Universidad del Valle de Guatemala

FACULTAD DE CIENCIAS Y HUMANIDADES
DEPARTAMENTO DE MATEMÁTICA

ÁLGEBRAS CON BASES QUE CONSISTEN ÚNICAMENTE DE UNIDADES

TRABAJO DE GRADUACIÓN PRESENTADO POR
SERGIO DAVID ZAPETA TZUL
PARA OPTAR AL GRADO ACADÉMICO
DE LICENCIADO EN MATEMÁTICAS

GUATEMALA
2017

Álgebras con bases que consisten únicamente de unidades

Universidad del Valle de Guatemala

FACULTAD DE CIENCIAS Y HUMANIDADES

DEPARTAMENTO DE MATEMÁTICA

ÁLGEBRAS CON BASES QUE CONSISTEN ÚNICAMENTE DE UNIDADES

TRABAJO DE GRADUACIÓN PRESENTADO POR

SERGIO DAVID ZAPETA TZUL

PARA OPTAR AL GRADO ACADÉMICO

DE LICENCIADO EN MATEMÁTICAS

GUATEMALA

2017

Vo.Bo.:

UNIVERSIDAD DEL VALLE DE GUATEMALA
DIRECCION
DEPARTAMENTO DE MATEMATICA

MA. Nancy Zurita

Tribunal Examinador:

MA. Nancy Zurita

Lic. Dorval Carías

Lic. Ricardo Barrientos

Fecha de aprobación:

Guatemala, 7 de Diciembre de 2017

Prefacio

Las ramas de las matemáticas se encuentran interconectadas entre sí. Los logros dentro de una rama suelen influenciar otros campos de las matemáticas. En particular, el álgebra se distingue por encontrar frecuentemente aplicaciones en otras ramas. El estudio de propiedades topológicas a través del algebra constituye el área conocida como Topología algebraica, aplicaciones de las teorías de grupos y de campos constituyen la teoría de Galois, la disciplina fundamental para el estudio de la resolubilidad de ecuaciones polinomiales.

En este trabajo se estudian, específicamente, aquellas álgebras que tienen bases que consisten únicamente de unidades. Estas álgebras han sido denominadas álgebras invertibles en proyectos doctorales recientes llevados a cabo en Ohio University. Considerando que este tema fue introducido hace apenas unos poco años, vale la pena señalar que el estudio de las álgebras invertibles esta todavía en su infancia. Eso hace que haya mucho todavía por hacer en cuanto a su investigación. Este trabajo de graduación propone ser un texto formal sobre el tema que ponga este interesante y prometedor tópico al alcance de estudiantes de Matemática a nivel de licenciatura de manera de una manera asequible, en particular, para estudiantes en el mundo de habla hispana.

Este trabajo es el resultado del esfuerzo de muchas personas. Quiero expresar infinito agradecimiento a mis padres, hermanos, hermanas y sobrinas, por apoyarme durante muchos años de mi vida y su cariño incondicional. Quiero agradecer a mi asesor Sergio López, quien me sugirió el tema de tesis, corrigió versiones preliminares y ayudó de muchas otras formas con la creación de este trabajo. Quiero agradecer profundamente a mi compañeros y profesores de olimpiadas de matemáticas. Así también quiero agradecer a mis amigos, profesores, compañeros y a todas las personas que me han apoyado a lo largo de este viaje académico.

Índice de contenido

Resumen

En este trabajo se cambiará levemente la definición de un R-álgebra. Desde un punto de vista, nuestra definición es más restrictiva que la usual pero desde otro, es más flexible. Primero que nada, no se permitirá que una imagen homomorfa del anillo R esté contenida en A, sino que se exige que esta copia sea isomorfa a R (básicamente, R está contenida en el álgebra A.) El segundo cambio será el no requerir que esa copia de R esté necesariamente contenida en el centro de A; solo pedimos que si a y b están en A y r está en R, entonces $r(ab) = (ra)b$; no requerimos que también sea cierto que $r(ab) = a(rb)$.

La idea de una parte del trabajo es considerar otras propiedades para los elementos de algunas bases de las algebras. Por ejemplo, considerar bases invertibles (aquellas cuyos elementos son todos invertibles con respecto a la multiplicación en el álgebra). Aquellas álgebras que tienen alguna base invertible serán denominadas algebras invertibles. Entre otras condiciones que uno puede considerar para las bases invertibles están, por ejemplo, el que sean cerradas bajo el producto, cerradas bajo inversos, etc. A partir de estas nuevas propiedades, uno trata de clasificarlas, caracterizarlas, y encontrar ejemplos específicos de álgebras que tengan bases que cumplen las condiciones dadas. Otros aspectos del proyecto incluyen como generar nuevas R-álgebras a partir de R-álgebras conocidas y considerar el impacto de esas construcciones sobre las propiedades que nos interesan. Por ejemplo, construir matrices cuyas entradas son elementos de R-álgebras invertibles o sumas directas de R-álgebras invertibles.

Otro enfoque del trabajo es estudiar álgebras invertibles y clasificarlas con base en su dimensión. Se estudian algebras invertibles finito e infinito-dimensionales. Comúnmente, el estudio de estructuras infinito-dimensionales, resulta ser más complejo que es estudio que estructuras finito-dimensionales. Por otra parte, la facilidad de trabajar con estructuras de dimensión finita se ha traducido, en la práctica, a una habilidad de desarrollar resultados contundentes que, sin embargo, requieren herramientas fuera del alcance de los lectores que anticipamos para este trabajo Resulta ser, entonces, que la demostración de uno de los resultados más impresionantes (que casi todas las álgebras finito-dimensionales son invertibles) es complejo, y sobrepasa el conocimiento de nivel licenciatura. Es por eso que en la sección correspondiente se omitirán las demostraciones de algunas propiedades, y se mostraran únicamente los enunciados de las proposiciones.

1 Introducción

Como ya se ha dicho anteriormente, en este trabajo se cambiará un poco la definición tradicional de R-álgebra, haciendola menos estricta (R no esta necesariamente contenido en el centro de A). Esto es debido a que varias de las propiedas y caracteristicas de estos álgebras no necesitan las condiciones extras que agrega la definición tradicional de R-ágebra. Además de pedir que las bases sean formadas únicamente por elementos con inversos, se trabajarán con bases que cumplen propiedades más especificas. Bases I2, bases cerradas bajo el producto, cerradas bajo inversos, entre otros. En particular los ágebras según la definición tradicional serán casos especiales de los álgebras que se considerán en este documento. Es decir, si el lector no se siente a gusto con la nueva definión de álgebras invertibles, puede considerar la definición tradicional de álgebras, esto no afectará a los resultados expuestos en este trabajo.

Es importante observar que no todos los álgebras invertibles poseen bases I2. Esta observación viene de que no todo conjunto de unidades linealmente independiente, tiene inversos que también forman un conjunto linealmente independiente. Consideresé $\frac{\mathbb{F}_2[x]}{x^3+x+1}$, el conjunto $\{1, x^2+1, x^2+x\}$ es linealmente independiente, pero el conjunto formados por sus inversos $\{1, x, x+1\}$ no es linelamente independiente. En el capitulo 3, algunos resultados similares al anterior serán mostrados, para ejemplificar la importancia de la clasificación de álgebras.

Finalmente, para poder entender este trabajo el lector debe tener conocimientos basicos en Álgebra lineal, en especial respecto a las propiedades de bases de espacios vectoriales, ya que la definición de una base de un álgebra y la base de un espacio vectorial son equivalentes. Así como también debe tener conocimientos en Álgebra Abstracta, debido a que se utilizan varios conceptos de teoria de grupos y teoria de anillos.

2 Preliminares

En esta sección se encuentran algunas definiciones, proposiciones y teoremas que serán útiles para el resto del documento.

Definición 2.1 Sea G un conjunto no vacío si existe $\cdot : G \times G \to G$ una operación binaria que cumple

* $a, b \in G \to a \cdot b \in G \; \forall a, b \in G$, (Cerradura)

* $a, b, c \in G \to (a \cdot b) \cdot c = a \cdot (b \cdot C)$ (Asociatividad)

* Existe $e \in G$ tal que $a \cdot e = e \cdot a \forall a \in G$ (Identidad)

* $\forall a \in G$ existe $a^{-1} \in G$, tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$ (Inversos)

Entonces se dice que $(G, \cdot)$, o simplemente G, es un grupo. Si además se cumple que $a \cdot b = b \cdot a$, $\forall \; a, b \in G$, entonces se dice que G es un grupo abeliano.

Definición 2.2 Sea R un conjunto no vacío, si existen dos operaciones binarias, $+, \cdot : G \times G \to G$, tal que $(R, +)$ es un grupo abeliano y ademas cumple

* $a, b \in G \to a \cdot b \in G \; \forall a, b \in G$, (Cerradura en $\cdot$)

* $a, b, c \in G \to (a \cdot b) \cdot c = a \cdot (b \cdot C)$ (Asociatividad en $\cdot$)

* $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a \; \forall a, b, c \in R$ (Distributividad)

Entonces se dice que $(R, +, \cdot)$, o simplemente R, es un anillo, Si además se cumple que $a \cdot b = b \cdot a \forall a, b \in R$, entonces se dice que G es un anillo conmutativo.

Un anillo al tener dos operaciones es difícil identificar el elemento neutro, por lo que al elemento neutro de la operación $+$, se denota como $0 \in R$, y al elemento neutro de la operación $\cdot$ (si es que este existe) se denota como $1 \in R$

Definición 2.3 Sea R un anillo, tal que $(R \setminus \{0\}, \cdot)$ es un grupo, se llama un anillo de división.

Definición 2.4 Sea R un anillo, con 1 su identidad multiplicativa, y M un conjunto no vacío, se dice que M es un $R-$modulo izquierdo, si M consiste de un grupo abeliano $(M, +)$ y una operación $\cdot : R \times M \to M$ tal que para todo $r, s \in R$ y $a, b \in M$ se cumple

* $r \cdot (a + b) = r \cdot a + r \cdot b$

* $(r + s) \cdot a = r \cdot a + s \cdot a$

* $(rs) \cdot a = r \cdot (s \cdot a)$

* $1 \cdot a = a$

Definición 2.5 Sea A y R anillos, tal que $R \subset A$, Si A es un $R-$modulo izquierdo y además $\forall a, b \in A$, $r \in R$ se cumple que :

$$r(ab) = (ra)b.$$

Entonces se dice que A es un $R-$álgebra, o bien A es un álgebra sobre R.

Definición 2.6 Sea A un $R-$álgebra y $B \subset A$. Si $\forall a \in A$ existen únicos $b_1, b_2, b_3, ...b_n \in B$, $r_1, r_2, r_3, ...r_n \in R$ tal que $a = \sum_{i=1}^{n} r_i b_i$, entonces se dice que B es una $R-$base para A, o que B es una base para A sobre R. Si además B está formado únicamente de elementos invertibles, entonces se dice que B es una $R-$base invertible de A, y también que A es un $R-$álgebra invertible.

Definición 2.7 Sea A un $R-$álgebra y B una base invertible de A. Se dice que B es una base I2, si $B^{-1} = \{b^{-1} | b \in B\}$ también es una base para A. Si A tiene una base I2, entonces se dice que A es un R-álgebra I2.

3 Una clasificación de álgebras invertibles

En esta sección se proporcionará de otras propiedades a las bases de álgebras invertibles para clasificarlas.

Definición 3.1 Sea A un álgebra sobre un anillo R y sea B una base invertible para A sobre B.

* Si $\forall v \in B$ existe $\alpha \in U(R)$ tal que $\alpha v^{-1} \in B$, entonces se dice que B es una base SCUI (scalarly closed under inverses). Un álgebra con una base SCUI es un álgebra SCUI. Si B es una base SCUI tal que $\alpha = 1$ para todo $v \in B$, entonces se dice que B es CUI (closed under inverses). Un álgebra con una base CUI es un álgebra CUI.

* Si $\forall v, w \in B$ existe $\alpha \in U(R)$ tal que $\alpha vw \in B$, entonces se dice que B es una base SCUP (scalarly closed under products). Un álgebra con una base SCUP es un álgebra SCUP. Si B es una base SCUP tal que $\alpha = 1$ $\forall v, w \in B$, entonces B se dice que es una base CUP (closed under products). Un álgebra con una base CUP es un álgebra CUP.

* Si B es una base SCUI, CUI, SCUP o CUP y además $1_R \in B$, entonces B es una base SCUI1, CUI1, SCUP1 o CUP1 respectivamente.

Ejemplo: Considérese el campo de extensión $\mathbb{C}$ sobre $\mathbb{R}$. $\mathcal{B} = \{1, i\}$ es una $\mathcal{R}-$base para $\mathcal{C}$. Es fácil ver qué $\mathcal{B}$ es una base SCUP y una base SCUI.

Proposición 3.2 Sea A un álgebra sobre un anillo R con B una base SCUP. Entonces $|B \cap U(R)| = 1$, y A tiene una base $SCUP1$. Si B es una base CUP, entonces $1 \in B$.

Demostración: Sea $B = \{b_i\}_{i \in I}$ una base para A sobre R (I es el conjunto de subíndices de la base), sea $1 \in A$, existen $b_1, b_2, ..., b_k \in B$, $\alpha_1, \alpha_2, ..., \alpha_k \in R$ tal que $1 = \sum_{j=1}^{k} \alpha_j b_j$, sea $b \in B$, multiplicando la ecuación anterior por la izquierda por b se obtiene $b = \sum_{j=1}^{k} \alpha_j b_j b$.

Sea A un álgebra SCUP, entonces $\forall b_i \in B$ existe $v_i \in U(R)$ tal que $v_i b_i b \in B$, es decir $v_i b_i b = b_{n_i} \in B$, en particular esto se cumple para $i \in \{1, 2, 3, ..., k\}$, entonces $b = \sum_{j=1}^{k} (\alpha_j v_j^{-1})(v_j b_j b) = \sum_{j=1}^{k} (\alpha_j v_j^{-1})(b_{n_j})$, v_j^{-1} existe ya que $v_j \in U(R)$. Debido a que cada elemento de A puede ser expresado de manera única como combinación lineal de elementos de la base B, existe $r \in \{1, 2, 3, ..., k\}$ tal que $b = (\alpha_r v_r^{-1})(b_{n_r})$, de esto, $1_R = \alpha_r v_r^{-1}$, $b = v_r b_r b$, de donde $b_r^{-1} = v_r \in U(R)$, $b_r \in B \cap U(R) \to B \cap U(R) \neq \emptyset$. Sean $b_{m_1}, b_{m_2} \in B \cap U(R)$, entonces $b_{m_1}^{-1}, b_{m_2}^{-1} \in U(R) \subseteq R$, luego

$1 = b_{m_1}^{-1} b_{m_1}$, $1_R = b_{m_2}^{-1} b_{m_2}$, como 1 tiene representación única, $b_{m_1} = b_{m_2}$, entonces $|B \cap U(R)| = 1$. Es claro que $B' = b_r^{-1} B = \{b_r^{-1} b_i\}_{i \in I}$, es una base SCUP para A, y $1 \in B'$. B' es una base SCUP1.

Supóngase que A es un álgebra CUP, entonces $\forall b_i \in B$ se cumple $b_i b \in B$, es decir $b_i b = b_{n_i} \in B$, en particular esto se cumple para $i \in \{1, 2, 3, ..., k\}$, entonces $b = \sum_{j=1}^{k} (\alpha_j)(b_j b) = \sum_{j=1}^{k} (\alpha_j)(b_{n_j})$, debido a que cada elemento de A puede ser expresado de manera única como combinación lineal de elementos de la base B, existe $r \in \{1, 2, 3, ..., k\}$ tal que $b = (\alpha_r)(b_{n_r})$, de esto, $1 = \alpha_r$, $b = b_r b$, de donde $1 = b_r \in B$■

Proposición 3.3 Sea A un álgebra sobre un anillo R con una base SCUP B, entonces B es también una base SCUI. Si B es una base CUP, entonces B es una base CUI, y B forma un grupo bajo la multiplicación en A.

Demostración Supóngase que B es una base SCUP, sea $b \in B$, b^{-1} existe y $b^{-1} \in A$, es decir existen $\alpha_1, \alpha_2, ...\alpha_k \in R$, $b_1, b_2, ..., b_k \in B$ tal que $b^{-1} = \sum_{j=1}^{k} \alpha_j b_j$, multiplicando a la izquierda por b se tiene $1 = \sum_{j=1}^{k} \alpha_j b_j b$, como B es una base SCUP, existe $c_j \in U(R)$ tal que $c_j b_j b \in B$, es decir $1 = \sum_{j=1}^{k} (\alpha_j c_j^{-1})(c_j b_j b_i)$, sea $b_r \in B \cap U(R)$, de esto, existe $s \in \{1, 2, 3, ..., k\}$ tal que $b_r^{-1} = \alpha_S c_s^{-1}$, $b_r = c_s b_s b_i$ entonces $c_s^{-1} b_r b_i^{-1} = b_s \in B$, además $c_s^{-1}, b_r \in U(R)$, entonces $c_s^{-1} b_r \in U(R)$, esto es $\forall b \in B$, entonces B es una base SCUI.

Sea B es una base CUP, sea $b \in B$, b^{-1} existe y $b^{-1} \in A$, es decir existen $\alpha_1, \alpha_2, ...\alpha_k \in R$, $b_1, b_2, ..., b_k \in B$ tal que $b^{-1} = \sum_{j=1}^{k} \alpha_j b_j$ multiplicando a la izquierda por b se tiene $1 = \sum_{j=1}^{k} \alpha_j b_j b$, como B es una base CUP entonces $b_j b \in B$, es decir $1 = \sum_{j=1}^{k} (\alpha_j)(b_j b)$, sea $1 \in B \cap U(R)$ (proposición 2.2), entonces existe $s \in \{1, 2, 3, ..., k\}$ tal que $1 = \alpha_S$, $1 = b_s b$ entonces $b^{-1} = b_s \in B$, y esto es $\forall b \in B$ entonces B es una base CUI. Considérese la estructura $(B, \cdot)$, esta estructura es asociativa, esto de hereda de la asociatividad de A. Es cerrado, esto es por ser una base CUP, $1 \in B$ y 1 es el neutro multiplicativo, por último, para todo $b \in B$, $b^{-1} \in B$ que demuestra la existencia de inversos multiplicativos, por lo que $(B, \cdot)$ es un grupo■

Definición 3.4 Sean R un anillo con identidad y G un grupo. Entonces el **producto cruz** $R*G$ es un anillo asociativo con $\overline{G}$ una R-base para $R*G$ ($\overline{G}$ es una copia de G). La multiplicación está determinada por las siguientes reglas.

* Para todo $x, y \in G$ existe una unidad $\tau(x, y) \in U(R)$ tal que $\overline{x}\ \overline{y} = \tau(x, y)\overline{xy}$.

* Para todo $x \in G$ existe $\sigma_x \in Aut(R)$ tal que para todo $r \in R$, $\overline{x} r = \sigma_x(r)\overline{x}$

Definición 3.5 Sea A un álgebra sobre un anillo R, y B una R-base para A. Si $\forall v \in B$ existe $\sigma_v \in Aut(R)$ tal que $\forall r \in R$, $vr = \sigma_v(r)v$, entonces se dice que R conmuta escalarmente con B. En el caso que $\forall v \in B$, $\sigma_v = 1$, se dice que R conmuta con B

Proposición 3.6 Sea A un álgebra sobre un anillo R. A es un producto cruz si y solo si A tiene una base SCUP que conmuta escalarmente con R.

Demostración ($\rightarrow$) Supóngase que A es un producto cruz, por definición, A tiene una R-base $\overline{G}$ tal que, si $\overline{x}, \overline{y} \in \overline{G}$ entonces existe $\tau(x,y) \in U(R)$ tal que $\overline{x}\ \overline{y} = \tau(x,y)\overline{xy}$, es decir $\tau(x,y)^{-1}\overline{x}\ \overline{y} = \overline{xy} \in \overline{G}$, entonces $\overline{G}$ es SCUP. Además $\forall x \in \overline{G}$ existe $\sigma_x \in Aut(R)$ tal que $\forall r \in R$ se tiene, $xr = \sigma_x(r)x$ entonces $\overline{G}$ conmuta escalarmente con R.

($\leftarrow$) Supóngase que A tiene una base SCUP B que conmuta escalarmente con R. Por la proposición 2.1 tenemos que existe $b \in B \cap U(R)$, sea $C = \{1_R\} \cup B \setminus \{b\}$, es claro que C es una base para A sobre R, como B conmuta escalarmente con R, y C tiene exactamente los mismos elementos que B, a excepción de b que fue cambiado por 1 , sin embargo ambos se encuentran en $U(R)$ por lo tanto 1 conmuta escalarmente con R, entonces C conmuta escalarmente con R, además $1 \in C$. Para $v, w \in C$ existen $\alpha_{v,w} \in U(R)$ y $z_{v,w} \in C$ tal que $vw = \alpha_{v,w} z_{v,w}$. Definamos $\star : C \times C \rightarrow C$ tal que $\star : (v,w) \rightarrow z$. Solo falta mostrar que $(C, \star)$ es un grupo.

Por la construcción $(C, \star)$ es cerrada, además $\star(1,v) = \star(v,1) = v$ ya que $1v \in C$, entonces $(C, \star)$ tiene elemento neutro. Como C es una base SCUI (proposición 2.2), para todo $v \in C$ existe $\alpha_v \in U(R)$, $w \in C$ tal que $\alpha_v v^{-1} = w$, además $\star(w,v) = z_{v,w}$ pero $\alpha_v = \alpha_v v^{-1} v = wv = \alpha_{w,v} z_{v,w}$ de esto, $z_{v,w} = \alpha_v \alpha_{w,v}^{-1} \in B \in U(R)$, entonces $z = 1$, es decir v, w son inversos. Ahora considérese $v, w, r \in C \subseteq A$, como A es asociativo entonces $(vw)r = v(wr)$, además $vw = \alpha_{v,w}(v \star w)$, para algún $\alpha_{v,w} \in U(R)$ (esto es por la cosntrucción de $\star$), entonces $(vw)r = \alpha_{v,w}(v \star w)r = \alpha_{v,w}\alpha_{v\star w,r}((v \star w) \star r))$ con $\alpha_{v \star w, r} \in U(R)$, por otro lado $v(wr) = v\alpha_{w,r}(w \star r)$ Como B conmuta escalarmente con R, existe $\sigma_v \in Aut(R)$ tal que, $v\alpha_{w,r}(w \star r) = \sigma_v(\alpha_{w,r})v(w \star r) = \sigma_v(\alpha_{w,r})\alpha_{v,w\star r}(v \star (w \star r))$, de donde $\alpha_{v,w}\alpha_{v\star w,r}((v \star w) \star r)) = \sigma_v(\alpha_{w,r})\alpha_{v,w\star r}(v \star (w \star r))$, con $\alpha_{v,w}, \alpha_{v\star w,r}, \sigma_v(\alpha_{w,r}), \alpha_{v,w\star r} \in R$ y $(v \star (w \star r)), ((v \star w) \star r)) \in C$, C una base de A sobre R, entonces las representaciones de cada elemento de A como combinación lineal de elementos de C es única, por lo que $(v \star (w \star r)) = ((v \star w) \star r))$ Por lo que $(C, \star)$ es asociativa, esto demuestra que $(C, \star)$ es un grupo. De donde A es un producto cruz ■

Ahora que se tienen diferentes tipos de álgebras invertibles. La proposición 3.3 dice que si A es un $R-$álgebra CUP, entonces A es un $R-$álgebra CUI. Sin embargo, el converso no es cierto. Los siguientes ejemplos muestran casos similares al anterior.

* Un álgebra I2 que no es un álgebra SCUI: Sea $A = \frac{\mathbb{F}_3[x,y]}{\langle x^2, y^2, xy \rangle}$. Y sea $U(A) = \{\alpha + \beta x + \gamma y | \alpha, \beta, \gamma \in \mathbb{F}_3, \alpha \neq 0\}$, el grupo de unidades de A. Es claro que si $a \in U(A)$ entonces $a^{-1} = (\alpha + \beta x + \gamma y)^{-1} = \alpha - \beta x - \gamma y$. Una base I2 para A es $\{1 + x, 1 + y, 1 + x + y\}$. Sea $\mathcal{B} = \{v, w, u\}$ una base SCUI para A, entonces existen $\delta_1, \delta_2, \delta_3 \in U(\mathbb{F}_3)$, tal que $\delta_1 v^{-1}, \delta_2 w^{-1}, \delta_3 u^{-1} \in \mathcal{B}$. Si $\delta_1 v^{-1} = v$, entonces $v^2 = \delta_1, v = \pm 1$. Si $\delta_1 v^{-1} = w$, entonces $\delta_2 w^{-1} = v$ y $\delta_3 u^{-1} = u$, de donde $u^2 = \delta_3$, $u = \pm 1$, es otro caso es equivalente a este.

En cualquiera de los casos anteriores $\pm 1 \in \mathcal{B}$,sin pérdida de generalidad $1 \in \mathcal{B}$, entonces $\mathcal{B} = \{1, v, \delta v^{-1}$, sea $v = \alpha + \beta x + \gamma y$, entonces $\delta v^{-1} = \delta\alpha - \delta\beta x - \delta\gamma y$, por lo que

$$1(v) + \delta(\delta v^{-1}) + \alpha(1) = 0$$

$\mathcal{B}$ es linealmente independiente. $\mathcal{B}$ no es una base para A. A no es un álgebra SCUI.

* Un álgebra CUI que no es un álgebra CUI1: Sea $A = M_2(\mathbb{F}_2)$. La proposición 3.6 dice que A es un álgebra CUI. A consiste de 16 elementos, 6 de estos son unidades, revisando los 10 conjuntos B tal que B está formado por unidades y $1 \in B$ es fácil ver qué B no es una CUI base. A no es un álgebra CUI1.

* Un álgebra CUI1 que no es un álgebra CUP: Considérese $A = \frac{\mathbb{F}_2[x,y]}{\langle x^2, y^2, xy\rangle}$. Es fácil ver qué $U(A) = \{1, 1+x, 1+y, 1+x+y\}$, además si B es una base, entonces $|B| = 3$, dado que el cuadrado de una unidad es 1, y el producto de dos unidades distintas a 1, es la tercera unidad distinta a 1. Ninguna base es CUP. A no es un álgebra CUP.

4 Anillos de matrices

Sabemos que para cualquier anillo R, el anillo matriz $A = M_n(R)$ (para $n \geq 1$) es un R-álgebra I2. En esta sección se buscarán mas resultados como este.

Proposición 4.1 Sea A un álgebra sobre un anillo R con una base B tal que $1 \in B$. Entonces $M_n(A)$ es un álgebra I2 sobre R para $n \geq 2$.

Demostración : Para $1 \leq i, j \leq n$, considérese e_{ij} la matriz con valor 1 en la entrada (i, j), y 0 en el resto de entradas. Sea I_n la matriz identidad, es decir 1 en las entradas (i, i) con $1 \leq i \leq n$ y 0 en las entradas (i, j) con $1 \leq i, j \leq n$, $j \neq i$. Para $1 \leq k \leq n-1$, sea $P_k = I_n - e_{k,k} - e_{k+1,k+1} + e_{k,k+1} + e_{k+1,k}$, P_k es la matriz que se obtiene al intercambiar las filas k y $k+1$ de la matriz identidad I_n. Para $b \in \mathcal{B}$, $1 \leq i, j \leq n$, $i \neq j$ sea $v_{ijb} = I_n + e_{ij}b$. Para $b \in \mathcal{B}$, $1 \leq i \leq n-1$ sea $e_{iib} = P_i + e_{ii}b$. Para $b \in \mathcal{B} \setminus \{1_R\}$, $v_{nnb} = P_{n-1} + e_{nn}b$ y $v_{nn1} = I_n$. Sea $\mathcal{V} = \{v_{ijb} | 1 \leq i, j \leq n, b \in \mathcal{B}\}$, se demostrará que $\mathcal{V}$ es una base $I2$ para $M_n(A)$ sobre R.

Si $1 \leq i, j \leq n$ y $i \neq j$ entonces $v_{ij1} = I_n + e_{ij}1 \Rightarrow e_{ij} = v_{ij1} - I_n = v_{ij1} - v_{nn1} \in gen(\mathcal{V})$, además para $2 \leq k \leq n$ $v_{nn1} + e_{k,k-1} + e_{k-1,k} - v_{k-1,k-1,1} \in gen(\mathcal{V})$ y $v_{nn1_R} + e_{k,k-1} + e_{k-1,k} - v_{k-1,k-1,1} = I_n + e_{k,k-1} + e_{k-1,k} - (P_{k-1} + e_{k-1,k-1}) = I_n + e_{k,k-1} + e_{k-1,k} - (In - e_{k-1,k-1} - e_{k,k} + e_{k-1,k} + e_{k,k-1} + e_{k-1,k-1}) = e_{k,k}$, por otro lado $v_{11} = v_{nn1} - \sum_{i=2}^{n} e_{ii} \in gen(\mathcal{V})$ por lo que $e_{ij} \in gen(\mathcal{V})$ para $1 \leq i, j \leq n$, y $P_k = I_n - e_{k,k} - e_{k+1,k+1} + e_{k,k+1} + e_{k+1,k} \in gen(\mathcal{V})$ para $1 \leq k \leq n-1$. Si $1 \leq i, j \leq n$ con $i \neq j$ es claro que $e_{ij}b = I_n - v_{ijb} \in gen(\mathcal{V})$, $\forall b \in \mathcal{B}$, si $1 \leq i \leq n-1$ $e_{ii}b = v_{iib} - p_i \in gen(\mathcal{V})$, si $b \in \mathcal{B} \setminus \{1\}$ $e_{nn}b = v_{nn}b - P_{n-1} \in gen(\mathcal{V})$, y $e_{nn}1 = e_{nn} \in gen(\mathcal{V})$. De donde $e_{ij}b \in gen(\mathcal{V})$ $\forall b \in \mathcal{B}$ y $1 \leq i, j \leq n$. Por lo que $\mathcal{V}$ genera a $M_n(A)$.

Supóngase que

$$\sum_{b \in \mathcal{B}, 1 \leq i,j \leq b} r_{ijb} v_{ijb} = 0$$

Sean $1 \leq k, m \leq n$, $[v_{ijb}]_{k,m}$ toma únicamente tres valores $b, 1, 0$, y si $b \in \mathcal{B} \setminus \{1\}$ entonces $[v_{ijb}]_{k,m} = b \Leftrightarrow k = i, m = j$. Dado que la suma anterior es una suma de matrices, considerando solamente la entrada (k, m) de cada matriz, la suma anterior se convierte en $\sum_{b \in \mathcal{B}, 1 \leq i,j \leq n} r_{ijb} [v_{ijb}]_{k,m} = 0$, pero esto se puede reescribir como $(\sum_{b \in \mathcal{B} \setminus \{1\}} r_{kmb} b) + x_{km} 1 = 0$ para algún $x \in R$. Dado que $\mathcal{B}$ es linealmente independiente $r_{kmb} = 0, x_{km} = 0$, para $1 \leq k, m \leq n$. Por lo que la suma se convierte en:

$$\sum_{1 \leq i,j \leq n} r_{ij1} v_{ij1} = 0$$

Nuevamente, se está trabajando con una suma de matrices, considérese la entrada $(1,1)$ y la entrada (k,k) para $2 \le k \le n$, primero es fácil ver qué $[v_{ij1_R}]_{11} = 1$ para todo $1 \le i,j \le n$, además $[v_{ij1}]_{kk} = 1$ para todo $1 \le i,j \le n$ excepto para $i = j = k-1$, donde $[v_{k-1,k-1,1}]_{kk} = 0$ entonces evaluando $(1,1)$ y (k,k) tenemos

$$\sum_{1 \le i,j \le n} r_{ij1} = 0$$

y

$$\left[\sum_{1 \le i,j \le n} r_{ij1} \right] - r_{k-1,k-1,1} = 0$$

De esto es claro que $r_{k-1,k-1,1} = 0$ para $2 \le k \le n$, Considérese la entrada (k,m) con $k \neq m$, los elementos de la forma v_{ii1} $i \neq n$ no se consideran ya que $r_{ii1} = 0$, Luego es fácil ver qué $[v_{ij1_R}]_{k,m} = 0$ para todo $i \neq j$ con $(i,j) \neq (k,m)$ y $[v_{ij1_R}]_{k,m} = 1$ cuando $(i,j) = (k,m)$, por último $v_{nn1} = I_n$ por lo que $[v_{nn1}]_{k,m} = 0$, con esto se tiene que $r_{ij1} = 0$ para $1 \le i,j \le n$ y $i \neq j$. Solo falta calcular el valor de r_{nn1} sin embargo $\sum_{1 \le i,j \le n} r_{ij1} = 0$, entonces $r_{nn1} = 0$ por lo que $\mathcal{V}$ es linealmente independiente, por lo que es una base para $M_n(A)$.

Es fácil ver que si $b \in \mathcal{B}$ entonces $v_{ijb}^{-1} = I_n - e_{ij}b = v_{ij-b}$ para $1 \le i,j \le n$ $i \neq j$, si $1 \le i \le n-1$ entonces $v_{iib}^{-1} = P_i - e_{k+1,k+1}b$, si $b \neq 1_R$ entonces $v_{nnb}^{-1} = v_{n-1,n-1,-b}$, por ultimo $v_{nn1_R}^{-1} = v_{nn1_R}$. Es fácil probar con los argumentos anteriores que el conjunto $\mathcal{V}^{-1} = \{a^{-1} | a \in \mathcal{V}\}$ es también base para $M_n(A)$. Por lo que $\mathcal{A}$ resulta ser una base I2 para $M_n(A)$ sobre R■

Corolario 4.2 Invertibilidad no es una invariante de Morita.

Demostración : El resultado es directo de la proposición 4.1, A no necesariamente es invertible sobre R para que $M_n(A)$ sea invertible sobre R■

Definición 4.3 Sea R un anillo y sea A un R-álgebra invertible. Entonces A es "bueno " si $A \oplus B$ es invertible sobre R para cualquier R-álgebra invertible B.

Proposición 4.4 Sea A un álgebra sobre un anillo R con una base $\mathcal{A}$, tal que $1 \in \mathcal{A}$. Entonces para $n \ge 2$, $M_n(A)$ es bueno. Además, si B es un R-álgebra I2, entonces $M_k(A) \oplus B$ es también I2.

Demostración: Sea $\mathcal{B}$ base invertible de B, considérese $\mathcal{V} = \{v_{ija} | 1 \le i,j \le n, a \in \mathcal{A}\}$ base I2 de $M_n(A)$ (La base que se construyó en la proposición 4.1).

Sea $b' \in \mathcal{B}$ y S una matriz invertible, con entradas unos y ceros únicamente, y la diagonal con ceros. Sea

$$\mathcal{C} = \{\mathcal{V} \times \{b'\}\} \cup \{\{I_n\} \times \mathcal{B} \setminus \{b'\}\} \cup \{(S, b')\}$$

Es fácil ver qué $\mathcal{C}$ está formado por elementos invertibles.

Solo falta mostrar que $\mathcal{C}$ es una base invertible de $M_n(A) \oplus B$.

Supóngase que

$$r_S(S,b')+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}(v_{ija},b')+\sum_{b\in\mathcal{B}\setminus\{b'\}} r_{nn1b}(I_n,b)=0$$

para $r_{ijab'}, r_{ijab}, r_S \in R$. Por las propiedades de suma directa, la igualdad anterior se reescribe como

$$\left(r_S S+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}v_{ija}+\sum_{b\in\mathcal{B}\setminus\{b'\}} r_{nn1b}I_n, r_S b'+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}b'+\sum_{b\in\mathcal{B}\setminus\{b'\}} r_{nn1b}b\right)=(0,0)$$

por lo que se obtiene dos ecuaciones :

$$b'\left[r_S+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}\right]+\sum_{b\in\mathcal{B}\setminus\{b'\}} r_{nn1b}b=0 \tag{4.1}$$

$$r_S S+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}v_{ija}+\sum_{b\in\mathcal{B}\setminus\{b'\}} r_{nn1b}I_n=0 \tag{4.2}$$

De la ecuación 4.1, como $\mathcal{B}$ es una base, entonces $r_{nn1b}=0\forall b\in\mathcal{B}\setminus\{b'\}$ y $r_S+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}=0$, despejando r_S queda $r_S=\sum_{1\leq i,j\leq n,a\in\mathcal{A}}(-r_{ijab'})$.

La ecuación 4.2 queda como $r_S S+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}v_{ija}=0$, sustituyendo r_S se obtiene $\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}(v_{ija}-S)=0$, con el mismo argumento usado en la proposición anterior (al estudiar los coeficientes de $\sum_{b\in\mathcal{B},1\leq i,j\leq b} r_{ijb}v_{ijb}=0$), se tiene que $r_{ijab'}=0$ y $r_{ii1b'}=0$ para $1\leq i,j\leq n$ y $a\in\mathcal{A}\setminus\{1_R\}$, entonces la ecuación 2) queda como $r_S S+\sum_{1\leq i,j\leq n,i\neq j} r_{ij1b'}v_{ij1}=0$, esta es una suma de matrices, considerando la entrada (1, 1) de la suma se obtiene $\sum_{1\leq i,j\leq n,i\neq j} r_{ij1b'}=0$.

Además

$$0=r_S+\sum_{1\leq i,j\leq n,a\in\mathcal{A}} r_{ijab'}=r_S+\sum_{1\leq i,j\leq n,i\neq j} r_{ij1b'}=r_S$$

Volviendo a la ecuación 4.2, como $r_S=0, r_{nn1b}=0\forall b\in\mathcal{B}\setminus\{b'\}$, la ecuación 4.2 queda reescrita como $sum_{1\leq i,j\leq n,a\in\mathcal{A}}r_{ijab'}v_{ija}=0$, y como $\mathcal{V}$ es una base, entonces $r_{ijab'}=0$ para $1\leq i,j\leq n$ y $\forall a\in\mathcal{A}$ por lo que $\mathcal{C}$ es linealmente independiente.

Nótese que para $i\neq j$, $(e_{ij},0)=(v_{ij1},b')-(I_n,b')$, y para $2\leq k\leq n$ se tiene

$$(e_{ii},0)=(I_n,b')-[(v_{i-1,i-1,1},b')-(e_{i-1,i},0)-(e_{i,i-1},0)]$$

Como S tiene entrada 0 en (1, 1) entonces $(0,b')=(S,b')-\sum_{i,j}(e_{ij},0)$ donde (i,j) son las coordenadas donde S tiene entrada 1, $(e_{11},0)=(I,b')-(0,b')-(\sum_{i=2}^{n}(e_i i,0))$. Y por último $(0,b)=(I_n,b)-(In,b')+(0,b')$. Por lo que $(e_{ij},0),(0,b)\in gen(\mathcal{C})$ para $1\leq i,j\leq n$ y $b\in\mathcal{B}$. $\mathcal{C}$ genera a $M_n(A)$ entonces $\mathcal{C}$ es una base para $M_n(A)\oplus B$. Si B es una base I2, claramente $\mathcal{C}$

también será una base I2, ya que $\mathcal{A}$ es una base I2$\blacksquare$.

La única condición en la proposición 4.1 para obtener que $M_n(A)$ es un álgebra I2 sobre R es que A tiene una base B tal que $1 \in B$, si se agregan algunas condiciones extras sobre R, A, o n se puede dar más resultados sobre $M_n(A)$.

Proposición 4.5 Sea A un álgebra sobre un anillo R con una base $\mathcal{A}$ tal que $1 \in \mathcal{A}$. Si n es par y $char(A) = 2$. Entonces $M_n(A)$ es un álgebra CUI sobre R.

Demostración Considérese e_{ij} las matrices con 1_R en la entrada (i,j), y 0 en el resto de entradas. Sea $P_{2k-1} = P_{2k} = I_n - e_{2k,2k} - e_{2k-1,2k-1} + e_{2k,2k-1} + e_{2k-1,2k}$, para $1 \leq i,j \leq n$, $i \neq j$, $a \in \mathcal{A}$, $v_{ija} = I_n + e_{ij}a$, y $v_{iia} = P_i + e_{ii}a$. Sea $\mathcal{V} = \{v_{ija} | 1 \leq i,j \leq n, a \in \mathcal{A}\}$. Se mostrará que $\mathcal{V}$ es una CUI base para $M_n(A)$.

Dado que $char(A) = 2$, $1+1 = 0 \to 1 = -1$, además $a + a = 0, \forall a \in \mathcal{A}$, es decir $a = -a, \forall a \in \mathcal{A}$. Considérese $\sum_{k=1}^{n/2}(v_{2k-1,2k-1,1} - v_{2k,2k,1}) = \sum_{k=1}^{n/2}(P_{2k-1} + e_{2k-1,2k-1} - P_{2k,2k} - e_{2k,2k}) = \sum_{k=1}^{n/2}(e_{2k-1,2k-1} - e_{2k,2k}) = \sum_{k=1}^{n/2}(e_{2k-1,2k-1} + e_{2k,2k}) = I_n$ de donde I_n es generado por $\mathcal{V}$ Por lo que si $i \neq j$ y $1 \leq i,j \leq n$ y $a \in \mathcal{A}$ entonces $e_{ij}b = v_{ijb} - I_n$ por lo que los $e_{i,j}$ perteneces al generado por $\mathcal{V}$ para $i \neq j$, $1 \leq i,j \leq n$. Para cualquier k tal que $1 \leq k \leq n$ se tiene $e_{k,k} = I_n - [v_{k-1.k-1,1} - e_{k-1,k} - e_{k,k-1}]$, esto implica que P_i es generado por $\mathcal{V}$, y de esto $e_{ii}a = v_{iia} - P_i$, por lo que si $1 \leq i,j \leq n$ y $a \in \mathcal{A}$ entonces $e_{ij}a \in gen(\mathcal{V})$. Entonces $\mathcal{V}$ genera a $M_n(A)$.

Considérese

$$\sum_{a \in \mathcal{A}, 1 \leq i,j \leq n} r_{ija} v_{ija} = 0$$

para algunos $r_{ija} \in R$. La suma anterior, es una suma de matrices, consideremos la entrada (k,m), $[v_{ija}]_{k,m}$ toma unicamente tres valores $1, 0, a$ y es claro que $[v_{ija}]_{k,m} = a$ si y solo si $i = k, j = m$. Por lo que la suma en la entrada (k,m) quedaría como $\sum_{a \in \mathcal{A} \setminus \{1\}} r_{k,m,a}a + x_{k,m} * 1 = 0$. Por la independencia lineal de $\mathcal{A}$, tenemos que $r_{k,m,a} = x_{k,m} = 0$ para todo $a \in \mathcal{A} \setminus \{1\}$, $1 \leq k,m \leq n$, la suma quedaría como $\sum_{1 \leq i,j \leq n} v_{ij1} v_{ij1} = 0$. Ahora bien si nuevamente se toma la entrada (k,m) de la última suma, sabemos que $[v_{ij1}]_{k,m}$ puede tomar unicamente 2 valores $1, 0$, sin embargo las entradas de si $|k - m| > 1$, $(k,m) = (2r, 2r+1)$ o $(i,j) = (2r+1, 2r)$ para algún r, entonces $[v_{ij1}]_{k,m} = 0$ excepto cuando $i = k, j = m$ por lo que $r_{k,m,1} = 0$ para todo k,m tal que $|k - m| > 1$, o $(k,m) = (2r, 2r+1)$ o $(i,j) = (2r+1, 2r)$. Ahora la suma se simplifica a:

$$\sum_{1 \leq k \leq n/2} r_{2k-1,2k-1,1} v_{2k-1,2k-1,1} + r_{2k,2k,1} v_{2k,2k,1} + r_{2k,2k-1,1} v_{2k,2k-1,1} + r_{2k-1,2k,1} v_{2k-1,2k,1} = 0$$

Sean $1 \leq k_1, k_2 \leq n$ con k_1 impar y k_2 par, considérese las entradas (k_1+1, k_1+1), $(k_2-1, k_2-1, 1)$

y $(2,2)$ de la suma $\sum_{1\leq i,j\leq n} v_{ij1}v_{ij1} = 0$, por la construcción de las v_{ij1} se tiene que :

$$\sum_{1\leq i,j\leq n} r_{ij1} - r_{k_1,k_1,1} = 0$$

$$\sum_{1\leq i,j\leq n} r_{ij1} - r_{k_2,k_2,1} = 0$$

$$\sum_{1\leq i,j\leq n} r_{ij1} - r_{1,1,1} = 0$$

Esto muestra que $r_{k_1,r_1,1} = r_{k_2,r_2,1} = r_{111}$, si se observa la entrada $(2k, 2k-1)$ de la suma, se obtiene $r_{2k,2k-1,1} + r_{2k-1,2k-1,1} + r_{2k,2k,1} = 0$, entonces $r_{2k,2k-1,1} = -2r_{2k-1,2k-1,1} = -2r_{111} = 0$ y de la misma manera se puede mostrar que $r_{2k-1,2k,1} = -2r_{111} = 0$. Además la $\sum_{1\leq i,j\leq n} r_{ij1} - r_{1,1,1} = 0$ se puede reescribir como

$$0 = \left[\sum_{1\leq k\leq n/2} r_{2k-1,2k-1,1} + r_{2k,2k,1} + r_{2k,2k-1,1} + r_{2k-1,2k,1}\right] - r_{111} = -(n+1)r_{111} = -nr_{111} - r_{111} = -r_{111}$$

Dado que $char(R) = 2$ y n es par. por lo que $r_{ija} = 0$ para todo $1 \leq i, j, \leq n$, y para todo $a \in \mathcal{A}$. Al ser $\mathcal{V}$ generador de $M_n(A)$ y también ser linealmente independiente, se puede concluir que $\mathcal{V}$ es una base para $M_n(A)$. Es fácil probar que $v_{ija}^{-1} = v_{ijb}$ cuando $i \neq j$ y que $v_{2k-1,2k-1,b}^{-1} = v_{2k,2k,b}$, para $1 \leq i, j \leq n$, $1 \leq k \leq n/2$ y $a \in \mathcal{A}$ esto es porque $a = -a$, entonces $\mathcal{V}$ es una CUI base para $M_n(A)$ sobre R■

Proposición 4.6 Para todo n, $M_n(\mathbb{F}_2)$ es un álgebra CUI sobre $\mathbb{F}_2$. Para n impar, $M_n(\mathbb{F}_2)$ es un álgebra CUI1 sobre $\mathbb{F}_2$.

Demostración Se demuestra por casos

Caso I : Si n es par, es claro que $char(\mathbb{F}_2) = 2$, usando la proposición 4.5, con $R = A = \mathbb{F}_2$ es claro que $M_n(A)$ es un algebra CUI sobre $\mathbb{F}_2$

Caso II: Si n es impar, considérese e_{ij} las matrices con 1_R en la entrada (i, j), y $0's$ en el resto de entradas. Para $1 \leq k \leq \frac{n-1}{2}$ sea $P_{2k-1} = P_{2k} = I_n - e_{2k,2k} - e_{2k-1,2k-1} + e_{2k,2k-1} + e_{2k-1,2k}$, para $1 \leq i, j \leq n$, $i \neq j$, $v_{ij} = I_n + e_{ij}$, y si $r < n$ $v_{rr} = P_r + e_{rr}$. Sea $\mathcal{V} = \{v_{ij} | 1 \leq i, j \leq n\}$. Se mostrará que $\mathcal{V}$ es una CUI1 base para $M_n(\mathbb{F}_2)$.

Si $i \neq j$ entonces $e_{ij} = v_{ij} - I_n$ de esto $e_{ij} \in gen(\mathcal{V})$, además

$$e_{2k,2k} = I_n - (v_{2k-1,2k-1} - e_{2k,2k-1} - e_{2k-1,2k})$$

$$e_{2k-1,2k-1} = I_n - (v_{2k,2k} - e_{2k-1.2k} - e_{2k,2k-1}$$

para $1 \leq k \leq \frac{n-1}{2}$, de esto $e_{ii} \in gen(\mathcal{V})$ para $1 \leq i \leq \frac{n-1}{2}$, por ultimo $e_{nn} = I_n - \sum_{i=1}^{n-1} e_{ii}$ por lo que $e_{ij} \in gen(\mathcal{V})$ para todo $1 \leq i, j \leq n$. De esto $\mathcal{V}$ genera a $M_n(\mathbb{F}_2)$. Por otro lado $|\mathcal{V}| = n^2$, de esto $\mathcal{V}$ es una base para $M_n(\mathbb{F}_2)$, además si $i \neq j$, $v_{ij}^{-1} = v_{ij}$, si $1 \leq k \leq \frac{n-1}{2}$ entonces y $v_{2k,2k}^{-1} = v_{2k-1,2k-1}$ y $v_{nn}^{-1} = v_{nn}$ por lo que $\mathcal{V}$ es una CUI base, ademas $I_n \in \mathcal{V}$ por lo que $\mathcal{V}$ es una base CUI1 de $M_n(\mathbb{F}_2)$ sobre $\mathbb{F}_2$ ■

Proposición 4.7 Sea R un anillo tal que 2 es invertible en R. Entonces $M_n(R)$ es un álgebra CUI1 sobre R.

Demostración Considérese $v_{nn} = I_n$. Para $1 \leq i, j \leq n$, $v_{ii} = v_{nn} - 2e_{ii}$, si $i > j$ entonces $v_{ij} = v_{jj} + e_{ij}$ y por ultimo si $i < j$ entonces $v_{ij} = v_{ii} + e_{ij}$, sea $\mathcal{V} = \{v_{ij} | 1 \leq i, j \leq n\}$. Sea 2^{-1} el inverso multiplicativo de 2, es claro que $e_{ii} = 2^{-1}(v_{nn} - v_{ii})$, por lo que $e_{ii} \in gen(\mathcal{V})$, si $i > j$ entonces $e_{ij} = v_{ij} - v_{jj}$, y si $i < j$ entonces $e_{ij} = v_{ij} - v_{ii}$, de esto $e_{ij} \in \mathcal{V}$ para $1 \leq i, j \leq n$. Por lo que $\mathcal{V}$ genera a $M_n R$ sobre R.

Ahora supóngase que

$$\sum_{1 \leq i,j \leq n} r_{ij} v_{ij} = 0$$

para algunos $r_{ij} \in R$, es una suma de matrices, si se considera la entrada (k, m) de la suma con $k \neq m$, se puede observar que $[v_{ij}]_{km}$ toma solo dos valores $0, 1$ y $[v_{ij}]_{km} = 1$ si y solo si $i = k, j = m$, entonces $0 = \sum_{1 \leq i,j \leq n} r_{ij}[v_{ij}]_{km} = r_{km}$, entonces $r_{km} = 0$ para todo $1 \leq k, m \leq n$, $k \neq m$. Ahora bien si $1 \leq k \leq n-1$, y se considera las entradas (k, k) y (n, n) de la suma, es claro que $[v_{ij}]_{nn} = 1]$, entonces la suma quedaría como $0 = \sum_{1 \leq i \leq n} r_{ii} = r_{kk} + \sum_{1 \leq i \leq n, i \neq k} r_{ii}$, además si $1 \leq k \leq n-1$ entonces $[v_{ii}]_{kk} = 1$ excepto para $i = k$ ya que $[v_{kk}]_{kk} = -1$, de esto $0 = \sum_{1 \leq i \leq n} r_{ii}[v_{ii}]_{kk} = 2r_{kk} + \sum_{1 \leq i \leq n, i \neq k} r_{ii}$, de esto $r_{kk} = 0$ para $1 \leq k \leq n-1$, entonces $r_{nn} = 0$. Por lo que $\mathcal{V}$ es una base para $M_n(R)$, y $I_n \in \mathcal{V}$, $v_{ij}^{-1} = v_{ij}$ para $1 \leq i, j \leq n$. Entonces $\mathcal{V}$ es una base CUI1 de $M_n(R)$ sobre R■

Ejemplo $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right\}$. es una CUI1 base para $M_2(\mathbb{F}_3)$

5 Álgebras Finito-dimensionales

En la mayor parte de esta sección se restringe la atención a las algebras sobre anillos de división D. Así como se caracterizan de invertibilidad semilocal D-álgebras. Sin embargo, los métodos utilizados para las demostraciones de las propiedades se encuentran fuera del alcance de un estudiante de licenciatura, por lo que en esta sección se omiten varias de las demostraciones.

Lema 5.1 Sea R un anillo tal que 1 es la suma de dos unidades y sean A y B álgebras invertibles sobre R. Entonces $A \oplus B$ es un álgebra invertible sobre R.

Demostración Sean $x, 1-x \in U(R)$, $\mathcal{A}$ R-base invertible de A, $\mathcal{B}$ R-base invertible de B, $a_1 \in \mathcal{A}$, $b_1 \in \mathcal{B}$. Considérese

$$\mathcal{C} = (\mathcal{A}, b_1) \cup (a_1, \mathcal{B} \setminus \{b_1\}) \cup \{(a_1, xb_1)\}$$

Es fácil ver que todos los elementos de $\mathcal{C}$ son invertibles. Ahora sea

$$\sum_{a\in\mathcal{A}} \alpha_a(a, b_1) + \sum_{b\in\mathcal{B}\setminus\{b_1\}} \beta_b(a_1, b) + \gamma(a_1, xb_1) = 0$$

Es decir que

$$\left(x\gamma + \sum_{a\in\mathcal{A}} \alpha_a\right) b_1 + \sum_{b\in\mathcal{B}\setminus\{b_1\}} \beta_b b = 0$$

y

$$\left(\alpha_{a_1} + \gamma + \sum_{b\in\mathcal{B}\setminus\{b_1\}} \beta_b\right) a_1 + \sum_{a\in\mathcal{A}\setminus\{a_1\}} \alpha_a a = 0$$

Dado que $\mathcal{B}$ y $\mathcal{A}$ son bases entonces $\alpha_a = 0\ \forall a \in \mathcal{A}\setminus\{a_1\}$, $\beta_b = 0\ \forall b \in \mathcal{B}\setminus\{b_1\}$, y $(x\gamma+\alpha_{a_1})b_1 = 0$, $(\alpha_{a_1} + \gamma)a_1 = 0$. Por lo que $\alpha_{a_1} = \gamma = 0$. $\mathcal{C}$ es linealmente independiente. Además se tiene

$$(\mathcal{A}, b_1) - [(1-x)^{-1}(a_1, b_1) - (1-x)^{-1}(a_1, xb_1)] = (\mathcal{A}, b_1) - (1-x)^{-1}[(a_1, b_1) - (a_1, xb_1)] =$$

$$(\mathcal{A}, b_1) - (1-x)^{-1}[(0, (1-x)b_1)] = (\mathcal{A}, b_1) - (0, b_1) = (\mathcal{A}, 0)$$

Todos los elementos de la forma $(\mathcal{A}, 0)$ pueden ser generados, por lo tanto, los elementos de la forma $(0, \mathcal{B})$ también pueden ser generados. $\mathcal{C}$ es una R-base invertible de $A \oplus B$ ■

Proposición 5.2 Sea D un anillo de división y sea A una semilocal $D-$álgebra. Si $D \neq \mathbb{F}_2$ entonces A es invertible. Si $D = \mathbb{F}_2$, entonces A es invertible si y solo si A no admite un epimosfismo algebraico a $\mathbb{F}_1 \oplus \mathbb{F}_2$.

Cuando A es finito-dimensional sobre D, se puede concluir más cosas.

Proposición 5.3 Sea D un anillo de división y sea A un D-álgebra finito-dimensional. Si $D \neq \mathbb{F}_2$, entonces A es I2. Si $D = \mathbb{F}_1$, entonces A es I2 si y solo si A no admite un epimosfismo algebraico a $\mathbb{F}_1 \oplus \mathbb{F}_2$.

La siguiente proposición para equivalente a la proposición 5.2, sin embargo, esta no necesita que R sea un anillo de división.

Proposición 5.4 Sea R un anillo y sea A un álgebra local libre. Entonces A es invertible.

6 Álgebras invertibles Infinito-dimensionales

Después de trabajar con álgebras finito-dimensionales, es natural pensar en estudiar álgebras infinito-dimensionales. En esta sección se vuelve a las álgebras que son generados por anillos arbitrarios, no se restringe a anillos de división como la sección anterior. Existen varios ejemplos de álgebras invertibles infinito-dimensionales, los grupos anillos son ejemplos de álgebras invertibles y en particular si el grupo es infinito, los grupos anillos generados por este serían álgebras invertibles infinito-dimensionales. Así como cualquier extensión de un anillo de división infinito también es un álgebra invertible infinito-dimensional. El siguiente ejemplo es importante ya que este provee una base invertible que no es I2.

Ejemplo Sea L un campo. Considérese el F-álgebra $F(x)$, el campo de las funciones racionales sobre F. Nótese que:

$$\mathcal{G} = \left\{ \frac{x^n}{f(x)} | n \in \{0, 1, 2, ...\}, f(x) \in F[x] \setminus \{0\} \right\}$$

genera a $F(x)$. Ademas $\mathcal{G}^{-1} \subset F[x, x^{-1}]$. De esto se puede concluir que $\mathcal{G}$ no genera a $F(x)$, entonces si B es una base invertible contenida en $\mathcal{G}$, B no es I2.

Lema 6.1 Sea A_0, A_1, A_2 anillos tal que A_2 es un álgebra invertible sobre A_1 con una A_1-base invertible B_2 y A_1 es un álgebra invertible sobre A_0 con una A_0-base invertible B_1. Entonces A_2 es un A_0-álgebra invertible y B_1B_2 es una A_0-base invertible para A_2.

Demostración Por definición $B_1B_2 = \{b_1b_2 | b_1 \in B_1, b_2 \in B_2\}$, como b_1, b_2 son invertibles entonces existen $b_1^{-1} \in A_1$, $b_2^{-1} \in A_2$ tal que $b_1b_1^{-1} = b_2b_2^{-1} = 1$, entonces si $b_1b_2 \in B_1B_2$, tome $b_2^{-1}b_1^{-1} \in A_2$, es claro que $b_1b_2b_2^{-1}b_1^{-1} = 1$, entonces los elementos de B_1B_2 son invertibles.

Sea $a \in A_2$, como A_2 es un A_1-álgebra entonces existen $c_i \in A_1$, $b_{2_i} \in B_2$ tal que $a = \sum_{i=1}^{n} c_i b_{2_i}$, además A_1 es un A_0-álgebra entonces existen $c_{ij} \in A_0$, $b_{1_j} \in B_1$ tal que $c_i = \sum_{j=1}^{n_i} c_{ij} b_{1_j}$, de esto

$$a = \sum_{i=1}^{n} \sum_{j=1}^{n_i} c_{ij} b_{2_i} b_{1_j}$$

donde $b_{2_i} b_{1_j} \in B_1B_2$,entonces B_1B_2 genera a A_2 sobre A_0.

Luego sea

$$\sum_{b_{1_i}\in B_1, b_{2_j}\in B_2} c_{ij} b_{1_i} b_{2_j} = 0$$

sea $c_j = \sum_{b_{1_i}\in B_1} c_{ij} b_{1_i}$ entonces

$$\sum_{b_{2_j}\in B_2} c_j b_{2_j} = \sum_{b_{1_i}\in B_1, b_{2_j}\in B_2} c_{ij} b_{1_i} b_{2_j} = 0$$

como B_2 es una base, entonces es linealmente independiente, de donde $c_j = 0$, de esto $c_j = \sum_{b_{1_i}\in B_1} c_{ij} b_{1_i} = 0$, por la independencia lineal de B_1, se tiene que $c_{ij} = 0$ para todo i, j, entonces $B_1 B_2$ es linealmente independiente. A_2 es un A_0-álgebra invertible y $B_1 B_2$ es una A_0-base invertible para A_2 ■

Proposición 6.2 Sea $A_0, A_1, ...$ una cadena de anillos tal que para $i \geq 1$, A_i es un álgebra invertible sobre A_{i-1}. Entonces $A = \cup_{i\geq 1} A_1$ es un A_0-álgebra invertible.

Demostración Sea B_i una $A_{i=1}$-base invertible para A_i, tal que $1 \in B_i$ (Existe por ser A_i un álgebra invertible sobre A_{i-1}), Sea $C_i = B_1 B_2 ... B_i$, como $1 \in B_i$ entonces $C_1 \subset C_2 \subset ....$ Por el lema 5.1 C_i es una A_0-base invertible para A_i, de esto si se toma $C = \cup_{i\geq 1} C_i$, C genera a A, además C es invertible ya que si $c \in C$, entonces existe $l \geq 1$ tal que $c \in C_l$ y como C_l es invertible, entonces c tiene inverso multiplicativo, por lo que C es invertible. Sea $\sum_{i=1}^{n} r_i c_i = 0$ tal que $n \in \mathbb{N}$, $r_i \in A_0$, $c_i \in C$. Entonces existe un C_l tal que $c_i \in C_l$ para $i = 1, 2, 3..., n$ y como C_l es una A_0-base para A_l entonces C_l es linealmente independiente. De esto $r_i = 0$ para $i = 1, 2, 3..., n$. Entonces C es linealmente independiente, de donde C es una A_0-base invertible de A■

Corolario 6.3 Sea $A_0, A_1, ...$ una cadena de anillos tal que para $i \geq 1$, A_i es un álgebra invertible sobre A_{i-1} con una A_{i-1}-base I2 que conmuta con todos los elementos de A_{i-1}. Entonces $A = \cup_{i\geq 1} A_1$ es un A_0-álgebra I2.

Demostración Sea B_i una A_{i-1}-base I2 para A_i, tal que $1 \in B_i$ y tal que conmuta con los elementos de A_{i-1} (existe por las hipótesis del corolario). Sea $C_i = B_1 B_2 ... B_i$, como $1 \in B_i$ entonces $C_1 \subset C_2 \subset ....$ Sea $C = \cup_{i\geq 1} C_i$, por la proposición 5.2, C es una A_0-base invertible para A. Sea $D_i = B_1^{-1} B_2^{-1} ... B_i^{-1}$, como $1 \in B_i^{-1}$ entonces $D_1 \subset D_2 \subset ....$ Sea $D = \cup_{i\geq 1} D_i$, sabiendo que B_i^{-1} es una A_0-base invertible para A (dado que B_i es una A_0-base I2 para A), por la proposición 5.2, D es una A_0-base invertible para A. Sea $c \in C$, existen $v_i \in B_i$ tal que $v = v_1 v_2 ... v_l$ para algún l. Entonces $v^{-1} = v_l^{-1} ... v_2^{-1} v_1^{-1} \in C^{-1}$. luego $v^{-1} = v_l^{-1} ... v_2^{-1} v_1^{-1} = (v_1 v_2 ... v_l)^{-1} = (v_l ... v_2 v_1)^{-1}$ esto es cierto gracias a que B_i conmuta con todos los elementos de A_{i-1}. De donde $v^{-1} = v_1^{-1} v_2^{-1} ... v_l^{-1} \in D$, entonces $C^{-1} \subset D$. De manera similar se puede probar que $D \subset C^{-1}$. Por lo que C es una A_0-base I2 para A■

En el corolario anterior si se remplaza la hipótesis de ser una base I2, por una base CUI1, SCUI1 o SCUP, usando argumentos similares se pueden llegar a los mismos resultados.

Corolario 6.4 Sea R un anillo y sea

$$A = \left\{ \begin{bmatrix} X & 0 & 0 & ... \\ 0 & X & 0 & ... \\ 0 & 0 & X & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | X \in M_n(R), n \geq 1 \right\}$$

entonces A es un $R-$álgebra invertible.

Demostración Sean $p_1, p_2, ...$ el conjunto de todos los números primos. Se define $n_0 = 1$, y si $i > 1$, $n_i = (p_1 p_2 ... p_i)^i$, $q_i = \frac{n_i}{n_{i-1}}$, es decir $n_i = q_i n_{i-1}$. Para $i \geq 0$ sean

$$A_i = \left\{ \begin{bmatrix} X & 0 & 0 & ... \\ 0 & X & 0 & ... \\ 0 & 0 & X & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | X \in M_{n_i}(R) \right\}$$

$$A_i = \left\{ \begin{bmatrix} X & 0 & 0 & ... \\ 0 & X & 0 & ... \\ 0 & 0 & X & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | X \in M_{q_i n_{i-1}}(R) \right\}$$

$$A_i = \left\{ \begin{bmatrix} X & 0 & 0 & ... \\ 0 & X & 0 & ... \\ 0 & 0 & X & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | X \in M_{q_i}(M_{n_{i-1}}(R)) \right\}$$

De estas igualdades es claro que $A_0 \subseteq A_1 \subseteq A_2 \subseteq ...$, como $A_i \in A$ $\forall i \geq 0$, entonces $\cup_{i \geq 0} A_i \subseteq A$. Sea $B \in A$, por la definición de A, existe $k \in \mathbb{N}$ tal que

$$B = \left\{ \begin{bmatrix} B_1 & 0 & 0 & ... \\ 0 & B_1 & 0 & ... \\ 0 & 0 & B_1 & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | B_1 \in M_k(R) \right\}$$

Además $k \in \mathbb{N}$ entonces k tiene factorización en números primos, sea $k = \prod_{j=11}^{r} p_j^{m_j}$, para algunos $r, m_j \in \mathbb{N}$. Sea $t = \max\{r, m_1, m_2, ..., m_j\}$, entonces $n_t = (p_1 p_2 ... p_t)^t$, de donde $k | n_t$, por lo que

$B \in A_t$, $A \subseteq \cup_{i\geq 0} A_i$. Esto demuestra que $A = \cup_{i\geq 0} A_i$, como $A_i = M_{n_i}(R)$, por la proposición 3.1, $M_{n_{i+1}}(R) = M_{q_{i+1}}(M_{n_i}(R))$ es invertible sobre $M_{n_i}(R)$. Esto significa que para $i \geq 0$ A_{i+1} es invertible sobre A_i, la proposición 5.2 asegura que A es un $R-$álgebra invertible■

Proposición 6.5 Sea R un anillo y sea

$$A = \left\{ \begin{bmatrix} X & 0 & 0 & \dots \\ 0 & r & 0 & \dots \\ 0 & 0 & r & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | n \in \mathbb{N}, X \in M_n(R), r \in R \right\}$$

entonces A es un $R-$álgebra invertible.

Demostración Sea I la matriz identidad de A. Para $i, j \in \mathbb{N}$, si $i \neq j$, sea $v_{ij} = I + e_{ij}$, $e_{ii} = I - e_{ii} + e_{i,i+1} + e_{i+1,i}$. Sea $B = \{I\} \cup \{v_{ij} | i, j \in \mathbb{N}\}$. Se debe probar que B es una base invertible. Primero si $i \neq j$ entonces $v_{ij}^{-1} = I - e_{ij}$, y $v_{ii}^{-1} = v_{ii} - e_{ii} - e_{i+1,i+1}$, B es invertible. Además si $i \neq j$ entonces $e_{ij} = v_{ij} - I$, $e_{ii} = I - v_{ii} + e_{i,i+1} + e_{i+1,i}$, y si

$$C = \left\{ \begin{bmatrix} X & 0 & 0 & \dots \\ 0 & r & 0 & \dots \\ 0 & 0 & r & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} | n \in \mathbb{N}, X \in M_n(R), X = 0, r \in R \right\}$$

entonces $C = r(I - \sum_{i=1}^{n} e_{ii})$. De esto, B genera a A sobre R.
Supóngase que para $1 \leq i, j \leq n$, $r, r_{ij} \in \mathbb{R}$ se tiene

$$rI + \sum_{1 \leq i,j \leq n} r_{ij} v_{ij} = 0$$

Para $1 \leq k \leq n$, considere las entrada (k,k) y $(n+1, n+1)$ de la suma de matrices. La suma queda como:

$$r + \sum_{1 \leq i,j \leq n} r_{ij} - r_{kk} = 0$$

y

$$r + \sum_{1 \leq i,j \leq n} r_{ij} = 0$$

Esto demuestra que para $1 \leq k \leq n$, $r_{kk} = 0$, ahora bien si se considera nuevamente la entrada (i, j) con $i \neq j$, se obtiene fácilmente que $r_{ij} = 0$. Por último $r = 0$ ya que $r_{ij} = 0$ para todo $1 \leq i, j \leq n$. De esto B es una base invertible de A sobre R■

7 Conclusiones

- Trabajar con la nueva definicón de R-álgebra resulta un poco más complicado, sin embargo los resultados son más generales, y se cumplen también para la deficinión usual de R-álgebra.
- Los R-álgebras invertibles presentan propiedades y características que suelen encontrarse en estructuras matemáticas ya conocidas, aún cuando estos no han sido estudiados profundamente debido a ser recientemente introducidos.
- Exigir que la base del R-álgebra sea formado únicamente por elementos con inversos, da oportunidad a un estudio más profundo y detallado de álgebras.
- Existen R-álgebras invertibles que solo pueden ser generadas por una base con infinitos elementos, ejemplos de estos R-álgebras son los R-álgebras presentados en las proposiciones 6.4 y 6.5.
- Para asegurar que $M_n(A)$ es un R-álgebra I2, solo se necesita construir las matrices con R-álgebras A que tiene una base con unidad.

8 Bibliografía

G. Abrams and G. Aranda Pino, 2005. *The Leavitt path algebra of a graph*, Journal of Algebra, 293, 319-334.

I.N. Herstein, 1964. *Topics in Algebra*, 12^a ed. E.E.U.U , Xerox Corporation. 388 págs.

Sergio R. López-Permouth, Jeremy Moore, Nick Pilewski, Steve Szabo, 2015. *Algebras having bases that consist solely of units* ,Israel Journal of Mathematics,208, 461-482.

Sergio R. López-Permouth, J. Moore, N. Pilewski and S. Szabo. *Units and linear Independence.* Articulo por sumitir.

Sergio R. López-Permouth, Jeremy Moore, Steve Szabo, 2009. *Algebras Having Bases consisting entirely of units*, American Mathematical Society, 499, 219-228.