Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

ESTUDIO ALGEBRAICO Y GEOMÉTRICO DE LAS K-ÁLGEBRAS DE DIMENSIÓN FINITA

Autor: David Palacios Morales

Tutor: José Manuel Aroca Hernández-Ros

Introducción

En este trabajo, de naturaleza elemental como corresponde a un trabajo de grado, hemos intentado responder a las preguntas siguientes:

Si K es un cuerpo de característica distinta de dos. ¿Es cierto que tanto las K-álgebras de dimensión dos, como las cuádricas en la recta proyectiva y las cuádricas reales (es decir con algún punto no singular) irreducibles en el espacio proyectivo de dimensión tres sobre K, son las clases de elementos de K módulo producto por cuadrados de K\{0}? ¿Existe alguna razón geométrica que justifique este hecho?

Para responder a las preguntas hemos estudiado la estructura general de las K-álgebras finitas y la de la recta proyectiva sobre una K-algebra finita, que es el elemento unificador que responde a la segunda pregunta.

También se exploran brevemente las K-álgebras de dimensión tres para comprender mejor las limitaciones que tenemos para poder generalizar nuestros resultados a dimensiones superiores.

En nuestro trabajo hemos usado técnicas y resultados de algebra conmutativa y de geometría proyectiva y lo hemos hecho autocontenido, salvo algunos resultados como el teorema del elemento primitivo, el lema de Nakayama, y los teoremas de descomposición y simplificación de Witt.

La utilización de ambos enfoques, algebraico y geométrico, nos muestra una vez más la estrecha relación entre ambas ramas y el potencial de su combinación.

Hemos procedido siempre pasando de lo particular (ejemplos) a los resultados generales y si bien en algunos casos se podría haber ahorrado alguna demostración no lo hemos hecho por insistencia del director del trabajo que nos ha forzado, como ejercicio, a hacer dichas demostraciones.

1. K-álgebras de dimensión finita

En todo el trabajo K será un cuerpo de característica distinta de dos y usaremos K-álgebras conmutativas con unidad (elemento neutro para el producto). Cuando manejemos una estructura cociente y no haya posibilidad de confusión usaremos $\bar{x}$ para indicar la clase de un elemento x.

Definición 1.1.– *V es un álgebra sobre el cuerpo K si cumple:*
1) V es anillo conmutativo con unidad.
2) V es K-espacio vectorial.
3) $\forall \alpha \in K$ y $\forall$ $a,b \in V$ $\alpha(ab) = (\alpha a)b = a(\alpha b)$.

Definición 1.2.– *Si K es un cuerpo llamamos K-álgebra de dimensión finita a toda álgebra que tenga dimensión finita como K-espacio vectorial. A dicha dimensión la llamaremos dimensión del álgebra y la representaremos $dim_K A$.*

Ejemplo.- Sea K un cuerpo, x una indeterminada y $f(x) \in K[x]$ un polinomio de grado g entonces $A = K[x]/(f(x))$ es una $K-$álgebra de dimensión g.

En efecto, A es obviamente una K-álgebra y llamando $\overline{P(x)} = P(x) + (f(x))$ $\forall P(x) \in K[x]$,es inmediato, como consecuencia de la división entera de polinomios que:

$$\left\{1, \bar{x}, ..., \bar{x}^{g-1}\right\}$$

es una base de A como K-espacio vectorial.

En particular, si α es algebraico sobre K, entonces $K(\alpha)$ es una K-álgebra finita. Podemos probar recíprocamente que:

Proposición 1.3.– *Si V es una K-álgebra finita, todos los elementos de V son algebraicos sobre K.*

Demostración:

Si $dim_K V = r$ y $\alpha \in V$ tenemos que $1, \alpha, ..., \alpha^r$ son necesariamente dependientes, luego $\exists f(x) \in K[x]$ con $f(x) = a_0 + a_1 x + ... + a_r x^r \neq 0$ tal que $P(\alpha) = 0$. ■

Ejemplo.- No es cierto que todas las K-álgebras finitas sean del tipo $K[x]/(f(x))$. $A = K[x]/(x,y)^2$ es un ejemplo de ello. Como $(x,y)^2$ es un ideal, A es un álgebra. En este caso $\bar{x}^2 = \bar{y}^2 = \overline{xy} = 0$. Así que $\{1, \bar{x}, \bar{y}\}$ es base de A, por lo que A tiene dimensión 3.

Si A fuera isomorfo a $K[x]/f(x)$ entonces f(x) tendría grado 3 y el isomorfismo Φ debería enviar la base $\{1, \bar{x}, \bar{x}^2\}$ en una base de A. Así que $\Phi(1) = 1$, $\Phi(\bar{x}) = a + b\bar{x} + c\bar{y}$, y $\Phi(\bar{x})^2 = a^2 + 2ab\bar{x} + 2ac\bar{y} = 2a(a + b\bar{x} + c\bar{y}) - a^2 = 2a\Phi(\bar{x}) - a^2\Phi(1)$, deberían formar una base de A, pero eso no es posible al ser linealmente dependientes.

Podemos construir nuevas álgebras finitas como producto finito de álgebras ya conocidas, y al mismo tiempo podemos probar a descomponer álgebras finitas en producto de álgebras elementales para así dar un teorema de estructura de álgebras finitas.

Proposición 1.4.– *Si $A_1, ..., A_r$ son K-álgebras entonces $A = A_1 \times ... \times A_r$ es una K-álgebra y las proyecciones $\pi_i : A \to A_i$ son homomorfismos de K-álgebras que llevan la unidad de A 1_A en las unidades (1_i) de las A_i. Además $\exists e_i \in A$ con $1 \leqslant i \leqslant r$ que cumplen que:*

i) e_i *es elemento idempotente de* A $\forall i$.
ii) $e_i e_j = 0$ $\forall i \neq j$
iii) $\pi_i(e_i) = 1_i$
iv) $\sum_{i=1}^{r} e_i = 1$

Demostración:

Las operaciones de A son las usuales de las estructuras producto:
$(a_1, ..., a_r) + (b_1, ..., b_r) = (a_1 + b_1, ..., a_r + b_r)$
$(a_1, ..., a_r)(b_1, ..., b_r) = (a_1 b_1, ..., a_r b_r)$
$h(a_1, ..., a_r) = (ha_1, ..., ha_r)$ $\forall h \in K$
Con ellas A es una K- álgebra. Si las A_i son finitas, A lo es también y su dimensión es la suma de las dimensiones de los factores.

Las proyecciones son claramente homomorfismos de K-álgebras y llevan el uno de la multiplicación de A, que es $1_A = (1_1, ..., 1_r)$, en los unos de los factores. Si llamamos e_i al elemento que tiene 1_i en su i-ésima coordenada y las demás nulas, entonces los e_i cumplen las propiedades enunciadas.

■

Veamos como son los ideales primos y maximales de un producto de anillos.

Proposición 1.5.– *Sea I un ideal propio de $A = A_1 \times ... \times A_r$ y $F = \{e_1, ..., e_n\}$ la familia de elementos idempotentes ortogonales descrita anteriormente, entonces $F \nsubseteq I$. Si P es primo entonces $\exists!$ i tal que $e_i \notin P$ y $F \setminus \{e_i\} \subseteq P$.*

Demostración:

$F \subseteq I \Rightarrow 1 = \sum_{i=1}^{r} e_i \in I \Rightarrow I = A$, luego se verifica la primera afirmación.

Sea P un ideal primo propio de A, como P es un ideal, hay un i con $e_i \notin P$ y como $e_i e_j = 0 \in P \ \forall j \neq i \Rightarrow e_j \in P \ \forall j \neq i$ al ser P primo. ■

Consecuencia 1.6.–

1. *Si P es un ideal primo de A y $e_i \notin P$, entonces:*
$$x \in \pi_i(P) \Rightarrow \pi_i^{-1}(x) \subset P$$
2. *Los ideales primos de $A = A_1 \times ... \times A_r$ son los de la forma $\pi_i^{-1}(J)$ siendo $\pi_i : A \to A_i$ la proyección i-ésima y J un ideal primo de A_i.*

Demostración:

Por la proposición anterior:

$$e_i \notin P \Rightarrow e_j \in P, \ \forall j \neq i$$

entonces $x \in \pi_i(P) \Rightarrow \exists z \in P, \ \pi_i(z) = x$ luego:

$$\forall y \in \pi_i^{-1}(x), \ y = z + \sum_{j \neq i} \pi_j(y - z) e_j \in P$$

Si J es ideal primo de A_i entonces $\pi_i^{-1}(J)$ es ideal primo de A porque

$$ab \in \pi_i^{-1}(J) \Leftrightarrow \pi_i(ab) \in J \Leftrightarrow \pi_i(a)\pi_i(b) \in J$$

y como J es primo $\pi_i(a) \in J$ o $\pi_i(b) \in J \Leftrightarrow a \in \pi_i^{-1}(J)$ o $b \in \pi_i^{-1}(J)$. Recíprocamente si P es un ideal primo de $A = A_1 x ... x A_r$ entonces $\pi_i(P)$ es un ideal de A_i, porque π_i es un homomorfismo sobre.

Además $\exists! i$ tal que $e_i \notin P$ y $e_j \in P \ \forall j \neq i$ y por la primera afirmación $P = \pi_i^{-1}(\pi_i(P))$ y $\pi_i(P)$ es primo porque si:

$$\forall x, y \in A_i, x.y \in \pi_i(P) \Rightarrow xye_i \in P \Rightarrow$$

$$\Rightarrow xe_i \in P, o, ye_i \in P \Rightarrow x \in \pi_i(P), o, y \in \pi_i(P)$$

■

Teniendo en cuenta que las proyecciones son homomorfismos sobre y por el mismo razonamiento se prueba que:

Consecuencia 1.7.– *Los ideales maximales de* $A = A_1 \times ... \times A_r$ *son los* $\pi_i^{-1}(M)$ *siendo M ideal maximal de* A_i.

El resultado recíproco del de la proposición 1,4 también es cierto:

Proposición 1.8.– *Si A es una K-álgebra tal que* $\exists \{e_1, ..., e_n\} \subseteq A$ *con*
i) $e_i^2 = e_i \ \forall i$.
ii) $e_i e_j = 0 \ \forall i \neq j$.
iii) $\sum_{i=1}^{r} e_i = 1$.
iv) $e_i \neq 0, \ \forall i$.

Entonces $A \simeq A_1 \times ... \times A_r$ *donde los* A_i *son K-álgebras no nulas.*

Demostración:

$A_i = Ae_i \subseteq A$ es una subálgebra no unitaria de A (es decir cuyo uno no coincide con el de A), cuya unidad es e_i, ya que A_i es un ideal y por tanto es cerrado para la diferencia y el producto por elementos de A (y por tanto de K), además $\forall ae_i \in Ae_i$ tenemos que $ae_i e_i = ae_i^2 = ae_i$.

Definimos la aplicación:

$$\varphi : A \to A_1 \times ... \times A_n, \ a \mapsto (ae_1, ..., ae_n)$$

Que claramente es homomorfismo de álgebras y veamos que es isomorfismo.

i) φ es inyectiva porque $\varphi(a) = \varphi(b) \Rightarrow ae_i = be_i \ \forall i \Rightarrow a = a\sum_{i=1}^n e_i = \sum_{i=1}^n ae_i = \sum_{i=1}^n be_i = b\sum_{i=1}^n e_i = b$.

ii) φ es sobre porque si $(ae_1, ..., ae_n) \in A_1 x ... x A_n$ entonces llamamos $a = \sum_{i=1}^n a_i e_i$ y tenemos que:

$$\varphi(a) = (\sum_{i=1}^n a_i e_i e_1, ..., \sum_{i=1}^n a_i e_i e_n) = (a_1 e_1, ..., a_n e_n)$$

por la ortogonalidad y la idempotencia de los e_i.

■

Vamos a probar ahora un teorema de descomposición de las K-álgebras finitas en suma directa de álgebras mas simples. Previamente daremos un ejemplo guía de la construcción que vamos a efectuar.

Proposición 1.9.– *Si $f(x), g(x) \in K[x]$ son polinomios primos entre si:*

$$K[x]/(f(x)g(x)) \simeq K[x]/(f(x)) \times K[x]/(g(x))$$

Demostración:

La identidad de Bezout garantiza la existencia de $h(x), q(x) \in P[x]$ con $1 = h(x)f(x) + q(x)g(x)$, así que $\overline{h(x)f(x)} + \overline{q(x)g(x)} = \overline{1}$. Además:

$$\overline{h(x)f(x)} \cdot \overline{q(x)g(x)} = \overline{h(x)f(x)q(x)g(x)} = \overline{0}$$

y

$$\overline{h(x)f(x)} = \overline{h(x)f(x)}(\overline{h(x)f(x)} + \overline{q(x)g(x)}) =$$
$$= \overline{h(x)^2 f(x)^2} + \overline{q(x)g(x)h(x)f(x)} = \overline{h(x)^2 f(x)^2}$$

del mismo modo comprobamos la idempotencia de $\overline{q(x)g(x)}$. Si $\overline{h(x)f(x)}$ fuera nulo entonces:

$$\overline{1} = \overline{q(x)g(x)} \Rightarrow \exists m(x) \in P[x],\ 1 = q(x)g(x) + m(x)f(x)g(x)$$

Entonces

$$\overline{1} = \overline{q(x)g(x) + m(x)f(x)g(x)} = \overline{0}$$

en $K[x]/(g(x))$ y eso no es posible. El mismo razonamiento nos sirve para $\overline{q(x)g(x)}$. Así que $\left\{\overline{h(x)f(x)}, \overline{q(x)g(x)}\right\}$ es un conjunto de idempotentes ortogonales no nulos con suma $\overline{1}$ y en consecuencia

$$K[x]/(f(x)g(x)) \simeq \overline{h(x)f(x)}K[x]/(f(x)g(x)) \times \overline{q(x)g(x)}K[x]/(f(x)g(x))$$

por la proposición 1.8

Además la aplicación:

$\varphi : K[x] \longrightarrow K[x]/(f(x)g(x)), \varphi(P(x)) = P(x)h(x)f(x)+(f(x)g(x))$

es un homomorfismo de K-álgebras cuya imagen es $\overline{h(x)f(x)}K[x]/(f(x)g(x))$ y cuyo núcleo es el ideal generado por $g(x)$, luego

$$\overline{h(x)f(x)}K[x]/(f(x)g(x)) \simeq K[x]/(g(x))$$

y lo mismo sucede con el otro factor. ■

Consecuencia 1.10.– *Si la descomposición en factores primos de un polinomio $f(x) \in K[x]$ es:*

$$f(x) = p_1(x)^{n_1}....p_r(x)^{n_r}$$

Entonces:

$$K[x]/(f(x)) \simeq K[x]/(p_1(x)^{n_1}) \times .... \times K[x]/(p_r(x)^{n_r})$$

Demostración:

Es consecuencia de aplicar iteradamente la proposición anterior, pero también podemos construir explícitamente el isomorfismo de la forma siguiente.

Definimos el homomorfismo de álgebras:

$$\varphi : A \to K[x]/(p_1(x)^{n_1}) \times .... \times K[x]/(p_r(x)^{n_r})$$

$$\varphi(Q(x) + (f(x))) = (Q(x) + \overline{P_1(x)^{n_1}}, ..., Q(x) + \overline{P_r(x)^{n_r}})$$

Es inyectivo porque si:

$$\varphi(Q(x) + \overline{f(x)}) = (0 + \overline{P_1(x)^{n_1}}, ..., 0 + \overline{P_r(x)^{n_r}})$$

entonces $Q(x)$ es múltiplo de $\overline{P_i(x)^{n_i}}$, $\forall i = 1, ..., r$ que son primos entre sí, por tanto, Q(x) es múltiplo de f(x) y en consecuencia $\overline{Q(x)} = 0$. Y como:

$$dim_K(K[x]/\overline{P_i(x)^{n_i}}) = grado(P_i(x)^{n_i})$$

y

$$dim_K(K[x]/f(x)) = grado(f(x)) = \sum_{i=1}^{r} grado(P_i(x)^{n_i})$$

tenemos que la dimensión de A coincide con la de

$$K[x]/P_1(x)^{n_1} \times ... \times K[x]/P_r(x)^{n_r}$$

luego $\varphi(x)$ también es sobre. Así que estamos ante un isomorfismo de álgebras.

■

Definición 1.11.– *Un anillo se llama local si tiene un único ideal maximal.*

Proposición 1.12.– *A es anillo local* $\Leftrightarrow$ *los elementos no invertibles de A forman un ideal. (Además será el ideal maximal de A.)*

Demostración:

$\Rightarrow$) Sea M el maximal de A, como M es ideal propio no tiene elementos invertibles, falta ver que todos los no invertibles están en M, o lo que es lo mismo que todos los que no estan en M son inversibles. Sea $a \notin M \Rightarrow aA \nsubseteq M \Rightarrow aA = A$ (Ya que todo ideal propio está contenido en un maximal) $\Rightarrow a$ invertible.
$\Leftarrow$) Sea H = $\{a \in A$ no invertibles$\}$ un ideal $\Rightarrow \forall J$ ideal propio de A tenemos que $J \subseteq H$ (Ya que en J sólo hay no invertibles). Así que H es ideal maximal y es el único maximal. ■

Proposición 1.13.–
1.-. Sea $A = K[x]/(P(x))$ *con* $P(x) \in K[x]$ *irreducible, entonces A es un cuerpo.*
2.- Sea $A = K[x]/(P(x)^n)$ *con* $P(x) \in K[x]$ *irreducible, entonces A es local y su ideal maximal esta generado por* $\overline{P(x)}$.
3.- Si $A = K[x]/(f(x))$, *A es suma directa de una familia finita de K-álgebras locales.*

Demostración:

Si $Q(x) \in K[x]$ no es múltiplo de P(x), entonces es primo con él y la identidad de Bezout nos garantiza la existencia de polinomios H(x) y J(x) tales que H(x)P(x) + J(x)Q(x) = 1, lo que significa que

$$\overline{H(x)P(x)} + \overline{J(x)Q(x)} = \overline{J(x)Q(x)} = 1$$

Es decir, $\forall \overline{Q(x)} \in A$ no nulo $\exists \overline{J(x)}$ elemento inverso. Como corolario obtenemos que (P(x)) es ideal maximal de K[x].

Por lo anterior sabemos que las clases de los polinomios primos con $(P(x)^n)$ son inversibles y por lo tanto los ideales que contengan a alguna de estas clases son el total. Así que los ideales propios de A son los engendrados por divisores de $(P(x)^n)$, o equivalentemente divisores multiplicados por elementos inversibles del anillo. Así que los ideales propios son los $(P(x)^r)$ con $1 \leq r \leq n$ y están todos contenidos en (P(x)), así que (P(x)) es el único ideal maximal. Recíprocamente si $A = K[x]/(P(x))$ con al menos 2 divisores irreducibles R(x) y T(x) de P(x) tenemos que (R(x)) y (T(x)) son ideales maximales de K[x] y por tanto de A, así que A no sería un anillo local.

La tercera afirmación se sigue de la consecuencia 1.10 ■

Proposición 1.14.– *Toda K-álgebra finita A es noetheriana y artiniana.*

Demostración:

Como los ideales son K-espacios vectoriales y $L_1 \subset L_2 \Rightarrow dim(L_1) < dim(L_2)$ tenemos que las cadenas de ideales, sean estrictamente ascendentes o descendentes tienen una longitud máxima de $dim_K A$, luego son finitas. ■

Proposición 1.15.– *Si A es anillo artiniano entonces A es local si y sólo si 0 y 1 son los únicos idempotentes de A.*

Demostración:

$\Rightarrow$) Sea M el maximal de A y sea $a = a^2$ entonces $a - a^2 = 0 \Rightarrow a(1-a) = 0 \in M \Rightarrow a \in M$ y $1-a \notin M$ o bien $a \notin M$ y $1-a \in M$ ya que $1 \notin M$. En el primer caso 1 - a es invertible y como a(1 - a) = 0 tenemos a = 0. En el segundo caso, por el mismo razonamiento, 1 - a = 0 $\Rightarrow$ a = 1.

$\Leftarrow$) Sea M un ideal maximal y $a \notin M$. Entonces $aA \supseteq a^2A \supseteq ... \supseteq a^rA \supseteq ...$ es una cadena descendente de ideales, al ser A artiniano $\exists$ r tal que $a^{r+1}A = a^rA \Rightarrow \exists \lambda \in A$ tal que $a^{r+1}\lambda = a^r \Rightarrow a^r(a\lambda - 1) = 0 \in M \Rightarrow a\lambda - 1 \in M$. Multiplicamos por $\sum_{i=0}^{r-1}(a\lambda)^i$ y por λ^r y nos queda $(a\lambda)^r((a\lambda)^r - 1) = 0 \Rightarrow (a\lambda)^r$ es idempotente. Si $(a\lambda)^r = 0 \in M \Rightarrow (a\lambda) \in M \Rightarrow 1 \in M$ que es absurdo. Así que $(a\lambda)^r = 1 \Rightarrow$ a es

invertible. Con lo cual M es el conjunto de elementos no invertibles de A por lo que es el único maximal y por tanto A es local. ■

Nota: Sólo ha sido necesario que A sea artiniano para probar la segunda implicación.

Teorema 1.16.– *Toda K-álgebra finita es suma directa de K-álgebras finitas locales.*

Demostración:

Sea A K-álgebra con $dim_k A = n \in \mathbb{N}$. Si A no es local entonces $\exists e \in A$ idempotente distinto de 0 y 1. Como $(1-e)^2 = 1-2e+e^2 = 1-e$ tenemos $\{e, 1-e\}$ una familia de idempotentes ortogonales de suma 1. Por la proposición 1.8 $A \simeq A_1$ x A_2 con A_1 y A_2 no nulos. Así que $dim_k A_1 = m < n$ y $dim_k A_2 = n-m < n$. Iteramos el proceso con cada álgebra hasta que sean locales o bajen a dimensión 1 (en ese caso el álgebra sería cuerpo y por tanto también local). ■

Vamos a ver que la descomposición anterior es única:

Proposición 1.17.– *Sea A una K-álgebra expresada como suma directa de r K-álgebras locales $(A_1, ..., A_r)$ con ideales maximales respectivos $M_1, ..., M_r$, los ideales maximales de A son los $\pi_i^{-1}(M_i)$. Recíprocamente si A es una K-algebra finita y tiene r ideales maximales $P_1 ..., P_r$, se va a descomponer en suma de r K-álgebras locales.*

Demostración:

La primera afirmación es una consecuencia inmediata de la consecuencia 1.7 y la segunda se sigue del teorema anterior, ya que A se descompone en producto de K-álgebras locales $A \simeq B_1 \times ... \times B_s$. Entonces por la primera parte de la proposición, $r = s$ y, ordenando adecuadamente los factores, si Q_i es el ideal maximal de B_i, es $P_i = \pi_i^{-1}(Q_i), \forall i$. ■

Proposición 1.18.– *Sea A una K-álgebra expresada como suma directa de r K-álgebras locales $(A_1, ..., A_r)$ con ideales maximales respectivos $M_1, ..., M_r$, y sean $N_i = \pi_i^{-1}(M_i)$ los ideales maximales de A entonces cada A_i es isomorfa al localizado de A respecto al ideal maximal N_i. En consecuencia la descomposición de 1.16 es única.*

Demostración:

Si $x \in A,\ x \notin N_i$ entonces $\pi_i(x) \notin M_i$ luego es inversible en A_i.Por tanto podemos definir la correspondencia:

$$\varphi : A_{N_i} \longrightarrow A_i,\ \varphi\left(\frac{x}{y}\right) = \pi_i(x).\pi_i(y)^{-1}$$

φ es aplicación, porque:

$$\frac{x}{y} = \frac{z}{t} \Leftrightarrow \exists u \notin N_i, u(xt - zy) = 0 \Rightarrow \pi_i(u)(\pi_i(x)\pi_i(t) - \pi_i(z)\pi_i(y)) = 0$$

y como $\pi_i(u) \in A_i$ es inversible:

$$\pi_i(x)\pi_i(t) - \pi_i(z)\pi_i(y) = 0 \Rightarrow \pi_i(x)\pi_i(y)^{-1} = \pi_i(z)\pi_i(t)^{-1}$$

φ es homomorfismo sobre por serlo π_i y es inyectivo porque:

$$\pi_i(x)\pi_i(y)^{-1} = \pi_i(z)\pi_i(t)^{-1} \Rightarrow \pi_i(x)\pi_i(t) - \pi_i(z)\pi_i(y) = 0 \Rightarrow e_i(xt - yz) = 0$$

y como $e_i \notin N_i$ es $x/y = z/t$. ■

2. K-álgebras locales de dimensión finita

En este capítulo vamos a dar un teorema de estructura de las álgebras locales finitas. Con ese teorema, teniendo en cuenta el resultado de la sección anterior, podemos conocer todas las K-álgebras finitas. Probaremos en primer lugar que el ideal maximal de una K-àlgebra local finita es nilpotente. Para ello usaremos el resultado siguiente cuya demostración está por ejemplo en el texto de Atiyah - Mc Donald.

Lema de Nakayama 2.1.– *Sea J un A-módulo con generación finita, y H un ideal de A contenido en el radical de Jacobson de A, entonces*

$$HJ = J \Rightarrow J = 0$$

Si A es un anillo local, su radical de Jacobson es su ideal maximal, por tanto si I es un ideal finito generado de A y M es su ideal maximal:

$$M \cdot I = I \Rightarrow I = 0$$

Proposición 2.2.– *Si A es una K-álgebra local finita de ideal maximal M y de dimensión d como K-espacio vectorial existe un $r \leq d$ tal que $M^r = 0$.*

Demostración:

Como $1 \notin M$, la dimension de M como K- espacio vectorial es menor o igual que $d-1$, entonces la cadena de subespacios vectoriales de M:

$$M \supseteq M^2 \supseteq ... \supseteq M^n \supseteq ...$$

no puede tener mas de d contenidos estrictos, luego teniendo en cuenta que al ser los M^j K-espacios de dimensión finita, son también ideales finito generados de A: $\exists r \leq d,\ M^{r+1} = M.M^r = M^r \Rightarrow M^r = 0$ ∎

Definición 2.3.– *Llamamos polinomio mínimo de $z \in V$ al polinomio mónico de menor grado P(x) tal que P(z)=0.*

Proposición 2.4.– *Si A es una K - algebra local finita de ideal maximal M, el polinomio mínimo de todo elemento $\alpha \in M$ es de la forma $P(x) = x^n$, con $n \leq dim_K(A)$.*

Demostración:

Por el teorema de división entera de polinomios el polinomio mínimo de un elemento α divide a todos los polinomios de $K[x]$ que se anulan en α. Como $\alpha \in M$ y $M^r = 0$, es $\alpha^r = 0$ y $r \leq d$, luego se sigue el resultado. ∎

Ejemplo.- No es cierto que:

$$\alpha^r = 0,\ \forall \alpha \in M \Rightarrow M^r = 0$$

En efecto: Si $K = \mathbb{Z}/(2)$ y $A = K[x, y]/(x^2, y^2)$, A es una K-álgebra de dimensión 4, con base $\{1, x, y, xy\}$, una base del ideal maximal M es $\{x, y, xy\}$ y:

$$\alpha \in M \Rightarrow \alpha = ax + by + cxy \Rightarrow \alpha^2 = 0$$

sin embargo $xy \in M^2$ y en consecuencia $M^2 \neq 0$.

Ejemplo.- No es cierto que si A es una K-álgebra local de ideal maximal M, sea $A/M \simeq K$, por ejemplo $A = \mathbb{C}[x]/(x^2)$ es una $\mathbb{R}$-algebra local de dimensión 4, con base $\{1, i, \overline{x}, i\overline{x}\}$, pero su ideal maximal M está generado por $\{\overline{x}, i\overline{x}\}$ y $A/M \simeq \mathbb{C}$

Proposición 2.5.– *Si A es una K - algebra local finita de ideal maximal M, el cuerpo A/M es una extensión finita de K. Es obvio porque A/M es una K-álgebra, es un cuerpo (con las mismas operaciones) y su dimensión como K- espacio es finita.*

Observemos que al ser M un subespacio de A como K-espacio vectorial:

$$dim_K(A/M) = dim_K(A) - dim_K(M) \Rightarrow A \simeq M \bigoplus A/M$$

pero en principio es un isomorfismo (no canónico, depende de la elección de una base en M) de K espacios vectoriales y no de álgebras.

Ejemplo.- $A = \mathbb{C}[x]/(x^2)$ es isomorfo a $xA \times \mathbb{C}$ como $\mathbb{C}$-espacios

vectoriales con el isomorfismo:

$$\varphi : A \longrightarrow xA \times \mathbb{C},\ \varphi(wx + z) = (wx, z)$$

que no es isomorfismos de álgebras, ya que por ejemplo $1 \cdot x = x$ mientras $\varphi(1) \cdot \varphi(x) = (0,1)(1,0) = (0,0) \neq \varphi(x)$.

Ejemplo.- El localizado de $\mathbb{R}[x]$ respecto del ideal primo generado por $x^2 + 1$, $A = \mathbb{R}[x]_{(x^2+1)}$, es una $\mathbb{R}$-álgebra local pero no es de dimensión finita como $\mathbb{R}$-espacio vectorial ya que contiene a $\mathbb{R}[x]$. Su ideal maximal es $(x^2 + 1)A$ y su cuerpo residual:

$$A/(x^2 + 1)A \simeq \mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$$

Sin embargo A no contiene ningún subcuerpo isomorfo a $\mathbb{C}$, ya que no contiene ningún elemento de cuadrado menos uno. En efecto:

$$\frac{p(x)}{q(x)} \in A,\ \frac{p(x)}{q(x)}^2 = -1 \Rightarrow p(x)^2 + q(x)^2 = 0 \text{ en } \mathbb{R}[x]$$

y comparando los términos de mayor grado se comprueba que esta igualdad es imposible

Vamos a probar ahora el resultado insinuado por los ejemplos, esto es, que toda K algebra local, A, de dimensión finita, contiene un subcuerpo isomorfo a su cuerpo residual. Para ello usaremos el conocido:

Teorema del elemento primitivo 2.6.– *Sea E extensión separable finita del cuerpo K, entonces $E = K(z)$ para algún $z \in E$.*

También introduciremos un concepto nuevo:

Definición 2.7.– *Sea B anillo local de ideal maximal M_B y $K = B/M_B$, B se llama henseliano si para todo polinomio mónico*

$$G(x) = a_0 + a_1 x + ... + x^s \in B[x]$$

y para todo $H \in B/M_B$ que es raíz simple de

$$\hat{G}(x) = a_0 + M_B + (a_1 + M_B)x + ... + (1 + M_B)x^s \in B/M_B[x]$$

$\exists h \in B$ con $G(h) = 0$ y $H = h + M_B$.

Proposición 2.8.– *Si A es una K-álgebra local finita entonces A es henseliana.*

Demostración:

Construiremos h a partir de H por un proceso de recurrencia. Sea

$$G(x) = a_0 + a_1 x + ... + x^s \in A[x]$$

y sea

$$\hat{G}(x) = a_0 + M_A + (a_1 + M_A)x + ... + (1 + M_A)x^s \in A/M_A[x]$$

Sea $H \in A/M_A$ una raíz simple de $\hat{G}$, tomando un representante arbitrario de H, podemos escribir $H = h_0 + M_A$ y:

$$\hat{G}(H) = 0 \Rightarrow G(h_0) \in M_A$$

Como H es raíz simple, no es raíz del polinomio derivado. Es decir, usando la notación habitual para la derivada:

$$\hat{G}'(H) \neq 0 \Rightarrow G(h_0) \notin M_A$$

Así que $G'(h_0)$ es inversible en el anillo local A, y podemos construir

$$h_1 = h_0 - \frac{G(h_0)}{G'(h_0)}$$

Claramente

$$h_1 - h_0 \in M_A \Rightarrow H = h_1 + M_A$$

Poniendo el polinomio $G(x)$ en forma de Taylor, podemos escribir:

$$G(x) = G(h_0) + G'(h_0)(x - h_0) + ... + \frac{G^{(s)}(h_0)}{s!}(x - h_0)^s$$

, así que

$$G(h_1) = G(h_0) + G'(h_0)(h_1 - h_0) + ... + \frac{G^{(s)}(h_0)}{s!}(h_1 - h_0)^s$$

Como $G(h_0) + G'(h_0)(h_1 - h_0) = 0$ y :

$$h_1 - h_0 = -\frac{G(h_0)}{G'(h_0)} \in M_A \Rightarrow (h_1 - h_0)^r \in M_a^r \subset M_A^2 \ \forall r \geq 2$$

$G(h_1) \in M_A^2$

Ahora $G'(h_1) \notin M_A$ ya que sustituyendo en la derivada $h_1 - h_0 = -\frac{G(h_0)}{G'(h_0)}$:

$$G'(h_1) = G'(h_0) + G''(h_0)(h_1 - h_0) + ... + \frac{G^{(s)}(h_0)}{s - 1!}(h_1 - h_0)^{s-1}$$

con $G'(h_0) \notin M_A$ y los demás sumandos sí.

Así que podemos definir $h_2 = h_1 - \frac{G(h_1)}{G'(h_1)}$ y aplicar nuevamente el proceso hasta construir h_r con $H = h_r + M_A$ y $G(h_r) \in M_A^{2^r} = 0$, por ser nilpotente el ideal maximal de A. ■

Ejemplo.- $A = \mathbb{R}[x]/(x^2+1)^2$ es un álgebra finita local de ideal maximal generado por $(\overline{x}^2 + 1)$, con $\overline{x} = x + (x^2+1)^2$. Su cuerpo residual es $L = A/(\overline{x}^2+1)A \simeq \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$. Veamos que A contiene un subcuerpo isomorfo a $\mathbb{C}$.

Para ello hay que probar que existe un $z \in A$ con $z^2 = -1$, A tiene como base $\{1, \overline{x}, \overline{x}^2, \overline{x}^3\}$, y buscar z por coeficientes indeterminados es largo y tedioso. Pero en esta caso podemos emplear el algoritmo de la proposición porque la ecuación $y^2 + 1 = 0$ tiene en $\mathbb{C} \simeq A/M_A$ la raíz simple $Z = \overline{x} + (x^2+1)^2$, entonces:

$$z_0 = \overline{x},\ z_0^2 + 1 \in M_A$$

$$z_1 = z_0 - \frac{z_0^2+1}{2z_0} = \overline{x} - \frac{\overline{x}^2+1}{2\overline{x}},\ z_1^2 + 1 \in M_A^2 = 0$$

Pero:

$$(\overline{x}^2+1)^2 = 0 \Rightarrow \overline{x}(-\overline{x}^3 - 2\overline{x}) = 1$$

Luego:

$$z_1 = \overline{x} - \frac{(\overline{x}^2+1)(-\overline{x}^3-2\overline{x})}{2} = \frac{\overline{x}^3+3\overline{x}}{2}$$

Entonces la aplicación

$$\mathbb{C} \longrightarrow A,\ a + ib \mapsto a + bz_1$$

es el isomorfismo buscado

Teorema 2.9.– *Si A es una K-álgebra local finita, tal que A/M_A es una extensión separable de K, existe una extensión finita L de K tal que A es una L-álgebra, $L \subset A$ y $A = L + M_A$ donde M_A es el ideal maximal de A y la suma es directa como suma de L -espacios vectoriales.*

Demostración:

Como ya hemos visto $L = A/M_A$ es un cuerpo extensión finita de K, si w es un elemento primitivo de la extensión y $G(x) \in K[x]$ es su polinomio mínimo, $A/M_A \simeq K[x]/(G(x))$, y además la ecuación $\hat{G}(x) = G(x) = 0$ tiene solución simple en A/M_A, y como A es

henseliano, tiene solución en A, sea esta solución Z. Entonces la aplicación:

$$K[x] \longrightarrow A,\ F(x) \mapsto F(Z)$$

es un homomorfismo de anillos con núcleo generado por $G(x)$, luego induce un homomorfismo inyectivo $A/M_A \longrightarrow A$ su imagen L es un subcuerpo de A, extensión finita de K.

Obviamente $L \cap M_A = \{0\}$ y $dim_K(L) + dim_K(M_A) = dim_K(A)$, y como $L \subset A$, M_A es L-espacio vectorial. Por tanto se verifica el teorema. ■

3. K-álgebras de dimensiones 2 y 3

En este capítulo escribiremos todas las K algebras de dimensiones 2 y 3 y clasificaremos las de dimensión dos. Previamente observemos que de los resultados del capítulo anterior se sigue que:

- Si A es una K-álgebra finita, por el teorema 1,16 $A = A_1 \oplus ... \oplus A_r$ con las A_i K- álgebras finitas locales.
- Por el teorema 2,9 $A_i = L_i \oplus m_i$ con L_i extensión algebraica de K y $L_i \subseteq A_i$,
- Como m_i es un L_i espacio vectorial, si el grado de la extensión L_i/K es r_i y la dimensión de m_i es d_i, $dim_K(A_i) = r_i(d_i + 1)$
- Los ideales m_i son nilpotentes.
- La única K-álgebra de dimensión 1 es K

Con estos datos es fácil escribir las K-álgebras de baja dimensión

Clasificación de las álgebras bidimensionales

Comencemos con ejemplos muy conocidos de álgebras bidimensionales sobre $\mathbb{R}$.

Definición 3.1.– *Sea* $\mathbb{M} = \{a + bj : a, b \in \mathbb{R} \ \ j^2 = 1\} \simeq \mathbb{R}[x]/(x^2 - 1)$. *Esta* $\mathbb{R}$*-algebra recibe el nombre de algebra de los números paracomplejos.*

Como $x^2 - 1$ no es irreducible $\mathbb{M}$ no es un cuerpo, esto se pone también de manifiesto por la presencia de divisores de cero.
Sean $z, w \in A$, entonces

$$zw = 0 \Leftrightarrow (a + bj)(c + dj) = ac + bd + j(bc + ad) = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{Bmatrix} ac + bd = 0 \\ bc + ad = 0 \end{Bmatrix} \Leftrightarrow \begin{Bmatrix} ac = -bd \\ -bc = ad \end{Bmatrix} \Leftrightarrow \begin{Bmatrix} ac^2 = -bcd \\ -bcd = ad^2 \end{Bmatrix} \Leftrightarrow$$

$$\Leftrightarrow ac^2 = ad^2 \Leftrightarrow a(c^2 - d^2) = 0$$

Si $a = 0$ entonces $b = 0$ ó $c = 0$ y $d = 0$; si $a \neq 0$ entonces

$$a(c^2 - d^2) = 0 \Leftrightarrow c^2 = d^2 \Leftrightarrow c = \pm d$$

Así que o c y d son nulos o se da una de estas condiciones:

$$c = d \; y \; a = -b$$

$$c = -d \; y \; a = b$$

En cualquier caso hemos probado que los divisores de cero son de la forma $a(1+j)$ o $c(1-j)$ con $a, c \in \mathbb{R}$.
Es decir si representamos, tal como se hace con los complejos, los elementos de $\mathbb{M}$ como puntos del plano real, de modo que $a+bj$ se representa como el punto (a, b), los divisores de cero son los elementos cuyos afijos están situados sobre las rectas $y + x = 0, \; y - x = 0$.

Al igual que en los complejos, la aplicación de conjugación:

$$\sigma : \mathbb{M} \longrightarrow \mathbb{M}, \; \sigma(a + bj) = a - bj$$

es un automorfismo, y si llamamos norma de un elemento a :

$$||a + bj|| = (a + bj)(a - bj) = a^2 - b^2$$

Observamos que los divisores de cero son los elementos de norma cero, y el plano queda dividido en las regiones de norma positiva y negativa, limitadas por las dos rectas de divisores de cero.

Definición 3.2.– *Sea* $\mathbb{D} = \{a + bk : a, b \in \mathbb{R} \;\; k^2 = 0\} \simeq \mathbb{R}[x]/(x^2)$. *Esta* $\mathbb{R}$*-álgebra recibe el nombre de álgebra de los números duales.*

Observemos que en $\mathbb{D}$, k juega el papel de un infinitésimo, de cuadrado despreciable. En este caso $\mathbb{D}$ tampoco es un cuerpo.
Estudiaremos también sus divisores de cero:
Sean $z, w \in A$, entonces

$$zw = 0 \Leftrightarrow (a + bk)(c + dk) = ac + k(bc + da) = 0 \Leftrightarrow \left\{ \begin{array}{c} ac = 0 \\ bc = -da \end{array} \right\}$$

lo que equivale a que se cumpla al menos una de estas tres condiciones:

$$a = 0 \; y \; c = 0$$

$$a = 0 \; y \; b = 0$$

$$d = 0 \; y \; c = 0$$

Así que los divisores de cero en este anillo son de la forma ak con $a \in \mathbb{R}$.Si hacemos la misma representación del caso anterior sobre el plano real, los divisores de cero son los elementos de $\mathbb{D}$ cuyos afijos están sobre el eje de ordenadas. En este caso podemos definir también una norma que es positiva fuera del eje de los divisores de cero.

Ejemplo.- Las $\mathbb{R}$-álgebras de dimensión dos $\mathbb{M}, \mathbb{D}$ y $\mathbb{C}$ no son isomorfas, ya que $\mathbb{C}$ es un cuerpo y por tanto no tiene divisores de cero a diferencia de $\mathbb{M}$ y $\mathbb{D}$. Por otro lado $k^2 = 0$ mientras que en $\mathbb{M}$ solo el cero tiene cuadrado nulo. Observemos también, y no es casual, que las cuadricas proyectivas reales irreducibles en el espacio proyectivo de dimensión tres son la cuadrica de puntos, la cuadrica de rectas y el cono real, el plano tangente a la cuadrica de puntos, la corta en un único punto, el plano tangente a la cuadrica hiperbólica la corta en dos rectas y el plano tangente al cono en un punto regular lo corta en una recta

En general las K-álgebras bidimensionales o bien son suma de dos álgebras locales de dimensión uno, o son ellas mismas álgebras locales de dimensión dos .

En caso de que A no sea local se descompone como producto de álgebras locales, pero como $dim_K A = 2$ sólo puede ser $A = K \oplus K$.

Si A es local sea M_A su ideal maximal, entonces $A \simeq L \times M_A$ como L-espacio vectorial, con L extensión de K. Entonces hay dos opciones:

- L/K es una extension de grado dos. Entonces $A = L$ es un cuerpo extensión de grado dos de K, y en consecuencia $A \simeq K[x]/(f(x))$ con $f(x)$ polinomio irreducible en $K[x]$
- $L = K$ entonces $dim_K(M_A) = 1$. Sea $x \in M_A$ no nulo, como $M_A^2 = 0$ por la proposición 2.2 tenemos $x^2 = 0$ y $\{1, x\}$ es base de A, así que $A \simeq K[x]/(x^2)$

Tal como hemos probado en el capítulo 1, si $f(x) \in K[x]$ polinomio de segundo grado tiene dos raíces distintas: $K \oplus K \simeq K[x]/(f(x))$ por tanto las K-álgebras de dimensión dos son todas de la forma $K[x]/(f(x))$. Mas precisamente si para un polinomio de segundo grado $f(x) = x^2 + ax + b$, llamamos $d_f = a^2 - 4b$ a su discriminante.

- Todas las algebras $K[x]/(f(x))$ con $f(x) = (x-a)^2$, es decir $d_f = 0$ son isomorfas a $K[x]/(x^2)$
- Todas las algebras $K[x]/(f(x))$ con $f(x) = (x-r)(x-s),\ r \neq s$, es decir $d_f \in K^{*2}$ son isomorfas a $K[x]/(x^2 - 1)$

- Las extensiones algebraicas de grado dos de K, $K[x]/(f(x))$ con $d_f \notin K^2$

Nos queda ahora clasificar las álgebras del tercer tipo:

Ejemplo.- Tomamos el cuerpo $\mathbb{Q}$ y sus extensiones $\mathbb{Q}(\sqrt{2}) \simeq Q[x]/(x^2-2)$ y $\mathbb{Q}(i) \simeq Q[x]/(x^2+1)$. Estos cuerpos no son isomorfos ya que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ no posee ninguna raíz cuadrada de -1. Por tanto las extensiones del tercer tipo no son toda isomorfas

El criterio del discriminante es el que nos ayudará a clasificar las álgebras del tercer tipo.

Proposición 3.3.– *Sea K un cuerpo y $f(x) = x^2+hx+m$ y $g(x) = x^2+px+q$ irreducibles en $K[x]$ entonces los cuerpos $K[x]/(f(x))$ y $K[x]]/(g(x))$ son isomorfos si y sólo si se cumple $\sqrt{\frac{h^2-4m}{p^2-4q}} \in K$. O equivalentemente, si y sólo sí $\exists \lambda \in K^*$ con $h^2-4m = \lambda^2(p^2-4q)$.*

Demostración:

Las raíces de $f(x)$ son $\frac{-h\pm\sqrt{h^2-4m}}{2}$ y por ser irreducible en K sabemos que $\alpha = \sqrt{h^2-4m} \notin K$ y del mismo modo $\beta = \sqrt{p^2-4q} \notin K$.

Los isomorfismos de cuerpos son también isomorfismos de espacios vectoriales, veamos lo que le hace falta a un isomorfismo de espacios vectoriales para ser isomorfismo de cuerpos:
$\varphi : K(\alpha) \to K(\beta)$ cumple siempre que $\varphi(1) = 1$ y

$$\varphi(\alpha) = a + b\beta$$

con $b \neq 0$ ya que si no $\varphi(\alpha - a) = 0$ siendo $\alpha \neq a \in K$.
La condición necesaria y suficiente para que sea isomorfismo de cuerpos es que $\varphi(\alpha)^2 = \varphi(\alpha^2)$.

Obviamente es necesaria. Y es suficiente porque

$$\forall (c+d\alpha), (e+r\alpha) \in K(\alpha)$$

$$\varphi((c+d\alpha)(e+r\alpha)) = \varphi(ce + \alpha(cr+de) + dr\alpha^2) =$$

$$= ce + \varphi(\alpha)(cr+de) + dr\varphi(\alpha^2) = ce + \varphi(\alpha)(cr+de) + dr\varphi(\alpha)^2 =$$

$$= (c+d\varphi(\alpha))(e+r\varphi(\alpha)) = \varphi(c+d\alpha)\varphi(e+r\alpha)$$

cuando $\varphi(\alpha^2) = \varphi(\alpha)^2$.

Ahora bien

$$\varphi(\alpha^2) = \varphi(h^2 - 4m) = h^2 - 4m$$

y

$$\varphi(\alpha)^2 = (a + b\beta)^2 = a^2 + b^2\beta^2 + 2ab\beta = a^2 + b^2(p^2 - 4q) + 2ab\beta$$

así que $2ab\beta = 0 \Rightarrow a = 0$ y

$$a^2 + b^2(p^2 - 4q) = h^2 - 4m \Rightarrow \sqrt{\frac{h^2 - 4m}{p^2 - 4q}} = b \in K^* \Leftrightarrow \frac{h^2 - 4m}{p^2 - 4q} = b^2$$

con

$$b \in K^* \Leftrightarrow h^2 - 4m = b^2(p^2 - 4q)$$

con $b \in K^*$. ■

Definimos en K la relación de equivalencia $a \sim b \Leftrightarrow \exists \lambda \in K^*$ con $a = b\lambda^2$, hay tantas K-álgebras como clases de equivalencia en $K/\sim$. Puede verse que $K \mathrm{x} K$ es la clase del 1 y $K[x]/(x^2)$ es la clase del 0 ya que la raíz cuadrada del discriminante de $f(x)$ está en K^* si y sólo si $f(x)$ tiene dos soluciones distintas $a, b \in K$ y eso equivale a que

$$A = K[x]/(x - a) \oplus K[x]/(x - b) = K \oplus K$$

y el discriminante (y equivalentemente su raíz cuadrada) es nulo si y sólo si $f(x) = (x - a)^2$ con $a \in K$. En este caso tenemos un único ideal maximal $(x - a)$ y no es nulo, por lo que $A \simeq K[x]/(x^2)$.

Consecuencia 3.4.– *Todas las $\mathbb{R}$-álgebras de dimensión dos son isomorfas a $\mathbb{M}, \mathbb{D}$ o $\mathbb{C}$. Además $\mathbb{M} \simeq \mathbb{R} \oplus \mathbb{R}$.*

Demostración:

Basta ver que $\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1)$ es la única extensión de grado dos de $\mathbb{R}$. Sea $\mathbb{R}[x]/(f(x))$ con $f(x)$ irreducible, sea m el discriminante de $f(x)$, entonces m es negativo. Como $\frac{m}{-4}$ es positivo su raíz es real no nula. Además $\mathbb{R} \oplus \mathbb{R}$ es una $\mathbb{R}$-álgebra de dimensión dos con divisores de cero y sólo (0,0) cero tiene cuadrado nulo, por lo que no es isomorfa a $\mathbb{C}$ ni a $\mathbb{D}$. También podemos construir directamente el isomorfismo

$$\varphi : \mathbb{M} \to \mathbb{R} \oplus \mathbb{R}$$
$$1 \mapsto (1,1)$$
$$\mathrm{j} \mapsto (1,-1)$$

■

Consecuencia 3.5.– *Si K es algebraicamente cerrado, entonces hay dos K-álgebras bidimensionales. En particular hay dos $\mathbb{C}$-álgebras bidimensionales.*

Demostración:

Obviamente $K[x]/(x^2)$ y KxK son las únicas ya que no hay polinomios irreducibles en $K[x]$. ■

Clasificación de las álgebras tridimensionales

En general las K-álgebras tridimensionales o bien son suma de tres álgebras locales de dimensión uno, de una de dimensión uno y otra de dimensión dos, o son ellas mismas álgebras locales de dimensión tres.

- En caso de que A se descomponga como producto de tres álgebras locales de dimensión uno, es $A \simeq K \oplus K \oplus K$
- En caso en que A se descomponga como producto de dos álgebras locales de dimensiones uno y dos hay dos posibilidades:
  - $A \simeq K \oplus L$ con L extension de grado dos de K
  - $A \simeq K \oplus K[x]/(x^2)$
- Si A es local de dimensión tres debe ser una de dos posibilidades:
  - $L = K$ y $dim_K(M_A) = 2$
  - $A = L$ extensión de grado tres de K

En el único caso por detallar $L = K$ y $dim_K(M_A) = 2$ sabemos que $\exists r \leq 3$ con $M^r = 0$, lo que nos permite dividir el caso en dos nuevos casos:

- El caso $M_A^2 = 0$ implica que si tomamos una base de M_A como Kespacio vectorial $\{j, k\}$ entonces $j^2 = k^2 = jk = 0$ así que

el álgebra es isomorfa a $K[x,y]/(x,y)^2$ con el isomorfismo que envía $1, j, k$ a $1, \overline{x}, \overline{y}$ respectivamente

- En el caso $M_A^3 = 0$ con $M_A^2 \neq 0$, tomamos una base $\{j,k\}$ de M_A y si $j^2 = 0 = k^2$ entonces $jk \neq 0$ pues en caso contrario $M_A^2 = 0$. Entonces $(j+k)^2 = j^2 + k^2 + 2jk = 2jk \neq 0$, así que $\exists h \in M_A,\ h^2 \neq 0$.

  Ahora veamos que $\{h, h^2\}$ son linealmente independientes, $h^2 = dh \Rightarrow h^3 = dh^2 = d^2h$ pero $h^3 \in M^3 = 0 \Rightarrow d = 0 \Rightarrow h^2 = 0$ que sabemos que no ocurre. Por último 1 es base de K así que $\{1, h, h^2\}$ es base de A con $h^3 = 0$ así que $A \simeq K[x]/(x^3)$.

Por tanto las K-álgebras de dimensión tres no son todas de la forma $K[x]/(f(x))$ con $f(x)$ polinomio de grado tres ya que son:

- $K[x,y]/(x,y)^2$
- $K[x]/(f(x))$ donde $f(x) \in K[x]$ es un polinomio de grado tres y en este caso hay los tipos siguientes:
  - $f(x)$ tiene en K tres raíces distintas
  - $f(x)$ tiene en K dos raíces distintas una de ellas doble
  - $f(x)$ tiene en K una raíz triple
  - $f(x)$ tiene una raíz en k
  - $f(x)$ es irreducible.

Hemos buscado las álgebras tridimensionales, solo para comprobar que la fuerte relación existente entre las cuadricas y las algebras bidimensionales no se extiende a las de dimensión tres.

Cuádricas sobre $\mathbb{P}^1_K$

Proposición 3.6.– *Toda cuádrica $[Q]$ no nula sobre $\mathbb{P}^1_K$ con forma cuadrática asociada Q admite una matriz de la forma* $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$.

Demostración:

Como Q es simétrica, si su matriz en una referencia es M, sabemos que $\exists P$ matriz 2×2 inversible con $D = PMP^t = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

Como la matriz M no es nula sabemos que a o b son distintos de cero. Si a fuese nulo podríamos realizar la siguiente transformación

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix}$$

$$\text{con } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$

Así que podemos suponer sin pérdida de generalidad que $a \neq 0$ y como la matriz de una cuadrica proyectiva se puede multiplicar por cualquier número, se puede suponer $a = 1$ y se sigue el resultado. ■

Proposición 3.7.– *Dos cuádricas* $[Q]$ *y* $[J]$ *con matrices respectivas* $A = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}$ *y* $B = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$ *son proyectivamente equivalentes si y sólo si* $\exists \lambda \in K^*$ *con* $r = s\lambda^2$.

Demostración:

Las cuadricas son proyectivamente equivalentes si existen un $\rho \in K^*$ y una matriz:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ \rho A = MBM^t \Leftrightarrow \rho M^{-1} A = BM^t$$

Si $\Delta = det(M)$:

$$M^{-1} = (1/\Delta) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Y la igualdad anterior es:

$$(\frac{\rho}{\Delta}) \begin{pmatrix} d & -br \\ -c & ar \end{pmatrix} = \begin{pmatrix} a & c \\ sb & cd \end{pmatrix}$$

Operando: se obtiene, llamando $u = (\rho/\Delta)$:

$$\left\{ \begin{matrix} u^2 br & = & bs \\ u^2 ar & = & as \end{matrix} \right\}$$

Y como es $a \neq 0$ o $b \neq 0$ r y s difieren en un cuadrado. El recíproco es trivial.

Por tanto los tipos de cuadricas en la recta proyectiva sobre el cuerpo K están en correspondencia con las K-álgebras de dimensión dos. ■

Pero hay aún algo mas.

Teorema de descomposición de Witt 3.8.– *Si Q es una forma cuadrática en un espacio vectorial V, el espacio cuadrático (V, Q) se descompone en suma directa de planos hiperbólicos y un subespacio L tal que $Q|_L$ no tiene vectores isótropos.*

Definición 3.9.– *Llamamos cuádricas reales a aquellas que contienen algún punto no singular (es decir, que no sea el vértice).*

Si tomamos una cuádrica real $[Q]$ en $\mathbb{P}^3_K$ sabemos por el teorema de Witt que existe al menos un plano hiperbólico para Q, es decir se da una de las siguientes posibilidades:

- $K^4 = H_1 \perp H_2$
- $K^4 = H_1 \perp L$ y $Q|_L = 0$
- $K^4 = H_1 \perp L$ y $Q|_L$ no tiene vectores isótropos

Por otra parte el teorema de simplificación de Witt establece que dos cuadricas reales en $\mathbb{P}^3_K$ son proyectivamente equivalentes si lo son las cuadricas $\mathbb{P}^1_K$ resultantes de suprimirles un plano hiperbólico. Es decir de nuevo hay tantas cuadricas irreducibles (que no contienen planos) en $\mathbb{P}^3_K$ como K-álgebras de dimensión dos.

Es claro también que por cuestión de numero es imposible obtener un resultado similar para las álgebras tridimensionales

4. Rectas proyectivas sobre K-álgebras finitas

El elemento unificador que justifica los resultados anteriores es la recta proyectiva sobre una K- álgebra finita.

Sea A una K-álgebra de dimensión finita, en todo lo que sigue designaremos con V al A-módulo libre de rango 2, A^2, a los elementos de V los representaremos como:

$$\mathbf{a} = (a_1, a_2)$$

y consideraremos en V el producto exterior:

$$\mathbf{a} \wedge \mathbf{b} = (a_1, a_2) \wedge (b_1, b_2) = a_1 b_2 - a_2 b_1 = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$$

Obviamente el producto exterior es bilineal y alternado, es decir $\forall \mathbf{a},\ \mathbf{b},\ \mathbf{c}\ \in V$:

- $\mathbf{a} \wedge \mathbf{b} = -\mathbf{b} \wedge \mathbf{a}$
- $\mathbf{a} \wedge \mathbf{a} = 0$
- $\mathbf{a} \wedge (\mathbf{b} + \mathbf{c}) = \mathbf{a} \wedge \mathbf{b} + \mathbf{a} \wedge \mathbf{c}$
- $(\mathbf{a} + (\mathbf{b}) \wedge \mathbf{c}) = \mathbf{a} \wedge \mathbf{c} + \mathbf{b} \wedge \mathbf{c}$

Proposición 4.1.– *Todos los elementos de una K-álgebra de dimensión finita A son o bien inversibles o bien divisores de cero (entendemos que el cero es un divisor de cero)*

Demostración:

Si A es local de ideal maximal M_A y $a \in A$, o bien $a \notin M_A$ y es inversible, o bien $a \in M_A$ y como M_A es nilpotente, a es nilpotente. Si A no es local, A es producto directo de K -álgebras locales finitas, $A = A_1 \times ... \times A_r$. Entonces si $(a_1, ..., a_r) \in A$ hay dos opciones:

- O bien todas las a_i son inversibles y

  $$(a_1, ..., a_r).(a_1^{-1}, ..., a_r^{-1}) = (1, ..., 1)$$

  luego $(a_1, ..., a_r)$ es inversible

- O bien existe un i con a_i nilpotente, es decir para un $s > 1,\ a_i^s = 0,\ a_i^{s-1} \neq 0$, entonces:

  $(a_1, ..., a_i, ..., a_r)(0, ..., a_i^{s-1}, ..., 0) = (0, ..., 0),\ (0, ..., a_i^{s-1}, ..., 0) \neq (0, ..., 0)$

  y $(a_1, ..., a_r)$ es divisor de cero.

■

Proposición 4.2.–
Si $\mathbf{a},\ \mathbf{b} \in V$*:*

1. $\mathbf{a} \wedge \mathbf{b}$ *es inversible si y solo si* $\{\mathbf{a}, \mathbf{b}\}$ *es una base de* V
2. $\mathbf{a} \wedge \mathbf{b}$ *es divisor de cero si y solo si existen* $\lambda, \mu \in A$ *con* $(\lambda, \mu) \neq (0, 0)$ *tales que:*
$$\lambda \mathbf{a} + \mu \mathbf{b} = \mathbf{0}$$

Demostración:
Si $\mathbf{a} \wedge \mathbf{b} = \Delta$ es inversible:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\Delta} \begin{pmatrix} b_2 & -b_1 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

Luego:
$$\left\{ \begin{matrix} (1,0) & = & \frac{b_2}{\Delta}\mathbf{a} & -\frac{b_1}{\Delta}\mathbf{b} \\ (0,1) & = & -\frac{a_2}{\Delta}\mathbf{a} & +\frac{a_1}{\Delta}\mathbf{b} \end{matrix} \right\}$$

Para la segunda afirmación, si $\lambda \mathbf{a} + \mu \mathbf{b} = \mathbf{0}$ y suponemos $\lambda \neq 0$ multiplicando por $\mathbf{b}$ es $\lambda \mathbf{a} \wedge \mathbf{b} = \mathbf{0}$, luego $\mathbf{a} \wedge \mathbf{b}$ es divisor de cero.

Recíprocamente, si suponemos en primer lugar que $\mathbf{a} = \mathbf{0}$ o $\mathbf{b} = \mathbf{0}$ el resultado es trivial. Si ambos vectores son distintos de cero y

$$\mathbf{a} \wedge \mathbf{b} = a_1 b_2 - a_2 b_1 = 0$$

entonces:
$$\left\{ \begin{matrix} b_2\mathbf{a} & - & a_2\mathbf{b} & = \mathbf{0} \\ b_1\mathbf{a} & - & a_1\mathbf{b} & = \mathbf{0} \end{matrix} \right\}$$

y alguna de las igualdades tiene un coeficiente distinto de cero.

Si $\mathbf{a} \wedge \mathbf{b} = t$ divisor de cero existe s con $st = 0$ entonces:

$$(s\mathbf{a}) \wedge \mathbf{b} = st = 0$$

y estamos en el caso anterior. ■

Consecuencia 4.3.– *Si* A *es una* K*-álgebra de dimensión finita y* $\mathcal{B} = \{\mathbf{a},\ \mathbf{b}\} \subset V$ *o bien* $\mathcal{B}$ *es una base de* V*, o bien* $\{\mathbf{a},\ \mathbf{b}\}$ *son*

linealmente dependientes. Es decir dos vectores independientes son una base.

Demostración:
Obvio porque al ser A una K-álgebra de dimensión finita $\mathbf{a} \wedge \mathbf{b}$ es inversible o divisor de cero, en el primer caso $\{\mathbf{a},\ \mathbf{b}\}$ es una base y en el segundo son dependientes. ■

Ejemplo.- La condición de K-álgebra finita es imprescindible, por ejemplo: Si $A = K[x]$, A es una K-álgebra, pero no de dimensión finita, y por $\{(x,0),\ (0,x)\}$ no son ni linealmente dependientes ni forman una base de $K[x]^2$

Definición 4.4.– *Una base de V,$\{\mathbf{a},\ \mathbf{b}\}$ se llama pura si $\mathbf{a}\wedge\mathbf{b} = 1$, un elemento $\mathbf{a} \in V$ se llama complementable si forma parte de una base de V*

Proposición 4.5.– *Si $\mathbf{a} \in V$ son equivalentes:*

1. $\mathbf{a}$ *es complementable*
2. *Existe* $\mathbf{b} \in V$ *con* $\mathbf{a} \wedge \mathbf{b}$ *inversible*
3. *Existe* $\mathbf{b} \in V$ *con* $\mathbf{a} \wedge \mathbf{b} = 1$

Demostración:
Trivial ■

Proposición 4.6.– *Si $\mathbf{a}, \mathbf{b}, \mathbf{c}$ son elementos de V*

$$(\mathbf{a} \wedge \mathbf{b})\mathbf{c} + (\mathbf{c} \wedge \mathbf{a})\mathbf{b} + (\mathbf{b} \wedge \mathbf{c})\mathbf{a} = \mathbf{0}$$

Demostración:
Por cálculo directo:

$$(\mathbf{a} \wedge \mathbf{b})\mathbf{c} + (\mathbf{c} \wedge \mathbf{a})\mathbf{b} + (\mathbf{b} \wedge \mathbf{c})\mathbf{a} =$$

$$= (a_1b_2 - a_2b_1)(c_1, c_2) + (c_1a_2 - c_2a_1)(b_1, b_2) + (b_1c_2 - b_2c_1)(a_1, a_2) = (0, 0)$$

■

Consecuencia 4.7.– *Si $\{\mathbf{a},\ \mathbf{b}\}$ es una base pura de V:*

$$\forall \mathbf{c} \in V,\ \mathbf{c} = (\mathbf{c} \wedge \mathbf{b})\mathbf{a} + (\mathbf{a} \wedge \mathbf{c})\mathbf{b}$$

Demostración:

Como $\mathbf{a} \wedge \mathbf{b} = 1$ sustituyendo en la fórmula anterior:

$$\mathbf{c} + (\mathbf{c} \wedge \mathbf{a})\mathbf{b} + (\mathbf{b} \wedge \mathbf{c})\mathbf{a} = \mathbf{0} \Rightarrow \mathbf{c} = -(\mathbf{c} \wedge \mathbf{a})\mathbf{b} - (\mathbf{b} \wedge \mathbf{c})\mathbf{a} \Rightarrow$$

$$\Rightarrow \mathbf{c} = (\mathbf{c} \wedge \mathbf{b})\mathbf{a} + (\mathbf{a} \wedge \mathbf{c})\mathbf{b}$$

■

Consecuencia 4.8.– *Si* $\mathbf{c} \in V$ *es complementable y* $\mathbf{a} \in V$*:*

1. $\mathbf{c} \wedge \mathbf{a} = 0 \Leftrightarrow \mathbf{a} = \lambda\mathbf{c},\ \lambda \in A$
2. *Si* $\mathbf{a}$ *es también complementable :* $\mathbf{c} \wedge \mathbf{a} = 0 \Leftrightarrow \mathbf{a} = \lambda\mathbf{c}$ *y* $\lambda \in A$ *es inversible*
3. $\mathbf{c} \wedge \mathbf{a}$ *es un divisor de cero si y solo si* $\mu\mathbf{a} = \lambda\mathbf{c},\ \lambda, \mu \in A,\ \mu$ *divisor de cero*

Demostración:

1. Si $\mathbf{c} \in V$ es complementable lo extendemos a una base pura $\{\mathbf{c}, \mathbf{d}\}$ de V, y por la proposición anterior:

   $$\mathbf{a} = (\mathbf{a} \wedge \mathbf{d})\mathbf{c} + (\mathbf{c} \wedge \mathbf{a})\mathbf{d} = (\mathbf{a} \wedge \mathbf{d})\mathbf{c}$$

   El recíproco es trivial

2. Aplicando 1 dos veces:

   $$\mathbf{a} = \lambda\mathbf{c},\ \mathbf{c} = \mu\mathbf{a}$$

   y como ambos son complementables $\lambda\mu = 1$

3. Si $\mathbf{c} \wedge \mathbf{a} = t$ divisor de cero existe s con $st = 0$ entonces:

   $$\mathbf{c} \wedge (s\mathbf{a}) = st = 0$$

   y por 1, $s\mathbf{a} = \mu\mathbf{c}$, el recíproco es trivial

■

Consecuencia 4.9.– $\mathbf{c} \in V$ *es no complementable si y solo si* $\forall \mathbf{a} \in V,\ \mathbf{c} \wedge \mathbf{a}$ *es un divisor de cero, en particular si* $\mathbf{c} = (c_1, c_2) \in V$ *es no complementable,* c_1 *y* c_2 *son divisores de cero.*

Demostración:

Basta observar que : $c_1 = \mathbf{c} \wedge (0, 1),\ c_2 = (1, 0) \wedge \mathbf{c}$ ■

Ejemplo.- El recíproco de la afirmación anterior no es cierto. Si $A = \mathbb{R}[x]/(x^2-1)$, $(\overline{x}+1, \overline{x}-1)$ tiene las dos componentes divisores de cero pero $\{(\overline{x}+1, \overline{x}-1), (1,1)\}$ es una base de A^2.

Sin embargo si A es un álgebra local finita como los divisores de cero forman el ideal maximal de A, si c_1 y c_2 son divisores de cero, están en el maximal M_A, luego:

$$\forall \mathbf{a} \in V,\ \mathbf{c} \wedge \mathbf{a} = a_2 c_1 - a_1 c_2 \in M_A$$

y es divisor de cero. Por tanto si si A es un álgebra local finita, $\mathbf{c} = (c_1, c_2) \in V$ es no complementable si y solo si c_1 y c_2 son divisores de cero

Proposición 4.10.– *La relación definida en V por:*

$$\forall \mathbf{a}, \mathbf{b} \in V,\ \mathbf{a} \sim \mathbf{b} \Leftrightarrow \exists \lambda \in A \textit{ inversible } \mathbf{a} = \lambda \mathbf{b}$$

es una relación de igualdad.

Demostración:

Propiedad reflexiva: $\mathbf{a} = 1\mathbf{a} \Rightarrow \mathbf{a} \sim \mathbf{a}$.

Propiedad simétrica: $\mathbf{a} \sim \mathbf{b} \Rightarrow \mathbf{a} = \lambda \mathbf{b}$ y λ inversible. Luego $\mathbf{b} = \lambda^{-1}\mathbf{a}$ y λ^{-1} inversible, luego $\mathbf{b} \sim \mathbf{a}$

Propiedad transitiva

$$\left.\begin{matrix} \mathbf{a} \sim \mathbf{b} & \Rightarrow & \mathbf{a} = \lambda \mathbf{b} \\ \mathbf{b} \sim \mathbf{c} & \Rightarrow & \mathbf{b} = \mu \mathbf{c} \end{matrix}\right\} \Rightarrow \mathbf{a} = \lambda\mu\mathbf{c}$$

y como λ, μ son inversibles, $\lambda\mu$ lo es también. ∎

Si ahora consideramos el conjunto $V/\sim$, hay una clase con solo un elemento, la $\{(0,0)\}$ y si $\mathbf{a}$ es complementable, su clase está compuesta por elementos complementables y si es no complementable, los elementos de su clase tampoco lo son. Podemos suprimir las clase de elementos no complementables, como se hace en los textos de proyectiva sobre anillos, pero como nuestros anillos son muy semejantes a cuerpos, nos limitaremos a suprimir la clase del cero, y consideraremos dos tipos de puntos distintos.

Definición 4.11.– *Llamaremos recta proyectiva asociada a la K-álgebra de dimensión finita A a*

$$\mathbb{P}^1_A = \mathbb{P}(V) = \frac{V \setminus \{(0,0)\}}{\sim}$$

Y llamaremos punto a cada clase de dicho conjunto, es decir los puntos son los conjuntos:

$$[\mathbf{a}] = \{\lambda\mathbf{a} \mid \lambda \in A \text{ inversible}\}$$

Si $\mathbf{a}$ *es complementable diremos que el punto es regular y si no lo es que es singular.*

Ejemplo.- Si $[\mathbf{a}]$ y $[\mathbf{b}]$ son puntos regulares

$$[\mathbf{a}] = [\mathbf{b}] \Leftrightarrow [\mathbf{a} \wedge \mathbf{b}] = 0$$

Pero eso no sucede si uno de los dos son singulares, ya que si uno es regular y el otro singular no pueden ser iguales y si ambos son singulares el ejemplo siguiente prueba que la afirmación no es cierta:

Sea $A = \mathbb{R}[x, y]/(x^2, y^2)$ entonces $[(\overline{x}, \overline{y})] \neq [(\overline{y}, \overline{x})]$ y

$$(\overline{x}, \overline{y}) \wedge (\overline{y}, \overline{x}) = \overline{x}^2 - \overline{y}^2 = 0$$

También puede ser que siendo $[\mathbf{a}]$ y $[\mathbf{b}]$ puntos regulares

$$[\mathbf{a}] \neq [\mathbf{b}] \text{ y } [\mathbf{a} \wedge \mathbf{b}] \text{ divisor de cero}$$

por ejemplo si $A = K[x]/(x^2)$, $[(\overline{x}, 1)] \neq [(\overline{x}, 2)]$ pero $(\overline{x}, 1) \wedge (\overline{x}, 2) = \overline{x}$ que es divisor de cero.

Ahora daremos una definición de sistema de referencias en estas rectas proyectivas para poder manejar los elementos con coordenadas.

Definición 4.12.– *Sean* $[\mathbf{a}] = [a_0, a_1], [\mathbf{b}] = [b_0, b_1] \in \mathbb{P}^1_A$ *dos puntos regulares, diremos que son un par de puntos independientes si*

$$\begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix} = \mathbf{a} \wedge \mathbf{b}$$

es un elemento inversible de A*. Y diremos que son dependientes en caso contrario*

La definición anterior es independiente del representante elegido, ya que el cambio de representante supone solamente el producto por un elemento inversible. Además los puntos $[\mathbf{a}], [\mathbf{b}]$ son independientes si y solo si dos cualesquiera de sus representantes lo son y son dependientes si lo son dos cualesquiera de sus representantes:

Proposición 4.13.–
Dados tres puntos $[\mathbf{a}], [\mathbf{b}], [\mathbf{c}] \in \mathbb{P}^1_A$ *son equivalentes:*

1. *Son dos a dos independientes.*
2. *Existe* $\mathcal{B} = \{\mathbf{u}, \mathbf{v}\} \subset V$ *tal que:*
   a) $\mathcal{B}$ *es una base de* V
   b) $[\mathbf{a}] = [\mathbf{u}],\ [\mathbf{b}] = [\mathbf{v}]$
   c) $[\mathbf{c}] = [\mathbf{u} + \mathbf{v}]$

Demostración:
(1) $\Rightarrow$ (2) Como $[\mathbf{a}], [\mathbf{b}]$ son independientes $\{\mathbf{a}, \mathbf{b}\}$ es base de V, si $\Delta = \mathbf{a} \wedge \mathbf{b}$ y $\mathbf{a}' = (1/\Delta)\mathbf{a}$, $\{\mathbf{a}', \mathbf{b}\}$ es una base pura de V, entonces:

$$\mathbf{c} = (\mathbf{c} \wedge \mathbf{b})\mathbf{a}' + (\mathbf{a}' \wedge \mathbf{c})\mathbf{b}$$

y como todos los vectores son complementables $\mathbf{c} \wedge \mathbf{b}$ y $\mathbf{a}' \wedge \mathbf{c}$ son inversibles, llamando:

$$\mathbf{u} = (\mathbf{c} \wedge \mathbf{b})\mathbf{a}',\ \mathbf{v} = (\mathbf{a}' \wedge \mathbf{c})\mathbf{b}$$

se sigue el resultado.
(2) $\Rightarrow$ (1) Como $[\mathbf{a}] = [\mathbf{u}],\ [\mathbf{b}] = [\mathbf{v}]$ y $\{\mathbf{u}, \mathbf{v}\}$ es una base $[\mathbf{a}], [\mathbf{b}]$ son independientes. Como $[\mathbf{c}] = [\mathbf{u} + \mathbf{v}]$ es $\mathbf{c} = \lambda\mathbf{u} + \lambda\mathbf{v}$ con λ inversible, luego $\mathbf{u} \wedge \mathbf{c} = \lambda\mathbf{u} \wedge \mathbf{v}$ y $\mathbf{v} \wedge \mathbf{c} = -\lambda\mathbf{u} \wedge \mathbf{v}$ son inversibles y por tanto se cumple (1) ∎

Definición 4.14.– *Diremos que tres puntos* $[\mathbf{a}], [\mathbf{b}], [\mathbf{c}] \in \mathbb{P}^1_A$ *forman una referencia si cumplen una de las condiciones equivalentes de la proposición anterior.*
La base $\mathcal{B} = \{\mathbf{u}, \mathbf{v}\}$ *de dicha proposición se llama base normalizada asociada a la referencia, y dado un punto* $[\mathbf{d}]$ *el conjunto de matrices:*

$$[d_0, d_1] = \{d_0\mathbf{u} + d_1\mathbf{v} \in [\mathbf{d}]\}$$

se llaman coordenadas de $\mathbf{d}$ *en la referencia* $\{[\mathbf{a}], [\mathbf{b}]; [\mathbf{c}]\}$

Proposición 4.15.– *Dada una referencia* $\{[\mathbf{a}], [\mathbf{b}]; [\mathbf{c}]\}$ *de* $\mathbb{P}^1_A$*:*

1. *Si* $\mathcal{B}_1 = \{\mathbf{u}_0, \mathbf{u}_1\}$ *y* $\mathcal{B}_2 = \{\mathbf{v}_0, \mathbf{v}_1\}$ *son bases normalizadas asociadas a ella:*

$$\exists \lambda \in A \text{ inversible}, \ \mathbf{u}_0 = \lambda \mathbf{v}_0, \ \mathbf{u}_1 = \lambda \mathbf{v}_1$$

2. *Las coordenadas de un punto en la referencia no dependen de la base normalizada que se use para construirlas.*

Demostración:

Por hipótesis:

$$\left\{ \begin{array}{ccc} [\mathbf{u}_0] = [\mathbf{v}_0] & \Rightarrow & \mathbf{u}_0 = \alpha \mathbf{v}_0 \\ [\mathbf{u}_1] = [\mathbf{v}_1] & \Rightarrow & \mathbf{u}_1 = \beta \mathbf{v}_1 \\ [\mathbf{u}_0 + \mathbf{u}_1] = [\mathbf{v}_0 + \mathbf{v}_1] & \Rightarrow & \mathbf{u}_0 + \mathbf{u}_1 = \lambda(\mathbf{v}_0 + \mathbf{v}_1) \end{array} \right\}$$

Luego:

$$\alpha \mathbf{v}_0 + \beta \mathbf{v}_1 = \lambda(\mathbf{v}_0 + \mathbf{v}_1) \Rightarrow (\lambda - \alpha)\mathbf{v}_0 + (\lambda - \beta)\mathbf{v}_1 = \mathbf{0}$$

Como $\{\mathbf{v}_0, \mathbf{v}_1\}$ es base $\lambda = \alpha, \ \lambda = \beta$ y se sigue el resultado.

La segunda afirmación es consecuencia trivial de la primera. ■

Definición 4.16.– *Dados cuatro puntos* $[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3], [\mathbf{a}_4] \in \mathbb{P}^1_A$ *llamamos razón doble de los cuatro puntos a la familia de matrices:*

$$[[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3], [\mathbf{a}_4]] = \{((\mathbf{u}_1 \wedge \mathbf{u}_3)(\mathbf{u}_2 \wedge \mathbf{u}_4), (\mathbf{u}_1 \wedge \mathbf{u}_4)(\mathbf{u}_2 \wedge \mathbf{u}_3))\}$$

donde los $\mathbf{u}_i$ *varían de todos los modos posibles con* $[\mathbf{a}_i] = [\mathbf{u}_i], \ \forall i, \ 1 \leq i \leq 4$

Proposición 4.17.– *Si* $\mathcal{R} = \{[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3]\}$ *es una referencia en* $\mathbb{P}^1_A$*, para todo punto* $[\mathbf{a}_4] \in \mathbb{P}^1_A$*,* $[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3], [\mathbf{a}_4]$ *coincide con las coordenadas de* $[\mathbf{a}_4]$ *en* $\mathcal{R}$

Demostración:

Elegimos como representantes de $[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3], \ \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_1 + \mathbf{u}_2$, siendo $\{\mathbf{u}_1, \mathbf{u}_2\}$ una base normalizada asociada a la referencia $\{[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3]\}$, entonces:

$$((\mathbf{u}_1 \wedge \mathbf{u}_2)(\mathbf{u}_2 \wedge \mathbf{a}_4), (\mathbf{u}_1 \wedge \mathbf{a}_4)(\mathbf{u}_2 \wedge \mathbf{u}_1)) =$$

$$= (\mathbf{u}_2 \wedge \mathbf{u}_1)(\mathbf{a}_4 \wedge \mathbf{u}_2, \mathbf{u}_1 \wedge \mathbf{a}_4)$$

Como el segundo miembro es el vector de coordenadas de $\mathbf{a}_4$ en la base normalizada multiplicado por el inversible $-(\mathbf{u}_1 \wedge \mathbf{u}_2)^2$, y

tanto las coordenadas de un punto como la razón doble se obtienen multiplicando un representante por todos los elementos inversibles del anillo se sigue el resultado. ■

Proyectividades en $\mathbb{P}^1_A$ y razón doble

Sea M una matriz 2x2 de elementos de A, M define una aplicación lineal:

$$\psi_M : V \longrightarrow V,\ \psi_M(x_0, x_1) = (y_0, y_1) \Leftrightarrow \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} M$$

La aplicación ψ_M es un isomorfismo si y solo si M es inversible.

Proposición 4.18.– $\psi_M(\mathbf{a}) \wedge \psi_M(\mathbf{b}) = det(M)(\mathbf{a} \wedge \mathbf{b})$

Demostración:

Por definicion:

$$\psi_M(\mathbf{a}) \wedge \psi_M(\mathbf{b}) = det\left(\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix} M\right) = det(M)(\mathbf{a} \wedge \mathbf{b})$$

Cuando M es inversible, el isomorfismo ψ_M induce una correspondencia:

$$[\psi_M] : \mathbb{P}^1_A \longrightarrow \mathbb{P}^1_A,\ [\psi_M]([\mathbf{a}]) = [\psi_M(\mathbf{a})]$$

A esa correspondencia le llamaremos proyectividad asociada a M. ■

Proposición 4.19.– *La correspondencia ψ_M es una aplicación biunívoca, conserva la dependencia lineal, transforma referencias en referencias, y dos matrices inversibles definen la misma correspondencia si y solo si difieren en el producto por un elemento inversible.*

Demostración:

$[\psi_M]$ es aplicación porque ψ_M es lineal, es biunívoca porque $[\psi_{M^{-1}}]$ es su inversa. Por ser ψ_M isomorfismo transforma puntos dependientes en dependientes y puntos independientes en independientes y en consecuencia transforma referencias en referencias.

Por último si $\{\mathbf{a}, \mathbf{b}\}$ es una base de V y M y N son matrices inversibles 2×2, con $M = \lambda N$, siendo λ un elemento inversible de A. Entonces $\forall [\mathbf{x}] \in \mathbb{P}^1_A$:

$$M = \lambda N \Rightarrow \psi_M(\mathbf{x}) = \lambda \psi_N(\mathbf{x}) \Rightarrow [\psi_M][\mathbf{x}] = [\psi_N][\mathbf{x}] \Rightarrow [\psi_M] = [\psi_N]$$

Recíprocamente, si $[\psi_M] = [\psi_N]$ entonces:

$$\left\{\begin{array}{ccc} [\psi_M]([\mathbf{a}]) = [\psi_N]([\mathbf{a}]) & \Rightarrow & \psi_M(\mathbf{a}) = \alpha\psi_N(\mathbf{a}) \\ [\psi_M]([\mathbf{b}]) = [\psi_N]([\mathbf{b}]) & \Rightarrow & \psi_M(\mathbf{b}) = \beta\psi_N(\mathbf{b}) \\ [\psi_M]([\mathbf{a}+\mathbf{b}]) = [\psi_N]([\mathbf{a}+\mathbf{b}]) & \Rightarrow & \psi_M(\mathbf{a}+\mathbf{b}) = \lambda\psi_N(\mathbf{a}+\mathbf{b}) \end{array}\right\}$$

Y el mismo razonamiento de mas arriba termina la prueba ■

Proposición 4.20.– *Dadas dos referencias* $\mathcal{R} = \{[\mathbf{a}_1], [\mathbf{a}_2]; [\mathbf{a}_3]\}$, $\mathcal{S} = \{[\mathbf{b}_1], [\mathbf{b}_2]; [\mathbf{b}_3]\}$ *existe una única proyectividad* $[\varphi]$ *tal que:*

$$[\varphi][\mathbf{a}_i] = [\varphi][\mathbf{b}_i],\ i = 1, 2, 3$$

Demostración:

Si tomamos bases normalizadas asociadas a las referencias $\{\mathbf{u}_1, \mathbf{u}_2\}$, $\{\mathbf{v}_1, \mathbf{v}_2\}$ existe un automorfismo de V φ tal que $\varphi(\mathbf{u}_1) = \mathbf{v}_1,\ \varphi(\mathbf{u}_2) = \mathbf{v}_2$. Entonces $[\varphi]$ cumple los requisitos de la proposición. La unicidad es consecuencia del mismo razonamiento de la proposición anterior.
■

Proposición 4.21.– *Las proyectividades conservan la razón doble.*

Demostración:

En efecto. Para cuatro puntos $[\mathbf{a}_1], [\mathbf{a}_2], [\mathbf{a}_3], [\mathbf{a}_4] \in \mathbb{P}^1_A$

$$(\psi_M(\mathbf{a}_1)\wedge\psi_M(\mathbf{a}_3))(\psi_M(\mathbf{a}_2)\wedge\psi_M(\mathbf{a}_4)), (\psi_M(\mathbf{a}_1)\wedge\psi_M(\mathbf{a}_4))(\psi_M(\mathbf{a}_2)\wedge\psi_M(\mathbf{a}_3)) =$$

$$= det(M)^2((\mathbf{a}_1 \wedge \mathbf{a}_3)(\mathbf{a}_2 \wedge \mathbf{a}_4), (\mathbf{a}_1 \wedge \mathbf{a}_4)(\mathbf{a}_2 \wedge \mathbf{a}_3))$$

Como dos de sus representantes difieren en producto por un elemento inversible, ambas razones dobles son iguales.
■

5. Proyección estereográfica

Recordemos la proyección estereográfica en la esfera:

Definición 5.1.– *Sea $\mathbb{S}^2$ la esfera de centro $(0,0,0)$ y radio 1, llamamos proyección estereográfica al homeomorfismo*

$$\pi : \mathbb{R}^2 \to \mathbb{S}^2 \backslash \{(0,0,1)\}, \pi(x,y) = \left(\frac{2x}{x^2+y^2+1}, \frac{2y}{x^2+y^2+1}, \frac{x^2+y^2-1}{x^2+y^2+1} \right)$$

Como podemos identificar

$$\mathbb{C} \equiv \mathbb{R}^2,\ z = x + iy \equiv (x,y)$$

y entonces:

$$2x = z + \overline{z},\ 2y = i(\overline{z} - z), x^2 + y^2 = z\overline{z}$$

La proyección estereográfica en versión compleja se escribe:

$$\pi : (C) \to \mathbb{S}^2 \setminus \{(0,0,1)\}, \pi(z) = \left(\frac{z+\overline{z}}{z\overline{z}+1}, \frac{z-\overline{z}}{i(z\overline{z}+1)}, \frac{z\overline{z}-1}{z\overline{z}+1} \right)$$

Podemos pasar al proyectivo identificando el punto complejo $[u,v] \in \mathbb{P}^1_{\mathbb{C}}$ con el complejo $z = u/v$, de este modo la correspondencia se extiende al infinito y se transforma en una aplicación:

$$\pi : \mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathbb{P}^3_{\mathbb{R}},\ \pi([u,v]) = [u\overline{v} + \overline{u}v, (1/i)(u\overline{v} - \overline{u}v), u\overline{u} - \overline{v}v, u\overline{u} + \overline{v}v]$$

cuya imagen es la cuadrica de puntos.

La proyección estereográfica entendida de esta forma se generaliza a las K -álgebras de dimensión dos, en este caso, para cada K-álgebra $A \simeq K[x]/(f(x))$ de dimensión dos hay solo dos K- automorfismos de A, la identidad y el automorfismo que permuta las dos raíces de $f(x)$.

Si $f(x) = x^2 + ax + b$, la transformación $x = y - (a/2)$ permite suponer que $f(x) = x^2 + c$ y que en consecuencia $A \simeq K(\beta),\ \beta^2 = -c$, entonces los K automorfismos de A son: la identidad y el automorfismo:

$$\sigma : A \longrightarrow A,\ \sigma(a + b\beta) = a - b\beta$$

Podemos definir la proyección estereográfica como:

$$\pi : \mathbb{P}^1_A \longrightarrow \mathbb{P}^3_K,\ \pi([u,v]) = [u\sigma v + \sigma u v, (1/\beta)(u\sigma v - \sigma u v), u\sigma u - \sigma v v, u\sigma u + \sigma v v]$$

Obviamente π es aplicación, y su imagen es la cuadrica de $\mathbb{P}^3_K$ de ecuación

$$z_0^2 + cz_1^2 + z_2^2 - z_3^2 = 0$$

Es decir tenemos una aplicación que de modo natural hace corresponder las K-álgebras de dimensión dos a las cuadricas reales irreducibles de $\mathbb{P}^3_K$ de modo que algebras isomorfas corresponden a cuadricas proyectivamente equivalentes.

Observemos además que si A es un cuerpo es decir si $-c \notin K^2$ la cuadrica imagen de la proyección estereográfica es una cuadrica de puntos y la proyección estereográfica es biunívoca entre $\mathbb{P}^1_A$ y la cuadrica. En los dos casos en que A no es un cuerpo es decir si $c = 0$ o $c = -1$, la imagen de la proyección es respectivamente, el cono real y la cuadrica hiperbólica. En estos casos la proyección estereográfica no es inyectiva.

En el caso $c = -1$, todos los puntos $[u, v] = [a(1+\beta), b(1+\beta)]$ y los $[u, v] = [a(1-\beta), b(1-\beta)]$ es decir los puntos singulares de $\mathbb{P}^1_A$, verifican que:

$$u\sigma(v) = v\sigma(u) = u\sigma(u) = v\sigma(v) = 0$$

Por tanto todos se aplican en el punto $[0, 0, -1, 1]$ y recíprocamente, todos los puntos en los que el plano tangente por $[0, 0, -1, 1]$ a la cuadrica imagen corta a la cuadrica,se aplican en el punto $[1, 0]$.

Un resultado similar se produce en el cono.

Bibliografía

[1] Aroca J.M., Fernandez M.J. Geometria Proyectiva. Notas de clase. U. Valladolid.

[2] Atiyah M. F., Macdonald I.G. *Introducción al Algebra conmutativa*. Reverté. Barcelona 1989.

[3] Mazuelas S. *Interpretación proyectiva de las geometrías métricas, equiformes e inversivas*. Tesis doctoral. Valladolid 2009.

[4] Mc Donald B. *Linear algebra over commutative rings*. Marcel Dekker New York 1984.

[5] Navarro J.A. *Algebra conmutativa básica* Univ. Extremadura 1996.

[6] Poonen B. *Isomorphism types of commutative algebras of finite rank over an algebraically closed field*. In Computational Arithmetic Geometry. Providence 2008.