$ *inversible cuya primera fila es* $(a_1, \ldots, a_n)$.

(3) *Un anillo* R *es Hermite si y sólo si todo vector* $(a_1, \ldots, a_n) \in R^n$, *para todo* n, *unimodular es complementable.*

Ejemplo 1.5.5 *Un cuerpo, el dominio* $\mathbb{Z}$ *y el anillo de polinomios* $K[x_1, \ldots, x_n]$, *con* K *cuerpo (Conjetura de la fila unimodular) son ejemplos de anillos de Hermite.*

Ahora veamos un ejemplo de un anillo que no es de Hermite.

Ejemplo 1.5.6 (Una fila unimodular que no es complementable)
Consideremos el anillo de coordenadas de funciones polinómicas reales sobre la 2-esfera real S^2, $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. *Entonces* $(\overline{x}, \overline{y}, \overline{z}) \in R^3$ *es una fila unimodular pues* $\overline{x}\ \overline{x} + \overline{y}\ \overline{y} + \overline{z}\ \overline{z} - 1 = \overline{0}$. *Ahora veamos que* $(\overline{x}, \overline{y}, \overline{z})$ *no es complementable:*
Supongamos que $(\overline{x}, \overline{y}, \overline{z})$ *es complementable es decir que existe* $Q \in GL_3(R)$ *tal que*

$$Q = \begin{pmatrix} \overline{x} & \overline{y} & \overline{z} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Note que $(Q^t)^{-1}Q^t = I_3$ *es por tanto*

$$\begin{pmatrix} ((Q^t)^{-1})_{11} & ((Q^t)^{-1})_{12} & ((Q^t)^{-1})_{13} \\ ((Q^t)^{-1})_{21} & ((Q^t)^{-1})_{22} & ((Q^t)^{-1})_{23} \\ ((Q^t)^{-1})_{31} & ((Q^t)^{-1})_{32} & ((Q^t)^{-1})_{33} \end{pmatrix} \begin{pmatrix} \overline{x} & a_{21} & a_{31} \\ \overline{y} & a_{22} & a_{32} \\ \overline{z} & a_{23} & a_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Entonces, la aplicación

$$\begin{array}{rccl} \phi: & S^2 & \to & \mathbb{R}^3 \\ & p & \mapsto & (((Q^t)^{-1})_{21}(p), ((Q^t)^{-1})_{22}(p), ((Q^t)^{-1})_{23}(p)) \end{array}$$

es un campo vectorial analítico sobre S^2 tal que nunca se anula y esto no es posible por la topología de S^2.

Lema 1.5.7 *Si R es un anillo local, entonces R es un anillo de Hermite.*

Demostración. Sea $\mathfrak{m}$ el ideal maximal de R. Para toda fila unimodular $(a_1, \ldots, a_n) \in R^n$ existen $x_1, \ldots, x_n \in R$ tales que $a_1x_1 + \cdots + a_nx_n = 1$. Entonces el ideal generado por $x_1, \ldots, x_n$ cumple que $(x_1, \ldots, x_n) \nsubseteq \mathfrak{m}$. Esto es, existe i tal que $x_i \notin \mathfrak{m}$. Luego x_i es inversible y existe $x_i^{-1} \in R$ tal que $x_i x_i^{-1} = 1$. En consecuencia existe una matriz con determinante 1,

$$\begin{vmatrix} x_1 & x_2 & \cdots & x_i & \cdots & x_{n-1} & x_n \\ \lambda & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 1 \end{vmatrix} = \lambda x_i = 1$$

$\lambda = x_i^{-1}$ para i impar y $\lambda = -x_i^{-1}$ para i par. Así, R es un anillo de Hermite. ■

Lema 1.5.8 *Sea $\{R_i\}_{i\in I}$ una familia de anillos de Hermite, entonces $R = \prod_{i\in I} R_i$ es un anillo de Hermite.*

Demostración. Consideremos la proyección $i-$ésima, $\pi_i : R \to R_i$. Para toda fila unimodular $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \in R^n$, existen $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in R$ tales que $\boldsymbol{b}_1\boldsymbol{a}_1 + \cdots + \boldsymbol{b}_n\boldsymbol{a}_n = \mathbf{1}$. Aplicando la proyección $i-$ésima, $\pi_i(\boldsymbol{b}_1)\pi_i(\boldsymbol{a}_1) + \cdots + \pi_i(\boldsymbol{b}_n)\pi_i(\boldsymbol{a}_n) = 1$, entonces $(\pi_i(\boldsymbol{a}_1), \ldots, \pi_i(\boldsymbol{a}_n))$ es una fila unimodular para todo $i \in I$. Por otra parte, como R_i es un anillo de Hermite, existe una matriz inversible $M_i = (\alpha_{rs}^i)_{1\le r,s\le n}$ con primera fila $(\pi_i(\boldsymbol{a}_1), \ldots, \pi_i(\boldsymbol{a}_n))$ para todo $i \in I$ por tanto existe $M = (\boldsymbol{\alpha}_{rs})_{1\le r,s\le n}$ inversible con primera fila $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$. En efecto, definiendo $\boldsymbol{\alpha}_{rs}$ como $\pi_i(\boldsymbol{\alpha}_{rs}) = \alpha_{rs}^i$ para todo $i \in I$

y como π_i es un homomorfismo de anillos entonces, para todo $i \in I$,

$$\pi_i\left(\det\begin{pmatrix} \boldsymbol{a}_1 & \dots & \boldsymbol{a}_n \\ \boldsymbol{\alpha}_{21} & & \boldsymbol{\alpha}_{2n} \\ \vdots & & \vdots \\ \boldsymbol{\alpha}_{n1} & & \boldsymbol{\alpha}_{nn} \end{pmatrix}\right) = \det \pi_i \begin{pmatrix} \boldsymbol{a}_1 & \dots & \boldsymbol{a}_n \\ \boldsymbol{\alpha}_{21} & & \boldsymbol{\alpha}_{2n} \\ \vdots & & \vdots \\ \boldsymbol{\alpha}_{n1} & & \boldsymbol{\alpha}_{nn} \end{pmatrix}$$

$$= \det \begin{pmatrix} \pi_i(\boldsymbol{a}_1) & \dots & \pi_i(\boldsymbol{a}_n) \\ \alpha^i_{21} & & \alpha^i_{2n} \\ \vdots & & \vdots \\ \alpha^i_{n1} & & \alpha^i_{nn} \end{pmatrix} = 1.$$

Luego la matriz M tiene determinante uno ya que $\det(\boldsymbol{\alpha}_{rs})_{1\leq r,s\leq n} = \mathbf{1}$ si y sólo si $\pi_i(\det(\boldsymbol{\alpha}_{rs})_{1\leq r,s\leq n}) = 1$ para todo $i \in I$. En consecuencia, R es un anillo de Hermite. ■

Corolario 1.5.9 *Un producto infinito de cuerpos es un anillo de Hermite.*

Un subanillo de un anillo de Hermite no es en general Hermite y un cociente de un anillo de Hermite tampoco es en general Hermite. Por ejemplo, el anillo del Ejemplo 1.5.6 es un dominio por tanto su cuerpo de fracciones $\mathrm{Fr}(R)$ es anillo de Hermite, $R \subset \mathrm{Fr}(R)$ y R no es Hermite. Además $\mathbb{R}[x, y, z]$ es un dominio por tanto es un anillo de Hermite y $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$ no lo es.

1.6. Apéndice.

En esta sección queremos comparar, mediante ejemplos, los diferentes tipos de anillos estudiados en este capítulo, anillo total de cocientes, $\beta-$anillo y anillo de Hermite.

(1) De acuerdo con la Proposición 1.4.7, un dominio es un $\beta-$anillo. En particular, si K es un cuerpo, $R = K[x]$ es un $\beta-$anillo y R es anillo de Hermite pero no es anillo total de cocientes pues x es un elemento no inversible ni divisor de cero en R.

(2) Por el Corolario 1.2.2, un producto infinito de cuerpos es anillo total de cocientes y es anillo de Hermite por el Corolario 1.5.9 pero no es $\beta-$anillo.

(3) Por el Ejemplo 1.5.6, $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$ no es anillo de Hermite pero por la Proposición 1.4.7, R es $\beta-$anillo pues R es un dominio.

Sospechamos que un anillo total de cocientes no es necesariamente un anillo de Hermite. Además el siguiente lema presenta otra relación entre los anillos.

Lema 1.6.1 *Sea R un anillo. Si R es $0-$dimensional y $\beta-$anillo entonces R es anillo de Hermite.*

Demostración. Puesto que R es $0-$dimensional, todos los ideales primos son maximales y como R es $\beta-$anillo, por la Proposición 1.4.14, Spec(R) tiene un número finito de componentes grafoconexas las cuales son los ideales maximales luego R es un anillo semilocal. Pero, como R es $\beta-$anillo, R es un producto finito de anillos locales y por el Lema 1.5.7 y el Corolario 1.5.9 se tiene que R es un anillo de Hermite. ■

El siguiente es ejemplo de un anillo total de cocientes, $\beta-$anillo y anillo de Hermite.

Ejemplo 1.6.2 (Un anillo total de cocientes con maximal no nilpotente) *Sea*

$$R = \frac{\mathbb{R}[[x,y]]}{(x(x+y), y(x+y))} = \{a + b\overline{y} + \overline{x}s(\overline{x}) : a, b \in \mathbb{R} \text{ y } s(\overline{x}) \in \mathbb{R}[[\overline{x}]]\}.$$

Note que los elementos de R satisfacen que $\overline{x}^2 = \overline{y}^2 = -\overline{x}\overline{y}$ y en general para cada $r \geq 2$, $\overline{x}^r = (-1)^s\overline{y}^s\overline{x}^{r-s}$ para todo $s = 1, \ldots, r$. El producto de dos elementos en R es $(a+b\overline{y}+\overline{x}s(\overline{x}))(c+d\overline{y}+\overline{x}t(\overline{x})) = ac+(ad+bc)\overline{y}+\overline{x}h(\overline{x})$ donde $h(\overline{x}) \in \mathbb{R}[[\overline{x}]]$. Veamos que R es un anillo total de cocientes.

(i) Si $a \neq 0$ entonces $a + b\overline{y} + \overline{x}s(\overline{x})$ es inversible. En efecto, si $a \neq 0$ entonces $(a + b\overline{y}+\overline{x}s(\overline{x}))(a-b\overline{y}+\overline{x}s(\overline{x})) = (a+\overline{x}s(\overline{x}))^2-b^2\overline{y}^2 = (a+\overline{x}s(\overline{x}))^2-b^2\overline{x}^2 = a^2+\overline{x}h(\overline{x})$ donde $h(\overline{x}) = 2as(\overline{x})+\overline{x}(s(\overline{x}))^2-b^2\overline{x}$. Note que $a^2+\overline{x}h(\overline{x}) \in \mathbb{R}[[\overline{x}]]$ es inversible ya que $a \neq 0$ luego existe $r(\overline{x}) \in \mathbb{R}[[\overline{x}]]$ tal que $(a+b\overline{y}+\overline{x}s(\overline{x}))(a-b\overline{y}+\overline{x}s(\overline{x}))r(\overline{x}) = 1$. En consecuencia, $a + b\overline{y} + \overline{x}s(\overline{x})$ es inversible.

(ii) Si $a = 0$ entonces $a+b\overline{y}+\overline{x}s(\overline{x})$ es un divisor de cero. En efecto, si $a = 0$ entonces existe $\overline{x} + \overline{y} \in R$ tal que $(b\overline{y} + \overline{x}s(\overline{x}))(\overline{x} + \overline{y}) = 0$.

Note que R es un anillo local con ideal maximal $(\overline{x}, \overline{y})$ pues esta formado por las no unidades de R. Además, R no es nilpotente pues si lo fuera existiría $n \in \mathbb{N}$ tal que $(\overline{x}, \overline{y})^n$ y en particular existiría $n \in \mathbb{N}$ tal que $\overline{x}^n = 0$. Como $\overline{x} = x + (x(x+y), y(x+y))$ entonces $\overline{x}^n = x^n + (x(x+y), y(x+y)) = 0$ esto es $x^n \in (x(x+y), y(x+y))$. Luego $x + y$ divide a x^n y esto es absurdo. En consecuencia, R es un anillo total de cocientes y un anillo local pero no es una $\mathbb{R}-$álgebra finita. Además, por los Lemas 1.4.3 y 1.5.7, R es también un $\beta-$anillo y un anillo de Hermite. Más aún, R no es $0-$dimensional.

Capítulo 2

$K-$álgebras de dimensión finita como espacios vectoriales

En el capítulo anterior hemos estudiado las $K-$álgebras finitas con producto $\mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}\mathbf{e}_i$. En este capítulo daremos resultados generales sobre $K-$álgebras finitas y clasificaremos las $K-$álgebras finitas en baja dimensión para el cuerpos $\mathbb{R}$.

2.1. Tensores y la estructura de $K-$álgebra de un espacio vectorial.

Sean K un cuerpo y V un $K-$espacio vectorial de dimensión finita. Un producto en V con el cual V tenga estructura de $K-$álgebra es una aplicación $K-$bilineal $V \times V \longrightarrow V$, que además es simétrica (propiedad conmutativa), que cumple la propiedad asociativa y la existencia de neutro. Como V es de dimensión finita, entonces se tiene el isomorfismo canónico

$$V \simeq \mathrm{Hom}(V^*, K) = (V^*)^*$$

El producto define entonces una aplicación bilineal

$$\begin{array}{rccc} \phi: & V \times V & \longrightarrow & \mathrm{Hom}(V^*, K) \\ & (\mathbf{u}_1, \mathbf{u}_2) & \mapsto & \phi_{(\mathbf{u}_1, \mathbf{u}_2)} \end{array}$$

con $\phi_{(\mathbf{u}_1,\mathbf{u}_2)} : V^* \longrightarrow K$ está dado por $\phi_{(\mathbf{u}_1,\mathbf{u}_2)}(v^*) = v^*(\mathbf{u}_1 \cdot \mathbf{u}_2)$ y donde $\cdot$ es el producto de la $K-$álgebra.

En consecuencia el producto es un elemento

$$\begin{aligned} P &\in \mathrm{Bil}(V\times V,\mathrm{Hom}(V^*,K))\simeq \mathrm{Hom}(V\otimes V,\mathrm{Hom}(V^*,K))\simeq \mathrm{Bil}((V\otimes V)\times V^*,K)) \\ &\simeq \mathrm{Mult}(V\times V\times V^*,K)\simeq \mathrm{Hom}(V\otimes V\otimes V^*,K)=(V\otimes V\otimes V^*)^*\simeq V^*\otimes V^*\otimes V. \end{aligned}$$

P se considerará indistintamente como elemento de uno cualquiera de los espacios canónicamente isomorfos construidos anteriormente.

Si $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ es una base de V y $\{\mathbf{e}_1^*,\ldots,\mathbf{e}_n^*\}$ es la base dual, entonces P como elemento de $\mathrm{Bil}(V\times V,V)$ está definido por

$$P(\mathbf{e}_i,\mathbf{e}_j)=\mathbf{e}_i\cdot\mathbf{e}_j=\sum_{k=1}^{n}\alpha_{ij}^k\mathbf{e}_k$$

donde para todo k la matriz $P_k=(\alpha_{ij}^k)_{1\le i,j\le n}$ es simétrica (propiedad conmutativa del producto). P como elemento de $\mathrm{Mult}(V\times V\times V^*,K)$ está dado por

$$P(\mathbf{e}_i,\mathbf{e}_j,\mathbf{e}_k^*)=\mathbf{e}_k^*(\mathbf{e}_i\cdot\mathbf{e}_j)=\sum_{l=1}^{n}\alpha_{ij}^l\mathbf{e}_k^*(\mathbf{e}_l)=\alpha_{ij}^k$$

y como elemento de $V^*\otimes V^*\otimes V$,

$$P=\sum_{i,j,k=1}^{n}\alpha_{ij}^k\ \mathbf{e}_i^*\otimes\mathbf{e}_j^*\otimes\mathbf{e}_k.$$

Ejemplo 2.1.1 *(1) Sea $V=K^n$ con el producto componente a componente. Por el Lema 1.2.4, existen $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_n\in V$ tales que $\boldsymbol{e}_i\cdot\boldsymbol{e}_j=\delta_{ij}\boldsymbol{e}_i$ y $\sum_{i=1}^n\boldsymbol{e}_i=\mathbf{1}$. Luego $\alpha_{ij}^k=\delta_{ij}$ y por tanto para todo $k=1,\cdots,n$, $P_k=(\alpha_{ij}^k)_{1\le i,j\le n}$ es la matriz con elemento 1 en la posición $i=j=k$ y cero en las otras posiciones.*

(2) Si consideramos la $\mathbb{R}-$álgebra de los números paracomplejos $\mathbb{P}=\frac{\mathbb{R}[x]}{(x^2-1)}$ y tomamos dos bases de $\mathbb{P}$, $\{u_1=\frac{1-\overline{x}}{\sqrt{2}},u_2=\frac{1+\overline{x}}{\sqrt{2}}\}$ y $\{v_1=1,v_2=\overline{x}\}$. En estas bases las matrices P_k son las siguientes

(i) $P_1=\begin{pmatrix}\sqrt{2}&0\\0&0\end{pmatrix}$ *y* $P_2=\begin{pmatrix}0&0\\0&\sqrt{2}\end{pmatrix}$ *para* $\{u_1,u_2\}$.

(ii) $P_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ *y* $P_2=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ *para* $\{v_1,v_2\}$.

Aparentemente no hay relación entre las matrices correspondientes en estas bases.

(3) Sea $V=\frac{K[x]}{(x^n)}$ con la estructura de álgebra inducida por la del anillo de polinomios.

Note que para todos i, j, $1 \leq i, j \leq n$, $x^i x^j = \begin{cases} x^{i+j} & si \quad 1 \leq i+j \leq n-1 \\ 0 & si \quad i+j > n-1 \end{cases}$
Por tanto para todo $k = 1, \cdots, n-1$, $P_k = (\alpha_{ij}^k)_{0 \leq i,j \leq n-1}$ *es la matriz con elemento 1 en las posiciones* $i+j=k$ *y cero en las otras posiciones.*

(4) Sea $V = V_1 \oplus V_2$, *la suma directa de dos* $K-$*álgebras finitas y consideremos el producto componente a componente. Sea* $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_s\}$ *una base de* V *con* $\boldsymbol{u}_i \cdot \boldsymbol{v}_j = \mathbf{0}$, $\boldsymbol{u}_i \cdot \boldsymbol{u}_j = \sum_{k=1}^r \alpha_{ij}^k \boldsymbol{u}_k$ *y* $\boldsymbol{v}_i \cdot \boldsymbol{v}_j = \sum_{t=1}^s \beta_{ij}^t \boldsymbol{v}_t$ *luego para todo* $l = 1, \cdots, r+s$, $P_l = \begin{pmatrix} (\alpha_{ij}^k)_{0 \leq i,j \leq r} & 0 \\ 0 & (\beta_{ij}^t)_{0 \leq i,j \leq s} \end{pmatrix}$.
Recíprocamente si todas las matrices P_l *tienen la misma estructura de cajas, es decir,* $P_l = \begin{pmatrix} M_l & 0 \\ 0 & N_l \end{pmatrix}$ *con todas las submatrices* M_l *y* N_l *del mismo número de filas para todo* l *entonces* V *se descompone en suma directa de dos* $K-$*álgebras finitas.*

2.1.1. Homomorfismos de $K-$álgebras.

Sea $f : V \to W$ un homomorfismo de $K-$espacios vectoriales. Si V y W tienen estructura de $K-$álgebras definidas por los tensores P y Q entonces, f es un homomorfismo de $K-$álgebras si y sólo si el diagrama

$$\begin{array}{ccc} V \times V & \xrightarrow{P} & V \\ \downarrow{\scriptstyle f \times f} & & \downarrow{\scriptstyle f} \\ W \times W & \xrightarrow{Q} & W \end{array}$$

es conmutativo, es decir, $f(P(\mathbf{u}_1, \mathbf{u}_2)) = Q(f(\mathbf{u}_1), f(\mathbf{u}_2))$.

Si $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es una base de V y $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ es una base de W, y $M = (\gamma_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ es la matriz asociada a f en éstas bases entonces

$$\begin{pmatrix} f(\mathbf{e}_1) \\ \vdots \\ f(\mathbf{e}_n) \end{pmatrix} = M \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix}$$

es decir $f(\mathbf{e}_i) = \sum_{j=1}^m \gamma_{ij} \mathbf{w}_j$ para todo i.

Dado un vector $\mathbf{v} \in V$, se tiene que $\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{e}_i = (a_1, \ldots, a_n) \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix}$. Luego

$$f(\mathbf{v}) = (a_1, \ldots, a_n) \begin{pmatrix} f(\mathbf{e}_1) \\ \vdots \\ f(\mathbf{e}_n) \end{pmatrix} = (a_1, \ldots, a_n) M \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix}.$$

En particular, para todo i, $f(\mathbf{e}_i) = \delta_i M \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix}$ donde δ_i es el vector de coordenada 1 en la posición i y las otras posiciones tienen coordenada 0. Note que

$$f(\mathbf{e}_i) = \delta_i M \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix} = (\mathbf{w}_1, \ldots, \mathbf{w}_m) M^t \delta_i^t.$$

Luego

$$f(\mathbf{e}_i) \cdot f(\mathbf{e}_j) = \delta_i M \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix} (\mathbf{w}_1, \ldots, \mathbf{w}_m) M^t \delta_j^t \tag{2.1}$$

donde

$$\begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix} (\mathbf{w}_1, \ldots, \mathbf{w}_m) = (\mathbf{w}_i \cdot \mathbf{w}_j)_{1 \leq i,j \leq m} = Q.$$

Si $\mathbf{w}_i \cdot \mathbf{w}_j = \sum_{k=1}^{m} \beta_{ij}^k \mathbf{w}_k$ entonces

$$Q = \left(\sum_{k=1}^{m} \beta_{ij}^k \mathbf{w}_k \right)_{1 \leq i,j \leq m} = \sum_{k=1}^{m} Q_k \mathbf{w}_k$$

donde $\{Q_k\}_{1 \leq k \leq m}$, con $Q_k = (\beta_{ij}^k)_{1 \leq i,j \leq m}$, son las matrices coordenadas del tensor Q.

Por tanto, reemplazando en la Ecuación (2.1),

$$f(\mathbf{e}_i) \cdot f(\mathbf{e}_j) = \sum_{k=1}^{m} \delta_i M Q_k M^t \delta_j^t \mathbf{w}_k = (\delta_i M Q_1 M^t \delta_j^t, \ldots, \delta_i M Q_m M^t \delta_j^t) \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix}.$$

Por otra parte

$$\begin{aligned} f(\mathbf{e}_i \cdot \mathbf{e}_j) &= f(\sum_{l=1}^{n} \alpha_{ij}^l \mathbf{e}_l) = \sum_{l=1}^{n} \alpha_{ij}^l f(\mathbf{e}_l) = \sum_{l=1}^{n} \alpha_{ij}^l \sum_{k=1}^{m} \gamma_{lk} \mathbf{w}_k = \sum_{k=1}^{m} (\sum_{l=1}^{n} \alpha_{ij}^l \gamma_{lk}) \mathbf{w}_k \\ &= (\alpha_{ij}^1, \ldots, \alpha_{ij}^n) M \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_m \end{pmatrix}. \end{aligned}$$

Como $f(\mathbf{e}_i \cdot \mathbf{e}_j) = f(\mathbf{e}_i) \cdot f(\mathbf{e}_j)$ entonces

$$(\alpha_{ij}^1, \ldots, \alpha_{ij}^n) M = (\delta_i M Q_1 M^t \delta_j^t, \ldots, \delta_i M Q_m M^t \delta_j^t). \tag{2.2}$$

En principio no podemos calcular las matrices $\{P_k\}_{1 \leq k \leq n}$, con $P_k = (\alpha_{ij}^k)_{1 \leq i,j \leq n}$, en función de las matrices $\{Q_k\}_{1 \leq k \leq m}$, con $Q_k = (\beta_{ij}^k)_{1 \leq i,j \leq m}$.

Ahora bien, si $f : V \to W$ es un isomorfismo de $K-$espacios vectoriales, f induce el isomorfismo

$$f^t : W^* \to V^*$$

y por tanto lleva asociada una aplicación lineal

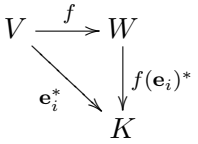
$$F: \quad W^* \otimes W^* \otimes W \quad \longrightarrow \quad V^* \otimes V^* \otimes V$$

dada por $F = f^t \otimes f^t \otimes f^{-1}$ que está bien definida porque es el producto tensorial de aplicaciones lineales.

Como $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es una base de V, $\{f(\mathbf{e}_1), \ldots, f(\mathbf{e}_n)\}$ es una base de W y su base dual cumple la igualdad siguiente

$$f^t(f(\mathbf{e}_i)^*) = \mathbf{e}_i^*$$

para todo i. En efecto, consideremos el diagrama



y concluimos que $f^t(f(\mathbf{e}_i)^*)(\mathbf{e}_j) = (f(\mathbf{e}_i)^* \circ f)(\mathbf{e}_j) = f(\mathbf{e}_i)^*(f(\mathbf{e}_j)) = \delta_{ij}$.

En estas condiciones

$$\begin{aligned} F(f(\mathbf{e}_i)^* \otimes f(\mathbf{e}_j)^* \otimes f(\mathbf{e}_k)) &= f^t(f(\mathbf{e}_i)^*) \otimes f^t(f(\mathbf{e}_j))^* \otimes f^{-1}(f(\mathbf{e}_k)) \\ &= \mathbf{e}_i^* \otimes \mathbf{e}_j^* \otimes \mathbf{e}_k. \end{aligned}$$

Por tanto la relación entre el tensor P, que define el producto en V, y el tensor Q, que define el producto en W, es

$$F(Q) = P.$$

En efecto, si el producto en V respecto de la base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ está dado por

$$P = \sum_{i,j,k=1}^{n} \alpha_{ij}^k \ \mathbf{e}_i^* \otimes \mathbf{e}_j^* \otimes \mathbf{e}_k$$

entonces el producto en W respecto de la base $\{f(\mathbf{e}_1), \ldots, f(\mathbf{e}_n)\}$ está dado por

$$Q = \sum_{i,j,k=1}^{n} \beta_{ij}^k \ f(\mathbf{e}_i)^* \otimes f(\mathbf{e}_j)^* \otimes f(\mathbf{e}_k)$$

con

$$\begin{aligned} \beta_{ij}^k &= Q(f(\mathbf{e}_i), f(\mathbf{e}_j), f(\mathbf{e}_k)^*) = f(\mathbf{e}_k)^*(f(\mathbf{e}_i) \cdot f(\mathbf{e}_j)) \\ &= f(\mathbf{e}_k)^*(f(\mathbf{e}_i \cdot \mathbf{e}_j)) = f(\mathbf{e}_k)^*(f(\sum_{l=1}^{n} \alpha_{ij}^l \mathbf{e}_l)) = f(\mathbf{e}_k)^*(\sum_{l=1}^{n} \alpha_{ij}^l f(\mathbf{e}_l)) = \alpha_{ij}^k. \end{aligned}$$

En conclusión los isomorfismos de $K-$espacios vectoriales que son isomorfismos de $K-$álgebras son exactamente aquellos tales que su isomorfismo asociado entre las $K-$álgebras tensoriales dejan invariante el tensor definido por el producto.

En coordenadas, por la Ecuación (2.2), como M es la matriz de un isomorfismo existe M^{-1} y

$$(\alpha_{ij}^1, \ldots, \alpha_{ij}^n) = (\delta_i M Q_1 M^t \delta_j^t, \ldots, \delta_i M Q_m M^t \delta_j^t) M^{-1}.$$

Esta fórmula hace ver que es inviable la búsqueda de formas canónicas de isomorfismos de la manera habitual.

Una vez estudiado que el producto se traduce en el tensor, y el comportamiento del tensor por los isomorfismos, veamos en qué se traduce la existencia de unidad y la propiedad asociativa. Observamos primero que la aplicación

$$\begin{array}{rccc} I: & V \times V^* & \longrightarrow & K \\ & (\mathbf{u}, v^*) & \mapsto & v^*(\mathbf{u}) \end{array}$$

es bilineal y como $\mathrm{Bil}(V \times V^*, K) \simeq \mathrm{Hom}(V \otimes V^*, K) = V^* \otimes V$ tenemos que I se puede ver como elemento de $V^* \otimes V$. Luego, si $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es una base de V y $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_n^*\}$ es su base dual,

$$I(\mathbf{e}_r, \mathbf{e}_s^*) = \delta_{rs}.$$

Note que esto se cumple para toda base de V. Por tanto, en cualquier base, I como elemento de $V^* \otimes V$ es

$$I = \sum_{i=1}^{n} \mathbf{e}_i^* \otimes \mathbf{e}_i.$$

Si $T = \sum_{i,j,k=1}^{n} \lambda_{ij}^k \ \mathbf{e}_i^* \otimes \mathbf{e}_j^* \otimes \mathbf{e}_k \in V^* \otimes V^* \otimes V$ y $\mathbf{v} \in V$ podemos definir el "contraído" de T por $\mathbf{v}$ como

$$T_{\mathbf{v}} = \sum_{i,j,k=1}^{n} \lambda_{ij}^k \ \mathbf{e}_i^*(\mathbf{v}) \ \mathbf{e}_j^* \otimes \mathbf{e}_k \in V^* \otimes V.$$

$T_{\mathbf{v}}$ está bien definido porque $T_{\mathbf{v}}$ visto como elemento de $\mathrm{Bil}(V \times V^*, K)$ es

$$\begin{array}{rccl} T_{\mathbf{v}}: & V \times V^* & \longrightarrow & K \\ & (\mathbf{u}, v^*) & \mapsto & T_{\mathbf{v}}(\mathbf{u}, v^*) = T(\mathbf{v}, \mathbf{u}, v^*). \end{array}$$

y T es multilineal. Note que la existencia de unidad se traduce entonces en que existe $\mathbf{v} \in V$ tal que $T_{\mathbf{v}} = I$.

Por otra parte, si P es un tensor que cumple la propiedad asociativa esto es $(\mathbf{v}_1 \cdot \mathbf{v}_2) \cdot \mathbf{v}_3 = \mathbf{v}_1 \cdot (\mathbf{v}_2 \cdot \mathbf{v}_3)$ para $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V$ y en términos de la base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ de V es

$$(\mathbf{e}_i \cdot \mathbf{e}_j) \cdot \mathbf{e}_k = \mathbf{e}_i \cdot (\mathbf{e}_j \cdot \mathbf{e}_k)$$

para todos i, j, k, entonces

$$(\mathbf{e}_i \cdot \mathbf{e}_j) \cdot \mathbf{e}_k = (\sum_{l=1}^{n} \alpha_{ij}^l \mathbf{e}_l) \cdot \mathbf{e}_k = \sum_{l=1}^{n} \alpha_{ij}^l (\mathbf{e}_l \cdot \mathbf{e}_k) = \sum_{l=1}^{n} \alpha_{ij}^l (\sum_{t=1}^{n} \alpha_{lk}^t \mathbf{e}_t) = \sum_{t=1}^{n} \sum_{l=1}^{n} \alpha_{ij}^l \alpha_{lk}^t \mathbf{e}_t$$

y

$$\mathbf{e}_i \cdot (\mathbf{e}_j \cdot \mathbf{e}_k) = \mathbf{e}_i \cdot (\sum_{r=1}^{n} \alpha_{jk}^r \mathbf{e}_r) = \sum_{r=1}^{n} \alpha_{jk}^r (\mathbf{e}_i \cdot \mathbf{e}_r) = \sum_{r=1}^{n} \alpha_{jk}^r (\sum_{t=1}^{n} \alpha_{ir}^t \mathbf{e}_t) = \sum_{t=1}^{n} \sum_{r=1}^{n} \alpha_{jk}^r \alpha_{ir}^t \mathbf{e}_t.$$

En consecuencia, si P cumple la propiedad asociativa equivale a que, para todos i, j, k, t,

$$\sum_{l=1}^{n} \alpha_{ij}^l \alpha_{lk}^t = \sum_{r=1}^{n} \alpha_{jk}^r \alpha_{ir}^t$$

Proposición 2.1.2 *Si $T \in V^* \otimes V^* \otimes V$ es un tensor que cumple las condiciones siguientes*

(1) Existe $\boldsymbol{v} \in V$ tal que $T_{\boldsymbol{v}} = I$.

(2) Para todos i, j, k, t

$$\sum_{l=1}^{n} \alpha_{ij}^{l}\alpha_{lk}^{t} = \sum_{r=1}^{n} \alpha_{jk}^{r}\alpha_{ir}^{t}.$$

(3) T *es simétrica en las dos primeras variables.*

entonces T *define un producto en* V *con el cual* V *es una* $K-$*álgebra.*

Demostración. Si consideramos el producto tensorial $V^* \otimes V^* \otimes V$, entonces todo $T \in V^* \otimes V^* \otimes V$ se puede ver como elemento de $\mathrm{Bil}(V \times V, V)$ luego

$$T: \quad V \times V \quad \longrightarrow \quad V$$

es bilineal. Definimos en V el producto: $\mathbf{v}_1 \cdot \mathbf{v}_2 = T(\mathbf{v}_1, \mathbf{v}_2)$. El producto está bien definido porque T es una aplicación. Por la condición (3), T es bilineal simétrica por tanto la operación producto es conmutativa y distributiva. Por la condición (1), el producto tiene unidad y veamos que es asociativa. En efecto, si $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V$ y $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es base de V, sean $\mathbf{v}_1 = \sum_{i=1}^{n} a_i\mathbf{e}_i, \mathbf{v}_2 = \sum_{j=1}^{n} b_j\mathbf{e}_j$ y $\mathbf{v}_3 = \sum_{k=1}^{n} c_k\mathbf{e}_k$, entonces

$$\begin{aligned}
\mathbf{v}_1 \cdot (\mathbf{v}_2 \cdot \mathbf{v}_3) &= \mathbf{v}_1 \cdot (\sum_{j,k=1}^{n} b_j c_k \ \mathbf{e}_j \cdot \mathbf{e}_k) = \sum_{i,j,k=1}^{n} a_i b_j c_k \ \mathbf{e}_i \cdot (\mathbf{e}_j \cdot \mathbf{e}_k) \\
&= \sum_{i,j,k=1}^{n} a_i b_j c_k (\mathbf{e}_i \cdot \mathbf{e}_j) \cdot \mathbf{e}_k = (\sum_{i,j=1}^{n} a_i b_j \ \mathbf{e}_i \cdot \mathbf{e}_j) \cdot \mathbf{v}_3 = (\mathbf{v}_1 \cdot \mathbf{v}_2) \cdot \mathbf{v}_3.
\end{aligned}$$

Luego es suficiente ver que la propiedad asociativa se cumple para una base. Por tanto, por la condición (2), el producto cumple la propiedad asociativa. ■

Proposición 2.1.3 *Si* V *es una* $K-$*álgebra de dimensión finita, el sistema lineal de formas bilineales simétricas*

$$\mathcal{P} = \{P_\varphi : V \times V \to K, \ P_\varphi(\boldsymbol{v}_1, \boldsymbol{v}_2) = \varphi(\boldsymbol{v}_1 \cdot \boldsymbol{v}_2), \ \forall \varphi \in V^*\}$$

es un invariante por isomorfismos.

Demostración. Note que

$$\mathrm{Bil}(V \times V, V) \simeq \mathrm{Hom}(V \otimes V, V) \simeq \mathrm{Hom}(V^*, \mathrm{Hom}(V \otimes V, K)) \simeq \mathrm{Hom}(V^*, \mathrm{Bil}(V \times V, K)).$$

Luego, el producto es una aplicación bilineal de $V \times V$ en V es decir un homomorfismo de $V \otimes V$ en V, pasando al dual induce un homomorfismo de V^* en $V^* \otimes V^* \simeq (V \otimes V)^*$ es decir un homomorfismo de V^* en $\mathrm{Bil}(V \times V, K)$ entonces $\mathcal{P}$ es precisamente la imagen de este homomorfismo y por tanto es un subespacio vectorial de $\mathrm{Bil}(V \times V, K)$ esto

es un sistema lineal de formas bilineales simétricas o de formas cuadráticas. Si f es un isomorfismo de álgebras como f conmuta con el tensor producto deja invariante el sistema lineal $\mathcal{P}$.
Para obtener las ecuaciones del sistema procedemos por otra vía observando que si $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es una base de V y $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_n^*\}$ es su base dual, entonces $\mathcal{P}$ está generado por las formas bilineales $P_k = P_{\mathbf{e}_k^*}$, $k = 1, \ldots, n$, cuyas matrices en la base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ son exactamente las $(\alpha_{ij}^k)_{1 \leq i,j \leq n}$ si

$$P = \sum_{i,j,k=1}^{n} \alpha_{ij}^k \ \mathbf{e}_i^* \otimes \mathbf{e}_j^* \otimes \mathbf{e}_k.$$

Por tanto, si $f : V \to W$ es un homomorfismo de $K-$álgebras, Q es el tensor producto de W y $\varphi \in W^*$, entonces $P_{f^t(\varphi)}(\mathbf{v}_1, \mathbf{v}_2) = f^t(\varphi)(\mathbf{v}_1 \cdot \mathbf{v}_2) = \varphi(f(\mathbf{v}_1 \cdot \mathbf{v}_2)) = \varphi(f(\mathbf{v}_1) \cdot f(\mathbf{v}_2)) = Q_\varphi(f(\mathbf{v}_1), f(\mathbf{v}_2)) = Q_\varphi \circ (f \times f)(\boldsymbol{v}_1, \boldsymbol{v}_2)$ para $\mathbf{v}_1, \mathbf{v}_2 \in V$. Es decir

$$P_{f^t(\varphi)} = Q_\varphi \circ (f \times f).$$

Y si f es un isomorfismo, entonces f^t también lo es y

$$P_{f^t(\varphi)} \circ (f^{-1} \times f^{-1}) = Q_\varphi.$$

Es decir, $P_{f^t(\varphi)}$ y Q_φ son linealmente equivalentes para todo φ. En consecuencia, el sistema lineal de formas cuadráticas $\mathcal{P}$ es invariante por isomorfismos. ■

Observación 2.1.4 *Si consideramos los sistemas lineales de cuádricas asociadas a estos sistemas lineales de formas bilineales, el conjunto de puntos base de cada uno de estos sistemas es*

$$\{[\boldsymbol{v}] \in \mathcal{P}(V) : \varphi(\boldsymbol{v}, \boldsymbol{v}) = 0, \forall \varphi \in V^*\} = \{[\boldsymbol{v}] \in \mathcal{P}(V) : \boldsymbol{v} \cdot \boldsymbol{v} = 0\}.$$

Es decir, es exactamente el proyectizado del conjunto de elementos de cuadrado cero de V. Sin embargo la condición de $\boldsymbol{v}^2 = 0 \ \Rightarrow \ f(\boldsymbol{v})^2 = 0$ significa solamente que f lleva la intersección de las cuádricas en la intersección de las cuádricas y el resultado anterior es más fuerte pues significa que lleva el haz de cuádricas sobre el haz de cuádricas y por tanto que el haz, y en consecuencia sus elementos invariantes, es invariante por f.

2.2. $K-$álgebras finitas

Sea K un cuerpo de característica cero. Diremos que A es una $K-$álgebra finita si es una $K-$álgebra conmutativa con uno y de dimensión finita como $K-$espacio vectorial.

Denotaremos por $\dim_K A$ a su dimensión como $K-$espacio vectorial.

Obviamente toda $K-$álgebra finita es artiniana y noetheriana, vamos a obtener un primer resultado de estructura para éste tipo de $K-$álgebras. La proposición está probada en el texto de Atiyah, ver [3], pero aquí damos una demostración distinta.

Lema 2.2.1 *Si A es una $K-$álgebra artiniana, entonces A es local si y sólo si los únicos idempotentes de A son 0 y 1.*

Demostración. $\Rightarrow$: Si A es una $K-$álgebra local de ideal maximal $\mathfrak{m}$ y $e \in A$ es idempotente, entonces $e^2 = e$. Luego, $e - e^2 = e(1-e) = 0$ y tenemos dos casos:
(i) Si $e \in \mathfrak{m}$ entonces $1 - e \notin \mathfrak{m}$. Como A es local, $1-e$ es inversible luego $e(1-e)(1-e)^{-1} = 0$ y por tanto $e = 0$.
(ii) Si $1-e \in \mathfrak{m}$ entonces $e \notin \mathfrak{m}$. Como A es local, e es inversible entonces $e(1-e)e^{-1} = 0$. Por tanto $1 - e = 0$ y $e = 1$.
$\Leftarrow$: A es artiniana y sus únicos idempotentes son 0 y 1, sea $\mathfrak{m}$ un ideal maximal de A y sea $a \in A$ con $a \notin \mathfrak{m}$. Si a es no inversible, aA es un ideal propio de A entonces

$$aA \supset a^2A \supset \cdots \supset a^nA$$

es una sucesión decreciente de ideales y como A es artiniana, A es estacionaria. Luego existe r tal que $a^rA = a^{r+1}A$ entonces $a^r \in a^{r+1}A$ y existe $\lambda \in A$ tal que $a^r = \lambda a^{r+1}$. Por tanto, $a^r(1-\lambda a) = 0$ y

$$0 = \lambda^r a^r(1-\lambda a) = \lambda^r a^r(1-\lambda a)(1+\lambda a+\cdots+(\lambda a)^{r-1}) = (\lambda a)^r(1-(\lambda a)^r).$$

Entonces $(\lambda a)^r$ es idempotente. Pero los únicos idempotentes de A son 0 y 1. Si

$$(\lambda a)^r = \lambda^r a^{r-1} a = 1$$

tenemos que a es inversible y esto es una contradicción. Si $(\lambda a)^r = 0$, entonces

$$\lambda^r a^r \in \mathfrak{m}.$$

Como $a \notin \mathfrak{m}$, $\lambda^r \in \mathfrak{m}$ pero $\mathfrak{m}$ es primo luego $\lambda \in \mathfrak{m}$. Lo cual es un absurdo pues $a^r(1-\lambda a) = 0$ implica que $1 - \lambda a \in \mathfrak{m}$ por tanto $\lambda \notin \mathfrak{m}$.
En consecuencia, para todo $a \in A$ tal que $a \notin \mathfrak{m}$ tenemos que a es inversible y A es local. ■

Proposición 2.2.2 *A es una $K-$álgebra finita si y sólo si A es un producto directo finito de $K-$álgebras locales finitas*

Demostración. $\Rightarrow$: Si $\dim_K A = 1$ como $K-$espacio vectorial, $A \simeq K$ luego A es local. Si $\dim_K A > 1$ y no tiene mas idempotentes que 0 y 1, por el Lema 2.2.1, A es una $K-$álgebra local finita. En caso contrario, existe $e \in A$ idempotente, $e \neq 1$ y $e \neq 0$. Entonces
(i) eA es un subanillo de A ya que eA es un ideal y por tanto es subanillo. Además el uno de eA es e pues $e(ea) = e^2a = ea$, para todo $ea \in eA$.
(ii) Todo ideal de eA es ideal de A. En efecto, sea $\mathfrak{p}$ ideal de eA luego para todo $\alpha \in \mathfrak{p}$ y para todo $a \in A$ se cumple que $ea\alpha \in \mathfrak{p}$. Note que $\alpha = eb$, $b \in A$. Entonces $\mathfrak{p}$ es ideal de A porque para todo $\alpha \in \mathfrak{p}$ y para todo $a \in A$, se tiene que

$$a\alpha = aeb = ae^2b = eaeb = ea\alpha \in \mathfrak{p}.$$

Además, como A es artiniana, eA es artiniana ya que cualquier sucesión decreciente de ideales de eA es una sucesión decreciente de ideales de A y por tanto estacionaria.
(iii) eA y $(1-e)A$ son subespacios vectoriales de A y $e(1-e) = 0$ entonces para todo $a \in A$, $a = ea + (1-e)a$ luego $A = eA + (1-e)A$ suma como $K-$espacios vectoriales. Además si $\beta \in eA \cap (1-e)A$, $\beta = ea = (1-e)b$ para $a, b \in A$ entonces $\beta = ea = e^2a = e(1-e)b = 0$.
En consecuencia, A es suma directa de eA y $(1-e)A$ como $K-$espacios vectoriales y tenemos el isomorfismo de $K-$espacios vectoriales

$$\begin{array}{rccc} \varphi: & A & \to & eA \times (1-e)A \\ & a & \mapsto & (ea, (1-e)a) \end{array}.$$

Tomando en $eA \times (1-e)A$ la estructura producto

$$\varphi(a)\varphi(b) = (ea, (1-e)a)(eb, (1-e)b) = (eab, (1-e)ab) = \varphi(ab)$$

pues $1-e$ es también idempotente. Luego

$$A \simeq eA \times (1-e)A$$

como $K-$álgebras.
Puesto que eA y $(1-e)A$ son subespacios no nulos y $\dim_K A$ es finita, se tiene que

$$\dim_K eA < \dim_K A \quad \text{y} \quad \dim_K (1-e)A < \dim_K A$$

es decir las dimensiones de eA y $(1-e)A$ son menores que la dimensión de A.
Si eA y $(1-e)A$ no tienen más elementos idempotentes que 0 y 1, por el Lema 2.2.1, eA y $(1-e)A$ son $K-$álgebras locales finitas. De lo contrario y como las dos álgebras son de dimensión menor que la de A seguimos el proceso inductivamente hasta obtener

el resultado deseado.
$\Leftarrow$: Se comprueba sin dificultad. ■

Observación 2.2.3 *En el ítem (ii) de la demostración de la Proposición 2.2.2, observe que si* $\mathfrak{p} \in \text{Spec}(eA)$, *no necesariamente* $\mathfrak{p} \in \text{Spec}(A)$. *Por ejemplo, sea* $A = \mathbb{R}^3$ *y* $e = (1,1,0)$ *entonces* $eA = \{(a,b,0) : a,b \in \mathbb{R}\}$. *Un ideal maximal y por tanto primo de* eA *es* $\mathfrak{m}_{eA} = \{(a,0,0) : a \in \mathbb{R}\}$ *y* $\mathfrak{m}_{eA}$ *no es ideal primo en* A *pues* $(0,1,0)$ *y* $(0,0,1)$ *no pertenecen a* $\mathfrak{m}_{eA}$ *y su producto es cero.*

Las tres proposiciones siguientes relacionan las $K-$álgebras finitas con los anillos estudiados en el primer capítulo. Es decir, una $K-$álgebra finita es anillo total de cocientes, $\beta-$anillo y anillo de Hermite.

Proposición 2.2.4 *Toda* $K-$*álgebra finita es un anillo total de cocientes.*

Demostración. Sean A una $K-$álgebra finita y $\dim_K A = n$. Para todo $u \in A$, existe $r < n$ tal que $1, u, \ldots, u^r$ son linealmente independientes y u^{r+1} depende linealmente de $\{1, u, \ldots, u^r\}$ luego existen $b_0, b_1, \ldots, b_r \in K$ tales que $u^{r+1} = b_r u^r + \cdots + b_0 1$ y tenemos dos casos:

(i) Si $b_0 = 0$ entonces $0 = u^{r+1} - b_r u^r - \cdots - b_1 u = u(u^r - \cdots - b_2 u - b_1 1)$ luego u es divisor de cero. Note que $u^r - \cdots - b_2 u - b_1 1 \neq 0$ ya que $1, u, \ldots, u^r$ son linealmente independientes.

(ii) Si $b_0 \neq 0$ entonces $1 = b_0^{-1} u(u^r - \cdots - b_2 u - b_1 1)$ por tanto u es inversible.
En consecuencia, A es un anillo total de cocientes. ■

Proposición 2.2.5 *Toda* $K-$*álgebra finita es un* $\beta-$*anillo.*

Demostración. Sea A una $K-$álgebra finita. De acuerdo a la Proposición 2.2.2, existen $A_1, \ldots, A_r$ $K-$álgebras locales finitas tales que $A = A_1 \times \cdots \times A_r$. Puesto que $A_1, \ldots, A_r$ son anillos locales, por el Lema 1.4.3, $A_1, \ldots, A_r$ son $\beta-$anillos y por el Lema 1.4.13 el producto finito de $\beta-$anillos es un $\beta-$anillo. En consecuencia, A es un $\beta-$anillo. ■

Proposición 2.2.6 *Toda* $K-$*álgebra finita es un anillo de Hermite.*

Demostración. Sea A una $K-$álgebra finita. De acuerdo a la Proposición 2.2.2, existen $A_1, \ldots, A_r$ $K-$álgebras locales finitas tales que $A = A_1 \times \cdots \times A_r$. Puesto que $A_1, \ldots, A_r$ son anillos locales, por el Lema 1.5.7, $A_1, \ldots, A_r$ son anillos de Hermite y por el Lema 1.5.8 el producto de anillos de Hermite es un anillo de Hermite. En consecuencia, A es un anillo de Hermite. ■

Los dos siguientes resultados muestran que una $K-$álgebra finita se descompone en forma única, salvo isomorfismos, en suma directa de $K-$álgebras finitas locales.

Lema 2.2.7 *Sea $A = \bigoplus_{i=1}^{r} A_i$ una $K-$álgebra finita donde cada A_i es una $K-$álgebra local finita. Para $i = 1, \ldots, r$ sea $\mathfrak{m}_i$ el ideal maximal de A_i. Entonces*

(1) $\mathrm{Max}(A) = \{M_1, \ldots, M_r\}$ *donde* $M_i = \prod_{j=1}^{r} m_j$ *con* $m_j = A_j$, *para todo* $j \neq i$ *y* $m_i = \mathfrak{m}_i$.

(2) Para todo $i = 1, \ldots, r$ *se tiene que* $A_{M_i} \simeq A_i$.

Demostración. *(1)* Es consecuencia del Lema 1.2.6(6).
(2) Para todo $i = 1, \ldots, r$,

$$A_{M_i} = \left\{ \frac{(a_1, \ldots, a_r)}{(b_1, \ldots, b_r)} : (b_1, \ldots, b_r) \notin M_i \right\} = \left\{ \frac{(a_1, \ldots, a_r)}{(b_1, \ldots, b_r)} : b_i \notin \mathfrak{m}_i \right\}.$$

Como A_i es local, b_i es inversible y la aplicación

$$\begin{array}{rccc} \phi_i : & A_{M_i} & \to & A_i \\ & \frac{(a_1,\ldots,a_r)}{(b_1,\ldots,b_r)} & \mapsto & b_i^{-1} a_i \end{array}$$

es un homomorfismo de anillos. Note que ϕ_i es inyectiva ya que si $b_i^{-1} a_i = 0$, entonces existe $(0, \ldots, b_i^{-1}, \ldots, 0) \notin M_i$ tal que $(a_1, \ldots, a_i, \ldots, a_r)(0, \ldots, b_i^{-1}, \ldots, 0) = (0, \ldots, 0)$ y esto equivale a que

$$\frac{(a_1, \ldots, a_r)}{(b_1, \ldots, b_r)} = (0, \ldots, 0)$$

para $\frac{(a_1,\ldots,a_r)}{(b_1,\ldots,b_r)} \in A_{M_i}$. Además, ϕ_i es sobreyectiva porque, para todo $a_i \in A_i$, existe $\frac{(a_i,\ldots,a_i)}{(1,\ldots,1)} \in A_{M_i}$ tal que $\phi_i \left(\frac{(a_i,\ldots,a_i)}{(1,\ldots,1)} \right) = a_i$. ■

Proposición 2.2.8 *Sean $A = \bigoplus_{i=1}^{r} A_i$ y $B = \bigoplus_{j=1}^{s} B_j$ dos $K-$álgebras finitas donde A_i, B_j son $K-$álgebras locales finitas. Entonces $A \simeq B$ como $K-$álgebras si y sólo si $r = s$ y, después de reordenar los B_j, para todo $i = 1, \ldots, r$ se tiene que $A_i \simeq B_i$ como $K-$álgebras.*

Demostración. $\Rightarrow$: Como $A = \bigoplus_{i=1}^{r} A_i$, por el Lema 2.2.7, $\mathrm{Max}(A) = \{M_1, \ldots, M_r\}$ y para todo $i = 1, \ldots, r$ se tiene $A_{M_i} \simeq A_i$. Además, por hipótesis, $A \simeq \bigoplus_{j=1}^{s} B_j$ luego por el Lema 2.2.7, $\mathrm{Max}(A) = \{N_1, \ldots, N_s\}$ y para todo $j = 1, \ldots, s$ se tiene $A_{N_j} \simeq B_j$. Entonces para todo i, existe j tal que $M_i = N_j$. Por tanto después de reordenar a los B_j, para todo $i = 1, \ldots, r$,

$$A_i \simeq A_{M_i} \simeq A_{N_i} \simeq B_i.$$

$\Leftarrow$: Si para todo $i = 1, \ldots, r$ se tiene que ϕ_i es el isomorfismo entre A_i y B_i, entonces

$$\prod_{i=1}^{r} \phi_i : \prod_{i=1}^{r} A_i \to \prod_{i=1}^{r} B_i$$

es un isomorfismo. ■

En consecuencia, por la Proposición 2.2.8, estudiar la estructura de las $K-$álgebras finitas se reduce a estudiar la estructura de las $K-$álgebras locales finitas.

El ejemplo más simple de las $K-$álgebras finitas es el de las $K-$álgebras $A = \frac{K[x]}{(f(x))}$ caracterizadas porque existe $u \in A$ tal que $1, u, \ldots, u^{n-1}$ es base de A como $K-$espacio vectorial. Obviamente no toda $K-$álgebra finita es de este tipo, por ejemplo $\frac{\mathbb{R}[x,y]}{(x,y)^2}$ ya que todo elemento al cuadrado de la ésta álgebra es cero, luego no puede existir $u \in A$ tal que $1, u, u^2$ sea base de A como $K-$espacio vectorial.

Lema 2.2.9 *La $K-$álgebra finita $A = \frac{K[x]}{(f(x))}$ es local si y sólo si existe $p(x) \in K[x]$, polinomio irreducible, tal que $f(x) = p(x)^n$. En este caso su ideal maximal es $(p(\overline{x}))$ y el cuerpo residual es $\frac{K[x]}{(p(x))}$.*

Demostración. Los elementos de $A = \frac{K[x]}{(f(x))}$ se escriben de forma única como $g(\overline{x})$ con $g(x) \in K[x]$ y grado(g) <grado(f).
$\Rightarrow$: Si $f(x)$ no es potencia de un irreducible, en particular $f(x)$ no es irreducible, entonces $f(x) = f_1(x)f_2(x)$ donde $\text{mcd}(f_1, f_2) = 1$ por tanto existen $g_1, g_2 \in K[x]$ tales que $g_1f_1 + g_2f_2 = 1$ luego $1 - g_1f_1 = g_2f_2$ y

$$g_1(\overline{x})f_1(\overline{x})(1 - g_1(\overline{x})f_1(\overline{x})) = g_1(\overline{x})g_2(\overline{x})f_1(\overline{x})f_2(\overline{x}) = 0.$$

En consecuencia, $g_1(\overline{x})f_1(\overline{x})$ es idempotente y note que $g_1(\overline{x})f_1(\overline{x}) \neq 0$ y $g_1(\overline{x})f_1(\overline{x}) \neq 1$. Si $g_1(\overline{x})f_1(\overline{x}) = 0$, entonces $g_2(\overline{x})f_2(\overline{x}) = 1$ es decir $f_2(\overline{x})$ es inversible pero esto es absurdo pues $f_2(\overline{x})$ es un divisor de cero de A. Por la misma razón $g_1(\overline{x})f_1(\overline{x}) \neq 1$.
$\Leftarrow$: Si $g(\overline{x}) \in A$ es idempotente entonces $g(\overline{x})(1 - g(\overline{x})) = 0$ y esto equivale a que $p(x)^n$ divide a $g(x)(1 - g(x))$ luego

$$p(x)|g(x)(1 - g(x)).$$

Por tanto, $p(x)|g(x)$ o $p(x)|(1-g(x))$ pero no a los dos a la vez pues $p(x) \nmid 1$. Si $p(x)|g(x)$ entonces $p(x) \nmid (1 - g(x))$ y por tanto $p(x)^n|g(x)$ luego $g(\overline{x}) = 0$ y si $p(x)|(1 - g(x))$ entonces $p(x) \nmid g(x)$ y por tanto $p(x)^n|(1 - g(x))$ luego $1 - g(\overline{x}) = 0$ y $g(\overline{x}) = 1$. En consecuencia, por el Lema 2.2.1, A es local. Además como $p(x)$ es irreducible, el ideal $(p(x))$ es maximal y contiene a $(p(x)^n)$. Luego $(p(\overline{x}))$ es el ideal maximal de A y su cuerpo residual es $\frac{K[\overline{x}]}{(p(\overline{x}))} \simeq \frac{K[x]}{(p(x))}$. ■

Lema 2.2.10 *Sean $f(x), g(x) \in K[x]$ tales que* $\text{mcd}(f, g) = 1$. *Entonces existe un isomorfismo de $K-$álgebras*

$$\frac{K[x]}{(f(x)g(x))} \simeq \frac{K[x]}{(f(x))} \times \frac{K[x]}{(g(x))}$$

dotando al producto cartesiano de estructura de K−álgebra con las operaciones suma y producto componente a componente.

Demostración. Para todo $f(x) \in K[x]$, sea $\varphi_f : K[x] \to \frac{K[x]}{(f(x))}$ el homomorfismo natural definido por $\varphi_f(p(x)) = p(x) + (f(x))$. Entonces

$$\begin{array}{rccc} \varphi_f \times \varphi_g : & K[x] & \to & \frac{K[x]}{(f(x))} \times \frac{K[x]}{(g(x))} \\ & p(x) & \mapsto & \big([p(x)]_{f(x)}, [p(x)]_{g(x)}\big) \end{array}$$

es homomorfismo de $K-$álgebras y $\mathrm{Ker}(\varphi_f \times \varphi_g) = (fg)$ ya que $h \in \mathrm{Ker}(\varphi_f \times \varphi_g)$ si y sólo si $h \in \mathrm{Ker}(\varphi_f) \cap \mathrm{Ker}(\varphi_g)$ y $\mathrm{Ker}(\varphi_f) \cap \mathrm{Ker}(\varphi_g) = (f) \cap (g) = (fg)$ pues $\mathrm{mcd}(f, g) = 1$. Además, $\varphi_f \times \varphi_g$ es sobreyectiva. En efecto, sea $\big([r(x)]_{f(x)}, [s(x)]_{g(x)}\big) \in \frac{K[x]}{(f(x))} \times \frac{K[x]}{(g(x))}$, como f y g son primos entre si, existen $c_1, c_2 \in K[x]$ tales que $c_1 f + c_2 g = 1$, entonces

$$\varphi_f \times \varphi_g(rc_2 g + sc_1 f) = ([r]_{f(x)}, [s]_{g(x)})$$

ya que $\varphi_f(rc_2 g + sc_1 f) = rc_2 g + (f) = r + (f) = [r]_{f(x)}$ y $\varphi_g(rc_2 g + sc_1 f) = sc_1 f + (g) = s + (g) = [s]_{g(x)}$. ■

La proposición siguiente presenta la descomposición en productos de $K-$álgebras locales y se demuestra usando iterativamente la prueba del Lema 2.2.10.

Proposición 2.2.11 *Si $f(x) = f_1(x)^{n_1} \cdots f_r(x)^{n_r} \in K[x]$ es un producto de factores irreducibles distintos entonces*

$$\frac{K[x]}{(f(x))} \simeq \frac{K[x]}{(f_1(x)^{n_1})} \times \cdots \times \frac{K[x]}{(f_r(x)^{n_r})}.$$

Lema 2.2.12 *(1) Un homomorfismo $\phi : K[x] \to K[x]$ queda unívocamente determinado por $\phi(x) = h(x) \in K[x]$.*

(2) ϕ es un isomorfismo de anillos si y sólo si $\phi(x) = ax + b$ con $a, b \in K$ y $a \neq 0$.

Demostración. *(1)* Sean $g(x) \in K[x]$ y ϕ un homomorfismo, como $\phi(g(x)) = \phi(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1\phi(x) + \cdots + a_n\phi(x)^n = g(h(x))$, ϕ queda determinado sólo por $\phi(x) = h(x) \in K[x]$.
(2) Si ϕ es un isomorfismo entonces existe ψ tal que $\psi(\phi(x)) = \phi(\psi(x)) = x$. Sean $\phi(x) = h(x) = a_0 + a_1 x + \cdots + a_r x^r$ y $\psi(x) = t(x) = b_0 + b_1 x + \cdots + b_s x^s$ entonces $\psi(\phi(x)) = \psi(a_0 + a_1 x + \cdots + a_r x^r) = b_0 + \cdots + b_s(a_0 + a_1 x + \cdots + a_r x^r)^s = x$ por tanto $rs = 1$ esto es $r = s = 1$. En consecuencia, $\phi(x) = ax + b$ con $a \neq 0$. Recíprocamente, si $\phi(x) = ax + b$ con $a, b \in K$ y $a \neq 0$ entonces existe $\psi(x) = \frac{1}{a}x - \frac{b}{a}$ tal que $\psi(\phi(x)) = \phi(\psi(x)) = x$. Por tanto ϕ es un isomorfismo. ■

Definición 2.2.13 *$p(x)$ es equivalente a $q(x)$, $p(x) \sim q(x)$, si y sólo si existen $a, b \in K$ con $a \neq 0$ tales que $q(x) = p(ax + b)$.*

Proposición 2.2.14 *(1) Si $K = \mathbb{R}$, entonces los polinomios irreducibles son $p(x) \sim x$ ó $p(x) \sim x^2 + 1$.*

(2) Si K es algebraicamente cerrado, entonces para todo $p(x)$ irreducible, $p(x) \sim x$.

Demostración. *(1)* Los polinomios irreducibles en $\mathbb{R}[x]$ son los lineales $p(x) = ax + b$ con $a \neq 0$ o de grado dos de la forma $ax^2 + bx + c$ con $b^2 - 4ac < 0$. Si $p(x) = ax + b$ con $a \neq 0$, por definición, $p(x) \sim x$. Además, note que $ax^2 + bx + c$ con $b^2 - 4ac < 0$ es equivalente a que $p(x) = (x - a')^2 + (b')^2$ con $b' \neq 0$. Luego,

$$p(x) = (x - a')^2 + (b')^2 = (\frac{x}{b'} - \frac{a'}{b'})^2 + 1 \sim x^2 + 1.$$

(2) Si K es algebraicamente cerrado, los polinomios irreducibles $p(x)$ son lineales y por definición, $p(x) \sim x$. ■

Lema 2.2.15 *Sea $n \in \mathbb{N}$. Si $p(x) \sim q(x)$ entonces*

$$\frac{K[x]}{(p(x)^n)} \simeq \frac{K[x]}{(q(x)^n)}.$$

Demostración. Como $p(x) \sim q(x)$, existen $a, b \in K$ con $a \neq 0$ tales que $q(x) = p(ax + b)$. Sea ϕ el homomorfismo

$$\begin{array}{rccc} \phi: & K[x] & \to & \frac{K[x]}{(p(ax+b)^n)} \\ & x & \mapsto & [ax + b] \end{array}$$

$\text{Ker}(\phi) = (p(x)^n)$ ya que para $h(x) \in K[x]$, $\phi(h(x)) = 0 \Leftrightarrow h(ax + b) \in (p(ax + b)^n) \Leftrightarrow h(x) \in (p(x)^n)$. Además, ϕ es sobreyectiva. En efecto, sea $[h(x)] \in \frac{K[x]}{(p(ax+b)^n)}$, por el Lema 2.2.12, existe $\widetilde{h}(x) \in K[x]$ tal que $h(x) = \widetilde{h}(ax + b)$ entonces $\phi(\widetilde{h}(x)) = [\widetilde{h}(ax + b)] = [h(x)]$. ■

El recíproco del Lema 2.2.15 no es cierto incluso bajo la hipótesis de que $p(x)$ y $q(x)$ sean irreducibles como lo prueba el ejemplo siguiente.

Ejemplo 2.2.16 *Sean $A = \frac{\mathbb{Z}/(3)[x]}{(x^3+x^2+2)}$ y $B = \frac{\mathbb{Z}/(3)[y]}{(y^3+2y^2+1)}$. $\{1, \overline{x}, \overline{x}^2\}$ y $\{1, \overline{y}, \overline{y}^2\}$ son bases de A y B respectivamente como espacios vectoriales.*

Definimos el homomorfismo de álgebras

$$\begin{array}{rccc} \widehat{\phi}: & \mathbb{Z}/(3)[x] & \to & \frac{\mathbb{Z}/(3)[y]}{(y^3+2y^2+1)} \\ & x & \mapsto & 2\overline{y}^2+1 \end{array}$$

Note que $\widehat{\phi}(x^2)=2\overline{y}^2+2\overline{y}$ *y* $\widehat{\phi}(x^3+x^2+2)=0$.
Como $(x^3+x^2+2)\subset \mathrm{Ker}(\widehat{\phi})$, $\widehat{\phi}$ *induce un homomorfismo*

$$\begin{array}{rccc} \phi: & \frac{\mathbb{Z}/(3)[x]}{(x^3+x^2+2)} & \to & \frac{\mathbb{Z}/(3)[y]}{(y^3+2y^2+1)} \\ & \overline{x} & \mapsto & 2\overline{y}^2+1 \end{array}$$

ϕ *es un isomorfismo. En efecto,* ϕ *es inyectivo ya que si* $\phi(a+b\overline{x}+c\overline{x}^2)=a+b(2\overline{y}^2+1)+c(2\overline{y}^2+2\overline{y})=a+b+2c\overline{y}+(2b+2c)\overline{y}^2=0$ *entonces* $a+b=0$, $c=0$ *y* $b+c=0$. *Luego* $a=b=c=0$ *y* ϕ *es inyectiva. Puesto que las álgebras tienen la misma dimensión, como espacios vectoriales, entonces* ϕ *es un isomorfismo.*
Observe que $x^3+x^2+2 \nsim y^3+2y^2+1$ *ya que no existe una transformación lineal que lleve un polinomio en el otro.*

Corolario 2.2.17 *1. Si* $f(x)=p_1(x)^{n_1}\cdots p_r(x)^{n_r}\in K[x]$ *es producto de factores irreducibles distintos y* $p_i(x)\sim q_i(x)$ *para todo* $i=1,\cdots,r$ *entonces*

$$\frac{K[x]}{(f(x))}\simeq \frac{K[x]}{(q_1(x)^{n_1})}\times\cdots\times\frac{K[x]}{(q_r(x)^{n_r})}$$

2. En particular, si K *es algebraicamente cerrado y* $f(x)=(x-a_1)^{n_1}\cdots(x-a_r)^{n_r}$ *entonces*

$$\frac{K[x]}{(f(x))}\simeq \frac{K[x]}{(x^{n_1})}\times\cdots\times\frac{K[x]}{(x^{n_r})}$$

Demostración. *(1)* Se tiene por la Proposición 2.2.11 y el Lema 2.2.15.
(2) Puesto que $x-a_i\sim x$ y por el item (1) tenemos el isomorfismo. ■

Corolario 2.2.18 *Sea* $K=\mathbb{R}$.

(1) Si $n\in\mathbb{N}$ *y* $a,b\in\mathbb{R}$ *con* $b\neq 0$ *entonces*

$$\frac{\mathbb{R}[x]}{(((x-a)^2+b^2)^n)}\simeq\frac{\mathbb{R}[x]}{((x^2+1)^n)}.$$

(2) Si $f(x)\in\mathbb{R}[x]$ *entonces existen* $n_1,\cdots n_r,m_1,\cdots m_s$ *tales que*

$$\frac{\mathbb{R}[x]}{(f(x))}\simeq\frac{\mathbb{R}[x]}{(x^{n_1})}\times\cdots\times\frac{\mathbb{R}[x]}{(x^{n_r})}\times\frac{\mathbb{R}[x]}{((x^2+1)^{m_1})}\times\cdots\times\frac{\mathbb{R}[x]}{((x^2+1)^{m_s})}.$$

Demostración. *(1)* Puesto que $(x-a)^2+b^2 \sim x^2+1$, por el Lema 2.2.15 tenemos el isomorfismo.
(2) Por la Proposición 2.2.14, existen $n_1, \cdots n_r, m_1, \cdots m_s \in \mathbb{R}$ tales que $f(x) = (x-a_1)^{n_1} \cdots (x-a_r)^{n_r}((x-b_1)^2+c_1^2)^{m_1} \cdots ((x-b_s)^2+c_s^2)^{m_s}$ y por la Proposición 2.2.11 y el item (1) se sigue el resultado. ■

Observe que se presenta el problema de la unicidad de la descomposición. En el caso de cuerpos cerrados la descomposición es única y queda determinada por los números $n_1, \cdots, n_r$ es decir para todo $f(x) \in K[x]$ existen $n_1, \cdots, n_r$ únicos con $\frac{K[x]}{f(x)} \simeq \frac{K[x]}{(x^{n_1})} \times \cdots \times \frac{K[x]}{(x^{n_r})}$. En el caso real la situación es la misma como prueba el resultado siguiente.

Lema 2.2.19 *Para todos m, n enteros positivos,*

$$\frac{\mathbb{R}[x]}{(x^n)} \ncong \frac{\mathbb{R}[x]}{((x^2+1)^m)}$$

Demostración. Por el Lema 2.2.9, el cuerpo residual de la $\mathbb{R}-$álgebra $\frac{\mathbb{R}[x]}{(x^n)}$ es $\frac{\mathbb{R}[x]}{(x)} \simeq \mathbb{R}$ y el cuerpo residual de $\frac{\mathbb{R}[x]}{((x^2+1)^m)}$ es $\frac{\mathbb{R}[x]}{(x^2+1)} \simeq \mathbb{C}$. Luego las álgebras no son isomorfas. ■

Lema 2.2.20 *Si $p(x)$ y $q(x)$ son elementos irreducibles de $\mathbb{R}[x]$ las condiciones siguientes son equivalentes:*

(1) $p(x) \sim q(x)$.

(2) $\frac{\mathbb{R}[x]}{(p(x)^n)} \simeq \frac{\mathbb{R}[x]}{(q(x)^n)}$ *para todo* $n \in \mathbb{N}$.

(3) $\frac{\mathbb{R}[x]}{(p(x))} \simeq \frac{\mathbb{R}[x]}{(q(x))}$.

Demostración. *(1)* $\Rightarrow$ *(2)* Se tiene por el Lema 2.2.15.
(2) $\Rightarrow$ *(3)* Por el Lema 2.2.9, $\frac{\mathbb{R}[x]}{(p(x)^n)}$ y $\frac{\mathbb{R}[x]}{(q(x)^n)}$ son álgebras locales con cuerpos residuales $\frac{\mathbb{R}[x]}{(p(x))}$ y $\frac{\mathbb{R}[x]}{(q(x))}$ respectivamente. Además como $\frac{\mathbb{R}[x]}{(p(x)^n)} \simeq \frac{\mathbb{R}[x]}{(q(x)^n}$) entonces $\frac{\mathbb{R}[x]}{(p(x))} \simeq \frac{\mathbb{R}[x]}{(q(x))}$.
(3) $\Rightarrow$ *(1)* Puesto que $p(x)$ y $q(x)$ son irreducibles en $\mathbb{R}[x]$ entonces $p(x) \sim x$ o $p(x) \sim x^2+1$, y $q(x) \sim x$ o $q(x) \sim x^2+1$. Como $\frac{\mathbb{R}[x]}{p(x)} \simeq \frac{\mathbb{R}[x]}{q(x)}$ y en virtud del Lema 2.2.19, tenemos dos casos:
(i) $p(x) \sim x$ y $q(x) \sim x$, entonces $p(x) \sim q(x)$.
(ii) $p(x) \sim x^2+1$ y $q(x) \sim x^2+1$, entonces $p(x) \sim q(x)$.
■

En consecuencia, para $f(x) \in \mathbb{R}[x]$, existen $n_1, \cdots n_r, m_1, \cdots m_s$ únicos tales que $\frac{\mathbb{R}[x]}{(f(x))} \simeq \frac{\mathbb{R}[x]}{(x^{n_1})} \times \cdots \times \frac{\mathbb{R}[x]}{(x^{n_r})} \times \frac{\mathbb{R}[x]}{((x^2+1)^{m_1})} \times \cdots \times \frac{\mathbb{R}[x]}{((x^2+1)^{m_s})}$. En el caso general lo que se puede decir es que:

Lema 2.2.21 *Sean $p(x)$ y $q(x)$ elementos irreducibles de $K[x]$. $\frac{K[x]}{(p(x)^n)} \simeq \frac{K[x]}{(q(x)^n)}$ si y sólo si $\frac{K[x]}{(p(x))} \simeq \frac{K[x]}{(q(x))}$.*

Demostración. $\Rightarrow$: Por el Lema 2.2.9, $\frac{K[x]}{(p(x)^n)}$ y $\frac{K[x]}{(q(x)^n)}$ son álgebras locales con cuerpos residuales $\frac{K[x]}{(p(x))}$ y $\frac{K[x]}{(q(x))}$ respectivamente. Además como $\frac{K[x]}{(p(x)^n)} \simeq \frac{K[x]}{(q(x)^n)}$ entonces $\frac{K[x]}{(p(x))} \simeq \frac{K[x]}{(q(x))}$.
$\Leftarrow$: Sea

$$\begin{array}{rccc} \varphi: & \frac{K[x]}{(p(x))} & \to & \frac{K[x]}{(q(x))} \\ & f(x)+(p(x)) & \mapsto & \varphi(f(x))+(q(x)) \end{array}$$

Como φ es un isomorfismo $q(x)|p(x)$ y $p(x)|q(x)$ entonces $q(x)^n|p(x)^n$ y $p(x)^n|q(x)^n$ y se tiene el isomorfismo

$$\begin{array}{rccc} \phi: & \frac{K[x]}{(p(x)^n)} & \to & \frac{K[x]}{(q(x)^n)} \\ & f(x)+(p(x)^n) & \mapsto & \varphi(f(x))+(q(x)^n) \end{array}$$

■

El ejemplo 2.2.16 muestra que $K[x]/(p(x)) \simeq K[x]/(q(x))$ no implica que $p(x) \sim q(x)$ entonces la descomposición que puede obtenerse $f(x) = p_1(x)^{n_1}...p_r(x)^{n_r}$ en componentes irreducibles induce un isomorfismo $\frac{K[x]}{(f(x))} \simeq \frac{K[x]}{(p_1(x)^{n_1})} \times \cdots \times \frac{K[x]}{(p_r(x)^{n_r})}$ pero $p_1(x), \cdots, p_r(x)$ no están unívocamente determinados salvo transformación lineal.

2.3. K-álgebras locales finitas

En toda esta sección K es un cuerpo de característica cero. Sean A una $K-$álgebra local finita y $\mathfrak{m}$ su ideal maximal. Como A es local, los elementos no inversibles forman el ideal maximal esto es $\mathfrak{m} = \{\alpha \in A : \alpha \text{ es no inversible}\}$. Pero, por la Proposición 2.2.4, A es un anillo total de cocientes entonces

$$\mathfrak{m} = \{\alpha \in A : \alpha \text{ es divisor de cero}\}.$$

Proposición 2.3.1 *Existe $r \in \mathbb{N}$ tal que $\mathfrak{m}^r = 0$.*

Demostración. Puesto que A es una $K-$álgebra finita, $\mathfrak{m}$ es un $K-$espacio vectorial de dimensión finita y por tanto $\mathfrak{m}$ es un $A-$módulo finito. Además como A es de dimensión finita, A es artiniano y por tanto la sucesión

$$\mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots \supset \mathfrak{m}^s$$

es estacionaria. Luego existe r tal que $\mathfrak{m}^r = \mathfrak{m}^{r+1}$. Entonces $\mathfrak{m}\mathfrak{m}^r = \mathfrak{m}^r$ y note que $\mathfrak{m}$ está contenido en el radical de Jacobson de A. Entonces, por el lema de Nakayama, $\mathfrak{m}^r = 0$. ■

Definición 2.3.2 *El mínimo número natural r tal que $\mathfrak{m}^r = 0$ se llamará orden de $\mathfrak{m}$ y*

será denotado por $o(\mathfrak{m})$. *Y llamaremos orden de* $\alpha \in \mathfrak{m}$ *al mínimo número natural* $o(\alpha)$ *tal que* $\alpha^{o(\alpha)} = 0$.

Proposición 2.3.3 *Sea* $\alpha \in \mathfrak{m}$.

(1) $o(\alpha) = n$ *si y sólo si el polinomio mínimo de* α *es* x^n.

(2) Si $o(\alpha) = n$, *entonces* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *son linealmente independientes.*

Demostración. *(1)* $\Rightarrow$: Si $o(\alpha) = n$, $\alpha^n = 0$ donde n es el mínimo número natural con esta propiedad. Supongamos que x^n no es el polinomio mínimo de α, si $p(x)$ es el polinomio mínimo de α, entonces $p(x)|x^n$ por tanto $p(x) = x^r$ con $r < n$ y $\alpha^r = 0$ lo cual es absurdo.
$\Leftarrow$: Si x^n es el polinomio mínimo de α, entonces $\alpha^n = 0$ y si $\alpha^r = 0$ se tiene que α es cero de x^r y $x^n|x^r$ entonces $n \leq r$ luego $o(\alpha) = n$.
(2) Si $o(\alpha) = n$, entonces por el item (1), x^n es el polinomio mínimo de α. Si

$$a_0 1 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

con $a_0, a_1, \ldots, a_{n-1} \in K$. Entonces α anula a $p(x) = a_0 1 + a_1 x + \cdots + a_{n-1}x^{n-1}$ y esto es absurdo a menos que $a_i = 0$ para todo $i = 0, \ldots, n-1$. Por tanto, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ son linealmente independientes. ■

Proposición 2.3.4 *Si* $\dim_K A = n$, *entonces* $o(\alpha) \leq n$ *para todo* $\alpha \in \mathfrak{m}$.

Demostración. Para todo $\alpha \in \mathfrak{m}$, $\alpha^n = 0$ por tanto $o(\alpha) < n$. Como $\mathfrak{m}$ es un subespacio vectorial de A y no contiene a 1, entonces $\mathfrak{m}$ es un subespacio propio y $\dim_K \mathfrak{m} \leq n-1$. Además por la Proposición 2.3.3(2), $1, \alpha, \alpha^2, \ldots, \alpha^{o(\alpha)-1}$ son linealmente independientes con $\alpha, \alpha^2, \ldots, \alpha^{o(\alpha)-1} \in \mathfrak{m}$ entonces $o(\alpha) - 1 \leq \dim_K \mathfrak{m} \leq n-1$. Por tanto $o(\alpha) \leq n$. ■

Proposición 2.3.5 *Sea* $\dim_K A = n$.

(1) Sean $o(\mathfrak{m}) = n$ *y* $\alpha \in \mathfrak{m}$. *Si* $1, \alpha, \ldots, \alpha^{n-1}$ *son linealmente independientes entonces* $\alpha^n = 0$ *y* $o(\alpha) = n$.

(2) $\mathfrak{m}$ *principal y* $o(\mathfrak{m}) = n$ *si y sólo si existe* $\alpha \in \mathfrak{m}$ *tal que* $1, \alpha, \ldots, \alpha^{n-1}$ *es base de* A.

Demostración. *(1)* Si $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ son linealmente independientes, entonces $\alpha^r \neq 0$ para $r = 1, \cdots, n-1$ entonces $o(\alpha) \geq n$. Por la Proposición 2.3.4, $o(\alpha) \leq n$ entonces $n \leq o(\alpha) \leq n = \dim_K A$. Así, $o(\alpha) = n$.
(2) $\Rightarrow$: Puesto que $\mathfrak{m}$ es principal, existe $\alpha \in A$ tal que $\mathfrak{m} = (\alpha)$ y como $o(\mathfrak{m}) = n$

entonces $o(\alpha) \leq n$. Si $o(\alpha) = r < n$ entonces $\alpha^r = 0$. Como cualquier $\beta \in \mathfrak{m}$ se escribe como $\beta = t\alpha$, con $t \in K$, se tiene que $\beta^r = t^r\alpha^r = 0$ y $o(\mathfrak{m}) = r$ lo cual es absurdo por tanto $o(\alpha)$ no puede ser $r < n$. Así $o(\alpha) = n$ y $\alpha^n = 0$. Por la Proposición 2.3.3(2), $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes y como $\dim_K A = n$ entonces $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es base de A.
$\Leftarrow$: Existe $\alpha \in \mathfrak{m}$ tal que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es base de A entonces $\{\alpha, \ldots, \alpha^{n-1}\}$ es base de $\mathfrak{m}$ luego $\mathfrak{m} = (\alpha)$ y $\mathfrak{m}$ es principal. Además, $\alpha^r \neq 0$ para $r = 1, \cdots, n-1$ entonces $o(\alpha) \geq n$. Pero por la Proposición 2.3.4, $o(\alpha) \leq n$ entonces $o(\alpha) = n$. Por otra parte, $\mathfrak{m}^n = 0$ para todo $x \in \mathfrak{m}$ pues de lo contrario, si $\mathfrak{m}^r = 0$ con $r < n$ entonces en particular $\alpha^r = 0$ y esto es absurdo. ■

Proposición 2.3.6 *Sea K algebraicamente cerrado. A es una $K-$álgebra local finita de la forma $\frac{K[x]}{(f(x))}$ si y sólo si el ideal maximal es principal.*

Demostración. Sean $\dim_K A = n$ y $\mathfrak{m}$ el ideal maximal de A. $\Rightarrow$: El ideal maximal de $\frac{K[x]}{(f(x))}$ es principal pues es un ideal que proviene del anillo $K[x]$ y en $K[x]$ todos los ideales son principales.
$\Leftarrow$: Como $\dim_K A = n$, $o(\beta) \leq n$ para todo $\beta \in \mathfrak{m}$ y puesto que $\mathfrak{m}$ es principal, existe $\alpha \in A$ tal que $\mathfrak{m} = (\alpha)$ entonces $o(\mathfrak{m}) = o(\alpha) = n$ luego $\alpha^n = 0$. Por la Proposición 2.3.5(2), $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de A como $K-$espacio vectorial luego $A = \frac{K[x]}{(x^n)}$. Como K es algebraicamente cerrado, por el Corolario 2.2.17, $\frac{K[x]}{(x^n)} \simeq \frac{K[x]}{(f(x))}$. ■

Proposición 2.3.7 *Si A es una $K-$álgebra local finita entonces A es completa y separada para la topología $\mathfrak{m}-$ádica y en consecuencia A es henseliana.*

Demostración. Por la Proposición 2.3.1, existe $r \in \mathbb{N}$ tal que $\mathfrak{m}^r = 0$ y como

$$0 = \mathfrak{m}^r \subset \cdots \subset \mathfrak{m}^2 \subset \mathfrak{m}$$

entonces $\bigcap_{s=1}^{r} \mathfrak{m}^s = 0$ y A es separada, además

$$\frac{A}{\mathfrak{m}} \xhookrightarrow{f_1} \frac{A}{\mathfrak{m}^2} \xhookrightarrow{f_2} \frac{A}{\mathfrak{m}^3} \xhookrightarrow{f_3} \cdots \xhookrightarrow{f_{r-1}} \frac{A}{\mathfrak{m}^r} = A$$

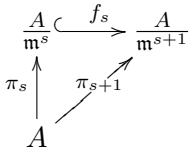
donde f_s, $s = 1, ..., r-1$, es la inclusión de $\frac{A}{\mathfrak{m}^s}$ en $\frac{A}{\mathfrak{m}^{s+1}}$.

Probar que A es completa para la topología $\mathfrak{m}-$ádica es equivalente a ver que

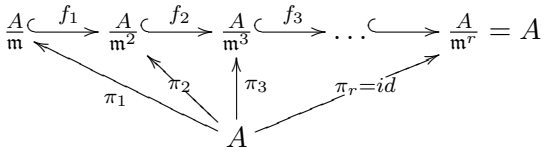
$$A = \varprojlim (A/\mathfrak{m}^s, f_s)_{1 \leq s \leq r}.$$

Luego vamos a probar que A es el límite proyectivo:
(i) Existe el morfismo proyección $\pi_s : A \to A/\mathfrak{m}^s$, para todo s.

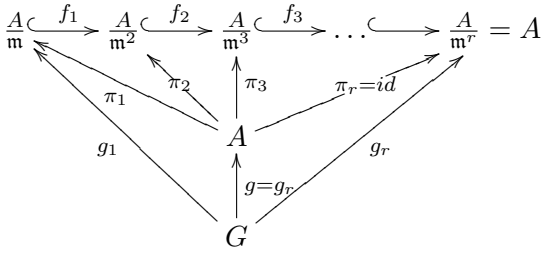
(ii) El diagrama



es conmutativo para todo s. Luego el diagrama



es conmutativo. De esta forma $f_s \circ \pi_s = \pi_{s+1}$.
(iii) Para todo G y para toda familia de morfismos $g_s : G \to \frac{A}{\mathfrak{m}^s}$ de manera que $g_{s+1} = f_s \circ g_s$, existe un único morfismo g de G en A tal que $\pi_s \circ g = g_s$ para todo s. En efecto,



para todo s, se tiene que $\pi_{s+1} \circ g = (f_s \circ \pi_s) \circ g = f_s \circ (\pi_s \circ g) = f_s \circ g_s = g_{s+1}$. La unicidad de g se da porque π_r es la proyección identidad. ■

Proposición 2.3.8 *Si $\Sigma_A = \frac{A}{\mathfrak{m}}$ es el cuerpo residual de A, entonces*

(1) Σ_A es un extensión algebraica finita de K.

(2) El homomorfismo canónico de Σ_A en A admite una sección que permite identificar a Σ_A como subcuerpo de A.

(3) $A = \Sigma_A \oplus \mathfrak{m}$ y la suma es directa.

Demostración. *(1)* Como A es un $K-$espacio vectorial de dimensión finita, $\Sigma_A = \frac{A}{\mathfrak{m}}$ es un $K-$espacio vectorial de dimensión finita y por tanto el cuerpo Σ_A es una extensión algebraica finita de K.
(2) Como $\Sigma_A = \frac{A}{\mathfrak{m}}$ es una extensión algebraica finita de K, por el teorema del elemento primitivo, Σ_A es un extensión simple esto es existe $\alpha \in \Sigma_A$ tal que $\Sigma_A = K[\alpha]$. Si $p(x) \in K[x]$ es el polinomio mónico mínimo de α, $p(\alpha) = 0$ y como $K \subset A$, $p(x) \in A[x]$. Note que α es una raíz simple de $p(x)$ ya que $p'(\alpha) \neq 0$ pues el grado de $p'(x)$ es menor que el grado de $p(x)$, $p(x)$ es el polinomio de grado mínimo con la propiedad $p(\alpha) = 0$ y

la característica de K es cero. Por la Proposición 2.3.7, A es completa y separada para la topología $\mathfrak{m}-$ádica entonces, por el lema de Hensel, existe $a \in A$ tal que $a + \mathfrak{m} = \alpha$ y $p(a) = 0$.
En consecuencia existe

$$\begin{array}{rccc} \overline{\varphi}: & K[x] & \to & A \\ & q(x) & \mapsto & q(a) \end{array}$$

donde $\text{Ker}(\overline{\varphi}) = (p(x))$. Note que $\overline{\varphi}$ induce un homomorfismo inyectivo de $K-$álgebras

$$\begin{array}{rccc} \varphi: & \Sigma_A = \frac{K[x]}{(p(x))} & \to & A \\ & q(x) + (p(x)) & \mapsto & q(a) \end{array}$$

Luego $\Sigma_A \subset A$ y se puede identificar a Σ_A con su imagen.
(3) Como $\Sigma_A = \frac{A}{\mathfrak{m}}$ entonces $A = \Sigma_A \oplus \mathfrak{m}$ y la suma es directa pues $\Sigma_A \bigcap \mathfrak{m} = \{0\}$. ■

Observe en la Proposición 2.3.8 que si K es algebraicamente cerrado, entonces $\Sigma_A = K$, y si $K = \mathbb{R}$ entonces $\Sigma_A = K$ o $\Sigma_A = \mathbb{C}$. Por ejemplo, sea $A = \frac{\mathbb{R}[x]}{(x^2+1)}$, A es una $\mathbb{R}-$álgebra local finita de ideal maximal $\mathfrak{m} = (\overline{x}^2 + 1)$, pero note que $\mathfrak{m} = 0$ en A. Además como $A \simeq \mathbb{C}$, A es también una $\mathbb{C}-$álgebra local finita de ideal maximal $\mathfrak{m} = 0$ y en ambos casos $\Sigma_A = \mathbb{C}$.

Proposición 2.3.9 *Si A es una $K-$álgebra local finita entonces existe L, extensión finita de K, tal que $A = L[x_1, ..., x_n]/I$ y*

(1) para todo i, $1 \leq i \leq n$, existen $a_{ij} \in L$ tales que los polinomios $u_i := x_i^2 - \sum_{j=1}^n a_{ij}x_j \in I$.

(2) para todos i, j, $1 \leq i < j \leq n$, existen $a_{ijk} \in L$ tales que los polinomios $v_{ij} := x_ix_j - \sum_{k=1}^n a_{ijk}x_k \in I$.

Además los polinomios $\{u_i, v_{ij}\}_{1 \leq i < j \leq n}$ generan el ideal I.

Demostración. Por la Proposición 2.3.8, $A = \Sigma_A \oplus \mathfrak{m}$ con $\Sigma_A = \frac{A}{\mathfrak{m}}$ extensión finita de K y $\mathfrak{m}$ maximal de A. Note que $\mathfrak{m}$ tiene estructura de Σ_A-espacio vectorial porque $\Sigma_A \subset A$ y $\mathfrak{m}$ es un ideal de A. Luego A es también Σ_A-espacio vectorial. Como $A = \Sigma_A \oplus \mathfrak{m}$, existe una base de A como Σ_A-espacio vectorial de la forma $\{1, \alpha_1, ..., \alpha_n\}$ con $\{\alpha_1, ..., \alpha_n\}$ base de $\mathfrak{m}$ entonces podemos definir un homomorfismo de Σ_A-álgebras

$$\varphi : \Sigma_A[x_1, ..., x_n] \to A$$

donde $\varphi|_{\Sigma_A}$ es el homomorfismo identidad y $\varphi(x_i) = \alpha_i$. El homomorfismo φ es sobreyectivo y si $I = Ker(\varphi)$ entonces $\Sigma_A[x_1, ..., x_n]/I \simeq A$ como Σ_A-álgebras. Esto prueba la primera parte de la proposición con $\Sigma_A = L$.

Observe que si $a_1x_1+...+a_nx_n \in I$ con $a_i \in L$, $1 \leq i \leq n$, entonces $a_1 = ... = a_n = 0$ porque $x_1+I, ..., x_n+I$ son linealmente independientes ya que son imágenes de $\alpha_1, ..., \alpha_n$ en un isomorfismo.

Como $\alpha_i^2 \in \mathfrak{m}$ para todo $i = 1, ..., n$ entonces $\alpha_i^2 = \sum_{j=1}^n a_{ij}\alpha_j$ con $a_{ij} \in L$ luego $u_i \in I$ y puesto que $\alpha_i\alpha_j \in \mathfrak{m}$ para todos i, j, $1 \leq i, j \leq n$, entonces $\alpha_i\alpha_j = \sum_{j=1}^n a_{ijk}\alpha_k$ con $a_{ijk} \in L$ luego $v_{ij} \in I$.

Sea $J = (\{u_i, v_{ij}\}_{1\leq i<j\leq n})L[x_1, ..., x_n] \subset I$. Vamos a probar que $J = I$. Sea $f \in I$, como $f \in L[x_2, ..., x_n][x_1]$ dividiendo a f entre u_1 se puede ver que $f = q_2(x_2, ..., x_n) + x_1q_1(x_2, ..., x_n) + u_1q_0(x_2, ..., x_n)$ con $u_1q_0(x_2, ..., x_n) \in J$.

Afirmación 2.3.10 *Para todo $r_1, \ldots, r_n \in \mathbb{Z}_{\geq 0}$ con $r_1 + \cdots + r_n > 0$ se tiene que*

$$x_1x_2^{r_2}...x_n^{r_n} = a_1x_1 + \widetilde{a}_1x_1x_2^{r_2'}...x_n^{r_n'} + g_1(x_2, ..., x_n) + g_0$$

donde $a_1, \widetilde{a}_1 \in L$, $r_2' + \cdots + r_n' = r_2 + ... + r_n - 1$ y $g_0 \in J$.

Demostración. Como $r_2 + \cdots + r_n \geq 1$, existe al menos un $r_i \neq 0$ luego $x_1x_i^{r_i} = (x_1x_i)x_i^{r_i-1} = (v_{1i} + a_{1i1}x_1 + \cdots + a_{1in}x_n)x_i^{r_i-1} = v_{1i}x_i^{r_i-1} + a_{1i1}x_1x_i^{r_i-1} + \widetilde{g}_1(x_2, ..., x_n)$ con $v_{1i}x_i^{r_i-1} \in J$. Entonces

$$\begin{aligned} x_1x_2^{r_2}...x_n^{r_n} &= x_1x_i^{r_i}(x_2^{r_2}...x_{i-1}^{r_{i-1}}x_{i+1}^{r_{i+1}}...x_n^{r_n}) \\ &= (v_{1i}x_i^{r_i-1} + a_{1i1}x_1x_i^{r_i-1} + \widetilde{g}_1(x_2, ..., x_n))(x_2^{r_2}...x_{i-1}^{r_{i-1}}x_{i+1}^{r_{i+1}}...x_n^{r_n}) \\ &= a_1x_1 + a_{1i1}x_1x_2^{r_2'}...x_n^{r_n'} + g_1(x_2, ..., x_n) + g_0 \end{aligned}$$

donde $g_0 = v_{1i}x_i^{r_i-1}(x_2^{r_2}...x_{i-1}^{r_{i-1}}x_{i+1}^{r_{i+1}}...x_n^{r_n}) \in J$, $a_1, \widetilde{a}_1 = a_{1i1} \in L$, $r_2' + ... + r_n' = r_2 + ... + r_n - 1$ y $g_1(x_2, ..., x_n) = \widetilde{g}_1(x_2, ..., x_n))(x_2^{r_2}...x_{i-1}^{r_{i-1}}x_{i+1}^{r_{i+1}}...x_n^{r_n})$. ■

Ahora aplicando iterativamente este resultado $r_2 + \cdots + r_n$ veces se consigue que el grado del monomio $x_2^{r_2} \cdots x_n^{r_n}$ sea cero. Además si hacemos este proceso con todos los monomios multiplicados por x_1 se tiene que $f = a_1x_1 + h_1(x_2, \ldots, x_n) + h_0$ con $h_0 \in J$. Después aplicamos el proceso anterior sucesivamente a x_2,...,x_n y se obtiene que

$$f = a_1x_1 + \cdots + a_nx_n + f_1$$

con $f_1 \in J$. Como $f \in I$ entonces $a_1x_1 + \cdots + a_nx_n \in I$ y por tanto $a_1 = \cdots = a_n = 0$. Así $f \in J$ y concluimos que los polinomios $\{u_i, v_{ij}\}_{1\leq i,j\leq n}$ generan el ideal I. ■

Teorema 2.3.11 *Si A es una $K-$álgebra son equivalentes*

1. *A es una $K-$álgebra local finita.*

2. *Existe L extensión finita de K tal que $A = L[x_1, ..., x_n]/I$ y existe r tal que $(x_1, ..., x_n)^r \subset I$*

3. *Existe L extensión finita de K tal que $A = L[x_1, ..., x_n]/I$ y $x_1 + I, ..., x_n + I$ son nilpotentes.*

Demostración. $1 \Rightarrow 2$: Por la Proposición 2.3.9, podemos construir L e I. Además como A es una $K-$álgebra local, por la Proposición 2.3.1, existe r tal que $\mathfrak{m}^r = 0$ y esto equivale a que $(x_1, ..., x_n)^r \subset I$.
$2 \Rightarrow 3$: Por hipótesis, existe r tal que $(x_1, ..., x_n)^r \subset I$ entonces $x_i^r \in I$ para todo i, $1 \leq i \leq n$. Luego $(x_i + I)^r = 0$ para todo i.
$3 \Rightarrow 1$: Para todo $\alpha \in A$, $\alpha = \sum_{r_1+...+r_n} a_{r_1...r_n} \overline{x}_1^{r_1} ... \overline{x}_n^{r_n}$, y como existe t_i tal que $\overline{x}_i^{t_i} = 0$ para todo i, $1 \leq i \leq n$, entonces

$$\alpha = \sum_{r_1+...+r_n} a_{r_1...r_n} \overline{x}_1^{r_1} ... \overline{x}_n^{r_n}$$

con $r_i < t_i$ para todo i. Luego $\{\overline{x}_1^{r_1} ... \overline{x}_n^{r_n}\}_{r_i<t_i, \forall i}$ es un sistema de generadores de A como $L-$espacio vectorial. Por tanto A es un $L-$espacio vectorial de dimensión finita porque L lo es.

Veamos ahora que $A = L[x_1, ..., x_n]/I$ es local. Sea $\mathfrak{a} = (x_1 + I, ..., x_n + I)$, como $x_1 + I, ..., x_n + I$ son nilpotentes entonces existen $t_1, ..., t_n$ tales que $\overline{x}_1^{t_1} = ... = \overline{x}_n^{t_n} = 0$ luego existe $r = t_1 + ... + t_n$ tal que $\mathfrak{a}^r = 0$. Por otra parte, si $\alpha \in A$ entonces $\alpha = a + b$ con $a \in L$ y $b \in \mathfrak{a}$. Veamos que si $\alpha \neq 0$ entonces α es inversible.
En efecto, $\alpha(a-b) = a^2 - b^2$, $\alpha(a-b)(a^2+b^2) = a^4 - b^4$ y $\alpha(a-b)(a^2+b^2)...(a^h+b^h) = a^{2h} - b^{2h}$. Si $2h > r$ entonces $b^{2h} = 0$ y $\alpha(a-b)(a^2+b^2)...(a^h+b^h) = a^{2h}$. Por tanto, $\alpha a^{-2h}(a-b)(a^2+b^2)...(a^h+b^h) = 1$ y en consecuencia α es inversible. Luego todos los elementos que no están en $(\overline{x}_1, ..., \overline{x}_n)$ son inversibles y A es local. ■

Definición 2.3.12 *Si $\alpha \in A$ entonces $\alpha = \alpha_1 + \alpha_2$ donde $\alpha_1 \in \Sigma_A$ y $\alpha_2 \in \mathfrak{m}$, a α_1 lo llamaremos $\alpha(0)$. En consecuencia $\alpha(0)$ es el único tal que $\alpha - \alpha(0) \in \mathfrak{m}$.*

Proposición 2.3.13 *Para todo $\alpha \in A$ se cumple una de las siguientes opciones*

(1) α es inversible si y sólo si $\alpha(0) \neq 0$.

(2) α es nilpotente si y sólo si $\alpha(0) = 0$.

Demostración. Por la Proposición 2.3.8, existe $\alpha(0) \in \Sigma_A$ único tal que $\alpha - \alpha(0) \in \mathfrak{m}$.
(1) $\Rightarrow$: Supongamos que α no es inversible entonces $\alpha \in \mathfrak{m}$ y como $\alpha - \alpha(0) \in \mathfrak{m}$, $\alpha(0) \in \mathfrak{m}$ pero $\alpha(0)$ pertenece al cuerpo Σ_A luego $\alpha(0) = 0$.

$\Leftarrow$: Si $\alpha(0) \neq 0$, como $\alpha - \alpha(0) \in \mathfrak{m}$ y por la Proposición 2.3.1, existe $r \in \mathbb{N}$ tal que $(\alpha - \alpha(0))^r = 0$. Desarrollando el binomio,

$$\alpha(\alpha^{r-1} - r\alpha^{r-2}\alpha(0) + \cdots + (-1)^{r-1}r\alpha(0)^{r-1}) = (-1)^{r-1}\alpha(0)^r.$$

En consecuencia, α es inversible.
(2) $\Rightarrow$: Si α es nilpotente entonces α es divisor de cero. Supongamos que $\alpha(0) \neq 0$, por el item *(1)*, α es inversible y esto es absurdo. Luego, $\alpha(0) = 0$.
$\Leftarrow$: Si $\alpha(0) = 0$, por la Proposición 2.3.8, $\alpha \in \mathfrak{m}$ y por la Proposición 2.3.1, existe $r \in \mathbb{N}$ tal que $\alpha^r = 0$. En consecuencia α es nilpotente. ■

Ejemplo 2.3.14 *Podría parecer que $\alpha(0) \in K$ pero $\alpha(0) \in \Sigma_A$, por ejemplo, si $A = \frac{\mathbb{R}[x]}{((x^2+1)^2)}$, el ideal maximal de A es $\mathfrak{m} = (\overline{x}^2 + 1)$ y su cuerpo residual es $\mathbb{C}$, entonces $A \simeq \mathbb{C} \oplus \mathfrak{m}$ y la descomposición se hace de la forma siguiente.*
Sea $\gamma = \frac{3}{2}\overline{x} + \frac{1}{2}\overline{x}^3 \in A$ entonces $\gamma^2 + 1 = 0$. De este modo, $\mathbb{R} + \gamma\mathbb{R} \subset A$ y $\mathbb{R} + \gamma\mathbb{R} \simeq \mathbb{C}$. Si llamamos $u = \overline{x}^2 + 1$ tenemos que $\{1, \gamma, u, \overline{x}u\}$ es base de A como $\mathbb{R}-$espacio vectorial. Note que $\mathfrak{m}$ como $A-$módulo está generado por u, pero como $\mathbb{R}-$espacio vectorial está generado por u y $\overline{x}u$ ya que cualquier elemento de $\mathfrak{m}$ se escribe como

$$p(\overline{x})u = (a + b\overline{x} + c\overline{x}^2 + d\overline{x}^3)u = au + b\overline{x}u + c\overline{x}^2u + d\overline{x}^3u$$

con $\overline{x}^2u = (u-1)u = u^2 - u = -u$ y $\overline{x}^3u = \overline{x}(\overline{x}^2u) = -\overline{x}u$. Por tanto tenemos el isomorfismo $\varphi : A \to \mathbb{C} \oplus \mathfrak{m}$ con $\varphi(\overline{x}) = \gamma - \frac{1}{2}\overline{x}u$, $\varphi(\overline{x}^2) = u - 1$ y $\varphi(\overline{x}^3) = -\gamma + \frac{3}{2}\overline{x}u$. Finalmente note que $\overline{x}(0) = \gamma$ y $\gamma \notin \mathbb{R}$.

En consecuencia, por la Proposición 2.3.13,

$$\mathfrak{m} = \{\alpha \in A : \alpha(0) = 0\} = \{\alpha \in A : \exists\ r \in \mathbb{N} \text{ tal que } \alpha^r = 0\}.$$

Proposición 2.3.15 *$\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ es base de A como $K-$espacio vectorial si y sólo si $\{1, \alpha_1 - \alpha_1(0), \ldots, \alpha_n - \alpha_{n-1}(0)\}$ es base de A como $K-$espacio vectorial.*

Demostración. La equivalencia se cumple ya que el determinante de la matriz de coordenadas de los segundos elementos en términos de los primeros es distinto de cero pues

$$\det \begin{pmatrix} 1 & -\alpha_1(0) & \ldots & -\alpha_{n-1}(0) \\ 0 & 1 & \ldots & 0 \\ & & & \\ 0 & 0 & \ldots & 1 \end{pmatrix} = 1.$$

■

Proposición 2.3.16 *Sea Σ_A el cuerpo cociente de A. Existe una base de A como Σ_A-espacio vectorial de la forma $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ con α_i nilpotente para todo i, $i = 1, \ldots, n-1$.*

Demostración. Por la Proposición 2.3.8, $A = \Sigma_A \oplus \mathfrak{m}$ donde $\mathfrak{m}$ es su ideal maximal y Σ_A es su cuerpo cociente. Luego existe una base de A como Σ_A-espacio vectorial $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ con $\alpha_1, \ldots, \alpha_{n-1} \in \mathfrak{m}$. Además, puesto que $\mathfrak{m} = \{\alpha \in A : \exists r \in \mathbb{N} \text{ tal que } \alpha^r = 0\}$ tenemos que α_i es nilpotente para todo $i = 1, \ldots, n-1$. ■

Proposición 2.3.17 *(1) $\Delta = \{o(\alpha) : \alpha \in \mathfrak{m}\}$ está acotado superiormente y en consecuencia tiene máximo.*

(2) Si $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ con $\alpha_1, \ldots, \alpha_{n-1} \in \mathfrak{m}$ es base de A, entonces

$$\text{máx}(o(\alpha_i)) \leq o(\mathfrak{m}) \leq \sum_{i=1}^{n-1} o(\alpha_i).$$

Demostración. *(1)* Para todo $\alpha \in \mathfrak{m}$, $o(\alpha) \leq o(\mathfrak{m})$ luego Δ está acotado superiormente por $o(\mathfrak{m})$ y en consecuencia tiene máximo.
(2) Como $\alpha_i \in \mathfrak{m}$, para todo $i = 1, \ldots, n-1$, $o(\alpha_i) \leq o(\mathfrak{m})$ y $\text{máx}(o(\alpha_i)) \leq o(\mathfrak{m})$.
Sea $N = \sum_{i=1}^{n-1} o(\alpha_i)$ y veamos que $\mathfrak{m}^N = 0$. Para todos $\beta_1 \ldots, \beta_N \in \mathfrak{m}$, existen $a_{ij} \in K$ tales que $\beta_i = \sum_{i=1}^{n-1} a_{ij}\alpha_j$, entonces $\beta_1 \cdots \beta_N = \sum_{i=1}^{n-1} a_{1j}\alpha_j \cdots \sum_{i=1}^{n-1} a_{Nj}\alpha_j = \sum b_{r_1 \cdots r_{n-1}} \alpha_1^{r_1} \cdots \alpha_{n-1}^{r_{n-1}}$ donde $r_1 + \cdots + r_{n-1} = N$ y $N = \sum_{i=1}^{n-1} o(\alpha_i)$ entonces existe i tal que $r_i \geq o(\alpha_i)$ y por tanto $\alpha_i^{r_i} = 0$. Así $\beta_1 \cdots \beta_N = 0$ y $\mathfrak{m}^N = 0$. En consecuencia $\text{máx}(o(\alpha_i)) \leq o(\mathfrak{m}) \leq \sum_{i=1}^{n-1} o(\alpha_i)$. ■

Podemos preguntarnos si hay una relación más precisa entre $\text{máx}(o(\alpha_i))$ y en general $\text{máx}\{o(\alpha) : \alpha \in \mathfrak{m}\}$ y $o(\mathfrak{m})$. Observemos que en la $\mathbb{R}-$álgebra $\frac{\mathbb{R}[x,y]}{(x^2,y^2)}$ el ideal maximal está generado por $\overline{x}$ y $\overline{y}$, y $o(\overline{x}) = o(\overline{y}) = 2$ pero $o(\overline{x}+\overline{y}) = 3$ ya que $(\overline{x}+\overline{y})^2 = 2\overline{xy} \neq 0$ y $(\overline{x}+\overline{y})^3 = 0$. En este ejemplo $o(\mathfrak{m}) = 3$ y $o(\overline{x}) + o(\overline{y}) = 4$ luego las dos desigualdades de la Proposición 2.3.17 son estrictas.
Más aún, si K es de característica dos, para todo $\alpha \in \mathfrak{m}$, $\alpha = a\overline{x} + b\overline{y}$ entonces $\alpha^2 = 0$ es decir $o(\alpha) = 2$ para todo $\alpha \in \mathfrak{m}$ pero $o(\mathfrak{m}) = 3$ ya que $0 \neq \overline{xy} \in \mathfrak{m}$. Este fenómeno no se da si $K = \mathbb{R}$ o $K = \mathbb{C}$ como veremos a continuación.

Sea $K = \mathbb{R}$ o $\mathbb{C}$. Para todos $r, n \in \mathbb{N}$, $n \geq 2$ y $r \geq 1$, definimos

$$\Delta_{nr} = \{(i_1, \ldots, i_n) : i_j \in \mathbb{Z}_{\geq 0} \text{ y } i_1 + \cdots + i_n = r\}$$

Ordenamos Δ_{nr} con el orden lexicográfico. Llamamos $N_{nr} = \#(\Delta_{nr}) = \binom{n+r-1}{r}$.

Consideremos la aplicación

$$\begin{array}{lcl} K^n & \to & K^{N_{nr}} \\ \boldsymbol{a}=(a_1,\ldots,a_n) & \mapsto & \boldsymbol{a}^*=(a_1^{i_1}\cdots a_n^{i_n})_{(i_1,\ldots,i_n)\in\Delta_{nr}} \end{array}$$

Para $x_1,\ldots,x_n$ indeterminadas, llamamos $\boldsymbol{x}=(x_1,\ldots,x_n)$ y $\boldsymbol{x}^*=(x_1^{i_1}\cdots x_n^{i_n})_{(i_1,\ldots,i_n)\in\Delta_{nr}}$ con el convenio que si $i_j=0$ entonces no aparece el término a_j^0 o x_j^0 en el monomio correspondiente.

Consideremos la aplicación

$$\begin{array}{rccl} \varphi_{nr}: & K^{N_{nr}\times n} & \to & K \\ & \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{N_{nr}} \end{pmatrix} & \mapsto & \det \begin{pmatrix} \boldsymbol{a}_1^* \\ \vdots \\ \boldsymbol{a}_{N_{nr}}^* \end{pmatrix}. \end{array}$$

Observación 2.3.18 *Si* $\varphi_{nr}\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{N_{nr}} \end{pmatrix}\neq 0$, *como* φ_{nr} *es continua, se tiene que para todo* $i=1,\ldots,N_{nr}$, *existe* $\epsilon_i>0$ *tal que* $\varphi_{nr}\begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_{N_{nr}} \end{pmatrix}\neq 0$ *para* $\boldsymbol{b}_i\in B_{\epsilon_i}(\boldsymbol{a}_i)$. *Luego si existen* $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{N_{nr}}\in K^n$ *tales que* $\varphi_{nr}\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{N_{nr}} \end{pmatrix}\neq 0$ *entonces existen* $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{N_{nr}}\in K^n$ *tales que* $\varphi_{nr}\begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_{N_{nr}} \end{pmatrix}\neq 0$ *y todas las componentes de cada* $\boldsymbol{b}_i$ *son distintas de cero para todo* i.

Proposición 2.3.19 *Para todos* $n,r\in\mathbb{N}$, $n\geq 2$, $r\geq 1$, *existen* $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{N_{nr}}\in K^n$ *tales que* $\varphi_{nr}\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{N_{nr}} \end{pmatrix}\neq 0$.

Demostración. Hacemos inducción sobre (n,r) con el orden lexicográfico.
Para $n=2$ y para todo r, se tiene que $\boldsymbol{x}=(x_1,x_2)$, $\Delta_{2r}=\{(0,r),(1,r-1),\ldots,(r,0)\}$, $N_{2r}=r+1$ y $\boldsymbol{x}^*=(x_2^r,x_1x_2^{r-1},\ldots,x_1^r)$. Sea $\boldsymbol{a}_i=(a_i,1)$ entonces $\boldsymbol{a}_i^*=(1,a_i,a_i^2,\ldots,a_i^r)$,

y si $a_i \neq a_j$, $i \neq j$, entonces $\det \begin{pmatrix} \boldsymbol{a}_1^* \\ \vdots \\ \boldsymbol{a}_{r+1}^* \end{pmatrix} = \begin{vmatrix} 1 & a_1 & \dots & a_1^r \\ \vdots & \vdots & & \vdots \\ 1 & a_{r+1} & \dots & a_{r+1}^r \end{vmatrix}$ y este es distinto de cero pues es el determinante de Vandermonde.

Para $r = 1$ y para todo n, se tiene que $\boldsymbol{x} = (x_1, \cdots, x_n)$, $\Delta_{n1} = \{1, 2, \dots, n\}$, $N_{n1} = n$ y por tanto $\boldsymbol{x}^* = \boldsymbol{x}$. Si $\boldsymbol{a}_1^* = (a_{11}, \dots, a_{1n}), \dots, \boldsymbol{a}_n^* = (a_{n1}, \dots, a_{nn})$ entonces $\det \begin{pmatrix} \boldsymbol{a}_1^* \\ \vdots \\ \boldsymbol{a}_n^* \end{pmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$ y es distinto de cero si $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\}$ es base de K^n.

Supongamos cierto el caso (m, s), para todo $(m, s) < (n, r)$ con el orden lexicográfico, y veamos que se verifica el caso (n, r).

Llamamos $M = \begin{pmatrix} \boldsymbol{a}_1^* \\ \vdots \\ \boldsymbol{a}_N^* \end{pmatrix}$ y sean $N = N_{nr}$, $N_1 = N_{(n-1)r}$ y $N_2 = N_{n(r-1)}$. Note que $N_1 + N_2 = N$ pues $\begin{pmatrix} n+r-2 \\ r \end{pmatrix} + \begin{pmatrix} n+r-2 \\ r-1 \end{pmatrix} = \begin{pmatrix} n+r-1 \\ r \end{pmatrix}$.

Dividimos la matriz M en cajas, $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ donde A es una submatriz de tamaño $N_1 \times N_1$ y D de $N_2 \times N_2$. La matriz A corresponde a los primeros N_1 vectores $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{N_1}$ con el orden lexicográfico que son los que tienen $a_{i1} = 0$. Por hipótesis de inducción en el caso $(n-1, r)$ podemos elegir vectores de K^{n-1}, $\widetilde{\boldsymbol{a}}_i = (a_{i2}, ..., a_{in})$, $i = 1, \cdots, N_1$, de modo que $\det \begin{pmatrix} \widetilde{\boldsymbol{a}}_1^* \\ \vdots \\ \widetilde{\boldsymbol{a}}_{N_1}^* \end{pmatrix} \neq 0$. Sea $\boldsymbol{a}_i = (0, a_{i2}, \cdots, a_{in})$, $1 \leq i \leq N_1$, entonces $A = \begin{pmatrix} \widetilde{\boldsymbol{a}}_1^* \\ \vdots \\ \widetilde{\boldsymbol{a}}_{N_1}^* \end{pmatrix}$, $\det A \neq 0$ y para estos vectores la matriz $B = 0$ ya que en todas sus entradas aparece algún a_{i1}.

Las entradas de la matriz D corresponde a los monomios de $\boldsymbol{a}_{N_1+1}^*, \cdots, \boldsymbol{a}_N^*$ en los que aparece el término a_{i1}. Sacando factor común a_{i1} en cada fila de la matriz D obtenemos la matriz $\begin{pmatrix} \widehat{\boldsymbol{a}}_{N_1+1}^* \\ \vdots \\ \widehat{\boldsymbol{a}}_N^* \end{pmatrix}$ que está definida por monomios de grado $r-1$ y por hipótesis de inducción en el caso $(n, r-1)$ su determinante es distinto de cero.

En consecuencia, los vectores $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{N_1}, \boldsymbol{a}_{N_1+1}, \cdots, \boldsymbol{a}_N \in K^n$ verifican que

$$\det \begin{pmatrix} \boldsymbol{a}_1^* \\ \vdots \\ \boldsymbol{a}_N^* \end{pmatrix} = \det(A)\det(D) = a_{(N_1+1)1} \cdots a_{N1} \det(A) \det \begin{pmatrix} \widehat{\boldsymbol{a}}_{N_1+1}^* \\ \vdots \\ \widehat{\boldsymbol{a}}_N^* \end{pmatrix} \neq 0.$$

Note que $a_{(N_1+1)1}, \cdots, a_{N1}$ son todos distintos de cero en virtud de la Observación 2.3.18. ■

Proposición 2.3.20 *Si A es una $K-$álgebra finita local con ideal maximal $\mathfrak{m}$, cuerpo residual L y $o(\mathfrak{m}) = r$ entonces existe $a \in \mathfrak{m}$ tal que $a, a^2, ..., a^{r-1}$ son linealmente independientes sobre L.*

Demostración. Por el Teorema 2.3.11, existe L extensión finita de K tal que $A = L[x_1, ..., x_n]/I$ con $\{x_1, ..., x_n\}$ base de $\mathfrak{m}$ como $L-$espacio vectorial. Tenemos dos casos:
(1) Si existe i tal que $x_i^{r-1} \neq 0$ entonces $o(x_i) = r$ y por la Proposición 2.3.3 se tiene que $x_i, ..., x_i^{r-1}$ son linealmente independientes.
(2) Para todo i, $x_i^{r-1} = 0$. Sean $\Delta = \Delta_{n(r-1)}$ y $N = N_{n(r-1)}$ y tomemos $\alpha \in \mathfrak{m}$ genérico, $\alpha = \alpha_1 x_1 + ... + \alpha_n x_n$ donde $\alpha_1, ..., \alpha_n \in L$ entonces

$$\alpha^{r-1} = \sum_{(i_1,...,i_n)\in\Delta} \lambda_{i_1...i_n} \alpha_1^{i_1} ... \alpha_n^{i_n} x_1^{i_1} ... x_n^{i_n}$$

Note que $\lambda_{i_1...i_n} \in \mathbb{Z}-\{0\}$. Si $\boldsymbol{\alpha}^* = (\alpha_1^{i_1} ... \alpha_n^{i_n})_{(i_1,...,i_n)\in\Delta}$ y $\boldsymbol{y}^* = (\lambda_{i_1...i_n} x_1^{i_1} ... x_n^{i_n})_{(i_1,...,i_n)\in\Delta}$ entonces α^{r-1} es el producto matricial de $\boldsymbol{\alpha}^*$ y la traspuesta de $\boldsymbol{y}^*$ esto es $\alpha^{r-1} = \boldsymbol{\alpha}^* \boldsymbol{y}^{*t}$.
En virtud de la Proposición 2.3.19, elegimos $\boldsymbol{a}_1, ..., \boldsymbol{a}_N \in L^n$ tales que

$$\varphi_{n(r-1)} \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_N \end{pmatrix} = \det \begin{pmatrix} \boldsymbol{a}_1^* \\ \vdots \\ \boldsymbol{a}_N^* \end{pmatrix} \neq 0.$$

Si $\boldsymbol{a}_i = (a_{i1}, \cdots, a_{in})$, llamamos $b_i = \sum_{j=1}^n a_{ij} x_j$ para todo $i = 1, \cdots, N$.
Como $\boldsymbol{a}_1^*, ..., \boldsymbol{a}_N^*$ son base de L^N, existen $\gamma_{\boldsymbol{i}1}, ..., \gamma_{\boldsymbol{i}N} \in L$ tales, que para todo $\boldsymbol{i} = (i_1, \cdots, i_n) \in \Delta$,

$$\gamma_{\boldsymbol{i}1} \boldsymbol{a}_1^* + ... + \gamma_{\boldsymbol{i}N} \boldsymbol{a}_N^* = \boldsymbol{e}_{\boldsymbol{i}}$$

donde $\boldsymbol{e}_{\boldsymbol{i}} \in L^N$ es el vector fila de entrada 1 en la posición $\boldsymbol{i}$ y cero en las otras entradas.
Si $\alpha^{r-1} = 0$ para todo $\alpha \in \mathfrak{m}$, y como $b_i \in \mathfrak{m}$ para todo $i = 1, \cdots, N$ entonces $b_i^{r-1} = \boldsymbol{a}_i^* \boldsymbol{y}^{*t} = 0$. Por tanto $\boldsymbol{e}_{\boldsymbol{i}} \boldsymbol{y}^{*t} = 0$ pero $\boldsymbol{e}_{\boldsymbol{i}} \boldsymbol{y}^{*t} = \lambda_{i_1...i_n} x_1^{i_1} ... x_n^{i_n}$ y $\lambda_{i_1...i_n} \neq 0$ luego $x_1^{i_1} ... x_n^{i_n} = 0$ para todo $\boldsymbol{i} = (i_1, ..., i_n) \in \Delta$ lo cual es absurdo pues $o(\mathfrak{m}) = r$. Porque

si $o(\alpha) < r$ para todo $\alpha \in \mathfrak{m}$, existe $s \leq r-1$ con $o(\alpha) \leq s$ para todo $\alpha \in \mathfrak{m}$ y $o(\mathfrak{m}) \leq s < r$. ■

Proposición 2.3.21 *Si $o(\mathfrak{m}) = r$ y $r = i_1 + \cdots + i_n$ con $i_j \in \mathbb{Z}_{\geq 0}$ para todo $j = 1, \ldots, n$, $n \leq r$, entonces para todos $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}$, $\alpha_1^{i_1} \cdots \alpha_n^{i_n} = 0$.*

Demostración. Si $o(\mathfrak{m}) = r$, entonces $\mathfrak{m}^r = 0$. Note que $\mathfrak{m}^r$ es el ideal generado por $\alpha_1 \cdots \alpha_r$ tales que $\alpha_1, \ldots, \alpha_r \in \mathfrak{m}$. Como $i_1 + \cdots + i_n = r$, $\alpha_1^{i_1} \cdots \alpha_n^{i_n} \in \mathfrak{m}^r$ y en consecuencia $\alpha_1^{i_1} \cdots \alpha_n^{i_n} = 0$. ■

2.4. $\mathbb{R}-$álgebras locales finitas

Sea A una $\mathbb{R}-$álgebra local de dimensión finita con maximal $\mathfrak{m} = \{a \in A : a \text{ es divisor de cero}\}$. Como $\mathbb{R}$ tiene sólo dos extensiones finitas, $\mathbb{R}$ y $\mathbb{C}$, y por el Teorema 2.3.11, A es una $\mathbb{R}-$álgebra local de dimensión finita si y sólo si $A = L[x_1, ..., x_n]/I$ y existe r tal que $(x_1, ..., x_n)^r \subset I \subset (x_1, \cdots, x_n)$ y $L = \mathbb{R}$ o $\mathbb{C}$.

Proposición 2.4.1 *Para todo $\alpha \in A$, existen $a, b \in \mathbb{R}$ y $d \in \mathbb{N}$ tales que $\beta = a\alpha + b$ y*

$$\beta^d = 0 \quad o \quad (\beta^2 + 1)^d = 0.$$

Demostración. Sea $\alpha \in A$, como $\dim_{\mathbb{R}} A$ es finita, existe el polinomio mínimo de α, $p(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$ esto es $p(\alpha) = 0$.
Caso 1. Si $p(x)$ tiene una raíz real a con multiplicidad r entonces $p(x) = (x-a)^r q(x)$, $1 \leq r \leq d$, con $(x-a) \nmid q(x)$, es decir, existe $h(x)$ tal que $q(x) = (x-a)h(x) + q(a)$ y $q(a) \neq 0$. Tenemos dos opciones:
(1) $r = d$. En este caso $q(x) = 1$ pues $p(x)$ es mónico y si $\beta = \alpha - a$ entonces $\beta^d = 0$.
(2) $1 \leq r < d$. Note que $(x-a)^r$ y $q(x)$ tienen grado menor que d, luego $(\alpha - a)^r \neq 0$ y $q(\alpha) \neq 0$. Como $0 = p(\alpha) = (\alpha - a)^r q(\alpha)$, $(\alpha - a)^r$ y $q(\alpha)$ son divisores de cero, y por tanto están en $\mathfrak{m}$. Veamos que $q(\alpha) \notin \mathfrak{m}$ y se llega a contradicción.
En efecto, como $(\alpha - a)^r \in \mathfrak{m}$, $(\alpha - a) \in \mathfrak{m}$ ya que $\mathfrak{m}$ es primo y puesto que $q(x) - q(a) = (x-a)h(x)$ entonces $q(\alpha) - q(a) = (\alpha - a)h(\alpha) \in \mathfrak{m}$. De esta forma, $q(\alpha) + \mathfrak{m} = q(a) + \mathfrak{m}$, pero $q(a) \in \mathbb{R}$ y $q(a) \neq 0$. En consecuencia $q(a) + \mathfrak{m} \neq 0$ y $q(\alpha) \notin \mathfrak{m}$.
Caso 2. Si $p(x)$ sólo tiene raíces complejas no reales, su grado es par $d = 2s$. Cada par de raíces complejas conjugadas corresponde a un par de reales a y $b \neq 0$ tales que $((x-a)^2 + b^2) | p(x)$. Con el cambio de variable $y = \frac{x-a}{b}$ tenemos que $(y^2 + 1) | \widetilde{p}(y)$ con $\widetilde{p}(y) = p(by + a)$ y si el par de raíces complejas conjugadas tienen multiplicidad r entonces $\widetilde{p}(y) = (y^2 + 1)^r q(y)$, $1 \leq r \leq s$, con $(y^2 + 1) \nmid q(y)$. Igual que en el caso 1, tenemos dos opciones:

(2.1) $r = s$ y $q(y)$ tiene grado cero. Sea $\beta = \frac{\alpha - a}{b}$ entonces $0 = \widetilde{p}(\beta) = (\beta^2+1)^s q(\beta)$ y $q(\beta) \in \mathbb{R}$, $q(\beta) \neq 0$. Por tanto $(\beta^2+1)^s = 0$.
(2.2) $1 \leq r < s$. Veamos que esto es imposible. Como $(y^2+1)^r$ y $q(y)$ tienen grado menor que s, para $\beta = \frac{\alpha-a}{b}$, $(\beta^2+1)^r \neq 0$ y $q(\beta) \neq 0$. Luego $0 = p(\beta) = (\beta^2+1)^r q(\beta)$ implica que $(\beta^2+1)^r$ y $q(\beta)$ son divisores de cero y por tanto están en el maximal. Veamos que $q(\beta) \in \mathfrak{m}$ lleva a una contradicción. En efecto, como $(\beta^2+1)^r \in \mathfrak{m}$, $(\beta^2+1) \in \mathfrak{m}$ ya que $\mathfrak{m}$ es primo y como $q(y)$ tiene otro par de raíces complejas conjugadas distintas del anterior con multiplicidad $t \geq 1$ entonces existen a_1 y b_1 reales distintos de 0 y ± 1 tales que $((y-a_1)^2+b_1^2)^t | q(y)$. Luego $q(y) = ((y-a_1)^2+b_1^2)^t h(y)$ donde o bien $h(y) \in \mathbb{R}$, $h(y) \neq 0$, o bien sólo tiene pares de raíces complejas conjugadas. Pero $q(\beta) = ((\beta-a_1)^2+b_1^2)^t h(\beta) \in \mathfrak{m}$, entonces $((\beta-a_1)^2+b_1^2)^t \in \mathfrak{m}$ o $h(\beta) \in \mathfrak{m}$.
(2.2.1) Si $((\beta-a_1)^2+b_1^2)^t \in \mathfrak{m}$, entonces $(\beta-a_1)^2+b_1^2 \in \mathfrak{m}$ porque $\mathfrak{m}$ es primo y

$$(\beta^2+1) - ((\beta-a_1)^2+b_1^2) = 2a_1\beta - a_1^2 - b_1^2 + 1 \in \mathfrak{m}.$$

Si $a_1 = 0$ entonces $1 - b_1^2 \in \mathfrak{m}$. Luego $b_1 = \pm 1$ lo que es absurdo. Entonces $a_1 \neq 0$ y si $c = \frac{a_1^2+b_1^2-1}{2a_1}$, $\beta - c \in \mathfrak{m}$. Por tanto $\beta^2 - c^2 \in \mathfrak{m}$ y como $\beta^2+1 \in \mathfrak{m}$ entonces $1+c^2 \in \mathfrak{m}$, lo cual es absurdo pues una suma de cuadrados reales donde uno de ellos es distinto de cero no puede estar en el maximal.
(2.2.2) Si $h(\beta) \in \mathfrak{m}$, entonces $h(y)$ sólo tiene pares de raíces complejas conjugadas. Repitiendo el argumento anterior inductivamente tenemos un absurdo porque suprimiendo pares de raíces conjugadas se llega a que $h(\beta) \in \mathbb{R}$, $h(\beta) \neq 0$, y no puede estar en $\mathfrak{m}$. ■

Definición 2.4.2 *Si $\alpha \in A$ verifica que existen $a, b \in \mathbb{R}$ y existe $d \in \mathbb{N}$ tales que $\beta = a\alpha + b$ y $\beta^d = 0$ diremos que α es de tipo real y si $\alpha \in A$ verifica que existen $a, b \in \mathbb{R}$ y existe $d \in \mathbb{N}$ tales que $\beta = a\alpha + b$ y $(\beta^2+1)^d = 0$ diremos que α es de tipo complejo.*

En la Proposición 2.4.4 vamos a mostrar una propiedad de las $\mathbb{R}-$álgebras locales finitas con elementos de tipo complejo, para esto necesitamos el lema siguiente.

Lema 2.4.3 *Sea $\beta \in A$. Para todo natural, $n \geq 1$,*

$$\sum_{i=0}^{n-1} \binom{n}{i+1} \beta^{2i} = \sum_{i=0}^{n-1} (\beta^2+1)^i$$

Demostración. Para la demostración utilizaremos inducción sobre n. El caso $n = 2$ es inmediato pues

$$\sum_{i=0}^{1} \binom{2}{i+1} \beta^{2i} = 2 + \beta^2 = 1 + (\beta^2+1) = \sum_{i=0}^{1} (\beta^2+1)^i.$$

Supongamos cierto el caso $n = k$,

$$\sum_{i=0}^{k-1} \binom{k}{i+1} \beta^{2i} = \sum_{i=0}^{k-1} (\beta^2+1)^i$$

y veamos que se cumple el caso $n = k+1$,

$$\sum_{i=0}^{k} \binom{k+1}{i+1} \beta^{2i} = \sum_{i=0}^{k} (\beta^2+1)^i.$$

En efecto,

$$\begin{aligned}
\sum_{i=0}^{k} (\beta^2+1)^i &= \sum_{i=0}^{k-1} (\beta^2+1)^i + (\beta^2+1)^k = \sum_{i=0}^{k-1} \binom{k}{i+1} \beta^{2i} + \sum_{i=0}^{k} \binom{k}{i} \beta^{2i} \\
&= \sum_{i=0}^{k-1} \left[\binom{k}{i+1} + \binom{k}{i} \right] \beta^{2i} + \beta^{2k} \\
&= \sum_{i=0}^{k-1} \binom{k+1}{i+1} \beta^{2i} + \beta^{2k} = \sum_{i=0}^{k} \binom{k+1}{i+1} \beta^{2i}.
\end{aligned}$$

En la segunda igualdad se ha usado la hipótesis de inducción y el desarrollo del binomio $(\beta^2+1)^k$ y en la cuarta igualdad se usó la identidad de Pascal. ■

Proposición 2.4.4 *Si en A existe un elemento α de tipo complejo entonces existe, salvo el signo, un único elemento $\gamma \in A$ tal que $\gamma^2 + 1 = 0$.*

Demostración. Como $\alpha \in A$ es un elemento de tipo complejo, existen $a, b \in \mathbb{R}$ y existe $d \in \mathbb{N}$ tales que $\beta = a\alpha + b$ y $(\beta^2+1)^d = 0$, pero

$$(\beta^2+1)^d = \sum_{i=1}^{d} \binom{d}{i} \beta^{2i} + 1,$$

entonces existe un polinomio en β^2, $p(\beta^2) = \sum_{i=1}^{d} \binom{d}{i} \beta^{2i}$, tal que $p(\beta^2) + 1 = 0$. Debemos ver que $p(\beta^2)$ es un cuadrado. Para esto, veamos primero que

$$\sum_{i=1}^{d} \binom{d}{i} \beta^{2i} = \beta^2 \sum_{i=0}^{d-1} (\beta^2+1)^i.$$

En efecto,

$$\sum_{i=1}^{d} \binom{d}{i} \beta^{2i} = \beta^2 \sum_{i=1}^{d} \binom{d}{i} \beta^{2(i-1)} = \beta^2 \sum_{i=0}^{d-1} \binom{d}{i+1} \beta^{2i} = \beta^2 \sum_{i=0}^{d-1} (\beta^2+1)^i$$

en la última igualdad se usó el Lema 2.4.3. Ahora probamos que existen $a_i \in \mathbb{R}$, $i = 0, \ldots, d-1$, tales que

$$\sum_{i=0}^{d-1}(\beta^2+1)^i = \left(\sum_{i=0}^{d-1} a_i(\beta^2+1)^i\right)^2.$$

Por facilidad en los cálculos hacemos el cambio de variable $x = \beta^2 + 1$. Así, debemos ver que si $x^d = 0$ entonces existen $a_i \in \mathbb{R}$, $i = 0, \ldots, d-1$, tales que

$$\sum_{i=0}^{d-1} x^i = \left(\sum_{i=0}^{d-1} a_i x^i\right)^2. \tag{2.3}$$

En efecto, $\left(\sum_{i=0}^{d-1} a_i x^i\right)^2 = \sum_{i=0}^{2(d-1)} \left(\sum_{k=0}^{i} a_k a_{i-k}\right) x^i$ pero $x^d = 0$ y en consecuencia $\left(\sum_{i=0}^{d-1} a_i x^i\right)^2 = \sum_{i=0}^{d-1} \left(\sum_{k=0}^{i} a_k a_{i-k}\right) x^i$. Por la Ecuación (2.3),

$$\sum_{i=0}^{d-1}\left(\sum_{k=0}^{i} a_k a_{i-k}\right) x^i = \sum_{i=0}^{d-1} x^i.$$

Por tanto, para cada $0 \leq i \leq d-1$, $\sum_{k=0}^{i} a_k a_{i-k} = 1$. Pero

$$\sum_{k=0}^{i} a_k a_{i-k} = \begin{cases} 2\sum_{k=0}^{\frac{i-1}{2}} a_k a_{i-k} & \text{si} \quad i \text{ es impar} \\ a_{\frac{i}{2}}^2 + 2\sum_{k=0}^{\frac{i-2}{2}} a_k a_{i-k} & \text{si} \quad i \text{ es par} \end{cases}$$

Luego $\sum_{k=0}^{i} a_k a_{i-k} = 1$ implica que $a_0 = \pm 1$ y, para cada $1 \leq i \leq d-1$,

$$a_i = \begin{cases} \left(1 - 2\sum_{k=1}^{\frac{i-1}{2}} a_k a_{i-k}\right)/2a_0 & \text{si} \quad i \text{ es impar} \\ \left(1 - a_{\frac{i}{2}}^2 - 2\sum_{k=1}^{\frac{i-2}{2}} a_k a_{i-k}\right)/2a_0 & \text{si} \quad i \text{ es par} \end{cases}$$

Note que cada a_i, $1 \leq i \leq d-1$, se obtiene iterativamente. Así tenemos la solución del sistema 2.3 y en consecuencia existe $\gamma = \sqrt{p(\beta^2)}$ tal que $\gamma^2 + 1 = 0$.
Unicidad de $\gamma \in A$, salvo el signo: si A tiene dos elementos de tipo complejo, existen γ y λ tales que $\gamma^2+1 = 0$ y $\lambda^2+1 = 0$. Luego, $0 = (\gamma^2+1)-(\lambda^2+1) = \gamma^2-\lambda^2 = (\gamma-\lambda)(\gamma+\lambda)$. Si $(\gamma-\lambda) \neq 0$ y $(\gamma+\lambda) \neq 0$ entonces $\gamma-\lambda$ y $\gamma+\lambda$ son divisores de cero y por tanto están en $\mathfrak{m}$. Como $(\gamma+\lambda)+(\gamma-\lambda) = 2\gamma \in \mathfrak{m}$ y $(\gamma+\lambda)-(\gamma-\lambda) = 2\lambda \in \mathfrak{m}$ entonces γ y λ están en $\mathfrak{m}$ pero $\gamma^2+1 \in \mathfrak{m}$ entonces $1 \in \mathfrak{m}$ lo que es absurdo. En consecuencia, $\gamma+\lambda = 0$ o $\gamma-\lambda = 0$ entonces $\gamma = \lambda$ o $\gamma = -\lambda$. ■

Ejemplo 2.4.5 *La $\mathbb{R}-$álgebra local finita $A = \frac{\mathbb{R}[x]}{((x^2+1)^2)}$ tiene elementos de tipo com-*

plejo y $\gamma = \frac{3}{2}\overline{x} + \frac{1}{2}\overline{x}^3 \in A$ *es el único elemento, salvo signo, tal que* $\gamma^2 + 1 = 0$.

Proposición 2.4.6 *Para todo n, entero positivo,*

$$\frac{\mathbb{R}[x]}{((x^2+1)^n)} \simeq \frac{\mathbb{C}[x]}{(x^n)}.$$

Demostración. Por el Lema 2.2.9, el ideal maximal de la $\mathbb{R}-$álgebra local finita $A = \frac{\mathbb{R}[x]}{((x^2+1)^n)}$ es $\mathfrak{m} = (\overline{x}^2+1)$ y como A tiene elementos de tipo complejo, por la Proposición 2.4.4, existe $\boldsymbol{\gamma} = \gamma(x) + ((x^2+1)^n) \in A$ con $\gamma(x) \in K[x]$, grado$(\gamma) < 2n$ y tal que $\boldsymbol{\gamma}^2 + 1 = 0$. Observe que
(i) Como $\boldsymbol{\gamma}^2 + 1 = 0$, $\gamma^2 + 1 \in ((x^2+1)^n)$.
(ii) $\boldsymbol{\gamma}$ es inversible ya que $\boldsymbol{\gamma}(-\boldsymbol{\gamma}) = 1$.
(iii) $\overline{x}^2+1 = (\overline{x}-\boldsymbol{\gamma})(\overline{x}+\boldsymbol{\gamma})$ en A, o equivalentemente $x^2+1-(x-\gamma)(x+\gamma) \in ((x^2+1)^n)$.
Veamos que $((x^2+1)^n) = ((x-\gamma)^n, \gamma^2+1)$.
$\subset]$ Como $x^2+1 = (x-\gamma)(x+\gamma) + (\gamma^2+1)$ entonces $(x^2+1)^n = (x-\gamma)^n(x+\gamma)^n + (\gamma^2+1)q(x)$ y por tanto $((x^2+1)^n) \subset ((x-\gamma)^n, \gamma^2+1)$.
$\supset]$ Por (iii), $(\overline{x}-\boldsymbol{\gamma})(\overline{x}+\boldsymbol{\gamma}) \in \mathfrak{m}$. Como $\mathfrak{m}$ es primo, $\overline{x}-\boldsymbol{\gamma} \in \mathfrak{m}$ o $\overline{x}+\boldsymbol{\gamma} \in \mathfrak{m}$ pero no las dos cosas ya que si $\overline{x}-\boldsymbol{\gamma}, \overline{x}+\boldsymbol{\gamma} \in \mathfrak{m}$ entonces $\overline{x}+\boldsymbol{\gamma}-(\overline{x}-\boldsymbol{\gamma}) = 2\boldsymbol{\gamma} \in \mathfrak{m}$ lo cual es absurdo pues 2 y $\boldsymbol{\gamma}$ son inversibles. Sin pérdida de generalidad supongamos que $\overline{x}-\boldsymbol{\gamma} \in \mathfrak{m}$, de lo contrario cambiamos $\boldsymbol{\gamma}$ por $-\boldsymbol{\gamma}$ ya que $\boldsymbol{\gamma}$ es único salvo el signo.
Como $\overline{x}+\boldsymbol{\gamma} \notin \mathfrak{m}$, $\overline{x}+\boldsymbol{\gamma}$ es inversible en A y existe $p(\overline{x}) \in A$ tal que $(\overline{x}+\boldsymbol{\gamma})p(\overline{x}) = 1$ luego $(x+\gamma)p(x) - 1 \in ((x^2+1)^n)$. Entonces $(x+\gamma)^n p(x)^n - 1 \in ((x^2+1)^n)$ y multiplicando por $(x-\gamma)^n$,

$$(x-\gamma)^n(x+\gamma)^n p(x)^n - (x-\gamma)^n \in ((x^2+1)^n). \tag{2.4}$$

Como $x^2+1-(x-\gamma)(x+\gamma) \in ((x^2+1)^n)$, $(x^2+1)^n - (x-\gamma)^n(x+\gamma)^n \in ((x^2+1)^n)$ y $(x-\gamma)^n(x+\gamma)^n \in ((x^2+1)^n)$. Luego de la Ecuación (2.4), $(x-\gamma)^n \in ((x^2+1)^n)$ y por el item (i), $(\gamma^2+1, (x-\gamma)^n) \subset ((x^2+1)^n)$.
En consecuencia,

$$\frac{\mathbb{R}[x]}{((x^2+1)^n)} \simeq \frac{\mathbb{R}[y,z]}{((y-z)^n, z^2+1)}.$$

Para finalizar comprobamos el isomorfismo $\frac{\mathbb{R}[y,z]}{((y-z)^n, z^2+1)} \simeq \frac{\mathbb{C}[t]}{(t^n)}$.
Sean $\overline{y} = y + ((y-z)^n, z^2+1)$ y $\overline{z} = z + ((y-z)^n, z^2+1)$.
Si $n = 1$, entonces $\frac{\mathbb{R}[x]}{(x^2+1)} \simeq \frac{\mathbb{R}[y,z]}{(y-z, z^2+1)} = \{a + \overline{z}b : a, b \in \mathbb{R}, \overline{z}^2 + 1 = 0\} = \mathbb{C}$.
Si $n \geq 2$, consideramos

$$\begin{array}{rccc} \phi: & \mathbb{C}[t] = \mathbb{R}[t] + i\mathbb{R}[t] & \to & \frac{\mathbb{R}[y,z]}{((y-z)^n, z^2+1)} \\ & t & \mapsto & \widetilde{t} = \overline{y} - \overline{z} \\ & i & \mapsto & \overline{z} \\ & p(t) + iq(t) & \mapsto & p(\widetilde{t}) + \overline{z}q(\widetilde{t}). \end{array}$$

- ϕ es un homomorfismo.
  $\phi((p(t)+iq(t))+(f(t)+ig(t))) = \phi((p+f)(t)+i(q+g)(t)) = (p+f)(\widetilde{t})+\overline{z}(q+g)(\widetilde{t}) = (p(\widetilde{t}) + \overline{z}q(\widetilde{t})) + (f(\widetilde{t}) + \overline{z}g(\widetilde{t})) = \phi(p(t) + iq(t)) + \phi(f(t) + ig(t))$.

- $\mathrm{Ker}(\phi) = (t^n)$. Primero observe que $\widetilde{t} \neq 0$ pues $n \geq 2$, y 1 y $\overline{z}$ son $\mathbb{R}[\overline{y}]-$linealmente independientes. Entonces $0 = \phi(p(t) + iq(t)) = \ p(\widetilde{t}) + \overline{z}q(\widetilde{t})$ implica $p(\widetilde{t}) = 0$ y $q(\widetilde{t}) = 0$. Luego $p(y-z), q(y-z) \in ((y-z)^n)$ es decir $p(t), q(t) \in (t^n)$. Así, $p(t) + iq(t) \in (t^n)$.

En consecuencia, $\overline{\phi} : \frac{\mathbb{C}[t]}{(t^n)} \to \frac{\mathbb{R}[y,z]}{((y-z)^n, z^2+1)}$ es inyectiva y como

$$\dim_{\mathbb{R}} \frac{\mathbb{C}[t]}{(t^n)} = \dim_{\mathbb{R}} \frac{\mathbb{R}[y,z]}{((y-z)^n, z^2+1)} = \dim_{\mathbb{R}} \frac{\mathbb{R}[x]}{((x^2+1)^n)} = 2n$$

se tiene que $\frac{\mathbb{R}[y,z]}{((y-z)^n,z^2+1)} \simeq \frac{\mathbb{C}[t]}{(t^n)}$. ■

Corolario 2.4.7 *Si*

$$f(x) = (x-a_1)^{n_1} \cdots (x-a_r)^{n_r}((x-c_1)^2 + b_1^2)^{m_1} \cdots ((x-c_s)^2 + b_s^2)^{m_s} \in \mathbb{R}[x]$$

entonces

$$\frac{\mathbb{R}[x]}{(f(x))} \simeq \frac{\mathbb{R}[x]}{(x^{n_1})} \times \cdots \times \frac{\mathbb{R}[x]}{(x^{n_r})} \times \frac{\mathbb{R}[x]}{((x^2+1)^{m_1})} \times \cdots \times \frac{\mathbb{R}[x]}{((x^2+1)^{m_s})} \simeq \bigoplus_{i=1}^{r} \frac{\mathbb{R}[x]}{(x^{n_i})} \times \bigoplus_{j=1}^{s} \frac{\mathbb{C}[x]}{(x^{m_j})}.$$

Proposición 2.4.8 *Si A es una $\mathbb{R}-$álgebra local finita, ocurre una de las dos opciones:*

(1) para todo $\alpha \in A$ existen $a, b \in \mathbb{R}$ y existe $d \in \mathbb{N}$ tales que $(a\alpha + b)^d = 0$.

(2) existe $\beta \in A$ único, salvo el signo, tal que $\beta^2 + 1 = 0$.

Demostración. Las dos opciones son consecuencia de la Proposición 2.4.1 y la existencia y unicidad de $\beta \in A$, en la opción 2, se tiene por la Proposición 2.4.4. ■

Proposición 2.4.9 *Una $\mathbb{R}-$álgebra local finita A es una $\mathbb{C}-$álgebra local finita si y sólo si existe en A un elemento de tipo complejo.*

Demostración. $\Leftarrow$: Si A es una $\mathbb{R}-$álgebra local finita con un elemento de tipo complejo entonces, por la Proposición 2.4.4, existe un $\gamma \in A$ tal que $\gamma^2 + 1 = 0$. Como $x^2 + 1$ es irreducible, $x^2 + 1$ es el polinomio mínimo de γ. Además, puesto que $\mathbb{R} \subset A$, el homomorfismo evaluación

$$\begin{array}{rccc} \varphi : & \mathbb{R}[x] & \to & A \\ & x & \mapsto & \gamma \end{array}$$

tiene $\mathrm{Ker}(\varphi) = (x^2+1)$ ya que $\varphi(q(x)) = 0 \Leftrightarrow q(\gamma) = 0 \Leftrightarrow x^2+1 | q(x) \Leftrightarrow q(x) \in (x^2+1)$. Además como $\mathbb{C} \simeq \frac{\mathbb{R}[x]}{(x^2+1)}$ entonces

$$\widetilde{\varphi} : \frac{\mathbb{R}[x]}{(x^2+1)} \to A$$

es un homomorfismo de anillos de $\mathbb{C}$ en A que dota a A de estructura de $\mathbb{C}-$álgebra. Note que A tiene dimensión finita como $\mathbb{C}-$espacio vectorial ya que $\dim_{\mathbb{R}} A = 2 \dim_{\mathbb{C}} A$ y $\dim_{\mathbb{R}} A$ es finita.
$\Rightarrow$: Si A es una $\mathbb{C}-$álgebra local finita, como $\mathbb{R} \subset \mathbb{C}$ y tenemos el morfismo estructural

$$\begin{array}{ccc} \mathbb{C} & \to & A \\ a & \mapsto & a1 \end{array}$$

entonces A es una $\mathbb{R}-$álgebra local finita y tiene un elemento de tipo complejo ya que existe $(1i) \in A$ tal que $(i1)^2 + 1 = 0$. ■

Por las Proposiciones 2.4.8 y 2.4.9, el problema de clasificar las $\mathbb{R}-$álgebras locales finitas se reduce a los siguientes dos problemas:

(1) clasificar las $\mathbb{R}-$álgebras locales finitas con todos los elementos de tipo real.

(2) clasificar las $\mathbb{C}-$álgebras locales finitas.

2.5. Criterios de isomorfía de $K-$álgebras locales finitas.

El problema que abordamos en esta sección es el de dar condiciones necesarias para que dos $K-$álgebras locales finitas sean isomorfas. Estos criterios nos permitirán saber si dos $K-$álgebras pertenecen a la misma clase de isomorfía.

2.5.1. Estructuras geométricas

Sea A un $K-$espacio vectorial de dimensión finita n. Llamamos estructura geométrica asociada a A a lo siguiente: consideremos los elementos de A que verifican una propiedad P invariante por isomorfismos. Es decir, $\alpha \in A$ verifica la propiedad P si y sólo si para todo isomorfismo f de A en B, $f(\alpha)$ verifica la propiedad P en B. Por ejemplo,

$$\begin{array}{l} \alpha^r = 0 \\ \alpha^r = \alpha \\ \alpha \ \text{ divisor de cero} \\ \alpha^r = 1 \end{array}$$

Sean $V_A(\mathrm{P})$ y $V_B(\mathrm{P})$ los conjuntos de elementos en A y B, respectivamente, que verifican la propiedad P.

Si $f : A \to B$ es un isomorfismo de $K-$álgebras finitas en particular f es $K-$lineal, como P es invariante por f, $V_A(\mathrm{P}) \backsimeq V_B(\mathrm{P})$. Por tanto las propiedades lineales o multilineales de $V_A(\mathrm{P})$ y $V_B(\mathrm{P})$ son las mismas.

2.5.2. Dimensión de las potencias del maximal

Proposición 2.5.1 *Si A es una $K-$álgebra local finita y $\mathfrak{m}$ su ideal maximal y sea $S_i = \dim_K \mathfrak{m}^i$ donde $S_0 = \dim_K A$ entonces la sucesión de números,*

$$S_A : \quad S_1 > S_2 > \cdots > S_r = S_{r+1}$$

(1) es estacionaria y su último término es cero.

(2) Si $A \simeq B$, entonces $S_A = S_B$.

Demostración. *(1)* Como A es de dimensión finita, la sucesión

$$\mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots \supset \mathfrak{m}^s$$

es finita. Note que $\mathfrak{m}^r = \mathfrak{m}^{r+1}$ implica que $\mathfrak{m}^s = \mathfrak{m}^r$ para todo $s > r$ ya que multiplicando por $\mathfrak{m}$,

$$\mathfrak{m}^r = \mathfrak{m}^{r+1} = \mathfrak{m}^{r+2} = \cdots .$$

Además, por la Proposición 2.3.1, existe s tal que $\mathfrak{m}^s = 0$. En conclusión la sucesión S_A es estacionaria y su último término es cero.
(2) Sea $f : A \to B$ un isomorfismo. Entonces

$$f(\mathfrak{m}^r) = (f(\mathfrak{m}))^r$$

En efecto, puesto que $f(\mathfrak{m}_A) = \mathfrak{m}_B$,

$$\begin{aligned} \alpha \in \mathfrak{m}_A^r \quad &\Leftrightarrow \quad \alpha = \sum_i \alpha_{i_1} \cdots \alpha_{i_r} \ \text{ con } \ \alpha_{i_j} \in \mathfrak{m}_A \\ &\Leftrightarrow \quad f(\alpha) = \sum_i f(\alpha_{i_1}) \cdots f(\alpha_{i_r}) \ \text{ con } \ f(\alpha_{i_j}) \in \mathfrak{m}_B \\ &\Leftrightarrow \quad f(\alpha) \in \mathfrak{m}_B^r. \end{aligned}$$

Por tanto, $S_A = S_B$. ■

En consecuencia,

$$\text{mín}\{s : \mathfrak{m}^s = 0\}$$

y las dimensiones

$$S_i = \dim_{\mathbb{R}} \mathfrak{m}^i \quad \text{y} \quad \dim_{\mathbb{R}} \mathfrak{m}^i/\mathfrak{m}^{i+1} = S_i - S_{i+1}$$

son invariantes por isomorfía.

2.5.3. Cuádricas.

Si A y B son $K-$álgebras locales finitas, por la Proposición 2.3.9, existen L_A y L_B extensiones finitas de K y existen ideales I y J de $L_A[x_1,...,x_n]$ y $L_B[y_1,...,y_m]$ respectivamente con $I = (\{u_i, v_{ij}\}_{1\leq i<j\leq n})$ donde $u_i := x_i^2 - \sum_{j=1}^n a_{ij}x_j$ y $v_{ij} := x_ix_j - \sum_{k=1}^n a_{ijk}x_k$, $J = (\{q_i, r_{ij}\}_{1\leq i<j\leq m})$ donde $q_i := y_i^2 - \sum_{j=1}^n b_{ij}y_j$ y $r_{ij} := y_iy_j - \sum_{k=1}^n b_{ijk}y_k$, y tales que $A = L_A[x_1,...,x_n]/I$ y $B = L_B[y_1,...,y_m]/J$.
Si $A \simeq B$ entonces $\mathfrak{m}_A \simeq \mathfrak{m}_B$ y $A/\mathfrak{m}_A \simeq B/\mathfrak{m}_B$ por tanto $n = m$ y $L_A \simeq L_B$. Es decir, si $\widetilde{\varphi} : A \to B$ es un isomorfismo entonces existe un cuerpo L tal que $A = L[x_1,...,x_n]/I$, $B = L[y_1,...,y_n]/J$ y $\widetilde{\varphi}$ induce un isomorfismo $\varphi : L[x_1,...,x_n]/I \to L[y_1,...,y_n]/J$ y $\varphi|_L = \tau$ con $\tau \in Aut(L/K)$. En consecuencia φ queda definido por $\varphi(\overline{x}_i) = p_i(\overline{y}_1,...,\overline{y}_n)$ para todo $i = 1,\cdots,n$. Por la Proposición 2.3.9, $p_i(\overline{y}_1,...,\overline{y}_n) = \sum_{j=1}^n c_{ij}\overline{y}_j$ luego $\varphi(\overline{x}_i) = \sum_{j=1}^n c_{ij}\overline{y}_j$ donde $(c_{ij})_{1\leq i,j\leq n}$ es una matriz inversible.
Un isomorfismo de $K-$álgebras de A en B está representado por muchos homomorfismos de $L[x_1,...,x_n]$ en $L[y_1,...,y_n]$ y lo que estamos afirmando es que φ está representado por uno que es $\tau-$semilineal.
En el Ejemplo 2.2.16, el isomorfismo

$$\begin{array}{rccc} \phi: & A = \frac{\mathbb{Z}/(3)[x]}{(x^3+x^2+2)} & \to & B = \frac{\mathbb{Z}/(3)[y]}{(y^3+2y^2+1)} \\ & \overline{x} & \mapsto & 2\overline{y}^2+1 \end{array}$$

proviene de un homomorfismo $\mathbb{Z}/(3)[x] \to \mathbb{Z}/(3)[y]$ que no es una transformación lineal en x pero si cambiamos los sistemas de generadores $A = \frac{\mathbb{Z}/(3)[x_1,x_2]}{(x_1^2+2x_2, x_2^2+2x_2+2x_1+1, x_1x_2+x_2+2)}$ y $B = \frac{\mathbb{Z}/(3)[y_1,y_2]}{(y_1^2+2y_2, y_2^2+2y_2+y_1+1, y_1y_2+2y_1+1)}$ entonces φ está asociado al homomorfismo

$$\begin{array}{rccc} \phi: & \mathbb{Z}/(3)[x_1,x_2] & \to & \mathbb{Z}/(3)[y_1,y_2] \\ & x_1 & \mapsto & y_1 = 2x_2+1 \\ & x_2 & \mapsto & y_2 = 2x_2+x_1+2 \end{array}$$

Definición 2.5.2 *Sea $A = L[x_1,...,x_n]/I$, al sistema lineal de formas cuadráticas de L^n generado por $\{u_i, v_{ij}\}_{1\leq i<j\leq n}$ donde $u_i := x_i^2 - \sum_{j=1}^n a_{ij}x_j \in I$ y $v_{ij} := x_ix_j - \sum_{k=1}^n a_{ijk}x_k \in I$ o al sistema de cuádricas de $\mathbb{P}(L^n)$ asociado lo llamamos sistema lineal asociado al álgebra.*

Proposición 2.5.3 *$A \simeq B$ si y sólo si los sistemas lineales asociados son proyectivamente equivalentes.*

Demostración. $\Rightarrow$: Como $A \simeq B$, existe un isomorfismo $\tau-$semilineal φ de A en B tal que $\varphi(I) = J$ y el sistema lineal de formas cuadráticas asociado a A es un sistema de generadores del ideal I. Como φ es isomorfismo, los polinomios $\{\varphi(u_i), \varphi(v_{ij})\}_{1\leq i<j\leq n}$ generan a J, por tanto definen una base del sistema lineal de formas cuadráticas asociadas a B. En consecuencia los sistemas son equivalentes.
$\Leftarrow$: Si los sistemas lineales asociados a A y B son proyectivamente equivalentes, y con las identificaciones $\mathfrak{m}_A \simeq L^n$ y $\mathfrak{m}_B \simeq L^n$ dadas por la Proposición 2.3.9 se tiene que existe una proyectividad $\overline{\varphi} : \mathbb{P}(L^n) \to \mathbb{P}(L^n)$ que transforma el sistema generado por $\{u_i, v_{ij}\}_{1\leq i<j\leq n}$ en el sistema $\{q_i, r_{ij}\}_{1\leq i<j\leq n}$.
Si φ_1 es un representante de $\overline{\varphi}$, $\varphi_1 : L[x_1, \ldots, x_n] \to L[y_1, \ldots, y_n]$ que transforma los generadores del ideal I en elementos independientes del ideal J, entonces estos generan necesariamente a J esto es $\varphi_1(I) = J$. De esta forma φ_1 induce un isomorfismo $L[x_1, \ldots, x_n]/I \simeq L[y_1, \ldots, y_n]/J$. ■

El criterio de isomorfía de la Proposición 2.5.3 no es aplicable en general dado que lleva a comprobar la equivalencia proyectiva de dos sistemas lineales de cuádricas que están generadas casi siempre por cuádricas degeneradas y el problema de clasificar estos sistemas no está bien resuelto en la literatura.

Si $\mathfrak{m}_A$ es el ideal maximal de A, $\mathfrak{m}_B$ es el ideal de B y $A \simeq B$ entonces $\mathfrak{m}_A \simeq \mathfrak{m}_B$ y en general $\mathfrak{m}_A^r \simeq \mathfrak{m}_B^r$. Además si $\varphi : A \to B$ es un isomorfismo, por la sección 2.1, el diagrama

$$\begin{array}{ccc} \mathfrak{m}_A^r \times \mathfrak{m}_A^r & \xrightarrow{\cdot} & \mathfrak{m}_A^r \\ \downarrow{\scriptstyle \varphi\times\varphi} & & \downarrow{\scriptstyle \varphi} \\ \mathfrak{m}_B^r \times \mathfrak{m}_B^r & \xrightarrow{\cdot} & \mathfrak{m}_B^r \end{array}$$

es conmutativo, es decir, $\varphi(\mathbf{u}_1 \cdot \mathbf{u}_2) = \varphi(\mathbf{u}_1) \cdot \varphi(\mathbf{u}_2)$. Luego el producto como forma bilineal es invariante.

Si $r < s$ y $2r < o(\mathfrak{m}_A) = o(\mathfrak{m}_B) \leq r + s$ entonces el producto induce una forma bilineal para esto veamos que

$$\begin{array}{rccc} \phi: & \mathfrak{m}_A^r/\mathfrak{m}_A^s \times \mathfrak{m}_A^r/\mathfrak{m}_A^s & \to & \mathfrak{m}_A^{2r} \\ & (a + \mathfrak{m}_A^s, a' + \mathfrak{m}_A^s) & \mapsto & aa' \end{array}$$

está bien definida. Sea $(a + b + \mathfrak{m}_A^s, a' + b' + \mathfrak{m}_A^s) \in \mathfrak{m}_A^r/\mathfrak{m}_A^s \times \mathfrak{m}_A^r/\mathfrak{m}_A^s$ con $b, b' \in \mathfrak{m}_A^s$ entonces $\phi((a + b + \mathfrak{m}_A^s, a' + b' + \mathfrak{m}_A^s)) = (a + b)(a' + b') = aa' + ab' + a'b = aa'$ pues $ab', a'b \in \mathfrak{m}_A^s$.
Si A y B son isomorfos entonces las dos formas bilineales asociadas al producto son

equivalentes.
Componiendo con los elementos de $(\mathfrak{m}_A^{2r})^*$ tenemos para cada álgebra A y cada par de enteros r y s con $2r < o(\mathfrak{m}_A) \leq r+s$, un sistema lineal de cuádricas en $\mathfrak{m}_A^r/\mathfrak{m}_A^s$,

$$\mathfrak{m}_A^r/\mathfrak{m}_A^s \times \mathfrak{m}_A^r/\mathfrak{m}_A^s \longrightarrow \mathfrak{m}_A^{2r} \xrightarrow{\phi} K$$

con $\phi \in (\mathfrak{m}_A^{2r})^*$.

2.6. Infinitas $\mathbb{R}-$álgebras locales de dimensión 6

Proposición 2.6.1 *Sean $\alpha \in \mathbb{R}$ y*

$$A_\alpha = \frac{\mathbb{R}[x,y,z]}{(x^3, y^3, z^2 - x^2 - \alpha y^2, xy - x^2 - y^2, xz - x^2, yz)}.$$

$\{A_\alpha\}_{\alpha\in\mathbb{R}}$ es una familia de $\mathbb{R}-$álgebras locales de dimensión 6 con $o(\mathfrak{m}_\alpha) = 3$, base como $\mathbb{R}-$espacio $\mathcal{B} = \{1, \overline{x}, \overline{x}^2, \overline{y}, \overline{y}^2, \overline{z}\}$ y tal que para todos $\alpha, \beta \in \mathbb{R}$, $\alpha \neq \beta$, excepto para un número finito, $A_\alpha \ncong A_\beta$.

Demostración. Como $o(\mathfrak{m}_\alpha) = 3$, podemos considerar la forma bilineal asociada al producto en $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$,

$$\phi : \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 \times \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2 \to \mathfrak{m}_\alpha^2.$$

$\{\widetilde{x}, \widetilde{y}, \widetilde{z}\}$ con $\widetilde{x} = \overline{x} + \mathfrak{m}_\alpha^2$, $\widetilde{y} = \overline{y} + \mathfrak{m}_\alpha^2$ y $\widetilde{z} = \overline{z} + \mathfrak{m}_\alpha^2$ es base de $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$. Note que $\phi(\widetilde{x}, \widetilde{x}) = \overline{x}^2$, $\phi(\widetilde{x}, \widetilde{y}) = \overline{x}^2 + \overline{y}^2$, $\phi(\widetilde{x}, \widetilde{z}) = \overline{x}^2$, $\phi(\widetilde{y}, \widetilde{y}) = \overline{y}^2$, $\phi(\widetilde{y}, \widetilde{z}) = 0$ y $\phi(\widetilde{z}, \widetilde{z}) = \overline{x}^2 + \alpha\overline{y}^2$. Por tanto el haz de formas cuadráticas asociada al producto en $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2$ está generado por

$q_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ y $q_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & b \end{pmatrix}$.

Como $q_1^{-1}q_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -\alpha \\ -1 & -1 & \alpha \end{pmatrix}$, su polinomio característico es $p_\alpha(x) = x^3 - (\alpha+2)x^2 + (\alpha+1)x - \alpha$. Observe que las raíces del polinomio dependen de α y $p_\alpha(x)$ no tiene raíces múltiples, más aún, un cambio variable lineal no puede llevar un polinomio característico $p_\alpha(x)$ en otro polinomio característico $p_\beta(x)$, $\alpha \neq \beta$. Por tanto para todos $\alpha, \beta \in \mathbb{R}$, $\alpha \neq \beta$, $A_\alpha \ncong A_\beta$. ■

Observación 2.6.2 *Se puede construir una familia infinita de $\mathbb{R}-$álgebras no isomorfas de dimensión mayor que 6 y con orden de maximal $o(\mathfrak{m}_\alpha) = 3$. Por ejemplo, la*

familia de $\mathbb{R}-$*álgebras locales de dimensión 7 y* $o(\mathfrak{m}_\alpha) = 3$, $\{A_\alpha\}_{\alpha\in\mathbb{R}}$ *con*

$$A_\alpha = \frac{\mathbb{R}[x,y,z,w]}{(x^3, y^3, w^2 - x^2 - y^2, z^2 - x^2 - \alpha y^2, xy - x^2 - y^2, xz - x^2, yz, xw, yw, zw)},$$

contiene infinitas $\mathbb{R}-$*álgebras no isomorfas.*

2.7. Clasificación de las $\mathbb{R}-$álgebras reales locales finitas en dimensión baja.

Clasificamos en esta sección las $\mathbb{R}-$álgebras reales locales finitas hasta dimensión cinco y que son de tipo real. Por facilidad en la notación, en las $\mathbb{R}-$álgebras, no tomamos las clases en las bases del maximal.

2.7.1. $\mathbb{R}-$álgebras locales finitas reales de dimensión 1, 2 y 3.

(1) Si $\dim_{\mathbb{R}} A = 1$, entonces $o(\mathfrak{m}) = 1$ y por tanto A es un cuerpo. Como A es una $\mathbb{R}-$álgebra, $A \simeq \mathbb{R}$.

(2) Si $\dim_{\mathbb{R}} A = 2$, entonces $o(\mathfrak{m}) = 2$ y por tanto existe $x \in \mathfrak{m}$ tal que $x \neq 0$ y $x^2 = 0$. Por la Proposición 2.3.5(2), se tiene que $\{1, x\}$ es base de A y

$$A \simeq \frac{\mathbb{R}[x]}{(x^2)}.$$

(3) Si $\dim_{\mathbb{R}} A = 3$, entonces $1 < o(\mathfrak{m}) \leq 3$ y tenemos dos casos:

(3.1) Si $o(\mathfrak{m}) = 3$, entonces existe $x \in \mathfrak{m}$ tal que $x^2 \neq 0$ y $x^3 = 0$. Por la Proposición 2.3.5(2), se tiene que $\{1, x, x^2\}$ es base de A y

$$A \simeq \frac{\mathbb{R}[x]}{(x^3)}.$$

(3.2) Si $o(\mathfrak{m}) = 2$, entonces para todo $x \in \mathfrak{m}$, $x^2 = 0$ y por la Proposición 2.3.21, para todos $x, y \in \mathfrak{m}$, $xy = 0$. Como $\dim_{\mathbb{R}} \mathfrak{m} = 2$, existen $x, y \in \mathfrak{m}$ tales que $\{x, y\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[x,y]}{(x,y)^2}.$$

En conclusión, salvo isomorfismos, para $\dim_{\mathbb{R}} A = 3$ se tiene

$$A_1 = \frac{\mathbb{R}[x]}{(x^3)} \quad \text{o} \quad A_2 = \frac{\mathbb{R}[x,y]}{(x,y)^2}.$$

Note que las dos $\mathbb{R}-$álgebras no son isomorfas pues el orden del ideal maximal de A_1 es $o(\mathfrak{m}_1) = 3$ y el orden del ideal maximal de A_2 es $o(\mathfrak{m}_2) = 2$.

2.7.2. $\mathbb{R}-$álgebras locales finitas reales de dimensión 4.

Si $\dim_{\mathbb{R}} A = 4$, entonces $1 < o(\mathfrak{m}) \leq 4$ y tenemos tres casos:

(1) Si $o(\mathfrak{m}) = 4$, entonces existe $x \in \mathfrak{m}$ tal que $x^3 \neq 0$ y $x^4 = 0$. Por la Proposición 2.3.5(2), $\{1, x, x^2, x^3\}$ es base de A y por tanto

$$A \simeq \frac{\mathbb{R}[x]}{(x^4)}.$$

(2) Si $o(\mathfrak{m}) = 3$, entonces para todo $x \in \mathfrak{m}$, $x^3 = 0$ y por la Proposición 2.3.21 para todos $x, y \in \mathfrak{m}$, $x^2y = 0$. Además, existe $x \in \mathfrak{m}$ tal que $x^2 \neq 0$, luego x y x^2 son linealmente independientes y puesto que $\dim_{\mathbb{R}} \mathfrak{m} = 3$, existe $y \in \mathfrak{m}$ tal que $\{x, x^2, y\}$ es base de $\mathfrak{m}$. Tenemos dos casos:

(2.1) Si $xy = 0$, como $y^2 \in \mathfrak{m}$, existen $a, b, c \in \mathbb{R}$ tales que $y^2 = ax + bx^2 + cy$.

Multiplicando por y, $0 = y^3 = axy + bx^2y + cy^2 = cy^2$ entonces $c = 0$, si $y^2 \neq 0$. Multiplicando por x, $0 = xy^2 = ax^2$ pero $x^2 \neq 0$ entonces $a = 0$. Por tanto

$$y^2 = bx^2.$$

Tenemos tres casos:

(2.1.1) Si $b > 0$, sea $\gamma = \sqrt{b}x$, entonces $\gamma y = \sqrt{b}xy = 0$, $\gamma^2 = bx^2 = y^2$ y como $\{x, x^2, y\}$ es base de $\mathfrak{m}$, $\{\gamma, \gamma^2, y\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma, y]}{(\gamma^3, \gamma^2 - y^2, \gamma y)}.$$

(2.1.2) Si $b < 0$, sea $\gamma = \sqrt{-b}x$, entonces $\gamma y = 0$, $\gamma^2 = -bx^2 = -y^2$ y $\{\gamma, \gamma^2, y\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma, y]}{(\gamma^3, \gamma^2 + y^2, \gamma y)}.$$

(2.1.3) Si $b = 0$, entonces $xy = y^2 = 0$ y $\{x, x^2, y\}$ es base de $\mathfrak{m}$. Por tanto

$$A \simeq \frac{\mathbb{R}[x, y]}{(x^3, y^2, xy)}.$$

(2.2) Si $xy \neq 0$, como $xy \in \mathfrak{m}$, entonces existen $a, b, c \in \mathbb{R}$ tales que $xy = ax + bx^2 + cy$.

Multiplicando por x, $0 = x^2y = ax^2 + cxy = ax^2 + c(ax + bx^2 + cy) = acx + (a + bc)x^2 + c^2y$ entonces $ac = a + bc = c^2 = 0$ esto es $a = c = 0$. Por tanto $xy = bx^2$ y

$$x(y - bx) = 0.$$

Sea $\gamma = y - bx$ entonces $x\gamma = 0$ y $\{x, x^2, \gamma\}$ es base de $\mathfrak{m}$. Luego estamos en el caso (2.1).

(3) Si $o(\mathfrak{m}) = 2$, entonces para todo $x \in \mathfrak{m}$, $x^2 = 0$ y por la Proposición 2.3.21, para todos $x, y \in \mathfrak{m}$, $xy = 0$. Además, como $\dim_{\mathbb{R}} \mathfrak{m} = 3$, existen $x, y, z \in \mathfrak{m}$ tales que $\{x, y, z\}$ es base de $\mathfrak{m}$ y cumple que $x^2 = y^2 = z^2 = xy = xz = yz = 0$. En consecuencia

$$A \simeq \frac{\mathbb{R}[x, y, z]}{(x, y, z)^2}.$$

En $\dim_{\mathbb{R}} A = 4$, hemos encontrado cinco $\mathbb{R}-$álgebras locales finitas. Vamos a ver que ningún par de estas $\mathbb{R}-$álgebras son isomorfas. Sean

$$A_1 = \frac{\mathbb{R}[x]}{(x^4)}, \quad A_2 = \frac{\mathbb{R}[x, y]}{(x^3, y^2, xy)}, \quad A_3 = \frac{\mathbb{R}[x, y]}{(x^3, x^2 - y^2, xy)},$$

$$A_4 = \frac{\mathbb{R}[x, y]}{(x^3, x^2 + y^2, xy)} \quad \text{y} \quad A_5 = \frac{\mathbb{R}[x, y, z]}{(x, y, z)^2}.$$

Note que el orden del maximal de las $\mathbb{R}-$álgebras A_1 y A_5 son $o(\mathfrak{m}_1) = 4$ y $o(\mathfrak{m}_5) = 2$ respectivamente. Mientras que las otras tres $\mathbb{R}-$álgebras tienen orden del maximal igual a 3. Por tanto $A_1 \ncong A_2$, $A_1 \ncong A_3$, $A_1 \ncong A_4$, $A_1 \ncong A_5$, $A_2 \ncong A_5$, $A_3 \ncong A_5$ y $A_4 \ncong A_5$.

Para mostrar que $A_2 \ncong A_3$, $A_3 \ncong A_4$ y $A_2 \ncong A_4$ vamos a estudiar los elementos de cuadrado cero de las $\mathbb{R}-$álgebras A_2, A_3 y A_4. Sean $\alpha \in A_2$, $\beta \in A_3$ y $\gamma \in A_4$ entonces

$$\begin{aligned} \alpha^2 &= (a_1x + b_1x^2 + c_1y)^2 = a_1^2x^2 \\ \beta^2 &= (a_2x + b_2x^2 + c_2y)^2 = a_2^2x^2 + c_2^2y^2 = (a_2^2 + c_2^2)x^2 \\ \gamma^2 &= (a_3x + b_3x^2 + c_3y)^2 = a_3^2x^2 + c_3^2y^2 = (a_3^2 - c_3^2)x^2. \end{aligned}$$

Observe que $\alpha = 0$ si y sólo si $a_1 = 0$, $\beta^2 = 0$ si y solo si $a_2 = c_2 = 0$ y $\gamma = 0$ si y sólo si $a_3^2 = c_3^2$. Entonces $\{\alpha \in A_2 : \alpha^2 = 0\}$ es un $\mathbb{R}-$espacio vectorial de dimensión 2 y $\{\beta \in A_3 : \beta^2 = 0\}$ es un $\mathbb{R}-$espacio vectorial de dimensión 1. Además $\{\gamma \in A_4 : \gamma^2 = 0\}$ es la cuádrica que consiste en un par de planos distintos que pasan por el origen de coordenadas. Por tanto $A_2 \ncong A_3$, $A_2 \ncong A_4$ y $A_3 \ncong A_4$.

En conclusión, si $\dim_{\mathbb{R}} A = 4$, salvo isomorfismos, A es

$$\frac{\mathbb{R}[x]}{(x^4)}, \quad \frac{\mathbb{R}[x, y]}{(x^3, y^2, xy)}, \quad \frac{\mathbb{R}[x, y]}{(x^3, x^2 - y^2, xy)}, \quad \frac{\mathbb{R}[x, y]}{(x^3, x^2 + y^2, xy)} \quad \text{o} \quad \frac{\mathbb{R}[x, y, z]}{(x, y, z)^2}.$$

Observe que

$$\frac{\mathbb{R}[\gamma,\delta]}{(\gamma^2,\delta^2)} \simeq \frac{\mathbb{R}[x,y]}{(x^3,x^2+y^2,xy)}.$$

Pues es un isomorfismo de $\mathbb{R}-$espacios vectoriales siendo $\gamma = x+y$ y $\delta = x-y$, y la matriz asociada al cambio de bases tiene determinante distinto de cero. Además se cumple la tabla de multiplicación ya que $\gamma^2 = \delta^2 = x^2+y^2 = 0$ y $\gamma\delta = x^2-y^2 = 2x^2$.

2.7.3. $\mathbb{R}-$álgebras locales finitas reales de dimensión 5.

Si $\dim_{\mathbb{R}} A = 5$, entonces $1 < o(\mathfrak{m}) \leq 5$ y tenemos cuatro casos:

(1) Si $o(\mathfrak{m}) = 5$, entonces existe $x \in \mathfrak{m}$ tal que $x^4 \neq 0$ y $x^5 = 0$. Por la Proposición 2.3.5(2), $\{1, x, x^2, x^3, x^4\}$ es base de A y por tanto

$$A \simeq \frac{\mathbb{R}[x]}{(x^5)}.$$

(2) Si $o(\mathfrak{m}) = 4$, entonces para todo $x \in \mathfrak{m}$, $x^4 = 0$ y por la Proposición 2.3.21 para todos $x, y \in \mathfrak{m}$, $x^3y = x^2y^2 = 0$. Además existe $x \in \mathfrak{m}$ tal que $x^3 \neq 0$ luego x, x^2 y x^3 son linealmente independientes. Como $\dim_{\mathbb{R}} \mathfrak{m} = 4$, existe $y \in \mathfrak{m}$ tal que $\{x, x^2, x^3, y\}$ es base de $\mathfrak{m}$ y tenemos dos casos:

(2.1) Si $xy = 0$, como $y^2, y^3 \in \mathfrak{m}$, entonces existen $a_i, b_i, c_i, d_i \in \mathbb{R}$, $i = 1, 2$, tales que

$$y^2 = a_1x + b_1x^2 + c_1x^3 + d_1y \quad \text{y} \quad y^3 = a_2x + b_2x^2 + c_2x^3 + d_2y.$$

Luego $0 = x^2y^2 = a_1x^3$ y $0 = x^2y^3 = a_2x^3$ pero $x^3 \neq 0$ por tanto $a_1 = a_2 = 0$. De la misma forma, $0 = xy^2 = b_1x^3$ y $0 = xy^3 = b_2x^3$ entonces $b_1 = b_2 = 0$. Así

$$y^2 = c_1x^3 + d_1y \quad \text{y} \quad y^3 = c_2x^3 + d_2y.$$

Note que $y^3 = d_1y^2 = d_1(c_1x^3 + d_1y) = c_1d_1x^3 + d_1^2y = c_2x^3 + d_2y$ entonces $c_2 = c_1d_1$ y $d_2 = d_1^2$.

Tenemos dos casos:

(2.1.1) Si $y^2 \neq 0$, entonces $d_2 = d_1 = c_2 = 0$ ya que $0 = y^4 = d_2y^2$. Luego $y^3 = 0$ y $y^2 = c_1x^3$.

Sea $\gamma = \sqrt[3]{c_1}x$ por tanto $\gamma^3 = c_1x^3 = y^2$, $y^3 = \gamma y = 0$ y $\{\gamma, \gamma^2, \gamma^3, y\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma,y]}{(\gamma^4,\gamma^3-y^2,\gamma y)}.$$

Note que y^3 no aparece como generador del ideal $\mathfrak{m}$ puesto que y^3 está generado por $\gamma^3 - y^2$. En efecto, como $\gamma^3 - y^2 \in \mathfrak{m}$, $\gamma^3 y - y^3 \in \mathfrak{m}$ y por tanto $y^3 \in \mathfrak{m}$ ya que $\gamma^3 y \in \mathfrak{m}$.

(2.1.2) Si $y^2 = 0$, entonces

$$A \simeq \frac{\mathbb{R}[x,y]}{(x^4, y^2, xy)}.$$

(2.2) Si $xy \neq 0$ y $x^2 y = 0$, como $xy \in \mathfrak{m}$, entonces existen $a, b, c, d \in \mathbb{R}$ tales que

$$xy = ax + bx^2 + cx^3 + dy.$$

Multiplicando por x^2, $0 = x^3 y = ax^3$ pero $x^3 \neq 0$ entonces $a = 0$. Multiplicando por x, $0 = x^2 y = bx^3 + dxy = bx^3 + d(bx^2 + cx^3 + dy) = bdx^2 + (b + cd)x^3 + d^2 y$ entonces $bd = b + cd = d^2 = 0$ esto es $b = d = 0$. Así $xy = cx^3$ y

$$x(y - cx^2) = 0.$$

Sea $\gamma = y - cx^2$ entonces $x\gamma = 0$ y $\{x, x^2, x^3, \gamma\}$ es base de $\mathfrak{m}$. Luego estamos en el caso (2.1).

(2.3) Si $x^2 y \neq 0$, como $x^2 y \in \mathfrak{m}$, existen $a, b, c, d \in \mathbb{R}$ tales que $x^2 y = ax + bx^2 + cx^3 + dy$.

Multiplicando por x^2, $0 = x^4 y = ax^3 + dx^2 y = ax^3 + d(ax + bx^2 + cx^3 + dy)$ entonces $ad = bd = a + cd = d^2 = 0$ esto es $a = d = 0$. Luego $x^2 y = bx^2 + cx^3$. Multiplicando por x, $0 = x^3 y = bx^3$ entonces $b = 0$. Así $x^2 y = cx^3$ y

$$x^2(y - cx) = 0.$$

Sea $\gamma = y - cx$ entonces $x^2\gamma = 0$ y $\{x, x^2, x^3, \gamma\}$ es base de $\mathfrak{m}$. Luego estamos en el caso (2.2).

(3) Si $o(\mathfrak{m}) = 3$, entonces para todo $x \in \mathfrak{m}$, $x^3 = 0$. Por la Proposición 2.3.21, para todos $x, y \in \mathfrak{m}$, $x^2 y = 0$, y para todos $x, y, z \in \mathfrak{m}$, $xyz = 0$.

Además como $o(\mathfrak{m}) = 3$, existe $x \in \mathfrak{m}$ tal que $x^2 \neq 0$ luego x y x^2 son linealmente independientes, y puesto que $\dim_{\mathbb{R}} \mathfrak{m} > 2$, existe $y \in \mathfrak{m}$ tal que x, x^2 y y son linealmente independientes. Tenemos dos casos:

(3.1) Si y^2 no depende linealmente de x, x^2 y y, como $\dim_{\mathbb{R}} \mathfrak{m} = 4$, entonces $\{x, x^2, y, y^2\}$ es base de $\mathfrak{m}$ y tenemos dos casos:

(3.1.1) Si $xy = 0$ entonces

$$A \simeq \frac{\mathbb{R}[x,y]}{(x^3, y^3, xy)}.$$

(3.1.2) Si $xy \neq 0$, como $xy \in \mathfrak{m}$, existen $a, b, c, d \in \mathbb{R}$ tales que $xy = ax + bx^2 + cy + dy^2$.

Multiplicando por x, $0 = x^2y = ax^2 + cxy = ax^2 + c(ax + bx^2 + cy + dy^2) = acx + (a+bc)x^2 + c^2y + cdy^2$ entonces $ac = a+bc = c^2 = cd = 0$ esto es $a = c = 0$. Así

$$xy = bx^2 + dy^2.$$

Note que el producto bd es invariante a cambios de productos por constantes de x y y. Además observe que si $b = 0$ entonces $xy = dy^2$ y

$$y(x - dy) = 0.$$

Sea $\gamma = x - dy$ entonces $\gamma y = 0$, $\gamma^2 = x^2 - 2dxy + d^2y^2 = x^2 - 2d^2y^2 + d^2y^2 = x^2 - d^2y^2$ y por tanto $\{\gamma, \gamma^2, y, y^2\}$ es base de $\mathfrak{m}$. En consecuencia estamos en el caso (3.1.1). Si $d = 0$, por simetría con y, tenemos el mismo razonamiento. Así $b \neq 0$ y $d \neq 0$.

Sin pérdida de generalidad podemos suponer que $b > 0$, porque podemos cambiar x por $-x$ y y por $-y$. Por tanto $0 = bx^2 + dy^2 - xy = \left(\sqrt{b}x - \frac{1}{2\sqrt{b}}y\right)^2 + \left(d - \frac{1}{4b}\right)y^2$ y tenemos que

$$\left(\sqrt{b}x - \frac{1}{2\sqrt{b}}y\right)^2 = \left(\frac{1}{4b} - d\right)y^2.$$

Observe que $\frac{1}{4b} - d > 0$ si y sólo si $bd < \frac{1}{4}$. Tenemos tres casos:

(3.1.2.1) Si $bd < \frac{1}{4}$, sean $\gamma_1 = \sqrt{b}x - \frac{1}{2\sqrt{b}}y$ y $\gamma_2 = \sqrt{\frac{1}{4b} - d}y$, entonces $\gamma_1^2 = \gamma_2^2$. Note que $\{\gamma_1, \gamma_2, \gamma_2^2, \gamma_1\gamma_2\}$ es base de $\mathfrak{m}$. En efecto, $\gamma_1\gamma_2 = (\sqrt{b}x - \frac{1}{2\sqrt{b}}y)\sqrt{\frac{1-4bd}{4b}}y = \frac{\sqrt{1-4bd}}{2}xy - \frac{\sqrt{1-4bd}}{4b}y^2 = \frac{b\sqrt{1-4bd}}{2}x^2 + \frac{(2bd-1)\sqrt{1-4bd}}{4b}y^2$. Por tanto

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \gamma_2^2 \\ \gamma_1\gamma_2 \end{pmatrix} = \begin{pmatrix} \sqrt{b} & 0 & -\frac{1}{2\sqrt{b}} & 0 \\ 0 & 0 & \sqrt{\frac{1-4bd}{4b}} & 0 \\ 0 & 0 & 0 & \frac{1}{4b} - d \\ 0 & \frac{b\sqrt{1-4bd}}{2} & 0 & \frac{(2bd-1)\sqrt{1-4bd}}{4b} \end{pmatrix} \begin{pmatrix} x \\ x^2 \\ y \\ y^2 \end{pmatrix}$$

y la matriz cambio de base tiene determinante igual a $\frac{(1-4bd)^2}{16} \neq 0$.

En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, \gamma_2]}{(\gamma_1^3, \gamma_2^3, \gamma_1^2 - \gamma_2^2)}.$$

Note que $\frac{\mathbb{R}[\gamma_1,\gamma_2]}{(\gamma_1^3,\gamma_2^3,\gamma_1^2-\gamma_2^2)} \simeq \frac{\mathbb{R}[x,y]}{(x^3,y^3,xy)}$ siento $x = \gamma_1 + \gamma_2$ y $y = \gamma_1 - \gamma_2$.

(3.1.2.2) Si $bd > \frac{1}{4}$, sean $\gamma_1 = \sqrt{b}x - \frac{1}{2\sqrt{b}}y$ y $\gamma_2 = \sqrt{d - \frac{1}{4b}}y$, entonces $\gamma_1^2 = -\gamma_2^2$.

Note que $\gamma_1\gamma_2 = (\sqrt{b}x - \frac{1}{2\sqrt{b}}y)\sqrt{\frac{4bd-1}{4b}}y = \frac{\sqrt{4bd-1}}{2}xy - \frac{\sqrt{4bd-1}}{4b}y^2 = \frac{b\sqrt{4bd-1}}{2}x^2 + \frac{(2bd-1)\sqrt{4bd-1}}{4b}y^2$ y de igual forma que en el caso (3.1.2.1), $\{\gamma_1, \gamma_2, \gamma_2^2, \gamma_1\gamma_2\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, \gamma_2]}{(\gamma_1^3, \gamma_2^3, \gamma_1^2 + \gamma_2^2)}.$$

(3.1.2.3) Si $bd = \frac{1}{4}$, sean $\gamma_1 = \sqrt{b}x$ y $\gamma_2 = \frac{1}{2\sqrt{b}}y$, entonces $2\gamma_1\gamma_2 = xy = bx^2 + \frac{1}{4b}y^2 = \gamma_1^2 + \gamma_2^2$ y $\{\gamma_1, \gamma_2, \gamma_1^2, \gamma_2^2\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, \gamma_2]}{(\gamma_1^3, \gamma_2^3, \gamma_1^2 + \gamma_2^2 - 2\gamma_1\gamma_2)}.$$

(3.2) Para todo $y \in \mathfrak{m}$ linealmente independiente de x y x^2 se cumple que y^2 depende linealmente de x, x^2 y y. Como y es linealmente independiente de x y x^2, entonces $y + x$ es linealmente independiente de x y x^2. Además

$$(y + x)^2 = y^2 + 2xy + x^2$$

depende linealmente de x, x^2 y y si y sólo si xy depende linealmente de x, x^2 y y. Por tanto existen $a_1, a_2, a_3 \in \mathbb{R}$ tales que

$$xy = a_1x + a_2x^2 + a_3y \tag{2.5}$$

y como y^2 depende linealmente de x, x^2 y y, existen $b_1, b_2, b_3 \in \mathbb{R}$ tales que

$$y^2 = b_1x + b_2x^2 + b_3y. \tag{2.6}$$

Multiplicando por x, en la Ecuación (2.5), $0 = a_1x^2 + a_3xy = a_1x^2 + a_3(a_1x + a_2x^2 + a_3y) = a_1a_3x + (a_1 + a_2a_3)x^2 + a_3^2y$. Entonces $a_1a_3 = a_1 + a_2a_3 = a_3^2 = 0$ esto es $a_3 = a_1 = 0$ y $xy = a_2x^2$. Multiplicando por y, en la Ecuación (2.6), $0 = b_1xy + b_3y^2 = b_1(a_2x^2) + b_3(b_1x + b_2x^2 + b_3y) = b_1b_3x + (a_2b_1 + b_2b_3)x^2 + b_3^2y$.. Entonces $b_1b_3 = a_2b_1 + b_2b_3 = b_3^2 = 0$ esto es $b_3 = b_1 = 0$ y $y^2 = b_2x^2$.

En conclusión, para todos $x, y \in \mathfrak{m}$ tales que x, x^2 y y son linealmente independientes y y^2 depende linealmente de x, x^2 y y, existen $a_2, b_2 \in \mathbb{R}$ tales que

$$xy = a_2x^2 \quad \text{y} \quad y^2 = b_2x^2.$$

Como $\dim_{\mathbb{R}} \mathfrak{m} = 4$, existe $z \in \mathfrak{m}$ linealmente independiente de x, x^2 y y. En particular z es linealmente independiente de x y x^2 luego, por hipótesis del caso (3.2), z^2 depende linealmente de x, x^2 y z. Por simetría con y, existen $c_2, d_2 \in \mathbb{R}$

tales que

$$xz = c_2x^2 \quad \text{y} \quad z^2 = d_2x^2.$$

Por otra parte, como $x+y+z$ es linealmente independiente de x, x^2 y y, y también linealmente independiente de x, x^2 y z, entonces

$$(x+y+z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz.$$

depende linealmente de x, x^2 y y, y también depende linealmente de x, x^2 y z. En particular, $y^2 + z^2 + 2yz$ depende linealmente de x, x^2 y y, y también depende linealmente de x, x^2 y z. Por tanto yz depende linealmente de x y x^2. Luego existen $r_1, r_2 \in \mathbb{R}$ tales que $yz = r_1x + r_2x^2$. Como $0 = xyz = r_1x^2$, se tiene que $r_1 = 0$ y

$$yz = r_2x^2.$$

En los casos $xy = a_2x^2$ y $xz = c_2x^2$ factorizamos x, luego $x(y - a_2x) = 0$ y $x(z - c_2x) = 0$. Llamando $y' = y - a_2x$ y $z' = z - c_2x$ tenemos que $\{x, x^2, y', z'\}$ es base de $\mathfrak{m}$. Además,

$$\begin{gathered}(y')^2 = y^2 - 2a_2xy + a_2^2x^2 = b_2x^2 - 2a_2^2x^2 + a_2^2x^2 = (b_2 - a_2^2)x^2\\ (z')^2 = z^2 - 2c_2xz + c_2^2x^2 = d_2x^2 - 2c_2^2x^2 + c_2^2x^2 = (d_2 - c_2^2)x^2\\ y'z' = (y - a_2x)(z - c_2x) = yz - a_2xz - c_2xy + a_2c_2x^2 = (r_2 - a_2c_2)x^2\end{gathered}$$

Sean $a = b_2 - a_2^2$, $b = d_2 - c_2^2$ y $c = r_2 - a_2c_2$. Entonces $(y')^2 = ax^2$, $(z')^2 = bx^2$ y $y'z' = cx^2$. En conclusión, cambiando y' por y y z' por z, existen $a, b, c \in \mathbb{R}$ tales que

$$\begin{gathered}y^2 = ax^2\\ z^2 = bx^2\\ yz = cx^2\\ xy = xz = 0\end{gathered}$$

Tenemos los casos siguientes:

(3.2.1) Si $a = b = c = 0$, entonces $y^2 = z^2 = xy = xz = yz = 0$ y $\{x, x^2, y, z\}$ es base de $\mathfrak{m}$. Luego

$$A \simeq \frac{\mathbb{R}[x, y, z]}{(x^3, y^2, z^2, xy, xz, yz)}.$$

(3.2.2) Si $a \neq 0$ y $b = c = 0$, entonces tenemos dos casos:

(3.2.2.1) Si $a > 0$, sea $\gamma = \sqrt{a}x$, entonces $\gamma^2 = ax^2 = y^2$, $z^2 = \gamma y = \gamma z = yz = 0$ y como

$\{x, x^2, y, z\}$ es base de $\mathfrak{m}$, $\{\gamma, \gamma^2, y, z\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma, y, z]}{(\gamma^3, y^2 - \gamma^2, z^2, \gamma y, \gamma z, yz)}.$$

(3.2.2.2) Si $a < 0$, sea $\gamma = \sqrt{-a}x$, entonces $\gamma^2 = -ax^2 = -y^2$, $z^2 = \gamma y = \gamma z = yz = 0$ y $\{\gamma, \gamma^2, y, z\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma, y, z]}{(\gamma^3, y^2 + \gamma^2, z^2, \gamma y, \gamma z, yz)}.$$

(3.2.3) Si $c \neq 0$ y $a = b = 0$, sea $\gamma = \frac{1}{c}y$, entonces $\gamma z = \frac{1}{c}yz = x^2$, $\gamma^2 = \frac{1}{c^2}y^2 = 0$, $x\gamma = \frac{1}{c}xy = 0$, $z^2 = xz = 0$ y $\{x, x^2, \gamma, z\}$ es base de $\mathfrak{m}$. En consecuencia

$$A \simeq \frac{\mathbb{R}[x, \gamma, z]}{(x^3, \gamma^2, z^2, x\gamma, xz, \gamma z - x^2)}.$$

(3.2.4) Si $a \neq 0$, $b \neq 0$ y $c = 0$, tenemos cuatro casos:

(3.2.4.1) Si $a > 0$ y $b > 0$, sean $\gamma_1 = \sqrt{a}x$ y $\gamma_2 = \sqrt{\frac{a}{b}}z$, entonces $\gamma_1^2 = ax^2 = y^2$, $\gamma_1^2 = ax^2 = \frac{a}{b}z^2 = \gamma_2^2$ y $\gamma_1 y = y\gamma_2 = \gamma_1\gamma_2 = 0$. Además $\{\gamma_1, \gamma_1^2, y, \gamma_2\}$ es base de $\mathfrak{m}$ y en consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, y, \gamma_2]}{(\gamma_1^3, y^2 - \gamma_1^2, \gamma_2^2 - \gamma_1^2, \gamma_1 y, y\gamma_2, \gamma_1\gamma_2)}.$$

(3.2.4.2) Si $a > 0$ y $b < 0$, sean $\gamma_1 = \sqrt{a}x$ y $\gamma_2 = \sqrt{-\frac{a}{b}}z$, entonces $\gamma_1^2 = ax^2 = y^2$, $\gamma_1^2 = ax^2 = \frac{a}{b}z^2 = -\gamma_2^2$ y $\gamma_1 y = y\gamma_2 = \gamma_1\gamma_2 = 0$. Además $\{\gamma_1, \gamma_1^2, y, \gamma_2\}$ es base de $\mathfrak{m}$ y en consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, y, \gamma_2]}{(\gamma_1^3, y^2 - \gamma_1^2, \gamma_2^2 + \gamma_1^2, \gamma_1 y, y\gamma_2, \gamma_1\gamma_2)}.$$

Note que esta $\mathbb{R}-$álgebra es isomorfa a la del caso (3.2.3). Es decir $\frac{\mathbb{R}[x,\gamma_1,\gamma_2]}{(x^3,\gamma_1^2-x^2,\gamma_2^2+x^2,x\gamma_1,x\gamma_2,\gamma_1\gamma_2)} \simeq \frac{\mathbb{R}[x,y,z]}{(x^3,y^2,z^2,xy,xz,yz-x^2)}$ siendo $\gamma_1 = \frac{1}{2}z + y$ y $\gamma_2 = \frac{1}{2}z - y$.

(3.2.4.3) Si $a < 0$ y $b > 0$, sea $\gamma_1 = \sqrt{-a}x$ y $\gamma_2 = \sqrt{-\frac{a}{b}}z$, entonces $\gamma_1^2 = -ax^2 = -y^2$, $\gamma_1^2 = -ax^2 = -\frac{a}{b}z^2 = \gamma_2^2$ y $\gamma_1 y = y\gamma_2 = \gamma_1\gamma_2 = 0$. Además $\{\gamma_1, \gamma_1^2, y, \gamma_2\}$ es base de $\mathfrak{m}$ y en consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, y, \gamma_2]}{(\gamma_1^3, y^2 + \gamma_1^2, \gamma_2^2 - \gamma_1^2, \gamma_1 y, y\gamma_2, \gamma_1\gamma_2)}.$$

Note que esta $\mathbb{R}-$álgebra es isomorfa a la del caso (3.2.4.2).

(3.2.4.4) Si $a < 0$ y $b < 0$, sea $\gamma_1 = \sqrt{-a}x$ y $\gamma_2 = \sqrt{\frac{a}{b}}z$, entonces $\gamma_1^2 = -ax^2 = -y^2$, $\gamma_1^2 = -ax^2 = -\frac{a}{b}z^2 = -\gamma_2^2$ y $\gamma_1 y = y\gamma_2 = \gamma_1\gamma_2 = 0$. Además $\{\gamma_1, \gamma_1^2, y, \gamma_2\}$ es base de $\mathfrak{m}$ y en consecuencia

$$A \simeq \frac{\mathbb{R}[\gamma_1, y, \gamma_2]}{(\gamma_1^3, y^2 + \gamma_1^2, \gamma_2^2 + \gamma_1^2, \gamma_1 y, y\gamma_2, \gamma_1\gamma_2)}.$$

Note que tomando $\gamma_1 = x - y + z$, $\gamma_2 = x + z$ y $\gamma_3 = y - x$,

$$\frac{\mathbb{R}[\gamma_1, \gamma_2, \gamma_3]}{(\gamma_1^3, \gamma_2^2 + \gamma_1^2, \gamma_3^2 + \gamma_1^2, \gamma_1\gamma_2, \gamma_1\gamma_3, \gamma_2\gamma_3)} \simeq \frac{\mathbb{R}[x, y, z]}{(x^3, y^2, z^2, xy, xz, yz - x^2)}.$$

(3.2.5) Si $a \neq 0$, $c \neq 0$ y $b = 0$, sean $\gamma_1 = \frac{1}{c}y$ y $\gamma_2 = z - \frac{c}{a}y$, entonces $\gamma_1\gamma_2 = \frac{1}{c}y(z - \frac{c}{a}y) = \frac{1}{c}yz - \frac{1}{a}y^2 = 0$, $\gamma_1^2 = \frac{a}{c^2}x^2$ y $\gamma_2^2 = (z - \frac{c}{a}y)^2 = -\frac{c^2}{a}x^2$. Además $\{x, x^2, \gamma_1, \gamma_2\}$ es base de $\mathfrak{m}$, luego estamos en el caso (3.2.4).

(3.2.6) Si $a \neq 0$, $b \neq 0$ y $c \neq 0$, entonces podemos hacer un cambio de los elementos de la base y y z por otros con producto cero. En efecto, sean $r_1, r_2, s_1, s_2 \in \mathbb{R}$ tales que

$$\gamma_1 = r_1 y + s_1 z \quad \text{y} \quad \gamma_2 = r_2 y + s_2 z.$$

Note que

$$\begin{aligned} 0 &= \gamma_1\gamma_2 = (r_1 y + s_1 z)(r_2 y + s_2 z) = r_1 r_2 y^2 + (r_1 s_2 + r_2 s_1)yz + s_1 s_2 z^2 \\ &= (r_1 r_2 a + (r_1 s_2 + r_2 s_1)c + s_1 s_2 b)x^2 = (r_1(r_2 a + s_2 c) + s_1(r_2 c + s_2 b))x^2 \end{aligned}$$

Si $r_1 = -(r_2 c + s_2 b)$, $s_1 = r_2 a + s_2 c$ y $\begin{vmatrix} r_1 & s_1 \\ r_2 & s_2 \end{vmatrix} = \begin{vmatrix} -r_2 c - s_2 b & r_2 a + s_2 c \\ r_2 & s_2 \end{vmatrix} \neq 0$, entonces γ_1 y γ_2 son dos elementos linealmente independientes tales que el conjunto $\{x, x^2, \gamma_1, \gamma_2\}$ es base de $\mathfrak{m}$ y $\gamma_1\gamma_2 = 0$. Luego estamos en el caso (3.2.4).

(4) Si $o(\mathfrak{m}) = 2$, entonces para todo $x \in \mathfrak{m}$, $x^2 = 0$ y por la Proposición 2.3.21 para todos $x, y \in \mathfrak{m}$, $xy = 0$. Puesto que $\dim_{\mathbb{R}} \mathfrak{m} = 4$, existen $x, y, z, w \in \mathfrak{m}$ tales que $\{x, y, z, w\}$ es base para $\mathfrak{m}$ y cumple que $xy = xz = xw = yz = yw = zw = 0$. En consecuencia

$$A \simeq \frac{\mathbb{R}[x, y, z, w]}{(x, y, z, w)^2}$$

En conclusión si $\dim_{\mathbb{R}} A = 5$, salvo isomorfismos, A es

$o(\mathfrak{m})$	A
5	$\mathbb{R}[x]/(x^5)$.
4	$A_1 = \mathbb{R}[x,y]/(x^4, y^2, xy)$, $A_2 = \mathbb{R}[x,y]/(x^4, x^3 - y^2, xy)$. (*)
3	$A_1 = \mathbb{R}[x,y]/(x^3, y^3, xy)$, $A_2 = \mathbb{R}[x,y]/(x^3, y^3, x^2 + y^2)$, $A_3 = \mathbb{R}[x,y]/(x^3, y^3, x^2 + y^2 - 2xy)$, $A_4 = \mathbb{R}[x,y,z]/(x^3, y^2, z^2, xy, xz, yz)$, $A_5 = \mathbb{R}[x,y,z]/(x^3, y^2 - x^2, z^2, xy, xz, yz)$, $A_6 = \mathbb{R}[x,y,z](x^3, y^2 + x^2, z^2, xy, xz, yz)$, $A_7 = \mathbb{R}[x,y,z]/(x^3, y^2, z^2, xy, xz, yz - x^2)$, $A_8 = \mathbb{R}[x,y,z]/(x^3, y^2 - x^2, z^2 - x^2, xy, xz, yz)$. (**)
2	$\mathbb{R}[x,y,z,w]/(x,y,z,w)^2$.

(*) Note que $A_1 \ncong A_2$ ya que si $\alpha \in A_1$ y $\beta \in A_2$ entonces

$$\alpha^2 = (a_1x + b_1x^2 + c_1x^3 + d_1y)^2 = a_1^2x^2 + 2a_1b_1x^3$$
$$\beta^2 = (a_2x + b_2x^2 + c_2x^3 + d_2y)^2 = a_2^2x^2 + d_2^2y^2 + 2a_2b_2x^3 = a_2^2x^2 + (d_2^2 + 2a_2b_2)x^3$$

Luego $\alpha^2 = 0$ si y sólo si $a_1^2 = 2a_1b_1 = 0$ esto es $a_1 = 0$ y $\{\alpha \in A_1 : \alpha^2 = 0\}$ es un $\mathbb{R}-$espacio vectorial de dimensión 3. Además, $\beta^2 = 0$ si y sólo si $a_2^2 = d_2^2 + 2a_2b_2 = 0$ es decir $a_2 = d_2 = 0$. Luego $\{\beta \in A_2 : \beta^2 = 0\}$ es un $\mathbb{R}-$espacio vectorial de dimensión 2.

(**) Vamos a ver que ningún par de éstas $\mathbb{R}-$álgebras son isomorfas. Observe que las $\mathbb{R}-$álgebras A_1, A_2 y A_3 no son isomorfas a las otras ya que $o(\mathfrak{m}_1^2) = o(\mathfrak{m}_2^2) = o(\mathfrak{m}_3^2) = 2$ pues $\mathfrak{m}_1^2 = (x^2, y^2)$, $\mathfrak{m}_2^2 = \mathfrak{m}_3^2 = (x^2, xy)$ y $o(\mathfrak{m}_4^2) = o(\mathfrak{m}_5^2) = o(\mathfrak{m}_6^2) = o(\mathfrak{m}_7^2) = o(\mathfrak{m}_8^2) = 1$ ya que $\mathfrak{m}_4^2 = \mathfrak{m}_5^2 = \mathfrak{m}_6^2 = \mathfrak{m}_7^2 = \mathfrak{m}_8^2 = (x^2)$.

$A_1 \ncong A_2$ ya que si $\alpha, \beta \in A_1$ y $0 = \alpha^2 + \beta^2 = (a_1x + b_1x^2 + c_1y + d_1y^2)^2 + (a_2x + b_2x^2 + c_2y + d_2y^2)^2 = (a_1^2 + a_2^2)x^2 + (c_1^2 + c_2^2)y^2$ entonces $a_1^2 + a_2^2 = 0$ y $c_1^2 + c_2^2 = 0$ esto es $a_1 = a_2 = c_1 = c_2 = 0$. Muy distinto sucede en la $\mathbb{R}-$álgebra A_2 donde existe una suma nula de cuadrados de elementos distintos de cero.

Veamos que $A_2 \ncong A_3$. Como $o(\mathfrak{m}_2) = o(\mathfrak{m}_3) = 3$, podemos considerar las matrices asociadas al producto en $\mathfrak{m}_2/\mathfrak{m}_2^2$ y $\mathfrak{m}_3/\mathfrak{m}_3^2$ respectivamente. Consideremos $\{\widetilde{x}, \widetilde{y}\}$, $\widetilde{x} = x + \mathfrak{m}_2^2$ y $\widetilde{y} = y + \mathfrak{m}_2^2$, base de $\mathfrak{m}_2/\mathfrak{m}_2^2$ y $\{\widehat{x}, \widehat{y}\}$, $\widehat{x} = x + \mathfrak{m}_3^2$ y $\widehat{y} = y + \mathfrak{m}_3^2$, base de $\mathfrak{m}_3/\mathfrak{m}_3^2$. Las matrices del producto son $P_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y $P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ para $\mathfrak{m}_2/\mathfrak{m}_2^2$, y $Q_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y $Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ para $\mathfrak{m}_3/\mathfrak{m}_3^2$. Los haces de cuádricas de $\mathfrak{m}_2/\mathfrak{m}_2^2$ y $\mathfrak{m}_3/\mathfrak{m}_3^2$ no son proyectivamente equivalentes ya que los valores propios de $P_1^{-1}P_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ son imaginarios dados por $\lambda^2 + 1 = 0$ y

los de $Q_1^{-1}Q_2 = \begin{pmatrix} 0 & 1 \\ -1 & -2 \end{pmatrix}$ son reales dados por $(\lambda+1)^2 = 0$. Así $A_2 \ncong A_3$.

Por otra parte, la dimensión del $\mathbb{R}-$espacio vectorial de los elementos de cuadrado cero de la $\mathbb{R}-$álgebra A_4 es tres, A_5 es dos y de la $\mathbb{R}-$álgebra A_8 es uno. En efecto, sean $\alpha \in A_4$, $\beta \in A_5$ y $\gamma \in A_8$,

$$\alpha^2 = (a_1x + b_1x^2 + c_1y + d_1z)^2 = a_1^2x^2$$
$$\beta^2 = (a_2x + b_2x^2 + c_2y + d_2z)^2 = a_2^2x^2 + c_2^2y^2 = (a_2^2 + c_2^2)x^2$$
$$\gamma^2 = (a_3x + b_3x^2 + c_3y + d_3z)^2 = a_3^2x^2 + c_3^2y^2 + d_3^2z^2 = (a_3^2 + c_3^2 + d_3^2)x^2$$

Entonces $\alpha^2 = 0$ si y sólo si $a_1 = 0$, $\beta^2 = 0$ si y sólo si $a_2 = c_2 = 0$, y $\gamma^2 = 0$ si y sólo si $a_3 = c_3 = d_3 = 0$.

El conjunto de elementos de cuadrado cero de la $\mathbb{R}-$álgebra A_6 es la cuádrica que consiste en un par de planos distintos que pasan por el origen de coordenadas pues si $\alpha \in A_6$, entonces $0 = \alpha^2 = (ax + bx^2 + cy + dz)^2 = a^2x^2 + c^2y^2 = (a^2 - c^2)x^2$. Luego, $a^2 = c^2$ y ésta es la ecuación de la cuádrica.

Por último, el conjunto de elementos de cuadrado cero de la $\mathbb{R}-$álgebra A_7 es una cuádrica que consiste en un cono pues si $\alpha \in A_7$ entonces $0 = \alpha^2 = (ax + bx^2 + cy + dz)^2 = a^2x^2 + 2cdyz = (a^2 + 2cd)x^2$. Luego, $a^2 + 2cd = 0$ y ésta es la ecuación del cono.

Con todo lo anterior concluimos que las ocho $\mathbb{R}-$álgebras de arriba no son isomorfas entre sí.

2.8. Clasificación de las $\mathbb{R}-$álgebras finitas

En la tabla siguiente se resumen las $\mathbb{R}-$álgebras finitas hasta la dimensión 5. Hacemos la clasificación según su dimensión como $\mathbb{R}-$espacio vectorial y luego, separadas por una línea, aparecen las $\mathbb{R}$-álgebras locales y las no locales.
Dentro de las locales listamos dos $\mathbb{R}-$álgebras más que las encontradas en la sección 2.7 pues corresponden a las $\mathbb{R}-$álgebras finitas locales de tipo complejo, $\frac{\mathbb{R}[x]}{(x^2+1)} \simeq \mathbb{C}$ y $\frac{\mathbb{R}[x]}{(x^2+1)^2} \simeq \frac{\mathbb{C}[z]}{(z^2)}$.

dim	A
1	$\mathbb{R}$
2	$\mathbb{R}[x]/(x^2)$, $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$,
	$\mathbb{R}[x]/(x^2-1) \simeq \mathbb{R}\times\mathbb{R}$.
3	$\mathbb{R}[x]/(x^3)$, $\mathbb{R}[x,y]/(x,y)^2$,
	$\mathbb{R}[x]/(x(x^2-1)) \simeq \mathbb{R}\times\mathbb{R}\times\mathbb{R}$, $\mathbb{R}[x]/(x(x^2+1)) \simeq \mathbb{R}\times\mathbb{C}$,
	$\mathbb{R}[x]/(x^2(x-1)) \simeq \mathbb{R}\times\mathbb{R}[x]/(x^2)$.
4	$\mathbb{R}[x]/(x^4)$, $\mathbb{R}[x,y]/(x^3,y^2,xy)$, $\mathbb{R}[x,y]/(x^3,x^2-y^2,xy)$,
	$\mathbb{R}[x,y]/(x^3,x^2+y^2,xy)$, $\mathbb{R}[x,y,z]/(x,y,z)^2$, $\mathbb{R}[x]/((x^2+1)^2) \simeq \mathbb{C}[z]/(z^2)$,
	$\mathbb{R}[x]/((x^2-2)(x^2-1)) \simeq \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$, $\mathbb{R}[x]/(x^3(x-1)) \simeq \mathbb{R}\times\mathbb{R}[x]/(x^3)$,
	$\mathbb{R}[x]/(x(x-1)(x^2+1)) \simeq \mathbb{R}\times\mathbb{R}\times\mathbb{C}$, $\mathbb{R}[x]/(x^2(x^2-1)) \simeq \mathbb{R}\times\mathbb{R}\times\mathbb{R}[x]/(x^2)$,
	$\mathbb{R}[x]/(x^2(x-1)^2) \simeq \mathbb{R}[x]/(x^2)\times\mathbb{R}[x]/(x^2)$, $\mathbb{R}[x]/((x^2+1)((x-1)^2+1)) \simeq \mathbb{C}\times\mathbb{C}$,
	$\mathbb{R}[x]/(x^2(x^2+1)) \simeq \mathbb{C}\times\mathbb{R}[x]/(x^2)$.
5	$\mathbb{R}[x]/(x^5)$, $\mathbb{R}[x,y,z,w]/(x,y,z,w)^2$, $\mathbb{R}[x,y]/(x^4,y^2,xy)$, $\mathbb{R}[x,y]/(x^4,x^3-y^2,xy)$,
	$\mathbb{R}[x,y]/(x^3,y^3,xy)$, $\mathbb{R}[x,y](x^3,y^3,x^2+y^2)$, $\mathbb{R}[x,y]/(x^3,y^3,x^2+y^2-2xy)$,
	$\mathbb{R}[x,y,z]/(x^3,y^2,z^2,xy,xz,yz)$, $\mathbb{R}[x,y,z]/(x^3,y^2-x^2,z^2,xy,xz,yz)$,
	$\mathbb{R}[x,y,z]/(x^3,y^2+x^2,z^2,xy,xz,yz)$, $\mathbb{R}[x,y,z]/(x^3,y^2,z^2,xy,xz,yz-x^2)$,
	$\mathbb{R}[x,y,z](x^3,y^2-x^2,z^2-x^2,xy,xz,yz)$,
	$\mathbb{R}[x]/(x(x^2-2)(x^2-1)) \simeq \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$,
	$\mathbb{R}[x]/(x(x^2-1)(x^2+1)) \simeq \mathbb{C}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$,
	$\mathbb{R}[x]/(x^2(x+1)(x^2-1)) \simeq \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}[x]/(x^2)$,
	$\mathbb{R}[x]/(x^2(x+1)(x^2+1)) \simeq \mathbb{R}\times\mathbb{C}\times\mathbb{R}[x]/(x^2)$,
	$\mathbb{R}[x]/(x^2(x+1)^2(x+2)) \simeq \mathbb{R}[x]/(x^2)\times\mathbb{R}[x]/(x^2)\times\mathbb{R}$,
	$\mathbb{R}[x]/(x(x^2+1)((x-1)^2+1)) \simeq \mathbb{C}\times\mathbb{C}\times\mathbb{R}$,
	$\mathbb{R}[x]/(x^3(x^2-1)) \simeq \mathbb{R}[x]/(x^3)\times\mathbb{R}\times\mathbb{R}$, $\mathbb{R}[x]/(x^4(x-1)) \simeq \mathbb{R}[x]/(x^4)\times\mathbb{R}$,
	$\mathbb{R}[x]/(x^3(x-1)^2) \simeq \mathbb{R}[x]/(x^3)\times\mathbb{R}[x]/(x^2)$, $\mathbb{R}[x]/(x^3(x^2+1)) \simeq \mathbb{R}[x]/(x^3)\times\mathbb{C}$,
	$\mathbb{R}[x]/(x(x^2+1)^2) \simeq \mathbb{R}\times\mathbb{C}[z]/(z^2)$.

Capítulo 3

Recta proyectiva sobre un anillo

3.1. Submódulos monógenos de un $R-$módulo libre de rango 2

Sean R un anillo y M un $R-$módulo libre de rango 2.
Iniciamos la sección estudiando condiciones para $\lambda \boldsymbol{a} = \boldsymbol{0}$ con $\lambda \in R$ y $\boldsymbol{a} \in M$, pero previamente observemos que si S es el conjunto de no divisores de cero de R y $\overline{R} = S^{-1}R$ es el anillo total de cocientes de R, entonces el $R-$módulo M se extiende a un $\overline{R}-$módulo libre $\overline{M} = S^{-1}M$. $\overline{M}$ es un $\overline{R}-$módulo libre de rango 2 y M se identifica con un subconjunto de $\overline{M}$ con la aplicación

$$\begin{array}{rccc} i_M: & M & \to & \overline{M} \\ & \boldsymbol{m} & \mapsto & \frac{\boldsymbol{m}}{1} \end{array}$$

Note que i_M es inyectiva. En efecto, si $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ es base de M como $R-$módulo, $\boldsymbol{m} = a\boldsymbol{u}_1 + b\boldsymbol{u}_2$ y $\frac{\boldsymbol{m}}{1} = \boldsymbol{0}$ entonces existe $\lambda \in S$ tal que $\lambda \boldsymbol{m} = \boldsymbol{0}$ pero $\lambda \boldsymbol{m} = \lambda a\boldsymbol{u}_1 + \lambda b\boldsymbol{u}_2$ y como λ es no divisor de cero, $a = b = 0$ esto es $\boldsymbol{m} = \boldsymbol{0}$.
Además, si $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ es base de M como $R-$módulo, $\mathcal{B}' = \{i_M(\boldsymbol{u}_1), i_M(\boldsymbol{u}_2)\}$ es base de $\overline{M}$ como $\overline{R}-$módulo y si $\varphi_{\mathcal{B}} : M \to R^2$ es el isomorfismo de $R-$módulos que asocia a todo elemento de M sus coordenadas en $\mathcal{B}$ entonces el diagrama

$$\begin{array}{ccc} M & \xrightarrow{\varphi_{\mathcal{B}}} & R^2 \\ \downarrow{\scriptstyle i_M} & & \downarrow{\scriptstyle i_{R^2}} \\ \overline{M} & \xrightarrow{\varphi_{\mathcal{B}'}} & \overline{R}^2 \end{array}$$

es conmutativo.

Definición 3.1.1 *Sean $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ una base de M y $\boldsymbol{a}, \boldsymbol{b} \in M$. Si $\boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ y $\boldsymbol{b} = b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2$, definimos el* producto exterior *relativo a la base $\mathcal{B}$ como,*

$$\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = a_1b_2 - a_2b_1 \in R.$$

Cuando no haya confusión en ello suprimimos la mención de la base.

Propiedades:

(1) $\wedge_{\mathcal{B}}$ es bilineal y alternada, en particular, $\boldsymbol{a} \wedge \boldsymbol{b} = -\boldsymbol{b} \wedge \boldsymbol{a}$ y $\boldsymbol{a} \wedge \boldsymbol{a} = 0$.

(2) Si $\mathcal{B}' = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ es otra base de M, entonces

$$\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} = (\boldsymbol{a} \wedge_{\mathcal{B}'} \boldsymbol{b})(\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2). \tag{3.1}$$

(3) $\mathcal{B}' = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ es base de M si y sólo si $\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2 \in R^*$.
En efecto, $\Rightarrow$: Como $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ y $\mathcal{B}' = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ son bases de M, aplicando la Ecuación (3.1) para $\boldsymbol{u}_1$ y $\boldsymbol{u}_2$, tenemos que $1 = \boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{u}_2 = (\boldsymbol{u}_1 \wedge_{\mathcal{B}'} \boldsymbol{u}_2)(\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2)$. Luego, $\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2 \in R^*$.
$\Leftarrow$: Sean $\boldsymbol{v}_1 = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ y $\boldsymbol{v}_2 = b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2$. Como $\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2 = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \in R^*$, la matriz $\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$ es inversible. Si $\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$, entonces $\boldsymbol{u}_1 = \alpha_1\boldsymbol{v}_1 + \alpha_2\boldsymbol{v}_2$ y $\boldsymbol{u}_2 = \beta_1\boldsymbol{v}_1 + \beta_2\boldsymbol{v}_2$. Ahora, como $\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ es una base de M entonces $\boldsymbol{v}_1$ y $\boldsymbol{v}_2$ generan a M. Y puesto que $\dim M = 2$, entonces $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ es base de M.

En consecuencia, si $\boldsymbol{a}, \boldsymbol{b} \in M$, las fórmulas

(1) $\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} = 0$.

(2) $\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b}$ es divisor de cero.

(3) $\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b}$ no es divisor de cero.

(4) $\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} \in R^*$.

son independientes de la base $\mathcal{B}$ elegida.

Proposición 3.1.2 *Sean M y N $R-$módulos libres de rango 2 y $\mathcal{B}$ una base de M. Si $\varphi : M \to N$ es un isomorfismo de $R-$módulos, entonces para todos $\boldsymbol{a}, \boldsymbol{b} \in M$,*

$$(\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b}) = \varphi(\boldsymbol{a}) \wedge_{\varphi(\mathcal{B})} \varphi(\boldsymbol{b}) = (\det \varphi)(\varphi(\boldsymbol{a}) \wedge_{\mathcal{B}} \varphi(\boldsymbol{b})).$$

Demostración. Sean $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ una base de M, $\boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ y $\boldsymbol{b} = b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2$, entonces $\varphi(\boldsymbol{a}) = a_1\varphi(\boldsymbol{u}_1) + a_2\varphi(\boldsymbol{u}_2)$ y $\varphi(\boldsymbol{b}) = b_1\varphi(\boldsymbol{u}_1) + b_2\varphi(\boldsymbol{u}_2)$ por tanto $(\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b}) = \varphi(\boldsymbol{a}) \wedge_{\varphi(\mathcal{B})} \varphi(\boldsymbol{b})$.
Aplicando la Ecuación 3.1 y como $\det\varphi = \varphi(\boldsymbol{u}_1) \wedge_{\varphi(\mathcal{B})} \varphi(\boldsymbol{u}_2)$ se tiene que $\varphi(\boldsymbol{a}) \wedge_{\varphi(\mathcal{B})} \varphi(\boldsymbol{b}) = (\varphi(\boldsymbol{a}) \wedge_{\mathcal{B}} \varphi(\boldsymbol{b}))(\varphi(\boldsymbol{u}_1) \wedge_{\varphi(\mathcal{B})} \varphi(\boldsymbol{u}_2)) = (\det\varphi)(\varphi(\boldsymbol{a}) \wedge_{\mathcal{B}} \varphi(\boldsymbol{b}))$. ■

Definición 3.1.3 *Diremos que un elemento $\boldsymbol{a} \in M$ es:*

(1) complementable *si existe $\boldsymbol{b} \in M$ tal que $\{\boldsymbol{a}, \boldsymbol{b}\}$ es una base de M como $R-$módulo libre.*

(2) simplificable *si existe $\lambda \in R$ no divisor de cero y $\boldsymbol{u} \in M$ complementable tal que $\boldsymbol{a} = \lambda\boldsymbol{u}$.*

(3) débilmente simplificable *si existe $\lambda \in R$ y $\boldsymbol{u} \in M$ complementable tal que $\boldsymbol{a} = \lambda\boldsymbol{u}$.*

(4) libre $\lambda\boldsymbol{a} = \boldsymbol{0}$ *implica que* $\lambda = 0$.

Observe que si un elemento es complementable entonces es simplificable, y si es simplificable es débilmente simplificable y también libre. Además, si denotamos por $L(S)$ el $R-$submódulo generado por S, $\boldsymbol{a}$ es complementable si y sólo si $L(\{\boldsymbol{a}\})$ es submódulo libre de M y sumando directo de M, y $\boldsymbol{a}$ es libre si y sólo si $L(\{\boldsymbol{a}\})$ es submódulo libre de M.

Ejemplo 3.1.4 *(1) Sean $R = \mathbb{Z}[x]$ y $M = R^2$. Observe que: $(2,3) \in M$ es complementable porque $\{(2,3),(1,1)\}$ es una base de M. $(2x, 3x) \in M$ es simplificable ya que $(2,3)$ es complementable y $x \in R$ es no divisor de cero. $(2,x) \in M$ es libre pero no es simplificable ni complementable.*
(2) Si $R = K[x,y]$ con K cuerpo, $(x,y) \in R^2$ es libre pero no es débilmente simplificable (y por tanto tampoco simplificable ni complementable).
(3) Si $R = \mathbb{Z}/(6)$ entonces $(2,2) \in R^2$ no es libre.

Si R es un anillo total de cocientes, entonces elemento simplificable en M equivale a elemento complementable en M ya que los no divisores de cero de R son inversibles. En consecuencia, si R no es cuerpo, existen en M elementos no simplificables y por tanto R no es un anillo de Hermite en la terminología de Kaplansky.
Para Kaplansky un anillo es de Hermite si todos los elementos de R^2 son simplificables. Kaplansky prueba que todo anillo de Hermite según su definición lo es con la que utilizamos en esta memoria, ver [12, Teorema 3.7]. El recíproco, como vimos antes, no es cierto.

En general, $\boldsymbol{a} \in M$ es simplificable si y sólo si $\boldsymbol{a}$ es complementable en $\overline{M}$ como $\overline{R}-$módulo. Usando el producto exterior es inmediato que, $\boldsymbol{a}$ es complementable si y sólo si existe $\boldsymbol{b}$ tal que $\boldsymbol{a} \wedge \boldsymbol{b} \in R^*$ y esto equivale a que existe $\boldsymbol{b} \in M$ tal que $\boldsymbol{a} \wedge \boldsymbol{b} = 1$.

Lema 3.1.5 *Si R es una $K-$álgebra local finita con ideal maximal $\mathfrak{m}$, M es un $R-$módulo libre de rango 2 y $\boldsymbol{a} \in M$, son equivalentes*

1. *$\boldsymbol{a}$ es complementable.*
2. *$\boldsymbol{a}$ es libre.*
3. *$\boldsymbol{a} \notin \mathfrak{m}M$.*

Demostración. *(1)⇒(2):* Inmediato por definición.
(2)⇒(3): Sean $\boldsymbol{a} \in \mathfrak{m}M$ y $o(\mathfrak{m}) = r$, por la proposición 2.6.1, existe un $\alpha \in \mathfrak{m}$ tal que $\alpha^{r-1} \neq 0$.
Para todo $\boldsymbol{a} \in \mathfrak{m}M$, $\boldsymbol{a} = \sum_{i=1}^{t} \beta_i \boldsymbol{e}_i$ con $\beta_i \in \mathfrak{m}$ y $\boldsymbol{e}_i \in M$ entonces $\alpha^{r-1}\boldsymbol{a} = \sum_{i=1}^{t} \alpha^{r-1}\beta_i \boldsymbol{e}_i$ y $\alpha^{r-1}\beta_i \in \mathfrak{m}^r$ luego $\alpha^{r-1}\beta_i = 0$ y por tanto $\alpha^{r-1}\boldsymbol{a} = \boldsymbol{0}$. En consecuencia $\boldsymbol{a}$ no es libre.
(3)⇒(1): Sean $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ una base de M y $\boldsymbol{a} = \alpha_1\boldsymbol{u}_1 + \alpha_2\boldsymbol{u}_2$. Si $\boldsymbol{a}$ no es complementable entonces α_1 y α_2 no son inversibles ya que si α_1 es inversible, $\boldsymbol{a} \wedge \boldsymbol{u}_2 = \alpha_1(\boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{u}_2) = \alpha_1$ y $\{\boldsymbol{a}, \boldsymbol{u}_2\}$ es base de M y si α_2 es inversible lo es $\{\boldsymbol{u}_1, \boldsymbol{a}\}$. Por tanto $\alpha_1, \alpha_2 \in \mathfrak{m}$ y $\boldsymbol{a} \in \mathfrak{m}M$. ■

Proposición 3.1.6 *Si R es una $K-$álgebra finita y M es un $R-$módulo libre de rango 2, $\boldsymbol{a} \in M$ es complementable si y sólo si $\boldsymbol{a}$ es libre.*

Demostración. Si R es una $K-$álgebra finita, por la proposición 2.2.2, $R \simeq R_1 \oplus \cdots \oplus R_t$ con R_r algebra local finita para todo $i = 1, \ldots, r$. Sea M un $R-$módulo libre de rango 2, $M \simeq R \oplus R$ y sea $\boldsymbol{m} \in R \oplus R$, $\boldsymbol{m} = ((a_1, \cdots, a_r), (b_1, \cdots, b_r))$ es complementable en $R \oplus R$ si existe $\boldsymbol{n} = ((s_1, \cdots, s_r), (t_1, \cdots, t_r)) \in R \oplus R$ tal que $\boldsymbol{m} \wedge \boldsymbol{n} = \left(\begin{vmatrix} a_1 & b_1 \\ s_1 & t_1 \end{vmatrix}, \cdots, \begin{vmatrix} a_r & b_r \\ s_r & t_r \end{vmatrix} \right) \in R^*$.
Pero esto equivale a que $\begin{vmatrix} a_i & b_i \\ s_i & t_i \end{vmatrix} \in R_i^*$ para todo $i = 1, \cdots, r$ lo cual equivale a que (a_i, b_i) es complementable en R_i y por el Lema 3.1.5, (a_i, b_i) es libre en R_i es decir si $\lambda_i(a_i, b_i) = (0, 0)$ entonces $\lambda_i = 0$ para todo i. Por tanto

$$\begin{aligned} (\lambda_1, \cdots, \lambda_r)((a_1, \cdots, a_r), (b_1, \cdots, b_r)) &= ((\lambda_1 a_1, \cdots, \lambda_r a_r), (\lambda_1 b_1, \cdots, \lambda_r b_r)) \\ &= ((0, \cdots, 0), (0, \cdots, 0)) \end{aligned}$$

entonces $(\lambda_1, \cdots, \lambda_r) = (0, \cdots, 0)$. ■

Corolario 3.1.7 *Si R es una $K-$álgebra finita, M es un $R-$módulo libre de rango 2 y $\boldsymbol{a} \in M$ entonces $\boldsymbol{a}$ o bien es complementable o bien existe $\lambda \in R$, $\lambda \neq 0$, tal que $\lambda \boldsymbol{a} = \boldsymbol{0}$.*

Estudiamos ahora las relaciones entre $\boldsymbol{a}, \boldsymbol{b} \in M$ según los valores de $\boldsymbol{a} \wedge \boldsymbol{b}$.

Teorema 3.1.8 *Sea M un $R-$módulo libre de rango 2. Para todos $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in M$ se tiene*

$$(\boldsymbol{a} \wedge \boldsymbol{b})\boldsymbol{c} + (\boldsymbol{c} \wedge \boldsymbol{a})\boldsymbol{b} + (\boldsymbol{b} \wedge \boldsymbol{c})\boldsymbol{a} = \boldsymbol{0}.$$

Demostración. Sean $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ una base de M y $\boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$, $\boldsymbol{b} = b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2$ y $\boldsymbol{c} = c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2$. Entonces $(\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b})\boldsymbol{c} + (\boldsymbol{c} \wedge_{\mathcal{B}} \boldsymbol{a})\boldsymbol{b} + (\boldsymbol{b} \wedge_{\mathcal{B}} \boldsymbol{c})\boldsymbol{a} = ((a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2) \wedge_{\mathcal{B}} (b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2))(c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2) + ((c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2) \wedge_{\mathcal{B}} (a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2))(b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2) + ((b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2) \wedge_{\mathcal{B}} (c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2))(a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2) = (a_1b_2 - a_2b_1)(\boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{u}_2)(c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2) + (c_1a_2 - c_2a_1)(\boldsymbol{u}_1 \wedge \boldsymbol{u}_2)(b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2) + (b_1c_2 - b_2c_1)(\boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{u}_2)(a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2) = ((a_1b_2 - a_2b_1)c_1 + (c_1a_2 - c_2a_1)b_1 + (b_1c_2 - b_2c_1)a_1)\boldsymbol{u}_1 + ((a_1b_2 - a_2b_1)c_2 + (c_1a_2 - c_2a_1)b_2 + (b_1c_2 - b_2c_1)a_2)\boldsymbol{u}_2 = \boldsymbol{0}$. ■

Proposición 3.1.9 *Si $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ es una base de M entonces para todo $\boldsymbol{a} \in M$,*

$$\boldsymbol{a} = (\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{u}_2)\boldsymbol{u}_1 + (\boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{a})\boldsymbol{u}_2.$$

Demostración. Aplicando el Teorema 3.1.8 a $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{a}$ se tiene que $(\boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{u}_2)\boldsymbol{a} + (\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{u}_1)\boldsymbol{u}_2 + (\boldsymbol{u}_2 \wedge_{\mathcal{B}} \boldsymbol{a})\boldsymbol{u}_1 = \boldsymbol{0}$. Entonces $\boldsymbol{a} = (\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{u}_2)\boldsymbol{u}_1 + (\boldsymbol{u}_1 \wedge_{\mathcal{B}} \boldsymbol{a})\boldsymbol{u}_2$. ■

Proposición 3.1.10 *Si $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ es una base de M y $\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} = \lambda$, entonces*

(1) $\lambda\boldsymbol{u}_1 = (\boldsymbol{u}_1 \wedge \boldsymbol{b})\boldsymbol{a} + (\boldsymbol{a} \wedge \boldsymbol{u}_1)\boldsymbol{b}$.

(2) $\lambda\boldsymbol{u}_2 = (\boldsymbol{u}_2 \wedge \boldsymbol{b})\boldsymbol{a} + (\boldsymbol{a} \wedge \boldsymbol{u}_2)\boldsymbol{b}$.

Demostración. Aplicando el Teorema 3.1.8 a $\boldsymbol{u}_1, \boldsymbol{a}, \boldsymbol{b}$ y a $\boldsymbol{u}_2, \boldsymbol{a}, \boldsymbol{b}$ se tiene que $(\boldsymbol{a} \wedge \boldsymbol{b})\boldsymbol{u}_1 = (\boldsymbol{a} \wedge \boldsymbol{u}_1)\boldsymbol{b} + (\boldsymbol{u}_1 \wedge \boldsymbol{b})\boldsymbol{a}$ y $(\boldsymbol{a} \wedge \boldsymbol{b})\boldsymbol{u}_2 = (\boldsymbol{a} \wedge \boldsymbol{u}_2)\boldsymbol{b} + (\boldsymbol{u}_2 \wedge \boldsymbol{b})\boldsymbol{a}$. ■

Proposición 3.1.11 *Con las notaciones anteriores,*

1. $\boldsymbol{a} \wedge \boldsymbol{b} = 0$ *si y sólo si para todo* $\boldsymbol{c}$, $(\boldsymbol{c} \wedge \boldsymbol{b})\boldsymbol{a} + (\boldsymbol{a} \wedge \boldsymbol{c})\boldsymbol{b} = \boldsymbol{0}$ *y esto equivale a que existe* $\boldsymbol{c}$ *complementable tal que* $(\boldsymbol{c} \wedge \boldsymbol{b})\boldsymbol{a} + (\boldsymbol{a} \wedge \boldsymbol{c})\boldsymbol{b} = \boldsymbol{0}$.
2. *Si* $\boldsymbol{a}$ *es complementable, entonces* $\boldsymbol{a} \wedge \boldsymbol{b} = 0$ *si y sólo si* $\boldsymbol{b} = \lambda\boldsymbol{a}$.
3. *Si* $\boldsymbol{a}$ *es simplificable, entonces* $\boldsymbol{a} \wedge \boldsymbol{b} = 0$ *si y sólo si existe* μ *no divisor de cero con* $\mu\boldsymbol{b} = \lambda\boldsymbol{a}$.

4. *Si* $\boldsymbol{a}$ *y* $\boldsymbol{b}$ *son complementables, entonces* $\boldsymbol{a}\wedge\boldsymbol{b}=0$ *si y sólo si* $\boldsymbol{b}=\lambda\boldsymbol{a}$ *con* $\lambda\in R^*$.

5. *Si* $\boldsymbol{a}$ *es complementable y* $\boldsymbol{b}$ *es simplificable, entonces* $\boldsymbol{a}\wedge\boldsymbol{b}=0$ *si y sólo si* $\boldsymbol{b}=\lambda\boldsymbol{a}$ *con* λ *no divisor de cero.*

6. $\boldsymbol{a}\wedge\boldsymbol{b}=\lambda$ *es divisor de cero si y sólo si existe* $\mu\neq 0$ *tal que para todo* $\boldsymbol{c}\in M$, $\mu(\boldsymbol{c}\wedge\boldsymbol{b})\boldsymbol{a}+\mu(\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b}=\boldsymbol{0}$ *y esto equivale a que existe* $\mu\neq 0$ *y existe* $\boldsymbol{c}$ *complementable tal que* $\mu(\boldsymbol{c}\wedge\boldsymbol{b})\boldsymbol{a}+\mu(\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b}=\boldsymbol{0}$.

7. $\boldsymbol{a}\wedge\boldsymbol{b}=\lambda$ *es no divisor de cero si y sólo si para todo* $\boldsymbol{c}$ *complementable,* $(\boldsymbol{c}\wedge\boldsymbol{b})\boldsymbol{a}+(\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b}$ *es simplificable.*

8. $\boldsymbol{a}\wedge\boldsymbol{b}=\lambda$ *es inversible si y sólo si* $\{\boldsymbol{a},\boldsymbol{b}\}$ *es base de* M.

Demostración. *1.* Inmediato por el Teorema 3.1.8.
2. Como $\boldsymbol{a}$ es complementable, existe $\boldsymbol{a}'\in M$ tal que $\mathcal{B}=\{\boldsymbol{a},\boldsymbol{a}'\}$ es base de M. Por 1, $\boldsymbol{b}=(\boldsymbol{a}\wedge_{\mathcal{B}}\boldsymbol{a}')\boldsymbol{b}=(\boldsymbol{b}\wedge_{\mathcal{B}}\boldsymbol{a}')\boldsymbol{a}$.
3. Como $\boldsymbol{a}$ es simplificable, existen $\boldsymbol{a}'\in M$ complementable y $\mu\in R$ no divisor de cero tal que $\boldsymbol{a}=\mu\boldsymbol{a}'$ y por ser $\boldsymbol{a}'$ complementable, existe $\boldsymbol{a}''\in M$ tal que $\mathcal{B}=\{\boldsymbol{a}',\boldsymbol{a}''\}$ es base de M. Por *1*, $\mu\boldsymbol{b}=\mu(\boldsymbol{b}\wedge_{\mathcal{B}}\boldsymbol{a}'')\boldsymbol{a}'=(\boldsymbol{b}\wedge_{\mathcal{B}}\boldsymbol{a}'')\boldsymbol{a}$.
4. Por *2*, $\boldsymbol{a}=\alpha\boldsymbol{b}$ y $\boldsymbol{b}=\beta\boldsymbol{a}$ entonces $\boldsymbol{a}=\alpha\boldsymbol{b}=\alpha\beta\boldsymbol{a}$ y $(1-\alpha\beta)\boldsymbol{a}=\boldsymbol{0}$ pero $\boldsymbol{a}$ es libre luego $1=\alpha\beta$ es decir $\alpha\in R^*$.
5. Por *2*, $\boldsymbol{b}=\lambda\boldsymbol{a}$ y por *3*, λ es no divisor de cero.
6. Como $\boldsymbol{a}\wedge\boldsymbol{b}=\lambda$ es divisor de cero, existe $0\neq\mu\in R$ tal que $\lambda\mu=0$ y por el Teorema 3.1.8, para todo $\boldsymbol{c}\in M$, $\mu(\boldsymbol{c}\wedge\boldsymbol{b})\boldsymbol{a}+\mu(\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b}=\lambda\mu\boldsymbol{c}=\boldsymbol{0}$.
7. Por el Teorema 3.1.8, para todo $\boldsymbol{c}\in M$, $\lambda\boldsymbol{c}=(\boldsymbol{c}\wedge\boldsymbol{b})\boldsymbol{a}+(\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b}$ y por hipótesis $\boldsymbol{a}\wedge\boldsymbol{b}=\lambda$ es no divisor de cero y $\boldsymbol{c}$ complementable luego $(\boldsymbol{c}\wedge\boldsymbol{b})\boldsymbol{a}+(\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b}$ es simplificable.
8. Inmediato por la propiedad *3* del producto exterior. ■

Observe que si R es un anillo total de cocientes, $\boldsymbol{a}\wedge\boldsymbol{b}=\lambda$ no divisor de cero implica que $\boldsymbol{a}\wedge\boldsymbol{b}$ es inversible en R y por tanto $\{\boldsymbol{a},\boldsymbol{b}\}$ es base de M.

Proposición 3.1.12 *Sean* $\boldsymbol{a},\boldsymbol{b}\in M$. $\boldsymbol{a}\wedge\boldsymbol{b}$ *es divisor de cero si y sólo si existen* $\alpha,\beta\in R$ *tales que* $(\alpha,\beta)\neq(0,0)$ *y* $\alpha\boldsymbol{a}+\beta\boldsymbol{b}=\boldsymbol{0}$.

Demostración. $\Rightarrow$: Como $\lambda=\boldsymbol{a}\wedge\boldsymbol{b}$ es divisor de cero, existe $\mu\neq 0$ tal que $\lambda\mu=0$ y por la proposición 3.1.10, $\boldsymbol{0}=\mu\lambda\boldsymbol{u}_1=\mu(\boldsymbol{u}_1\wedge\boldsymbol{b})\boldsymbol{a}+\mu(\boldsymbol{a}\wedge\boldsymbol{u}_1)\boldsymbol{b}$ y $\boldsymbol{0}=\mu\lambda\boldsymbol{u}_2=\mu(\boldsymbol{u}_2\wedge\boldsymbol{b})\boldsymbol{a}+\mu(\boldsymbol{a}\wedge\boldsymbol{u}_2)\boldsymbol{b}$. Si alguno de los términos $\boldsymbol{u}_1\wedge\boldsymbol{b}$, $\boldsymbol{a}\wedge\boldsymbol{u}_1$, $\boldsymbol{u}_2\wedge\boldsymbol{b}$ o $\boldsymbol{a}\wedge\boldsymbol{u}_2$ es distinto de cero, se verifica el resultado y, si todos son cero entonces por la proposición 3.1.9, $\mu\boldsymbol{a}=\mu(\boldsymbol{a}\wedge_{\mathcal{B}}\boldsymbol{u}_2)\boldsymbol{u}_1+\mu(\boldsymbol{u}_1\wedge_{\mathcal{B}}\boldsymbol{a})\boldsymbol{u}_2=\boldsymbol{0}$ luego se tiene el resultado.
$\Leftarrow$: Si $\alpha\boldsymbol{a}+\beta\boldsymbol{b}=\boldsymbol{0}$ y $(\alpha,\beta)\neq(0,0)$, entonces $0=(\alpha\boldsymbol{a}+\beta\boldsymbol{b})\wedge\boldsymbol{b}=\alpha(\boldsymbol{a}\wedge\boldsymbol{b})$. Por tanto,

si $\alpha \neq 0$ se tiene que $\boldsymbol{a} \wedge \boldsymbol{b}$ es un divisor de cero, y si $\alpha = 0$ entonces $\beta \neq 0$ y $\beta \boldsymbol{b} = \boldsymbol{0}$ luego $\beta(\boldsymbol{a} \wedge \boldsymbol{b}) = \boldsymbol{a} \wedge \beta \boldsymbol{b} = \boldsymbol{a} \wedge \boldsymbol{0} = 0$. En consecuencia, $\boldsymbol{a} \wedge \boldsymbol{b}$ es un divisor de cero. ■

Vamos a estudiar propiedades de los submódulos monógenos de M, estos submódulos no son necesariamente libres y aunque sean libres no son necesariamente sumando directos de M.

Definición 3.1.13 *Sea M un $R-$módulo libre de rango 2. Si $\boldsymbol{a} \in M$ y M_1, M_2 son submódulos monógenos de M, llamamos*

1. $I(\boldsymbol{a}) = \{\boldsymbol{a} \wedge \boldsymbol{b} : \boldsymbol{b} \in M\}$.
2. $I(M_1) = \{\boldsymbol{b} \wedge \boldsymbol{c} : \boldsymbol{b} \in M_1 \ \ y \ \ \boldsymbol{c} \in M\}$.
3. $I(M_1 M_2) = \{\boldsymbol{b} \wedge \boldsymbol{c} : \boldsymbol{b} \in M_1 \ \ y \ \ \boldsymbol{c} \in M_2\}$.

Proposición 3.1.14 *1. $I(\boldsymbol{a})$, $I(M_1)$ y $I(M_1 M_2)$ son ideales de R independientes de la base elegida para definir el producto exterior.*

2. Si M_1 es libre y $\{\boldsymbol{a}\}$ es una base de M_1 entonces $I(M_1) = I(\boldsymbol{a})$.

Demostración. *1.* Sin dificultad se prueba que $I(\boldsymbol{a})$, $I(M_1)$ y $I(M_1 M_2)$ son ideales de R y veamos que son independientes de la base elegida para definir el producto exterior. Sean $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ y $\mathcal{B}' = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ bases de M, como $\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} = (\boldsymbol{a} \wedge_{\mathcal{B}'} \boldsymbol{b})(\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2)$, para todo $\boldsymbol{a}, \boldsymbol{b} \in M$, entonces $\{\boldsymbol{a} \wedge_{\mathcal{B}} \boldsymbol{b} : \boldsymbol{b} \in M\} = \{\boldsymbol{a} \wedge_{\mathcal{B}'} [(\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2)\boldsymbol{b}] : \boldsymbol{b} \in M\} = \{\boldsymbol{a} \wedge_{\mathcal{B}'} \boldsymbol{b}' : \boldsymbol{b}' \in M\}$, $\{\boldsymbol{b} \wedge_{\mathcal{B}} \boldsymbol{c} : \boldsymbol{b} \in M_1 \ \text{ y } \ \boldsymbol{c} \in M\} = \{\boldsymbol{b} \wedge_{\mathcal{B}'} [(\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2)\boldsymbol{c}] : \boldsymbol{b} \in M_1 \ \text{ y } \ \boldsymbol{c} \in M\} = \{\boldsymbol{b} \wedge_{\mathcal{B}'} \boldsymbol{c}' : \boldsymbol{b} \in M_1 \ \text{ y } \ \boldsymbol{c}' \in M\}$ y $\{\boldsymbol{b} \wedge_{\mathcal{B}} \boldsymbol{c} : \boldsymbol{b} \in M_1 \ \text{ y } \ \boldsymbol{c} \in M_2\} = \{\boldsymbol{b} \wedge_{\mathcal{B}'} [(\boldsymbol{v}_1 \wedge_{\mathcal{B}} \boldsymbol{v}_2)\boldsymbol{c}] : \boldsymbol{b} \in M_1 \ \text{ y } \ \boldsymbol{c} \in M_2\} = \{\boldsymbol{b} \wedge_{\mathcal{B}'} \boldsymbol{c}' : \boldsymbol{b} \in M_1 \ \text{ y } \ \boldsymbol{c}' \in M_2\}$.
2. Como $\boldsymbol{a} \in M_1$ entonces $I(\boldsymbol{a}) \subset I(M_1)$ y $I(M_1) \subset I(\boldsymbol{a})$ ya que si $\boldsymbol{b} \wedge \boldsymbol{c} \in I(M_1)$, como $\boldsymbol{b} \in M_1$ entonces $\boldsymbol{b} = \lambda \boldsymbol{a}$ con $\lambda \in R$ luego $\boldsymbol{b} \wedge \boldsymbol{c} = \lambda \boldsymbol{a} \wedge \boldsymbol{c} = \boldsymbol{a} \wedge \lambda \boldsymbol{c} \in I(\boldsymbol{a})$. ■

Proposición 3.1.15 *Las condiciones siguientes son equivalentes:*

1. *M_1 y M_2 son libres, y si $\boldsymbol{a}_1$ es base de M_1 y $\boldsymbol{a}_2$ es base de M_2 entonces $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ es base de M.*
2. *$I(M_1 M_2) = R$.*
3. *$M_1 + M_2 = M$.*

Proposición 3.1.16 *Sea $\boldsymbol{a} \in M$. Entonces $\boldsymbol{a}$ es simplificable si y sólo si $I(\boldsymbol{a})$ está generado por un no divisor de cero.*

Demostración. $\Rightarrow$: Si $\boldsymbol{a}$ es simplificable, entonces $\boldsymbol{a} = \lambda\boldsymbol{b}$ con $\boldsymbol{b}$ complementable y λ no divisor de cero, luego $\boldsymbol{b}$ se puede completar a una base $\{\boldsymbol{b}, \boldsymbol{b}'\}$ y $\boldsymbol{a} = \lambda\boldsymbol{b} + 0\boldsymbol{b}'$. En consecuencia, $I(\boldsymbol{a}) = L(\lambda)$.
$\Leftarrow$: Si $I(\boldsymbol{a}) = L(\lambda)$ con $\lambda \in R$ no divisor de cero, y si $\boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ entonces el ideal generado por a_1 y a_2, $L(a_1, a_2) = L(\lambda)$. Además como $\lambda \in L(a_1, a_2)$ entonces existen $\alpha_1, \alpha_2 \in R$ tales que $\lambda = \alpha_1 a_1 + \alpha_2 a_2$ pero $\alpha_1 a_1 + \alpha_2 a_2 = \alpha_1\lambda b_1 + \alpha_2\lambda b_2 = \lambda(\alpha_1 b_1 + \alpha_2 b_2)$ entonces $\lambda(1 - \alpha_1 b_1 - \alpha_2 b_2) = 0$. Como λ es no divisor de cero, $1 - \alpha_1 b_1 - \alpha_2 b_2 = 0$ esto es $\alpha_1 b_1 - \alpha_2 b_2 = 1$ luego existe $\boldsymbol{b} = L((b_1, b_2))$ complementable tal que $\boldsymbol{a} = \lambda\boldsymbol{b}$ y $\boldsymbol{a}$ es simplificable. ■

Definición 3.1.17 *Sean M un $R-$módulo libre de rango 2. Un submódulo A de M se llama complementable si está generado por $\boldsymbol{a} \in M$ complementable.*

Para cada $\boldsymbol{a} \in M$, el submódulo $L(\boldsymbol{a})$ es monógeno y si $\boldsymbol{a} = \lambda\boldsymbol{b}$ con $\lambda \in R^*$, entonces $L(\boldsymbol{a}) = L(\boldsymbol{b})$ pero el recíproco no es cierto. Por ejemplo, sea $R = \frac{\mathbb{R}[x,y]}{(xy^2 - x, y^3 - y, x^3)}$, note que $y(x, y) = (xy, y^2)$, $y(xy, y^2) = (xy^2, y^3) = (x, y)$ y $L(x, y) = L(xy, y^2)$ pero $y \notin R^*$. Sin embargo si nos limitamos a elementos complementables y submódulos libres sumando directo, la correspondencia es biunívoca.

Proposición 3.1.18 *Sea M un $R-$módulo libre de rango 2.*

1. *Si $B \subset M$ es un submódulo libre de rango 1, B es complementable si y sólo si B es sumando directo de M.*

2. *Si B es monógeno, B es complementable si y sólo si existe C monógeno con $M = B \oplus C$.*

3. *Si $\boldsymbol{a}, \boldsymbol{b} \in M$ son libres y $L(\boldsymbol{a}) = L(\boldsymbol{b})$ entonces $\boldsymbol{a} = \lambda\boldsymbol{b}$ con $\lambda \in R^*$.*

Demostración. *1.* $\Rightarrow$: Como B es complementable, existe $\boldsymbol{b} \in M$ complementable tal que $B = L(\boldsymbol{b})$. Además existe $\boldsymbol{c} \in M$ tal que $\{\boldsymbol{b}, \boldsymbol{c}\}$ es base de M, entonces $C = L(\boldsymbol{c})$ es tal que $B + C = M$ y $B \cap C = \{\boldsymbol{0}\}$. Así, B es sumando directo de M.
$\Leftarrow$: Sea $\{\boldsymbol{u}, \boldsymbol{v}\}$ una base de M. Como $B = L(\boldsymbol{b})$ es sumando directo de M, existe B' tal que $M = B + B'$ y como $\boldsymbol{b} \in M$ existen $\alpha_1, \alpha_2 \in R$ tales que $\boldsymbol{b} = \alpha_1\boldsymbol{u} + \alpha_2\boldsymbol{v}$ pero $\boldsymbol{u}, \boldsymbol{v} \in M$ entonces existen $\beta_1, \beta_2 \in R$ tales que $\boldsymbol{u} = \beta_1\boldsymbol{b} + \boldsymbol{b}'_1$ y $\boldsymbol{v} = \beta_2\boldsymbol{b} + \boldsymbol{b}'_2$ con $\boldsymbol{b}'_1, \boldsymbol{b}'_2 \in B$. Luego, $\boldsymbol{b} = \alpha_1(\beta_1\boldsymbol{b} + \boldsymbol{b}'_1) + \alpha_2(\beta_2\boldsymbol{b} + \boldsymbol{b}'_2) = (\alpha_1\beta_1 + \alpha_2\beta_2)\boldsymbol{b} + \alpha_1\boldsymbol{b}'_1 + \alpha_2\boldsymbol{b}'_2$ y $\boldsymbol{b}(1 - \alpha_1\beta_1 - \alpha_2\beta_2) = \alpha_1\boldsymbol{b}'_1 + \alpha_2\boldsymbol{b}'_2$ pero $\boldsymbol{b}(1 - \alpha_1\beta_1 - \alpha_2\beta_2) \in B$, $\alpha_1\boldsymbol{b}'_1 + \alpha_2\boldsymbol{b}'_2 \in B'$ y $B \cap B' = \{\boldsymbol{0}\}$. Entonces $\boldsymbol{b}(1 - \alpha_1\beta_1 - \alpha_2\beta_2) = \boldsymbol{0}$, como $\boldsymbol{b}$ es libre, $\alpha_1\beta_1 + \alpha_2\beta_2 = 1$ esto es $I(\boldsymbol{b}) = R$ y por tanto $\boldsymbol{b}$ es complementable.
2. $\Rightarrow$: Como B es complementable, existe $\boldsymbol{b} \in M$ complementable tal que $B = L(\boldsymbol{b})$. Además existe $\boldsymbol{c} \in M$ tal que $\{\boldsymbol{b}, \boldsymbol{c}\}$ es base de M, entonces $C = L(\boldsymbol{c})$ es monógeno tal

que $B + C = M$ y $B \cap C = \{\mathbf{0}\}$. Así, $B \oplus C = M$.
$\Leftarrow$: Sean $\boldsymbol{b}$ es un generador de B, $\boldsymbol{c}$ un generador de C y $\{\boldsymbol{u}, \boldsymbol{v}\}$ una base de M. Como $M = B \oplus C$, existen $\alpha_1, \alpha_2, \beta_1, \beta_2 \in R$ tales que $\boldsymbol{u} = \alpha_1\boldsymbol{b} + \alpha_2\boldsymbol{c}$ y $\boldsymbol{v} = \beta_1\boldsymbol{b} + \beta_2\boldsymbol{c}$. Por tanto

$$\boldsymbol{u} \wedge \boldsymbol{v} = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix} \boldsymbol{b} \wedge \boldsymbol{c}.$$

Como $\boldsymbol{u} \wedge \boldsymbol{v}$ es inversible, $\boldsymbol{b} \wedge \boldsymbol{c}$ es inversible y $\{\boldsymbol{b}, \boldsymbol{c}\}$ es base de M.
3. Existen $\alpha, \beta \in R$ tales que $\boldsymbol{a} = \alpha\boldsymbol{b}$ y $\boldsymbol{b} = \beta\boldsymbol{a}$ entonces $\boldsymbol{a} = \alpha\beta\boldsymbol{a}$ es decir $(1-\alpha\beta)\boldsymbol{a} = \mathbf{0}$ y como $\boldsymbol{a}$ es libre, $1 - \alpha\beta = 0$. Por tanto $\alpha \in R^*$. ■

Sean $A \subset M$ un $R-$submódulo y $\mathcal{B} = \{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ una base de M. Se pueden construir las proyecciones

$$\begin{array}{rccc} \pi_1 : & A & \to & R \\ & a\boldsymbol{u}_1 + b\boldsymbol{u}_2 & \mapsto & a \end{array} \quad \text{y} \quad \begin{array}{rccc} \pi_2 : & A & \to & R \\ & a\boldsymbol{u}_1 + b\boldsymbol{u}_2 & \mapsto & b \end{array}$$

Veamos que $\pi_1(A)$ y $\pi_2(A)$ son ideales de R. Sean $x, y \in \pi_1(A)$, existen $z, w \in R$ tales que $x\boldsymbol{u}_1 + z\boldsymbol{u}_2, y\boldsymbol{u}_1 + w\boldsymbol{u}_2 \in A$, $\pi_1(x\boldsymbol{u}_1 + z\boldsymbol{u}_2) = x$ y $\pi_1(y\boldsymbol{u}_1 + w\boldsymbol{u}_2) = y$. Entonces $x + y = \pi_1(x\boldsymbol{u}_1 + z\boldsymbol{u}_2) + \pi_1(y\boldsymbol{u}_1 + w\boldsymbol{u}_2) = \pi_1((x + y)\boldsymbol{u}_1 + (z + w)\boldsymbol{u}_2) \in \pi_1(A)$ y si $k \in R$, $kx = k\pi_1(x\boldsymbol{u}_1 + z\boldsymbol{u}_2) = \pi_1(kx\boldsymbol{u}_1 + kz\boldsymbol{u}_2) \in \pi_1(A)$.
En consecuencia $\pi_1(A)$ es ideal de R y, por simetría en la prueba, $\pi_2(A)$ es ideal de R.

Proposición 3.1.19 *(1) Para $i = 1, 2$, $\pi_i(A)$ depende de la base elegida en M.*

(2) $I(A) = \pi_1(A) + \pi_2(A)$.

(3) A es monógeno si y sólo si $\pi_1(A)$ y $\pi_2(A)$ son principales.

(4) A es complementable si y sólo si $R = I(A)$.

(5) Si A es complementable entonces $\pi_1(A) \cap \pi_2(A) = \pi_1(A)\pi_2(A)$.

Demostración. *(1)* Sean $\mathcal{B}_1$ una base de M y $\mathcal{B}_2$ la base de M que se obtiene al intercambiar las columnas de la base $\mathcal{B}_1$. Entonces en la base $\mathcal{B}_2$ tenemos imágenes distintas para $\pi_1(A)$ y $\pi_2(A)$ que las de la base $\mathcal{B}_1$. Por tanto $\pi_i(A)$, $i = 1, 2$, depende de la base elegida.
(2) Sea $\boldsymbol{a} = a\boldsymbol{u}_1 + b\boldsymbol{u}_2 \in A$ entonces $\pi_1(\boldsymbol{a}) = a$ y $\pi_2(\boldsymbol{a}) = b$. Como $I(\boldsymbol{a}) = \{\alpha_1 a + \alpha_2 b : \alpha_1, \alpha_2 \in R\}$, $z = \alpha_1 a + \alpha_2 b \in I(\boldsymbol{a})$ es equivalente a que $z = \alpha_1 a + \alpha_2 b \in \pi_1(A) + \pi_2(A)$.
(3) Si A es monógeno, entonces existe $\boldsymbol{a} = a\boldsymbol{u}_1 + b\boldsymbol{u}_2 \in A$ tal que $A = L(\boldsymbol{a})$. Como $\lambda(a\boldsymbol{u}_1 + b\boldsymbol{u}_2) = \lambda a\boldsymbol{u}_1 + \lambda b\boldsymbol{u}_2$ para todo $\lambda \in R$, $A = L(\boldsymbol{a})$ es equivalente a que $\pi_1(A) = L(a)$ y $\pi_2(A) = L(b)$.
(4) Es consecuencia de la Proposición 3.1.14.

(5) Veamos primero que $\pi_1(A) \cap \pi_2(A) \subset \pi_1(A)\pi_2(A)$. Como $A = L(a\boldsymbol{u}_1 + b\boldsymbol{u}_2)$ es complementable, por el item 3, $\pi_1(A) = l(a)$ y $\pi_2(A) = L(b)$. Sea $x \in \pi_1(A) \cap \pi_2(A)$ entonces $x = \alpha a$ y $x = \beta b$ con $\alpha, \beta \in R$. Luego $\alpha a - \beta b = 0$ y $(a, b) \wedge (\beta, \alpha) = 0$ en consecuencia $(\beta, \alpha) = \rho(a, b)$ con $\rho \in R$. Entonces $\beta = \rho a$ y $x = \beta b = \rho ab \in (a)(b)$. Ahora veamos que $\pi_1(A)\pi_2(A) \subset \pi_1(A) \cap \pi_2(A)$. Sea $ab \in \pi_1(A)\pi_2(A)$, si $a \in \pi_1(A)$ y $b \in \pi_2(A)$ entonces $ab \in \pi_1(A)$ y $ab \in \pi_2(A)$ ya que $\pi_1(A)$ y $\pi_2(A)$ son ideales de R. En consecuencia, $ab \in \pi_1(A) \cap \pi_2(A)$. ■

El recíproco del item 5 de la Proposición 3.1.19 no es cierto, por ejemplo, sean $R = \mathbb{Z}[x]$ y $\boldsymbol{a} = (2, x) \in R^2$. Entonces $\pi_1(2, x) \cap \pi_2(2, x) = L(2) \cap L(x) = L(2x)$ y $(2, x) \in R^2$ no es complementable.

No todo submódulo de un módulo libre de rango 2 se puede generar con 2 o menos elementos.

Ejemplo 3.1.20 *Sean A un submódulo de $M = R^2$ y $\pi_i(A)$ una de las proyecciones. $\pi_i(A)$ es un ideal de R y si $A = L((a_1, a_2), (b_1, b_2))$, entonces $\pi_i(A) = L(a_i, b_i)$. En particular, si A es monógeno, $\pi_i(A)$ lo es también.*
Sean $R = \mathbb{Z}[x]$, $M = R^2$ y $A = L((2, 0), (x, 0), (0, 1))$ submódulo de M. A es un submódulo con tres generadores que no se puede generar con menos de tres elementos. En efecto, $\pi_1(A)$ no es monógeno pues está generado por 2 y x, y por tanto A no es monógeno. Veamos ahora que para todos $\boldsymbol{u}, \boldsymbol{v} \in A$, $A \neq L(\boldsymbol{u}, \boldsymbol{v})$.
Sean $\boldsymbol{a}, \boldsymbol{b} \in A$ generadores, $\boldsymbol{a} = (a_1, a_2)$ y $\boldsymbol{b} = (b_1, b_2)$. Como $(2, 0), (x, 0), (0, 1) \in A$, $(x, 0) = \alpha_1\boldsymbol{a} + \alpha_2\boldsymbol{b}$, $(2, 0) = \beta_1\boldsymbol{a} + \beta_2\boldsymbol{b}$ y $(0, 1) = \gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b}$ con $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2 \in R$. Observe que $(x, 0) \wedge \boldsymbol{a} = \alpha_2(\boldsymbol{b} \wedge \boldsymbol{a}) = xa_2$ y $(x, 0) \wedge \boldsymbol{b} = \alpha_1(\boldsymbol{a} \wedge \boldsymbol{b}) = xa_1$ entonces $x|\alpha_1(\boldsymbol{a} \wedge \boldsymbol{b})$, $x|\alpha_2(\boldsymbol{b} \wedge \boldsymbol{a})$ y tenemos dos casos:
(i) *Si $x \nmid (\boldsymbol{a} \wedge \boldsymbol{b})$ entonces $x|\alpha_1$ y $x|\alpha_2$ luego $\alpha_1 = x\alpha_1'$, $\alpha_2 = x\alpha_2'$ con $\alpha_1', \alpha_2' \in R$ y $x(1, 0) = x\alpha_1'\boldsymbol{a} + x\alpha_2'\boldsymbol{b}$. Por tanto $(1, 0) = \alpha_1'\boldsymbol{a} + \alpha_2'\boldsymbol{b} \in A$, lo cual es absurdo.*
(ii) *Si $x|(\boldsymbol{a} \wedge \boldsymbol{b})$, como $(2, 0) \wedge \boldsymbol{a} = \beta_2(\boldsymbol{b} \wedge \boldsymbol{a}) = 2a_2$ y $(2, 0) \wedge \boldsymbol{b} = \beta_1(\boldsymbol{a} \wedge \boldsymbol{b}) = 2b_2$ entonces $x|2a_2$ y $x|2b_2$ luego $x|a_2$ y $x|b_2$. Por otra parte, $(0, 1) \wedge \boldsymbol{a} = \gamma_2(\boldsymbol{b} \wedge \boldsymbol{a}) = -a_1$ y $(0, 1) \wedge \boldsymbol{b} = \gamma_1(\boldsymbol{a} \wedge \boldsymbol{b}) = -b_1$ entonces $x|a_1$ y $x|b_1$. En consecuencia, $a_1 = xa_1'$, $a_2 = xa_2'$, $b_1 = xb_1'$, $b_2 = xb_2'$ con $a_1', a_2', b_1', b_2' \in R$ y, $\boldsymbol{a} = x\boldsymbol{a}' = x(a_1', a_2')$ y $\boldsymbol{b} = x\boldsymbol{b}' = x(b_1', b_2')$. Así, $(0, 1) = \gamma_1 x\boldsymbol{a}' + \gamma_2 x\boldsymbol{b}'$ lo cual es absurdo.*
En conclusión A no admite dos generadores. De la misma forma se pueden construir ejemplos de submódulos con un número finito de generadores que no se pueden generar con menos elementos.

Además, incluso si $A \subset M$ es un submódulo libre de rango 1 no necesariamente existe $B \subset M$ tal que $A \oplus B = M$. Por ejemplo,

Ejemplo 3.1.21 *Sean $R = \mathbb{Z}$, $M = \mathbb{Z}^2$ y $A = L((2, 4))$.*

El hecho de que A y B sean submódulos complementarios de M de rango 1 no implica que A y B sean complementarios entre si o iguales como sucede si R es un cuerpo, incluso A y B pueden tener un complementario común, ser distintos y no ser complementarios el uno del otro.

Ejemplo 3.1.22 *1. En* $M = \mathbb{Z}^2$, $L((4,1))$ *y* $L((2,1))$ *son complementarios de* $L((1,0))$ *pero* $\begin{vmatrix} 4 & 1 \\ 2 & 1 \end{vmatrix} = 2$, *luego* $L((4,1))$ *y* $L((2,1))$ *no son complementarios entre si.*

2. Sean $R = \mathbb{R}[x]/(x^3 - x)$ *y* $M = R^2$. $L(\overline{x}, 1-\overline{x})$ *y* $L(\overline{x}, 1+\overline{x})$ *son complementarios de* $L(-1-\overline{x}, \overline{x})$ *y* $L(-1+\overline{x}, \overline{x})$ *respectivamente, y no son complementarios entre si ya que* $\begin{vmatrix} \overline{x} & 1-\overline{x} \\ \overline{x} & 1+\overline{x} \end{vmatrix} = 2\overline{x}^2$, *pero tienen un elemento simplificable en común,* $(\overline{x}^2 - 1)(\overline{x}, 1-\overline{x}) = (\overline{x}^2 - 1)(\overline{x}, 1+\overline{x})$.

3.2. Rectas proyectivas

Sean R un anillo y M un $R-$módulo libre de rango 2. Definimos

$$\mathbb{P}^1_R(M) = \{A \ : \ A \ \text{ es submódulo monógeno y complementable de } M\}.$$

Todo generador de $A \in \mathbb{P}^1_R(M)$ se llama un *representante de* A. En particular, si $M = R^2$ entonces un submódulo monógeno A de M es complementable si admite una base complementable, por tanto los submódulos complementables de R^2 se corresponden con las clases de pares complementables (a, b) módulo la relación $(a, b) \sim (c, d) \Leftrightarrow \exists \lambda \in R^*$ tal que $(a, b) = \lambda(c, d)$. Al submódulo generado por (a, b) lo representamos por $[a, b]$ y cada generador de este módulo, es decir, cada par (c, d) con $(c, d) = \lambda(a, b)$ y $\lambda \in R^*$ se llama un *representante de* $[a, b]$.

Sea $\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ una base de M, observemos que la aplicación

$$\begin{array}{rccc} \varphi: & \mathbb{P}^1_R(R^2) & \to & \mathbb{P}^1_R(M) \\ & [a_1, a_2] & \mapsto & A \\ & & \boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2 & \end{array}$$

es biyectiva. Veamos que φ es inyectiva. Si $\boldsymbol{a}$ y $\boldsymbol{b}$ son dos representantes de A entonces existe $\lambda \in R^*$ tal que $\boldsymbol{b} = \lambda\boldsymbol{a}$ pero $\boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ con $a_1, a_2 \in R$ y $\boldsymbol{b} = \lambda\boldsymbol{a} = \lambda(a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2) = b_1\boldsymbol{u}_1 + b_2\boldsymbol{u}_2$ con $b_1, b_2 \in R$. Como $\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$ es una base de M, $b_1 = \lambda a_1$ y $b_2 = \lambda a_2$ es decir (b_1, b_2) y (a_1, a_2) son representantes de $[a_1, a_2]$. φ es sobreyectiva porque para todo $A = L(\boldsymbol{a}) \in \mathbb{P}^1_R(M)$, existe $[a_1, a_2] \in \mathbb{P}^1_R(R^2)$ con $\boldsymbol{a} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ y tal que $\varphi([a_1, a_2]) = L(\boldsymbol{a}) = A$.

Esta biyección permite sustituir $\mathbb{P}^1_R(M)$ por $\mathbb{P}^1_R(R^2) = \mathbb{P}^1_R$.

Proposición 3.2.1 *Si S es el conjunto de no divisores de cero de R y consideramos $\overline{M} = S^{-1}M$, el $\overline{R}-$módulo asociado a M, entonces la correspondencia*

$$\begin{array}{rccc} \varphi: & \mathbb{P}^1_R(M) & \to & \mathbb{P}^1_{\overline{R}}(\overline{M}) \\ & A & \mapsto & \overline{A} = S^{-1}A \end{array}$$

es una aplicación inyectiva.

La demostración de la Proposición 3.2.1 se basa en el lema siguiente.

Lema 3.2.2 *Sean B y C dos R-submódulos complementables de M tales que $B \cap C$ contiene algún elemento simplificable entonces $B = C$.*

Demostración. Sean $\{\boldsymbol{b}\}$ y $\{\boldsymbol{c}\}$ bases de B y C respectivamente. Si $\boldsymbol{m} \in B \cap C$ es simplificable entonces $\boldsymbol{m} = \lambda\boldsymbol{b}$ con λ no divisor de cero porque si λ fuera divisor de cero existiría $0 \neq \beta \in R$ tal que $\beta\lambda = 0$ y $\beta\boldsymbol{m} = \boldsymbol{0}$, lo cual es absurdo porque $\boldsymbol{m}$ es simplificable y por tanto libre. De la misma forma, $\boldsymbol{m} = \mu\boldsymbol{c}$ con μ no divisor de cero. Note que $0 = \boldsymbol{m} \wedge \boldsymbol{m} = \lambda\boldsymbol{b} \wedge \mu\boldsymbol{c} = \lambda\mu(\boldsymbol{b} \wedge \boldsymbol{c})$ pero λ y μ son no divisores de cero entonces $\boldsymbol{b} \wedge \boldsymbol{c} = 0$. Como $\boldsymbol{b}$ y $\boldsymbol{c}$ son complementables, por la Proposición 3.1.11, existe $\gamma \in R^*$ tal que $\boldsymbol{c} = \gamma\boldsymbol{b}$. En consecuencia $B = C$. ■

Demostración. (de la Proposición 3.2.1)
(1) φ está bien definida pues para todo A complementable, $\varphi(A)$ está unívocamente determinado y es complementable porque si $\{\boldsymbol{a}\}$ es una base de A, existe $\boldsymbol{a}'$ tal que $\{\boldsymbol{a}, \boldsymbol{a}'\}$ es base de M como $R-$módulo entonces $\{\boldsymbol{a}, \boldsymbol{a}'\}$ es base de $\overline{M}$ como $\overline{R}-$módulo y $\varphi(A)$ es complementable.
(2) Veamos que φ es inyectiva. Sean $B, C \in \mathbb{P}^1_R(M)$, $\{\boldsymbol{b}\}$ y $\{\boldsymbol{c}\}$ bases de B y C como $R-$módulos respectivamente. Como $\{\boldsymbol{b}\}$ es bases de $\overline{B}$, $\{\boldsymbol{c}\}$ es base de $\overline{C}$ y $\varphi(B) = \varphi(C)$, existe $\alpha \in \overline{R}^*$ tal que $\boldsymbol{b} = \alpha\boldsymbol{c}$, por ser α inversible en $\overline{R}^*$, $\alpha = \frac{r}{s}$ con $r, s \in S$ y existe s' tal que $s'(s\boldsymbol{b} - r\boldsymbol{c}) = \boldsymbol{0}$ entonces $s's\boldsymbol{b} = s'r\boldsymbol{c}$ con s', s, r no divisores de cero esto es $B \cap C$ tiene es un elemento simplificable, por el Lema 3.2.2, $B = C$. ■

Observación 3.2.3 *(1) La aplicación φ de la Proposición 3.2.1 no es sobreyectiva. Por ejemplo, consideremos el dominio $R = \mathbb{Z}[x]$ entonces $\Sigma = \mathbb{Q}(x)$ es un cuerpo. Note que $(2, x)$ es complementable en Σ^2 pero veamos que $L(2, x)$ no proviene de ningún submódulo complementable en R^2. Sea $\overline{A}$ el $\mathbb{Q}(x)-$submódulo generado por $(2, x)$, si $\overline{A} = \varphi(A)$, entonces existe $(a(x), b(x)) \in R^2$ tal que $(a(x), b(x)) = \alpha(2, x)$ con $\alpha = \frac{p(x)}{q(x)} \in \mathbb{Q}(x)$ es decir $q(x), p(x) \in \mathbb{Z}[x]$ son distintos de cero y no tienen factores comunes.*
Como $(a(x), b(x)) = \frac{p(x)}{q(x)}(2, x)$ entonces $a(x)q(x) = 2p(x)$ y $b(x)q(x) = xp(x)$

luego $2|a(x)q(x)$. *Si* $2|q(x)$ *se tiene que* $2|xp(x)$ *y como* $2 \nmid x$, $2|p(x)$ *lo cual es absurdo, así que* $2|a(x)$. *Por la misma razón anterior* $x|b(x)$.
Existen $a'(x), b'(x) \in R$ *tales que* $a(x) = 2a'(x)$ *y* $b(x) = xb'(x)$, *como* $(a(x), b(x))$ *es complementable existe* $(c(x), d(x)) \in R^2$ *tal que* $\begin{vmatrix} 2a'(x) & xb'(x) \\ c(x) & d(x) \end{vmatrix} = 1$. *Esto es,* $2a'(x)d(x) - xb'(x)c(x) = 1$ *y por tanto* $1 \in (\{2, x\}\mathbb{Z}[x])$ *lo cual es absurdo.*

(2) Si R es un dominio, el Lema 3.2.2 significa que, si B y C son submódulos complementables de M tales que $B \cap C \neq \{0\}$ entonces $B = C$. Este enunciado no es válido si R no es un dominio, por ejemplo, en $R = \mathbb{Z}/(6)$, $L(2,3)$ y $L(1,0)$ son complementables y $L(2,3) \cap L(1,0) \neq \{(0,0)\}$ porque $(4,0) \in L(2,3) \cap L(1,0)$ pero $L(2,3) \neq L(1,0)$ ya que $(1,0) \notin L(2,3)$.

3.3. Puntos fuertemente independientes en $\mathbb{P}^1_R$

Definición 3.3.1 *Sean $A, B \in \mathbb{P}^1_R(M)$. $A = L(\boldsymbol{a})$ y $B = L(\boldsymbol{b})$. Diremos que*

1. *A y B son fuertemente independientes si $\boldsymbol{a} \wedge \boldsymbol{b} \in R^*$.*
2. *A y B son independientes si $\boldsymbol{a} \wedge \boldsymbol{b} \in R$ es no divisor de cero.*
3. *A y B son dependientes si $\boldsymbol{a} \wedge \boldsymbol{b} \in R$ es divisor de cero.*

Observación 3.3.2 *1. Las definiciones anteriores son independientes de las bases elegidas de A y B respectivamente y de la base de M que usamos para construir el producto exterior.*

2. *A y B son fuertemente independientes si y sólo si $\{\boldsymbol{a}, \boldsymbol{b}\}$ es base de M.*
3. *A y B son fuertemente independientes si y sólo si $\overline{A}$ y $\overline{B}$ son fuertemente independientes en $\overline{M}$.*
4. *A y B son fuertemente dependientes si y sólo si existen $\alpha, \beta \in R$ tales que $(\alpha, \beta) \neq (0,0)$ y $\alpha\boldsymbol{a} + \beta\boldsymbol{b} = \boldsymbol{0}$.*
5. *Si R es un anillo total de cocientes, para todos $A, B \in \mathbb{P}^1_R(M)$, A y B son fuertemente independientes o son dependientes.*

Definición 3.3.3 *Diremos que tres puntos $A, B, C \in \mathbb{P}^1_R(M)$ forman una referencia si los conjuntos $\{A, B\}$, $\{A, C\}$, $\{B, C\}$ son fuertemente independientes.*

Proposición 3.3.4 *Sean $A = L(\boldsymbol{a})$, $B = L(\boldsymbol{b})$ y $B = L(\boldsymbol{c})$. Son equivalentes:*

(1) $\{A, B, C\}$ *es una referencia.*

(2) A *y* B *son fuertemente independientes y existen* $\gamma_1, \gamma_2 \in R^*$ *tales que*

$$(c_1, c_2) = \gamma_1(a_1, a_2) + \gamma_2(b_1, b_2).$$

(3) A *y* B *son fuertemente independientes y existen representantes de los tres puntos tales que*

$$(c_1, c_2) = (a_1, a_2) + (b_1, b_2).$$

Demostración. *(1)* $\Rightarrow$ *(2)* Puesto que $\{A, B, C\}$ es una referencia, $\{A, B\}$, $\{B, C\}$ y $\{A, C\}$ son fuertemente independientes y como $\{\boldsymbol{a}, \boldsymbol{b}\}$, $\{\boldsymbol{a}, \boldsymbol{c}\}$ y $\{\boldsymbol{b}, \boldsymbol{c}\}$ son base de M, existen $\gamma_1, \gamma_2, \gamma_1', \gamma_2' \in R$ tales que $(c_1, c_2) = \gamma_1(a_1, a_2) + \gamma_2(b_1, b_2)$ y $(a_1, a_2) = \gamma_1'(b_1, b_2) + \gamma_2'(c_1, c_2)$. Entonces

$$(c_1, c_2) = (\gamma_1\gamma_1' + \gamma_2)(b_1, b_2) + \gamma_1\gamma_2'(c_1, c_2) \Leftrightarrow \gamma_1\gamma_1' + \gamma_2 = 0,\ \gamma_1\gamma_2' = 1.$$

Luego γ_1 es inversible y, por simetría en la prueba, γ_2 es inversible.
(2) $\Rightarrow$ *(1)* Por hipótesis, $\boldsymbol{c} = \gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b}$ con $\gamma_1, \gamma_2 \in R^*$ entonces $\boldsymbol{a} \wedge \boldsymbol{c} = \gamma_2(\boldsymbol{a} \wedge \boldsymbol{b})$ y $\boldsymbol{b} \wedge \boldsymbol{c} = \gamma_1(\boldsymbol{a} \wedge \boldsymbol{b})$ pero $\gamma_1, \gamma_2, \boldsymbol{a} \wedge \boldsymbol{b} \in R^*$ luego $\{A, C\}$ y $\{B, C\}$ son fuertemente independientes.
(2) $\Leftrightarrow$ *(3)* Inmediato. ■

En consecuencia de la Proposición 3.3.4 tenemos el siguiente resultado:

Proposición 3.3.5 *Sean* $\{A, B, C\}$ *una referencia de* $\mathbb{P}^1_R(M)$, $A = L(\boldsymbol{a}) = L(\boldsymbol{a}')$ *y* $B = L(\boldsymbol{b}) = L(\boldsymbol{b}')$. *Si* $C = L(\boldsymbol{a}+\boldsymbol{b}) = L(\boldsymbol{a}'+\boldsymbol{b}')$ *entonces existe* $\lambda \in R^*$ *tal que* $\boldsymbol{a}' = \lambda\boldsymbol{a}$ *y* $\boldsymbol{b}' = \lambda\boldsymbol{b}$.

Demostración. Existen $\alpha, \beta \in R^*$ tales que $\boldsymbol{a}' = \alpha\boldsymbol{a}$, $\boldsymbol{b}' = \beta\boldsymbol{b}$ y existe $\lambda \in R^*$ tal que $\boldsymbol{a}' + \boldsymbol{b}' = \lambda(\boldsymbol{a} + \boldsymbol{b})$ entonces $\lambda(\boldsymbol{a} + \boldsymbol{b}) = \alpha\boldsymbol{a} + \beta\boldsymbol{b}$ luego $(\lambda - \alpha)\boldsymbol{a} + (\lambda - \beta)\boldsymbol{b} = \boldsymbol{0}$. Como $\boldsymbol{a}$ y $\boldsymbol{b}$ son base, $\lambda = \alpha = \beta$. ■

Definición 3.3.6 *Sea* $\{A, B, C\}$ *una referencia de* $\mathbb{P}^1_R(M)$ *con* $\{\boldsymbol{a}, \boldsymbol{b}\}$ *base de* M. *Se llama base normalizada asociada a la referencia si* $A = L(\boldsymbol{a})$, $B = L(\boldsymbol{b})$ *y* $C = L(\boldsymbol{a}+\boldsymbol{b})$.

Observe que la Proposición 3.3.5 establece que toda referencia tiene una base asociada y ésta es única salvo producto por unidades.

Proposición 3.3.7 *Si* $\{A, B, C\}$ *es una referencia de* $\mathbb{P}^1_R(M)$ *y* $D \in \mathbb{P}^1_R(M)$, *entonces existe* $[\gamma_1, \gamma_2] \in \mathbb{P}^1_R$ *único tal que si* $\{\boldsymbol{a}, \boldsymbol{b}\}$ *es una base de* M *asociada a la referencia,* $D = L(\gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b})$.

Demostración. Si $D = L(\boldsymbol{d})$, como $\{\boldsymbol{a}, \boldsymbol{b}\}$ es una base de M, $\boldsymbol{d} = \gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b}$ con $\gamma_1, \gamma_2 \in R$ y por tanto existe $[\gamma_1, \gamma_2] \in \mathbb{P}^1_R$ tal que $D = L(\gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b})$. Para comprobar la unicidad, consideremos $\{\boldsymbol{a}', \boldsymbol{b}'\}$ otra base normalizada de M y $D = L(\boldsymbol{d}')$, por la Proposición 3.3.5, existe $\lambda \in R^*$ tal que $\boldsymbol{a}' = \lambda\boldsymbol{a}$ y $\boldsymbol{b}' = \lambda\boldsymbol{b}$, y existen $\gamma_1', \gamma_2' \in R^*$ tales que $\boldsymbol{d}' = \gamma_1'\boldsymbol{a}' + \gamma_2'\boldsymbol{b}'$ y como existe $\mu \in R^*$ tal que $\boldsymbol{d}' = \mu\boldsymbol{d}$ entonces $\boldsymbol{d} = \mu^{-1}\gamma_1'\lambda\boldsymbol{a} + \mu^{-1}\gamma_2'\lambda\boldsymbol{b} = \gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b}$ luego $(\gamma_1 - \mu^{-1}\gamma_1'\lambda)\boldsymbol{a} + (\gamma_2 - \mu^{-1}\gamma_2'\lambda)\boldsymbol{b} = \boldsymbol{0}$ y por tanto $\gamma_1 = \mu^{-1}\gamma_1'\lambda$ y $\gamma_2 = \mu^{-1}\gamma_2'\lambda$ es decir $[\gamma_1, \gamma_2] = [\gamma_1', \gamma_2']$. ■

Observemos que la Proposición 3.3.7 significa que cada referencia $\mathcal{R} = \{A, B, C\}$ induce una aplicación

$$\begin{array}{rccc} \varphi_{\mathcal{R}}: & \mathbb{P}^1_R(M) & \to & \mathbb{P}^1_R \\ & D & \mapsto & [\gamma_1, \gamma_2] \\ & & D = L(\gamma_1\boldsymbol{a} + \gamma_2\boldsymbol{b}) & \end{array}$$

con $\{\boldsymbol{a}, \boldsymbol{b}\}$ base normalizada asociada a $\mathcal{R}$.

Definición 3.3.8 *$\varphi_{\mathcal{R}}(D)$ se llama coordenadas de D en la referencia $\mathcal{R}$.*

3.4. Razón doble y cuaternas armónicas

Sean R un anillo donde $2 \in R^*$ y M un $R-$módulo libre de rango 2.

Definición 3.4.1 *Si $A = L(\boldsymbol{a}), B = L(\boldsymbol{b}), C = L(\boldsymbol{c}), D = L(\boldsymbol{d})$ son cuatro puntos de $\mathbb{P}^1_R(M)$, diremos que son compatibles si existe $(\alpha, \beta) \in R^2 - \{(0,0)\}$ tal que*

$$\alpha(\boldsymbol{a} \wedge \boldsymbol{c})(\boldsymbol{b} \wedge \boldsymbol{d}) - \beta(\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{b} \wedge \boldsymbol{c}) = 0$$

donde $\wedge$ se toma en una base arbitraria. En estas condiciones $\{\rho(\alpha, \beta) : \rho \in R^*\}$ se llama razón doble de $A,\ B,\ C,\ D$.

Observación 3.4.2 *(1) La definición de ser compatibles no depende de la base elegida ni de los representantes de los puntos. En efecto, sean $\{\boldsymbol{a}'\}, \{\boldsymbol{b}'\}, \{\boldsymbol{c}'\}, \{\boldsymbol{d}'\}$ otras bases de los submódulos A, B, C, D respectivamente. Entonces existen $\alpha', \beta', \gamma', \delta' \in R^*$ tales que $\boldsymbol{a}' = \alpha'\boldsymbol{a},\ \boldsymbol{b}' = \beta'\boldsymbol{b},\ \boldsymbol{c}' = \gamma'\boldsymbol{c}$ y $\boldsymbol{d}' = \delta'\boldsymbol{d}$.*
Luego, $\alpha(\boldsymbol{a}' \wedge \boldsymbol{c}')(\boldsymbol{b}' \wedge \boldsymbol{d}') - \beta(\boldsymbol{a}' \wedge \boldsymbol{d}')(\boldsymbol{b}' \wedge \boldsymbol{c}') = \alpha\alpha'\gamma'(\boldsymbol{a} \wedge \boldsymbol{c})\beta'\delta'(\boldsymbol{b} \wedge \boldsymbol{d}) - \beta\alpha'\delta'(\boldsymbol{a} \wedge \boldsymbol{d})\ \beta'\gamma'(\boldsymbol{b} \wedge \boldsymbol{c}) = \alpha'\beta'\gamma'\delta'(\alpha\boldsymbol{a} \wedge \boldsymbol{c}\ \boldsymbol{b} \wedge \boldsymbol{d} - \beta\boldsymbol{a} \wedge \boldsymbol{d}\ \boldsymbol{b} \wedge \boldsymbol{c}) = 0$.
Si cambiamos la base $\mathcal{B}$ por $\mathcal{B}'$ para calcular el producto exterior, por la ecuación 3.1, se tiene que la definición de ser compatible en la nueva base difiere de la anterior en producto por una unidad y por tanto no depende de la base elegida.

(2) *El cambio de representantes y el cambio de base supone representar* (α, β) *por un elemento inversible.*

(3) *La condición de ser compatibles es independiente del orden de los puntos, lo que varía es el par* (α, β)*. Los posibles valores de* (α, β) *módulo unidades, cuando varía el orden de los puntos, son* (α, β), (β, α), $(\alpha - \beta, \alpha)$, $(\beta - \alpha, \beta)$, $(\alpha, \alpha - \beta)$ *y* $(\beta, \beta - \alpha)$*. Por ejemplo, si* $[A, B; C, D] = (\alpha, \beta)$ *entonces* $[A, C; B, D] = (\alpha, \alpha - \beta)$ *ya que* $\alpha(\boldsymbol{a} \wedge \boldsymbol{b})(\boldsymbol{c} \wedge \boldsymbol{d}) - (\alpha - \beta)(\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{c} \wedge \boldsymbol{b}) = \alpha(\boldsymbol{a} \wedge \boldsymbol{b})(\boldsymbol{c} \wedge \boldsymbol{d}) - \alpha(\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{c} \wedge \boldsymbol{b}) + \beta(\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{c} \wedge \boldsymbol{b}) = \alpha(\boldsymbol{a} \wedge \boldsymbol{b})(\boldsymbol{c} \wedge \boldsymbol{d}) - \alpha(\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{c} \wedge \boldsymbol{b}) - \alpha(\boldsymbol{a} \wedge \boldsymbol{c})(\boldsymbol{b} \wedge \boldsymbol{d}) = \alpha((\boldsymbol{a} \wedge \boldsymbol{b})\boldsymbol{c} - (\boldsymbol{a} \wedge \boldsymbol{d})\boldsymbol{c} - (\boldsymbol{a} \wedge \boldsymbol{c})\boldsymbol{b}) \wedge \boldsymbol{d} = 0$ *la última igualdad se tiene porque* $(\boldsymbol{a} \wedge \boldsymbol{b})\boldsymbol{c} + (\boldsymbol{c} \wedge \boldsymbol{a})\boldsymbol{b} + (\boldsymbol{b} \wedge \boldsymbol{c})\boldsymbol{a} = \boldsymbol{0}$.

Proposición 3.4.3 *Si* $\{A, B, C\}$ *es una referencia de* $\mathbb{P}^1_R(M)$ *entonces* $[A, B; C, D] = (\alpha, \beta)$ *donde* $[\alpha, \beta]$ *son las coordenadas de* D *en la referencia* $\{A, B, C\}$.

Demostración. Inmediato por la Definición 3.3.8. ■

Proposición 3.4.4 *Si tres de los cuatro puntos* A, B, C, D *son fuertemente independientes dos a dos entonces* $[A, B; C, D] \in \mathbb{P}^1_R(R^2)$ *donde* $[\alpha, \beta]$ *son las coordenadas de* D *en la referencia* $\{A, B, C\}$.

Demostración. Los puntos A, B, C, D siempre se pueden reordenar de tal forma que $\{A, B, C\}$ sea una referencia y por la Proposición 3.4.3, $[\alpha, \beta]$ son las coordenadas de D en la referencia $\{A, B, C\}$. ■

Proposición 3.4.5 *La razón doble es invariante por isomorfismos.*

Demostración. Inmediato porque es igual a cambiar los representantes de los puntos. ■

Definición 3.4.6 $[A, B; C, D]$ *es una cuaterna armónica, ó* A, B *y* C, D *están armónicamente separados, ó* D *es el cuarto armónico de* A, B, C*, si eligiendo bases* $\{\boldsymbol{a}\}, \{\boldsymbol{b}\}, \{\boldsymbol{c}\}$, $\{\boldsymbol{d}\}$ *de* A, B, C, D *respectivamente, se cumple que* A, B, C, D *son compatibles y* $[A, B; C, D] = (1, -1)$ *es decir* $(\boldsymbol{a} \wedge \boldsymbol{c})(\boldsymbol{b} \wedge \boldsymbol{d}) + (\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{b} \wedge \boldsymbol{c}) = 0$.

Observación 3.4.7 *(1) La definición de cuaterna armónica no depende de la elección de las bases ni de los representantes de los puntos.*

(2) *La relación de estar armónicamente separados no depende del orden de los pares de puntos, y es simétrica. Es decir, si* $[A, B; C, D]$ *es una cuaterna armónica entonces* $[C, D; A, B] = [B, A; C, D] = [A, B; C, D]$*. En efecto,* $(\boldsymbol{a} \wedge \boldsymbol{c})(\boldsymbol{b} \wedge \boldsymbol{d}) + (\boldsymbol{a} \wedge \boldsymbol{d})(\boldsymbol{b} \wedge \boldsymbol{c}) = (\boldsymbol{c} \wedge \boldsymbol{a})(\boldsymbol{d} \wedge \boldsymbol{b}) + (\boldsymbol{c} \wedge \boldsymbol{b})(\boldsymbol{d} \wedge \boldsymbol{a}) = (\boldsymbol{b} \wedge \boldsymbol{c})(\boldsymbol{a} \wedge \boldsymbol{d}) + (\boldsymbol{b} \wedge \boldsymbol{d})(\boldsymbol{a} \wedge \boldsymbol{c})$*. De igual*

forma, $[D,C;A,B] = [A,B;D,C] = [C,D;B,A] = [D,C;B,A] = [B,A;D,C] = [A,B;C,D]$.

(3) Sea $\{A,B,C\}$ *una referencia.* $[A,B;C,D]$ *es una cuaterna armónica si y sólo si* D *tiene coordenadas* $[1,-1]$ *en la base asociada a la referencia.*

Sean $A,B,C,X \in \mathbb{P}^1_R$ y $\{\boldsymbol{a}\},\{\boldsymbol{b}\},\{\boldsymbol{c}\},\{\boldsymbol{x}\}$ bases de A,B,C,X respectivamente. Si $[A,B;C,X]$ es una cuaterna armónica, $(\boldsymbol{a}\wedge\boldsymbol{c})(\boldsymbol{b}\wedge\boldsymbol{x}) + (\boldsymbol{a}\wedge\boldsymbol{x})(\boldsymbol{b}\wedge\boldsymbol{c}) = ((\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b} + (\boldsymbol{b}\wedge\boldsymbol{c})\boldsymbol{a})\wedge\boldsymbol{x} = 0$. Sea $\boldsymbol{v} = (\boldsymbol{a}\wedge\boldsymbol{c})\boldsymbol{b} + (\boldsymbol{b}\wedge\boldsymbol{c})\boldsymbol{a}$, entonces

$$\boldsymbol{v}\wedge\boldsymbol{x} = 0. \tag{3.2}$$

Proposición 3.4.8 *Sea* R *un anillo.*

1. *Si* $\boldsymbol{v}$ *es complementable, entonces* $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ *si y sólo si* $\boldsymbol{x} = \lambda\boldsymbol{v}$.

2. *Si* $\boldsymbol{v}$ *es complementable, entonces* $\boldsymbol{x} = \lambda\boldsymbol{v}$, $\lambda \in R^*$ *si y sólo si* $\boldsymbol{x}$ *es complementable.*

Demostración. Inmediato por la Proposición 3.1.11. ■

Proposición 3.4.9 *Sea* R *un anillo. Si* $\boldsymbol{v} \in R\boldsymbol{w}$ *con* $\boldsymbol{w}$ *complementable entonces* $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ *tiene solución única* $\boldsymbol{x} \in \mathbb{P}^1_R$ *complementable si y sólo si* $\boldsymbol{v}$ *es simplificable.*

Demostración. $\Rightarrow$: Supongamos que $\boldsymbol{v} = \lambda\boldsymbol{w}$, con λ divisor de cero y $\boldsymbol{w}$ complementable. Existe $\boldsymbol{w}' \in R^2$ tal que $\{\boldsymbol{w},\boldsymbol{w}'\}$ es una base de R^2 y existe $0 \neq \mu \in R$ tal que $\mu\lambda = 0$. Puesto que $\boldsymbol{v}\wedge\boldsymbol{x} = \lambda\boldsymbol{w}\wedge\boldsymbol{x} = 0$, entonces $\boldsymbol{x} = \boldsymbol{w}$ o $\boldsymbol{x} = \boldsymbol{w} + \mu\boldsymbol{w}'$ son soluciones no proporcionales. Por tanto la solución de $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ no es única, lo cual es absurdo.
$\Leftarrow$: Por hipótesis, $\boldsymbol{v} = \lambda\boldsymbol{w}$ con λ no divisor de cero, como $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ entonces $\lambda\boldsymbol{w}\wedge\boldsymbol{x} = 0$ pero λ es no divisor de cero luego $\boldsymbol{w}\wedge\boldsymbol{x} = 0$ y por tanto $[\boldsymbol{x}] = [\boldsymbol{w}]$. ■

En general, si entre $A,B,C \in \mathbb{P}^1_R$ no hay dos fuertemente independientes entonces puede no existir $X \in \mathbb{P}^1_R$, el cuarto armónico de A,B,C, o puede existir más de un punto con esta propiedad.

Ejemplo 3.4.10 *(1) Sea* $R = \mathbb{Z}[x,y]$ *y supongamos que* $A = [2,1], B = [x,1], C = [y,1] \in \mathbb{P}^1_R$. *Veamos que no es posible encontrar* $X = [\alpha,\beta] \in \mathbb{P}^1_R$, *el cuarto*

armónico de A, B, C. En efecto, $[A, B; C, X]$ es una cuaterna armónica si

$$\begin{aligned} 0 &= \boldsymbol{a} \wedge \boldsymbol{c}\ \boldsymbol{b} \wedge \boldsymbol{x} + \boldsymbol{a} \wedge \boldsymbol{x}\ \boldsymbol{b} \wedge \boldsymbol{c} = (2-y)(\beta x - \alpha) + (2\beta - \alpha)(x-y) \\ &= 2\beta x - 2\alpha - \beta xy + \alpha y + 2\beta x - 2\beta y - \alpha x + \alpha y \\ &= -\alpha(2 - 2y + x) + \beta(4x - xy - 2y). \end{aligned}$$

Luego $\alpha = 4x - xy - 2y$, $\beta = 2 - 2y + x$ y no es posible escribir el par (α, β) como el producto de un inversible de R por $(1, -1)$ es decir no existe un submódulo complementable X tal que $[A, B; C, X]$ es una cuaterna armónica.

(2) Sea $R = \mathbb{Z}/(6)$ y tomemos $A = [2, 1], B = [4, 1], C = [0, 1] \in \mathbb{P}^1_R$. Encontrar $X = [\alpha, \beta] \in \mathbb{P}^1_R$ tal que $[A, B; C, X]$ sea una cuaterna armónica tiene más de una solución. En efecto,

$$0 = \boldsymbol{a} \wedge \boldsymbol{c}\ \boldsymbol{b} \wedge \boldsymbol{x} + \boldsymbol{a} \wedge \boldsymbol{x}\ \boldsymbol{b} \wedge \boldsymbol{c} = 2(4\beta - \alpha) + 4(2\beta - \alpha) = 4\beta.$$

Luego tomando las parejas $\alpha = 1$, $\beta = 0$ y $\alpha = 1$, $\beta = 3$ se tienen dos submódulos complementables distintos $X_1 = [1, 0], X_2 = [1, 3] \in P^1_R$ tales que $[A, B; C, X_i]$, $i = 1, 2$, son cuaternas armónicas.

Proposición 3.4.11 *Sea R un dominio de factorización única. Entre $A, B, C \in \mathbb{P}^1_R$ existen dos puntos distintos si y sólo si existe $X \in \mathbb{P}^1_R$ único complementable tal que $[A, B; C, X]$ es una cuaterna armónica.*

Demostración. Como R es un dominio de factorización única, para todos $s, t \in R$,

$$(s, t) \in R^2 \text{ es complementable } \Leftrightarrow \operatorname{mcd}(s, t) = 1.$$

Por la Proposición 3.4.9, dados $A, B, C \in \mathbb{P}^1_R$ la existencia de $X \in \mathbb{P}^1_R$ único complementable tal que $\boldsymbol{v} \wedge \boldsymbol{x} = 0$ es equivalente a que $\boldsymbol{v} = \lambda \boldsymbol{w}$ con λ no divisor de cero y $\boldsymbol{w}$ complementable. Como R es un dominio de factorización única, R es un dominio de ideales principales y para todo $\boldsymbol{v} = (a, b) \in R^2$, $\boldsymbol{v} = \alpha(a', b')$ con $\alpha = \operatorname{mcd}(a, b)$ y (a', b') complementable. ■

Proposición 3.4.12 *Sea $2 \in R^*$. $A, B \in \mathbb{P}^1_R$ son independientes si y sólo si existe $X \in \mathbb{P}^1_R$ único complementable tal que $[A, A; B, X]$ es una cuaterna armónica.*

Demostración. $\Rightarrow$: $[A, A; B, X]$ es una cuaterna armónica si tomando bases $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}$ de A, B, X respectivamente,

$$\boldsymbol{v} \wedge \boldsymbol{x} = 0 \text{ con } \boldsymbol{v} = 2(\boldsymbol{a} \wedge \boldsymbol{b})\boldsymbol{a}$$

donde 2 y $\boldsymbol{a}\wedge\boldsymbol{b}$ son no divisores de cero ya que $A, B \in \mathbb{P}^1_R$ son independientes. Por tanto $\boldsymbol{v} = 2(\boldsymbol{a}\wedge\boldsymbol{b})\boldsymbol{a}$ tiene la forma $\boldsymbol{v} = \lambda\boldsymbol{a}$ con λ no divisor de cero y $\boldsymbol{a}$ complementable. Por la Proposición 3.4.9 existe X único complementable que satisface $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ y $X = A$. $\Leftarrow$: Por la Proposición 3.4.9, si $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ tiene solución única complementable entonces $\boldsymbol{v} = 2(\boldsymbol{a}\wedge\boldsymbol{b})\boldsymbol{a}$ y $\boldsymbol{v}\wedge\boldsymbol{a} = 2(\boldsymbol{a}\wedge\boldsymbol{b})(\boldsymbol{a}\wedge\boldsymbol{a}) = 0$. Por tanto $\boldsymbol{w} = \boldsymbol{a}$ y $\boldsymbol{a}\wedge\boldsymbol{b}$ es no divisor de cero ya que si $\boldsymbol{a}\wedge\boldsymbol{b}$ es divisor de cero, $\boldsymbol{v}\wedge\boldsymbol{x} = 0$ tiene más de una solución. En consecuencia A y B son independientes. ■

Corolario 3.4.13 *Sea $2 \in R^*$. Si entre A, B, C existen dos que sean fuertemente independientes, entonces existe $X \in P^1_R$ único complementable tal que $[A, B; C, X]$ es una cuaterna armónica.*

Por la Proposición 3.4.12, observe que el recíproco del Corolario 3.4.13 no se cumple.

Definición 3.4.14 *Sea*

$$\sigma : \mathbb{P}^1_R \to \mathbb{P}^1_R$$

una correspondencia biunívoca. La biyección σ se llama propia si para todos A, B, C, D tales que $[A, B; C, D]$ es una cuaterna armónica se cumple que $[\sigma(A), \sigma(B); \sigma(C), \sigma(D)]$ es una cuaterna armónica.

Proposición 3.4.15 *Sean R un dominio de factorización única y σ una correspondencia propia. Si entre $A, B, C \in \mathbb{P}^1_R$ hay dos distintos entonces entre $\{\sigma(A), \sigma(B), \sigma(C)\}$ existen dos distintos.*

Demostración. Por la Proposición 3.4.11, si entre $\{A, B, C\}$ hay dos distintos entonces existe $X \in \mathbb{P}^1_R$ único tal que $[A, B; C, X]$ es una cuaterna armónica. Como σ conserva cuaternas armónicas entonces $[\sigma(A), \sigma(B); \sigma(C), \sigma(X)]$ es una cuaterna armónica y nuevamente por la Proposición 3.4.11 entre $\{\sigma(A), \sigma(B), \sigma(C)\}$ existen dos distintos. ■

Proposición 3.4.16 *Sean $2 \in R^*$, $A, B \in \mathbb{P}^1_R$ y σ una correspondencia propia. Si $\{A, B\}$ son independientes entonces $\{\sigma(A), \sigma(B)\}$ son independientes.*

Demostración. Si A y B son independientes entonces $\boldsymbol{a}\wedge\boldsymbol{b}$ es no divisor de cero. Por la Proposición 3.4.12 existe $X \in \mathbb{P}^1_R$ único complementable tal que $[A, A; B, X]$ es una cuaterna armónica. Como σ es biunívoca y conserva cuaternas armónicas, existe $Y \in \mathbb{P}^1_R$ único complementable tal que $[\sigma(A), \sigma(A); \sigma(B), Y]$ es una cuaterna armónica. Luego, por la Proposición 3.4.12, $\{\sigma(A), \sigma(B)\}$ son independientes. ■

Proposición 3.4.17 *Sean R un anillo total de cocientes, $2 \in R^*$, $A, B \in \mathbb{P}^1_R$ y σ una correspondencia propia. Si $\{A, B\}$ son fuertemente independientes entonces $\{\sigma(A), \sigma(B)\}$ son fuertemente independientes.*

Demostración. En un anillo total de cocientes los elementos no divisores de cero coinciden con los elementos inversibles, por tanto $\{A, B\}$ son fuertemente independientes si y sólo si $\{A, B\}$ son independientes y se aplica la Proposición 3.4.16. ■

Proposición 3.4.18 *Sean R un anillo total de cocientes, $2 \in R^*$ y σ una aplicación propia. Si $\{A, B, C\}$ es una referencia entonces $\{\sigma(A), \sigma(B), \sigma(C)\}$ es una referencia.*

Demostración. $\{A, B, C\}$ es una referencia si $\{A, B\}$, $\{A, C\}$, $\{B, C\}$ son fuertemente independientes. Por la Proposición 3.4.17, $\{\sigma(A), \sigma(B)\}$, $\{\sigma(A), \sigma(C)\}$, $\{\sigma(B), \sigma(C)\}$ son fuertemente independientes. En consecuencia $\{\sigma(A), \sigma(B), \sigma(C)\}$ es una referencia. ■

Lema 3.4.19 *Para todo $\alpha, \beta \in R$, $\alpha \neq \pm\beta$, donde $2 \in R^*$, se tiene que*

(1) $[[1, \alpha], [1, \beta]; [0, 1], [1, \frac{\alpha+\beta}{2}]]$

(2) $[[1, 0], [1, \alpha]; [0, 1], [1, \frac{\alpha}{2}]]$

(3) $[[1, \alpha], [1, \beta]; [1, 0], [\alpha + \beta, 2\alpha\beta]]$

forman cuaternas armónicas.

Demostración. El cálculo es directo, por ejemplo, $[[1, \alpha], [1, \beta]; [0, 1], [1, \frac{\alpha+\beta}{2}]] = (1, \alpha) \wedge (0, 1)\ (1, \beta) \wedge (1, \frac{\alpha+\beta}{2}) + (1, \alpha) \wedge (1, \frac{\alpha+\beta}{2})\ (1, \beta) \wedge (0, 1) = \frac{\alpha-\beta}{2} + \frac{\beta-\alpha}{2} = 0$. ■

Teorema 3.4.20 *Sea R un anillo total de cocientes y $2 \in R^*$. σ es una correspondencia propia si y sólo si existe $\tau \in Aut(R)$ y un isomorfismo $\tau-$semilineal φ entre los espacios vectoriales asociados, tal que $\sigma = [\varphi]$. Esto es, existen $\tau \in Aut(R)$ y $M \in GL_2(R)$ tal que*

$$\sigma([\alpha_1, \alpha_2]) = [\beta_1, \beta_2]; \quad \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = M \begin{pmatrix} \tau(\alpha_1) \\ \tau(\alpha_2) \end{pmatrix}.$$

Demostración. $\Leftarrow$: Inmediato.
$\Rightarrow$: Sean σ una correspondencia propia y $\mathcal{R} = \{A, B, C\}$ una referencia de $\mathbb{P}^1_R$, por la Proposición 3.4.18, sabemos que $\mathcal{R}' = \{\sigma(A), \sigma(B), \sigma(C)\}$ es también una referencia. Para cada $x \in R$, llamo $X := [1, x] \in \mathbb{P}^1_R$ y $\sigma(X) := [y_1, y_2]$. Veamos que y_1 es inversible. En efecto, $\boldsymbol{x} = (1, x)$ hace parte de una base, luego tomamos $\{(1, x), (0, 1)\}$ como base de R^2. Por la Proposición 3.4.17, $\{\sigma([1, x]), \sigma([0, 1])\}$=$\{[y_1, y_2], [0, 1]\}$ son fuertemente independientes, entonces

$$\begin{vmatrix} y_1 & y_2 \\ 0 & 1 \end{vmatrix} = y_1 \in R^*$$

por tanto,

$$\sigma(X) := [y_1, y_2] = [1, y].$$

La forma de construir el automorfismo es la siguiente: definimos la correspondencia

$$\begin{array}{rccc} \tau: & R & \to & R \\ & x & \mapsto & \tau(x)=y \end{array}$$

τ es una aplicación biunívoca que transforma el cero en el cero y el uno en uno. En efecto, τ es inyectiva pues para $x_1, x_2 \in R$,

$$\sigma([1,x_1]) = \sigma([1,x_2]) \;\Leftrightarrow\; [1,\tau(x_1)] = [1,\tau(x_2)] \;\Leftrightarrow\; \tau(x_1) = \tau(x_2)$$

y como σ es inyectiva entonces $x_1 = x_2$. τ es sobreyectiva ya que σ también lo es.
τ es un automorfismo de anillos. Para probar que τ transforma suma en suma necesitamos ver primero que $\tau(\frac{\alpha}{2}) = \frac{\tau(\alpha)}{2}$.
Por el Lema 3.4.19, en la referencia $\mathcal{R}$,

$$[[1,0],[1,\alpha];[0,1],[1,\frac{\alpha}{2}]]$$

es una cuaterna armónica y como σ conserva cuaternas armónicas entonces

$$[\sigma([1,0]),\sigma([1,\alpha]);\sigma([0,1]),\sigma([1,\frac{\alpha}{2}])]$$

es una cuaterna armónica. Ahora bien, $\sigma([1,0]) = [1,0]$, $\sigma([0,1]) = [0,1]$, $\sigma([1,\alpha]) = [1,\tau(\alpha)]$ y $\sigma([1,\frac{\alpha}{2}]) = [1,\tau(\frac{\alpha}{2})]$, luego $0 = (1,0) \wedge (0,1)\ (1,\tau(\alpha)) \wedge (1,\tau(\frac{\alpha}{2})) + (1,0) \wedge (1,\tau(\frac{\alpha}{2}))\ (1,\tau(\alpha)) \wedge (0,1)$. Entonces

$$\tau(\frac{\alpha}{2}) = \frac{\tau(\alpha)}{2}.$$

Veamos ahora que $\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta)$. Si $\alpha = \beta$, es inmediato por el apartado anterior. Si $\alpha \neq \beta$, por el Lema 3.4.19, en la referencia $\mathcal{R}$,

$$[[1,\alpha],[1,\beta];[0,1],[1,\frac{\alpha+\beta}{2}]]$$

es una cuaterna armónica y por tanto

$$[\sigma([1,\alpha]),\sigma([1,\beta]);\sigma([0,1]),\sigma([1,\frac{\alpha+\beta}{2}])]$$

es una cuaterna armónica y en la referencia $\mathcal{R}$'tenemos que $0 = (1,\tau(\alpha))\wedge(0,1)\ (1,\tau(\beta))\wedge (1,\tau(\frac{\alpha+\beta}{2})) + (1,\tau(\alpha)) \wedge (1,\tau(\frac{\alpha+\beta}{2}))\ (1,\tau(\beta)) \wedge (0,1)$. Entonces

$$\tau(\frac{\alpha+\beta}{2}) = \frac{\tau(\alpha)+\tau(\beta)}{2},$$

pero $\tau(\frac{\alpha+\beta}{2}) = \frac{\tau(\alpha+\beta)}{2}$ luego

$$\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta).$$

Para probar que τ transforma producto en producto, necesitamos ver primero resultado adicional $\tau(\alpha^2) = (\tau(\alpha))^2$. En efecto, por el Lema 3.4.19, para $\alpha \neq -\beta$

$$[[1,\alpha],[1,\beta];[1,0],[\alpha+\beta,2\alpha\beta]]$$

es una cuaterna armónica entonces en particular para $\beta = 1-\alpha$ y $\alpha \neq \frac{1}{2}$, se tiene que

$$[[1,\alpha],[1,1-\alpha];[1,0],[1,2\alpha(1-\alpha)]]$$

es una cuaterna armónica y como σ conserva cuaternas armónicas, en la referencia $\mathcal{R}'$ tenemos que

$$[[1,\tau(\alpha)],[1,\tau(1-\alpha)];[1,0],[1,\tau(2\alpha(1-\alpha))]]$$

es una cuaterna armónica. Como $\tau(\frac{1}{2}) = \frac{1}{2}$ entonces para $\alpha \neq \frac{1}{2}$ se tiene que $\tau(\alpha) \neq \frac{1}{2}$ ya que τ es inyectiva. Además $\tau(1-\alpha) = 1-\tau(\alpha)$ luego $[[1,\tau(\alpha)],[1,\tau(1-\alpha)];[1,0],[1,\tau(2\alpha(1-\alpha))]] = [[1,\tau(\alpha)],[1,1-\tau(\alpha)];[1,0],[1,\tau(2\alpha(1-\alpha))]]$ es una cuaterna armónica y por tanto

$$\tau(2\alpha(1-\alpha)) = 2\tau(\alpha)(1-\tau(\alpha))$$

De donde se deduce que $\tau(\alpha^2) = (\tau(\alpha))^2$, también se cumple que $\tau((\frac{1}{2})^2) = (\tau(\frac{1}{2}))^2$. Ahora bien $(\tau(\alpha+\beta))^2 = \tau((\alpha+\beta)^2)$ entonces $(\tau(\alpha))^2 + 2\tau(\alpha)\tau(\beta) + (\tau(\beta))^2 = \tau(\alpha^2) + 2\tau(\alpha)\tau(\beta) + \tau(\beta^2)$ y por tanto

$$\tau(\alpha\beta) = \tau(\alpha)\tau(\beta).$$

Luego, τ es un automorfismo de anillos. En consecuencia tomando el punto $X = [\alpha_1, \alpha_2]$ en la referencia $\{A, B, C\}$ y si $\alpha_2 = 0$ entonces $X = A = [1,0]$ y $\sigma(X) = A'$ tiene también coordenadas $[1,0]$, y si $\alpha_2 \neq 0$ entonces $X = [\frac{\alpha_1}{\alpha_2}, 1]$ con lo cual

$$\sigma(X) = [\tau(\frac{\alpha_1}{\alpha_2}), 1] = [\frac{\tau(\alpha_1)}{\tau(\alpha_2)}, 1] = [\tau(\alpha_1), \tau(\alpha_2)].$$

Luego la aplicación $\tau-$semilineal φ que tiene matriz

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

respecto de las bases normalizadas asociadas a las referencias $\{A, B, C\}$ y $\{A', B', C'\}$ verifica que $[\varphi] = \sigma$. Y queda probado el teorema. ■

Proposición 3.4.21 *El automorfismo τ del teorema 3.4.20 no depende de la elección de $\{A, B, C\}$ en $\mathbb{P}^1_R$.*

Demostración. Elijamos dos referencias en $\mathbb{P}^1_R$, $\{A_1, A_2, A_3\}$, $\{B_1, B_2, B_3\}$ y llamamos $\sigma(A_i) = A'_i$ y $\sigma(B_i) = B'_i$. Si $P \in \mathbb{P}^1_R$ tiene coordenadas $[x_1, x_2]$, $[t_1, t_2]$ en las referencias $\{A_1, A_2, A_3\}$ y $\{B_1, B_2, B_3\}$ respectivamente y $\sigma(P)$ tiene coordenadas $[y_1, y_2]$, $[z_1, z_2]$ en las referencias $\{A'_1, A'_2, A'_3\}$ y $\{B'_1, B'_2, B'_3\}$ respectivamente, se verifica que si los automorfismos asociados a σ en las dos parejas de referencias son τ_1 y τ_2 entonces

$$[y_1, y_2] = \sigma[x_1, x_2] = [\tau_1(x_1), \tau_1(x_2)]$$

$$[z_1, z_2] = \sigma[t_1, t_2] = [\tau_2(t_1), \tau_2(t_2)].$$

Por otra parte, por las fórmulas de cambio de referencia en $\mathbb{P}^1_R$ tenemos que

$$\rho \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}. \tag{3.3}$$

Aplicando también las fórmulas de cambio de referencia en $\mathbb{P}^1_R$ en sentido contrario a $\sigma(P)$, se tiene

$$\mu \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = N \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}. \tag{3.4}$$

Ahora, aplicando τ_2 a la ecuación 3.3 y sustituyendo las y y las z en 3.4 se obtiene

$$\tau_2(\rho) \begin{pmatrix} \tau_2(t_1) \\ \tau_2(t_2) \end{pmatrix} = \tau_2(M) \begin{pmatrix} \tau_2(x_1) \\ \tau_2(x_2) \end{pmatrix}$$
$$\mu \begin{pmatrix} \tau_1(x_1) \\ \tau_1(x_2) \end{pmatrix} = N \begin{pmatrix} \tau_2(t_1) \\ \tau_2(t_2) \end{pmatrix}$$

sustituyendo y agrupando los factores de proporcionalidad

$$\lambda \begin{pmatrix} \tau_1(x_1) \\ \tau_1(x_2) \end{pmatrix} = Q \begin{pmatrix} \sigma(x_1) \\ \sigma(x_2) \end{pmatrix} \tag{3.5}$$

con $\lambda = \lambda([x_1, x_2])$ variable según el punto y $Q = N\tau_2(M)$. Como τ_1 y τ_2 son automorfismos, $\tau_1(1) = \tau_2(1) = 1$ y $\tau_1(0) = \tau_2(0) = 0$. Sea $Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ entonces,

sustituyendo en 3.5 para los puntos $[1,0]$, $[0,1]$ y $[1,1]$, tenemos que

$$\lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = Q \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \Rightarrow a = \lambda_1,\ c = 0$$

$$\lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = Q \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix} \Rightarrow d = \lambda_2,\ b = 0$$

$$\lambda_3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = Q \begin{pmatrix} 1 \\ 1 \end{pmatrix} \Rightarrow \lambda_1 = \lambda_2 = \lambda_3$$

Luego Q se puede tomar como $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y $\lambda \begin{pmatrix} \tau_1(y_1) \\ \tau_1(y_2) \end{pmatrix} = \begin{pmatrix} \tau_2(y_1) \\ \tau_2(y_2) \end{pmatrix}$ donde

$$\frac{\tau_1(y_1)}{\tau_1(y_2)} = \frac{\tau_2(y_1)}{\tau_2(y_2)} \Rightarrow \tau_1(\frac{y_1}{y_2}) = \tau_2(\frac{y_1}{y_2}),\ \ \forall\ y_1, y_2 \in R.$$

Por tanto, $\tau_1 = \tau_2$. ■

Bibliografía

[1] Abellanas P.: *Geometría básica*. Editorial ROMO, S.L. Madrid, 1969.

[2] Alonso Garcia M. E., Lombardi H. and Perdry H.: *Elementary constructive theory of Henselian local rings*. Math. Logic Quarterly 54(3), p. 253–271, 2008.

[3] Atiyah M. F. and Macdonald I. G.: *Introducción al álgebra conmutativa*. Editorial Reverté S. A. Barcelona, 1980.

[4] Arapovic M.: *Characterizations of the 0-dimensional rings.* Glasnik Matematicki, vol. 18(38), pp.39–46, 1983.

[5] Aroca J.M., Fernández M.J.: *Geometría proyectiva*. Publicaciones Universidad de Valladolid, 2009.

[6] Brewer J. and Richman F.: *Subrings of zero-dimensional rings*. Multiplicative, p. 1380–1383, ideal theory in commutative Algebra, Springer pp. 73–88, 2006.

[7] Fernández Bermejo E.: *Tesis doctoral: Esctructura del grupo simplético sobre un anillo conmutativo*. Directores: J.M. Aroca y P. Abellanas, Universidad Complutense de Madrid, Facultad de Matemáticas, 1976.

[8] Jech T.: *Set theory, The third millenium editions, revised and expanded*. Springer Monographs in Matematics, Springer-Verlag, Berlin, 2003.

[9] Havlicek H.: *From pentacyclic coordinates to chain geometries, and back*. Mitt. Math. Ges. Hamburg 26, pp. 75-94, 2007.

[10] Havlicek H. and List K.: *A three-Dimensional Laguerre geometry and its visualization*. In proceedinhs-Dresden Symposium geometry: constructive and kinematic. Institut für geometrie TU Dresden, Dresden pp. 122-129, 2003. arXiv:1304.0223v1 [math.AG] 31 Mar 2013.

[11] van der Kallen W.: *The K_2 of rings with many units.* Ann. Sci. École Norm. Sup. (4) 10, 1977.

[12] Kaplansky I.: *Elementary divisors and modules.* University of Chicago, pp. 464-491, 1948.

[13] Lafon J. P.: *Algébre commutative langages géométrique et algégrique.* Collection enseignement des sciences 24, Herman, Paris, 1977.

[14] Lam T. Y.: *Serre's conjeture.* Springer-Verlag, New York, 1978.

[15] Lawton W. M. and Lin Z.: *Matrix completion problems in multidimensional systems.* Proceedings-IEEE International Symposium on Circuits and Systems, vol. 5 pp. 45-48, 1999.

[16] Markova O. V.: *Classification of matrix subalgebras of length 1.* Journal of Mathematics Sciences 185(3), p. 458-472, 2012.

[17] Mazuelas S.: *Tesis de doctoral: Interpretación proyectiva de las geometrías métricas, equiformes e inversivas.* Director: J.M. Aroca, Universidad de Valladolid, 2008.

[18] McDonald B.: *Linear algebra over conmutative rings.* Marcel Dekker, Inc. New York and Basel, 1984.

[19] McDonald B. and Waterhouse W.: *Projective modules over rings with many units.* Proceedings of the American Mathematical Society, Vol. 83, N^{o} 3, november 1981.

[20] McDonald B.: *Projectivities over rings with many units.* Communications in algebra, 9(2), 1981.

[21] Morales G. M.: *Tesis de doctoral: Métricas, compactificaciones y extensiones del cuerpo real.* Director: J.M. Aroca, Universidad de Valladolid, 1996.

[22] Navarro J. A.: *Algebra conmutativa básica.* Manuales Unex No 19, Universidad de Extremadura, 1996.

[23] Olivert Pellicer J.: *Estructuras de álgebra Multilineal.* Universitat de València, 1996.

[24] Poonen B.: *Isomorphism types of commutative algebras of finite rank over an algebraically closed field.* In Computational Arithmetic Geometry: AMS Special Session on computational Arithmetic Geometry. April 29-30, 2006, San Francisco State University, 2006. Ed. K. E. Lauter and K. Ribert. Springer 2008.

[25] Rao R.: *The Vaserstein symbol in dimension two.* 2011.

[26] Roitman M.: *Completing Unimodular Rows to Invertible Matrices.* Journal of algebra 49, p. 206-211, 1977.

[27] Shores S. and Wiegand R.: *Some criteria for Hermite rings and elementary divisor rings.* Canadian Journal of Mathematics 6, p. 1380-1383, 1974.