Aplicación del Algebra Lineal a la deducción de propiedades de la Sucesión de Fibonacci.

Víctor Juan Hernández Del Toro

Trabajo de grado
Para optar al título de matemático

Asesor
Julio Cesar Hernández Arzusa

Universidad de Cartagena
Facultad de Ciencias Exactas y Naturales
Programa de Matemáticas

Cartagena de Indias D. T. y C.

Marzo de 2011

Dedico este trabajo a la memoria de un gran amigo,
Rafael Alberto Escobar Rodriguez.

Doy gracias a Dios por haberme permitido alcanzar este logro,
a mis padres, mi familia por su apoyo incondicional, y
a todos los amigos que me apoyaron de un modo u otro.

Índice general

Introducción

El álgebra es una de las ramas de la matemática que tiene más aplicabilidad a otras áreas de la misma matemática. En este trabajo se muestra una aplicación del álgebra básica a las propiedades de una de las sucesiones de mayor importancia de la matemática, la sucesión de Fibonacci. Se llama sucesión de Fibonacci a la sucesión definida por la fórmula de recurrencia $F_{n+2} = aF_{n+1} + bF_n$ donde a, b son números reales fijos, y $F_0 = 0$ y $F_1 = 1$. Posteriormente se define un espacio $C(a, b)$, $b \neq 0$ que consta de todas las sucesiones con fórmula de recurrencia $A_{n+2} = aA_{n+1} + bA_n$, donde a, b son reales fijos y A_0, A_1 son complejos dados. También se definen los operadores $\Lambda : C^\infty \longrightarrow C^\infty$ como $(\Lambda(A))_n = A_{n+1}$ y $\Omega_k : C^\infty \longrightarrow C^\infty$ como $(\Omega_k(A))_n = A_{nk}$, donde $k = 1, 2, 3, ...$ y C^∞ es el espacio de todas las sucesiones con valor complejos, que serán de suma importancia en el trabajo. Del Operador Λ se deducirá:

$$\begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^k = \begin{bmatrix} bF_{k-1} & F_k \\ bF_k & F_{k+1} \end{bmatrix}.$$

Este resultado es consecuencia de la representación matricial del operador Λ en la base $\{E, F\}$ de $C(a, b)$, donde $E_0 = 1, E_1 = 1$ y $F_0 = 0, F_1 = 1$. Si se igualan los determinantes de estas matrices se tiene que $(-1)^k b^k = bF_{k-1}F_{k+1} - bF_k^2$. Para hallar fórmulas explícitas de las sucesiones de $C(a, b)$ se encuentran las coordenadas de $A \in C(a, b)$ en $\{E, F\}$. El resto de propiedades serán deducidas a partir de Ω_k.

Capítulo 1

Conceptos Preliminares

En este capítulo se establecen algunas definiciones y notaciones básicas, necesarias para la comprensión de este trabajo.

1.1. Espacios Vectoriales

Definición 1. *Sea V un conjunto no vacío y F un campo. Se consideran dos operaciones, una entre elementos de V, que se simboliza por $+$ y una entre un elemento de V y uno de F que se simboliza por $\cdot$, que gozan de las siguentes propiedades:*

Para $x, y, z \in V$ y $\alpha, \beta \in F$ se cumple:

i. $x + y \in V$, $\alpha \cdot x \in V$.

ii. $x + y = y + x$.

iii. $(x + y) + z = x + (y + z)$, $(\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x)$.

iv. $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$, $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$.

v. *Existe un elemento en V que se simboliza por 0 tal que para todo $x \in V$ se tiene que $x + 0 = x$.*

vi. *Para cada* $x \in V$ *existe un elemento de* V*, que se simboliza por* $-x$*, tal que* $x + (-x) = 0$.

vii. *Para el* $1 \in F$ *se tiene que* $1 \cdot x = x$.

Se dice entonces que V es un *Espacio Vectorial* sobre el Campo F.

Definición 2. *Sea* $W \subseteq V$*,* $W \neq \phi$*, donde* V *es un Espacio Vectorial sobre el Campo* F*. Si* W *con las operaciones heredadas de* V *es un Espacio Vectorial sobre* F*, entonces se dice que* W *es un Subespacio Vectorial de* V*.*

Teorema 1. *Sea* V *un Espacio Vectorial sobre el Campo* F*. Sea* $W \subseteq V$*,* $W \neq \phi$*.* W *es Subespacio de* V *si y solo si* $\alpha \cdot x + \beta \cdot y \in W$ *para todo* $x, y \in W$ *y todo* $\alpha, \beta \in F$*.*

Definición 3. *Sea* V *un Espacio Vectorial sobre un Campo* F*. Una Combinación Lineal de elementos de* V *es una expresión de la forma* $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n$*, donde los* $x_i \in V$ *y* $\alpha_i \in F$*, para* $i = 1, 2, ..., n$*.*

Definición 4. *Sea* V *un Espacio Vectorial. Un conjunto de vectores* $\{x_1, x_2, ..., x_n\}$ *de* V*, se dice que es Linealmente Independiente si* $\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n = 0$ *implica que* $\alpha_i = 0$ $(i = 1, 2, ..., n)$*, donde los* α_i *son elementos del Campo.*

Definición 5. *Sea* V *un Espacio Vectorial sobre el Campo* F *y* $\phi \neq M \subseteq V$*. Sea* $\{x_1, x_2, ..., x_n\}$ *un conjunto de vectores de* M*. Se dice que* M *es generado por* $\{x_1, x_2, ..., x_n\}$ *si todo elemento de* M *se puede escribir como Combinación Lineal de elementos de* $\{x_1, x_2, ..., x_n\}$*.*

Definición 6. *Sea* V *un Espacio Vectorial sobre el campo* F*. A un conjunto de vectores* $\{x_1, x_2, ..., x_n\}$ *Linealmente Independientes de* V *se le dice que es una Base para* V *si genera a* V*.*

Teorema 2. *Todas las Bases de un Espacio Vectorial tienen el mismo número de elementos.*

Un Espacio Vectorial tiene dimensión n si tiene una Base de n elementos.

NOTA: De ahora en adelante el producto $\alpha \cdot x$, donde α es escalar y x es vector, se denota αx. El lector debe estar en capacidad de diferenciarlo del producto definido entre elementos del Campo.

1.2. Transformaciones Lineales

Definición 7. *Sean V y S dos Espacios Vectoriales sobre el mismo Campo F. Una transformación lineal de V en S es una función T de V en S tal que $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$, para todo α, β en F y todo x, y en V.*

Definición 8. *Si V es un espacio vectorial sobre el Campo F, un Operador lineal es una transformación lineal de V en V.*

Definición 9. *Sea $T : V \longmapsto S$ una Transformación Lineal. El conjunto $\{x \in V \mid T(x) = 0\}$ se llama el Kernel de T y se simboliza por $Ker(T)$.*

Teorema 3. *Si $T : V \longmapsto S$ es una Transformación Lineal, entonces $Ker(T)$ es un Subespacio Vectorial de V.*

1.3. Valores propios

Definición 10. *Sea $T : V \longmapsto S$ una Transformació Lineal. Un escalar λ se le llama un $Valor$ Propio o Autovalor de T si existe un elemento x no nulo de V tal que $T(x) = \lambda x$. Al elemento x se le llama $Vector$ propio de T y al escalar λ Valor propio asociado a x.*

Teorema 4. *Sea $T : V \longmapsto S$ una Transformació Lineal y $x_1, x_2, ..., x_n$ vectores propios de T y $\lambda_1, \lambda_2, ..., \lambda_n$ los Autovalores correspondientes asociados. Si dichos Autovalores son distintos, entonces $\{x_1, x_2, ..., x_n\}$ es Linealmente Independientes.*

1.4. Otros simbolos y propiedades

Se simboliza el Máximo Común Divisor de dos números enteros no nulos m y n por $M.C.D(m, n)$.

Teorema 5. *$M.C.D(tn, tm) = t \cdot M.C.D(n, m)$ donde t es un entero positivo.*

Teorema 6. *Si m y n son enteros tales que $M.C.D(m, n) = k$,entonces existen dos enteros r y s únicos tales que $rm + sn = k$.*

Definición 11. *Sean m,n dos enteros, y p un número entero primo positivo. Se dice que m es equivalente módulo p a n si $m - n$ es divisible por p,se nota por $[m] \equiv [n]$.*

NOTA: Recuerde que $[mn] = [m][n]$ y $[m + n] = [m] + [n]$.

Capítulo 2

Sucesión de Fibonacci

Definición 12. *Una sucesión de Fibonacci, es una sucesión F, cuya fórmula de recurrencia está dada por $F_{n+2} = aF_{n+1} + bF_n$, donde $F_0 = 0, F_1 = 1$ y a, b son reales, $b \neq 0$.*

Se denota $C(a, b)$, donde $b \neq 0$, como el conjunto de todas las sucesiones con fórmula de recurrencia $A_{n+2} = aA_{n+1} + bA_n$ donde A_0 y A_1 son complejos dados y a, b son reales.

Ejemplo 1. *En $C(4, 2)$ la Sucesión de Fibonacci es* $0, 1, 2, 10, 44, ...$

Ejemplo 2. *En $C(-2, 2)$ la Sucesión de Fibonacci es* $0, 1, -2, 6, -16, ...$

Ejemplo 3. *En $C(5, 5)$ la Sucesión de Fibonacci es* $0, 1, 5, 30, 175, ...$

Ejemplo 4. *En $C(11, -10)$ la Sucesión de Fibonacci es* $0, 1, 11, 111, ...$

Ejemplo 5. *En $C(2, 1)$ la Sucesión de Fibonacci es la sucesión de Pell* $0, 1, 2, 5, 12, 29, ...$

Ejemplo 6. *En $C(3, -2)$ la Sucesión de Fibonacci es* $0, 1, 3, 7, 15, 31, ...$

Se denota C^∞ como el Espacio Vectorial de todas las sucesiones complejas sobre C, cuya suma de vectores será la suma usual de sucesiones y la multiplicación de un vector por un escalar será la multiplicación usual de una sucesión por un complejo.

Sean $A, B \in C^\infty$ tales que $A = B$. De la definición de igualdad de sucesiones se tiene que $A_{n+1} = B_{n+1}$ y $A_{nk} = B_{nk}$, para k entero positivo.

Este hecho permite establecer la siguiente definición.

Definición 13. *Se definen funciones como:*

i. $\Lambda : C^\infty \longrightarrow C^\infty$ *por* $(\Lambda(A))_n = A_{n+1}$.

ii. $\Omega_k : C^\infty \longrightarrow C^\infty$ *por* $(\Omega_k(A))_n = A_{nk}$, *donde* $k = 1, 2, 3, ...$

La siguiente proposición muestra que las funciones anteriormente definidas son Operadores Lineales.

Proposición 1. *Las funciones* Λ *y* Ω_k *son Operadores Lineales sobre* C^∞.

Demostración. Sean $A, B \in C^\infty$ y $\alpha, \beta \in C$. Entonces:

i. Λ es un Operador Lineal. En efecto:

$$\begin{aligned}(\Lambda(\alpha A + \beta B))_n &= (\alpha A + \beta B)_{n+1} \\ &= \alpha A_{n+1} + \beta B_{n+1} \\ &= \alpha(\Lambda(A))_n + \beta(\Lambda(B))_n \\ &= (\alpha\Lambda(A) + \beta\Lambda(B))_n.\end{aligned}$$

Esto prueba que $\Lambda(\alpha A + \beta B) = \alpha\Lambda(A) + \beta\Lambda(B)$.

ii. Ω_k es un Operador Lineal. En efecto:

$$
\begin{aligned}
(\Omega_k(\alpha A+\beta B))_n &= (\alpha A+\beta B)_{nk} \\
&= \alpha A_{nk}+\beta B_{nk} \\
&= \alpha(\Omega_k(A))_n+\beta(\Omega_k(B))_n \\
&= (\alpha\Omega_k(A)+\beta\Omega_k(B))_n.
\end{aligned}
$$

Esto prueba que $\Omega_k(\alpha A+\beta B)=\alpha\Omega_k(A)+\beta\Omega_k(B)$.

□

Proposición 2. *$C(a,b)$ es Subespacio Vectorial de C^∞.*

Demostración. $A\in C(a,b)$ si y solo si $A_{n+2}=aA_{n+1}+bA_n$, esto es $A_{n+2}-aA_{n+1}-bA_n=0$, lo que a su vez es:

$$(\Lambda^2(A))_n-a(\Lambda(A))_n-bA_n=0$$

$$(\Lambda^2(A)-a\Lambda(A)-bA)_n=0$$

$$((\Lambda^2-a\Lambda-b)(A))_n=0.$$

Esto muestra que $(\Lambda^2-a\Lambda-b)(A)=0$, es decir que $C(a,b)$ es el Kernel del Operador $\Lambda^2-a\Lambda-b$ y por tanto Subespacio de C^∞.

□

NOTA: Se simboliza la compuesta $\Lambda\Lambda$ por Λ^2.

Proposición 3. *El subespacio $C(a,b)$ tienen dimensión dos.*

Demostración. Sean $F, E \in C(a,b)$ donde $F_0 = 0, F_1 = 1$ y $E_0 = 1, E_1 = 0$. El conjunto $\{E, F\}$ forma una base para $C(a,b)$. En efecto:
Es fácil ver que estos elementos son linealmente independientes, pués, si $\alpha F + \beta E = 0$, entonces $\alpha F_0 + \beta E_0 = 0$ asi $\alpha \cdot 0 + \beta \cdot 1 = \beta = 0$. También $\alpha F_1 + \beta E_1 = 0$, de igual modo tenemos que $\alpha \cdot 1 + \beta \cdot 0 = \alpha = 0$.

A continuación se demuestra que $A \in C(a,b)$ implica $A = A_0 E + A_1 F$. Este hecho se prueba por inducción. $A_0 = A_0 \cdot 1 + A_1 \cdot 0 = A_0 E_0 + A_1 F_0$. Asúmase que se cumple $A_k = A_0 E_k + A_1 F_k$ para $k \leq n$. Entonces:

$$\begin{aligned} A_{n+1} = aA_n + bA_{n-1} &= a(A_0 E_n + A_1 F_n) + b(A_0 E_{n-1} + A_1 F_{n-1}) \\ &= A_0(aE_n + bE_{n-1}) + A_1(aF_n + bF_{n-1}) \\ &= A_0 E_{n+1} + A_1 F_{n+1}. \end{aligned}$$

□

2.1. Fórmulas de Binet

En esta sección se encuentran fórmulas explicitas para las sucesiones de $C(a,b)$. Sea B, $B_n = \lambda^n$. Observe que $(\Lambda(B))_n = B_{n+1} = \lambda \cdot \lambda^n$, esto es, $\Lambda(B) = \lambda B$. Esto muestra que una sucesión geométrica es un Vector Propio de Λ. Ahora se buscan condiciones para que una sucesión geométrica pertenezca a $C(a,b)$. Si esta sucesión pertenece al Kernel de $\Lambda^2 - a\Lambda - b$ entonces pertenece al espacio $C(a,b)$. Por tanto

$$(\Lambda^2 - a\Lambda - b)(B) = 0$$

$$(\Lambda^2(B))_n - a\Lambda(B)_n - bB_n = 0$$

$$\lambda^{n+2} - a\lambda^n - b\lambda^n = 0$$

$$\lambda^2 - a\lambda - b = 0.$$

El hecho $b \neq 0$ excluye el caso $\lambda \neq 0$, pués si $\lambda = 0$ en la ecuación entoces $b = 0$ contradiciendo $b \neq 0$. Todo se reduce a resolver la ecuación $\lambda^2 - a\lambda - b = 0$.

Si λ y μ son soluciones distintas de esta ecuación, entonces $\{E, B\}$ es una base para $C(a, b)$, donde $E_n = \mu^n, B_n = \lambda^n$. Es decir, si $A \in C(a, b)$, entonces existen constantes c_λ, c_μ tales que $A_n = c_\lambda \lambda^n + c_\mu \mu^n$. Para determinar las constantes c_λ, c_μ se hace uso de $A_0 = c_\lambda + c_\mu$ y $A_1 = c_\lambda \lambda + c_\mu \mu$, resolviendo tenemos que

$$\begin{aligned} c_\lambda &= \frac{A_1 - \mu A_0}{\lambda - \mu} \\ c_\mu &= \frac{\lambda A_0 - A_1}{\lambda - \mu}. \end{aligned}$$

Si $\lambda = \mu$, entonces $\{E, B\}$, donde $E_n = n\lambda^n$ y $B_n = \lambda^n$, es una Base para $C(a, b)$.
$\{E, B\}$ es Linealmente Independiente. En efecto; Si $cE + dB = 0$ entonces $cE_0 + dB_0 = 0$ luego $d = 0$, por la forma como se define E y B, además $cE_1 + 0B_1 = 0$ lo cual implica que $c\lambda = 0$, así $c = 0$, pués $\lambda \neq 0$.
Para terminar la prueba, bastaría probar que las sucesiones están en $C(a, b)$.

B está en $C(a, b)$ ya que

$$\lambda^2 - a\lambda - b = 0$$

$$\lambda^{n+2} - a\lambda^{n+1} - b\lambda^n = 0$$

$$(\Lambda^2(B))_n - a(\Lambda(B))_n - bB_n = 0$$

$$((\Lambda^2 - a\Lambda - b)(B))_n = 0$$

$$(\Lambda^2 - a\Lambda - b)(B) = 0.$$

E está en $C(a, b)$ ya que

$$
\begin{aligned}
(\Lambda^2(E))_n - a(\Lambda(E))_n - bE_n &= (n+2)\lambda^{n+2} - a(n+1)\lambda^{n+1} - bn\lambda^n \\
&= (n+2)\lambda^2 - a(n+1)\lambda - bn \\
&= n\lambda^2 + 2\lambda^2 - an\lambda - a\lambda - bn \\
&= n(\lambda^2 - a\lambda - b) + \lambda(2\lambda - a) \\
&= 0.
\end{aligned}
$$

Recuerde que si λ y μ son raices de $x^2 - ax - b$ entonces $\lambda + \mu = a$ y $\lambda\mu = -b$, en este caso $\lambda = \mu$, así $2\lambda = a$ esto es $2\lambda - a = 0$.

Si $A \in C(a, b)$, entonces $A = cE + dB$ luego $A_n = cn\lambda^n + d\lambda^n = (cn + d)\lambda^n$. En particular $A_0 = d$ y $A_1 = (c + d)\lambda$ despejando c se obtiene que:

$$c = \frac{A_1 - \lambda A_0}{\lambda}.$$

Observe que el discriminante de la ecuación $x^2 - ax - b$ es $a^2 + 4b$ y si este es nulo, la ecuación tendrá dos raices λ, μ iguales, y si es no nulo tendrá dos raices λ, μ distintas.

La fórmula de Binet para una sucesión $A \in C(a, b)$ viene dada por

$$A_n = \frac{A_1 - \mu A_0}{\lambda - \mu}\lambda^n + \frac{\lambda A_0 - A_1}{\lambda - \mu}\mu^n$$

si $a^2 + 4b \neq 0$.

$$A_n = \frac{A_1 - \lambda A_0}{\lambda}(n\lambda^n) + A_0\lambda^n$$

si $a^2 + 4b = 0$.

2.2. Matriz con elementos de una sucesión de Fibonacci

El conjunto $\{E, F\}$ donde $F_0 = 0, F_1 = 1$ y $E_0 = 1, E_1 = 0$, es una Base para $C(a, b)$, $b \neq 0$, por la Proposición 3. Para encontrar la representación matricial de Λ en esta Base se necesita demostrar que $\Lambda(E) = bF$ lo cuál es $E_{n+1} = bF_n$. El resultado se prueba por inducción. Si $n = 0$ entonces $E_1 = 0 = bF_0$. Supónganse que se cumple $E_{k+1} = bF_k$ para $k \leq n-1$. Entonces $E_{n+1} = aE_n + bE_{n-1} = abF_{n-1} + b^2F_{n-2} = b(aF_{n-1} + bF_{n-2}) = bF_n$. Demostrar que $\Lambda(F) = E + aF$ equivale a probar que $F_{n+1} = E_n + aF_n$.

Si $n = 0$ entonces $F_1 = 1 + 0 = E_0 + aF_0$.

Supóngase $F_{k+1} = E_k + aF_k$ para $k \leq n - 1$.

$$\begin{aligned} F_{n+1} &= aF_n + bF_{n-1} \\ &= a(E_{n-1} + aF_{n-1}) + b(E_{n-2} + aF_{n-2}) \\ &= (aE_{n-1} + bE_{n-2}) + a(aF_{n-1} + bF_{n-2}) \\ &= E_n + aF_n. \end{aligned}$$

En resumen, se mostró que $\Lambda(E) = bF$ y $\Lambda(F) = E + aF$. Este resultado muestra que $\Lambda(E), \Lambda(F) \in C(a, b)$ y por tanto para un elemento $A \in C(a, b)$ se tiene que $\Lambda(A) \in C(a, b)$, es decir, Λ es invariante por $C(a, b)$, por tanto, se puede considerar $\Lambda : C(a, b) \longrightarrow C(a, b)$.

La representación matricial de este Operador con respecto a esta Base es:

$$M = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}.$$

Ahora, si se multiplica una matriz 2×2 por los elementos $\begin{bmatrix} 1 & 0 \end{bmatrix}^T$ y $\begin{bmatrix} 0 & 1 \end{bmatrix}^T$ se tiene como resultado:

$$\begin{bmatrix} c & d \\ e & f \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} c \\ e \end{bmatrix} y \begin{bmatrix} c & d \\ e & f \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} d \\ f \end{bmatrix} (*)$$

las columnas de la matriz 2×2. La Proposición 3 demuestra que cualquier elemento $A \in C(a,b)$ se puede expresar en la Base $\{E,F\}$ como $A = A_0E + A_1F$ en particular $E = 1 \cdot E + 0 \cdot F$ y $F = 0 \cdot E + 1 \cdot F$, es decir, las coordenadas de E y F en esta Base, respectivamente son $\begin{bmatrix} 1 & 0 \end{bmatrix}^T$ y $\begin{bmatrix} 0 & 1 \end{bmatrix}^T$. Con esto se puede observar que las coordenadas de un elemento de $C(a,b)$ son sus valores iniciales.

La sucesión $\Lambda^k(E)$ tendrá como valores iniciales E_k, E_{k+1}, y por tanto la coordenadas en la Base $\{E,F\}$ son $\begin{bmatrix} E_k & E_{k+1} \end{bmatrix}^T$. De igual manera la sucesión $\Lambda^k(F)$ tiene como valores iniciales F_k, F_{k+1}, y por tanto la coordenadas en la Base $\{E,F\}$ son $\begin{bmatrix} F_k & F_{k+1} \end{bmatrix}^T$. Los valores iniciales de F son F_0, F_1, los de $\Lambda(F)$ son F_1, F_2, los de $\Lambda^2(F)$ son F_2, F_3, los de $\Lambda^3(F)$ son F_3, F_4. En general los valores iniciales de $\Lambda^k(F)$ son F_k, F_{k+1}. Entonces:

$$\begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^k \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} E_k \\ E_{k+1} \end{bmatrix} y \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^k \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} F_k \\ F_{k+1} \end{bmatrix}$$

Por $(*)$ se tiene que:

$$\begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^k = \begin{bmatrix} E_k & F_k \\ E_{k+1} & F_{k+1} \end{bmatrix}.$$

Del hecho $E_{n+1} = bF_n$ y lo anterior se deduce :

$$\begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^k = \begin{bmatrix} bF_{k-1} & F_k \\ bF_k & F_{k+1} \end{bmatrix}.$$

El determinante de la matriz que está a la izquierda de la igualdad es $(-b)^k$ y el de la derecha $bF_{k-1}F_{k+1} - bF_k^2$, igualando los determinantes se tiene $(-b)^k = bF_{k-1}F_{k+1} - bF_k^2$, que equivale a $(-1)^k b^{k-1} = F_{k-1}F_{k+1} - F_k^2$.

2.3. Propiedades con el M.C.D

En esta sección se considera la sucesión de Fibonacci, F, en el espacio $C(a,b)$,$b \neq 0$, con $a^2 + 4b \neq 0$ y a,b enteros para garantizar que F_n sea entero para todo entero no negativo n. El objetivo de esta sección es demostrar el siguiente hecho:

Sea $F \in C(a,b)$, la sucesión de Fibonacci donde a y b son primos relativos. Si m,n son enteros tales que $M.C.D(m,n) = k$ entonces $M.C.D(F_n, F_m) = F_k$.

NOTA 1
Usando la fórmula de Binet para $a^2 + 4b \neq 0$ con valores iniciales $F_0 = 0$ y $F_1 = 1$ se obtiene una fórmula explicita para esta sucesión.

$$F_n = \frac{1}{\lambda - \mu}\lambda^n - \frac{1}{\lambda - \mu}\mu^n.$$

Donde λ y μ son raices distintas de $x^2 - ax - b$ y por tanto $\lambda + \mu = a$ y $-(\lambda\mu) = b$.

NOTA 2
Si $A \in C(a,b)$, entonces $A_n = c_\lambda \lambda^n + c_\mu \mu^n$, luego

$$\begin{aligned}
(\Omega_k(A))_n &= c_\lambda \Omega_k(\lambda^n) + c_\mu \Omega_k(\mu^n) \\
&= c_\lambda \lambda^{nk} + c_\mu \mu^{kn} \\
&= c_\lambda (\lambda^k)^n + c_\mu (\mu^k)^n,
\end{aligned}$$

es decir λ^k y μ^k son raices de un polinomio de la forma $x^2 - \hat{a}x - \hat{b}$ y por tanto $\Omega_k(A) \in C(\hat{a}, \hat{b})$ donde $\hat{a} = \lambda^k + \mu^k$ y $\hat{b} = -\mu^k \cdot \lambda^k = -(\lambda\mu)^k = -(-b)^k$. Se puede decir entonces que:

$$\Omega_k : C(a,b) \longmapsto C(\lambda^k + \mu^k, -(-b)^k).$$

Se seguirá notando $\lambda^k + \mu^k$ por $\hat{a}$ y $-(-b)^k$ por $\hat{b}$.

NOTA 3
Se escribe $\{E^{(\hat{a},\hat{b})}, F^{(\hat{a},\hat{b})}\}$ para referirse a la Base de $C(\hat{a}, \hat{b})$ que muestra la Proposición 3.

NOTA 4
$bF_{k-1}+F_{k+1}=\hat{a}$. En efecto;

$$\begin{aligned}
bF_{k-1}+F_{k+1} &= b\frac{\lambda^{k-1}-\mu^{k-1}}{\lambda-\mu}+\frac{\lambda^{k+1}-\mu^{k+1}}{\lambda-\mu} \\
&= \frac{b\lambda^{k-1}-b\mu^{k-1}+\lambda^{k+1}-\mu^{k+1}}{\lambda-\mu} \\
&= \frac{-(\lambda\mu)\lambda^{k-1}+(\lambda\mu)\mu^{k-1}+\lambda^{k+1}-\mu^{k+1}}{\lambda-\mu} \\
&= \frac{-\mu\lambda^{k}+\lambda\mu^{k}+\lambda^{k+1}-\mu^{k+1}}{\lambda-\mu} \\
&= \frac{\lambda^{k+1}-\mu\lambda^{k}+\lambda\mu^{k}-\mu^{k+1}}{\lambda-\mu} \\
&= \frac{\lambda^{k}(\lambda-\mu)+\mu^{k}(\lambda-\mu)}{\lambda-\mu} \\
&= \lambda^{k}+\mu^{k} \\
&= \hat{a}.
\end{aligned}$$

A continuación se demuestran proposiciones que ayudaran a llegar a el objetivo principal de la sección. Supóngase a y b primos relativos.

Proposición 4. *F_k es divisor de F_{nk} para $n \geq 1$.*

Demostración. De la nota 2 se tiene que $\Omega_k(F) \in C(\hat{a},\hat{b})$. Recuerde que las coordenadas de un elemento $A \in C(\hat{a},\hat{b})$ en la Base ordenada $\{E^{(\hat{a},\hat{b})}, F^{(\hat{a},\hat{b})}\}$ están dadas por $\begin{bmatrix} A_0 & A_1 \end{bmatrix}$ (proposición 3). Si se aplica este hecho a $\Omega_k(F)$, se tiene $(\Omega_k(F))_n = F_{kn}$ y por tanto las coordenadas en esta Base para este elemento son $\begin{bmatrix} 0 & F_k \end{bmatrix}$,de donde $\Omega_k(F) = F_k F^{(\hat{a},\hat{b})}$. Así

$$(\Omega_k(F))_n = F_{nk} = F_k F_n^{(\hat{a},\hat{b})}.$$

□

Proposición 5. *F_n y b son primos relativos para $n \geq 1$.*

Demostración. Sea p un divisor primo de b. Como a y b son primos relativos entonces p no es divisor de a. De la fórmula de recurrencia $F_{n+2} = aF_{n+1} + bF_n$ tenemos que $[F_{n+2}] \equiv [aF_{n+1}]$ $(Modulo\ p)$ es decir que $[F_n] \equiv [F_1][a^{n-1}]$ para $n \geq 1$. Es fácil probar este hecho por inducción. Para $n = 1$ se tiene trivialmente que $[F_1] \equiv [F_1][a^{1-1}] = [F_1]$. Supóngase que se cumple para n. Entonces $[F_{n+1}] \equiv [aF_n] \equiv [a(F_1 a^{n-1})] = [a^n F_1] = [a^n][F_1]$.Con esto se deduce que F_n no es equivalente $(Modulo\ p)$ a 0 ya que p no divide a a y por tanto p no divide a F_n. Esto muestra que F_n y b son primos relativos para $n \geq 1$. □

Proposición 6. *Si $A \in C(a,b)$, y si p es un divisor común primo de A_k y A_{k+1}, pero no es divisor de b, entonces p es divisor de A_n para todo $n \geq 1$.*

Demostración. Sea $k \geq 1$. Luego $A_{k+1} = aA_k + bA_{k-1}$ de donde $A_{k+1} - aA_k = bA_{k-1}$.Como p es divisor común primo de A_k y A_{k+1} entonces divide a bA_{k-1}, así que p divide a A_{k-1}, ya que no divide a b. De manera análoga $A_k = aA_{k-1} + bA_{k-2}$ y p divide a A_k y A_{k-1} pero no a b entonces p divide a A_{k-2}. Siguiendo este procedimiento $A_{k-1} = aA_{k-2} + bA_{k-3}$ y como p divide a A_{k-2} y A_{k-1} pero no a b, entonces divide a A_{k-3}. Haciendo $k-$pasos se llega a que A_0 y A_1 son divisibles por p. El siguiente paso es demostrar por inducción que p divide a A_n para todo $n \geq 1$. En efecto: Para $n = 1$ se cumple, pués se mostró anteriormente. Supóngase que p divide a A_m para todo $m \leq n$. Veamos que p divide a A_{n+1}. Por la fórmula de recurrencia se tiene que $A_{n+1} = aA_n + bA_{n-1}$, por la hipótesis de inducción se obtiene que p divide tanto a A_n y A_{n-1}, por tanto divide a A_{n+1} que era lo que se queria mostrar. □

Proposición 7. *Si h y k son números enteros positivos primos relativos, entonces F_h y F_k son primos relativos.*

Demostración. Si h o k es 1 el resultado es trivial, ya que $F_1 = 1$. Supóngase $h \neq k$ y mayores que 1. La prueba se hace por contradicción. Sea p un divisor primo de F_h y F_k. Por la Proposición 5 se tiene que F_h es primo relativo con b, por tanto p no puede ser divisor de b. Como h y k son primos relativos, entonces el $M.C.D(h,k) = 1$, luego existen enteros s y r tales que $rh + sk = 1$. Observe que r y s poseen signos diferentes. Si s o r fuera nulo, sin pérdida de generalidad $r = 0$ se tiene que $sk = 1$ de donde $k = s = 1$ lo que contradice lo anteriormente supuesto. Si r es positivo entonces $sk = 1 - rh \leq 0$, es decir, s es negativo porque k es positivo y s es no nulo. Si r es negativo entonces $sk = 1 - rh \geq 0$, es decir, s es positivo porque k es positivo y s es no nulo. En cualquiera de los caso s y r poseen signos distintos. Sin pérdida de generalidad, supóngase r negativo. Sea $t = -r$, esto es $sk - th = 1$, lo cual dice que sk y th son enteros consecutivos. De la Proposición 4 se tiene que F_{sk} es divisible por F_k y de manera similar F_{th} es divisible por F_h. Como p es un divisor primo común de F_h y F_k entonces, también es un divisor primo común a F_{sk} y F_{th}, además anteriormente se probó que p no divide a b y como consecuencia de la Proposición anterior, p es divisor de F_n para todo $n \geq 1$, lo cual es absurdo, ya que p sería un divisor primo de $F_1 = 1$. □

Proposición 8. *$\hat{a}$ y $\hat{b}$ definidos en la nota 4 son primos relativos.*

Demostración. Asúmase lo contrario. Sea p un divisor primo común a $\hat{a}$ y $\hat{b}$. Entonces p es divisor de b, ya que $\hat{b} = -(-b)^k$. De la Nota 4 se tiene que $\hat{a} = bF_{k-1} + F_{k+1}$, es decir, $\hat{a} - bF_{k-1} = F_{k+1}$ por tanto p es divisor de F_{k+1}. En resumen, se demostró que p es un divisor primo de b y F_{k+1}, lo que contradice la Propocisión 5. □

Teorema 7. *Sea $F \in C(a, b)$, la sucesión de Fibonacci donde a y b son primos relativos. Entonces si m, n son enteros tales que $M.C.D(m, n) = k$ entonces $M.C.D(F_n, F_m) = F_k$.*

Demostración. Sea $s = \dfrac{m}{k}$ y $t = \dfrac{n}{k}$. Los enteros s y t son primos relativos. En efecto; $sk = m$ y $tk = n$. Ahora $k = M.C.D(m, n) = M.C.D(sk, tk) = k \cdot M.C.D(s, t)$ así $M.C.D(s, t) = 1$. Sea $A = \Omega_k(F)$, recuerde que $\hat{a}$ y $\hat{b}$ son primos relativos por la Proposición 8.

La Proposición 4 muestra que $A = F_k F^{(\hat{a},\hat{b})}$. De esto se deduce que A_j es múltiplo de F_k, para todo $j \geq 0$, en particular F_k es divisor de $A_s = (\Omega_k(F))_s = F_{ks} = F_m$ y $A_t = (\Omega_k(F))_t = F_{kt} = F_n$. Esto es $F_n = A_t = F_k F_t^{(\hat{a},\hat{b})}$ y $F_m = A_s = F_k F_s^{(\hat{a},\hat{b})}$. Así $\frac{F_m}{F_k} = F_s^{(\hat{a},\hat{b})}$ y $\frac{F_n}{F_k} = F_t^{(\hat{a},\hat{b})}$ son primos relativos por la Proposición 7. Ahora:

$$
\begin{aligned}
M.C.D(F_m, F_n) &= M.C.D(F_k F_s^{(\hat{a},\hat{b})}, F_k F_t^{(\hat{a},\hat{b})}) \\
&= F_k \cdot M.C.D(F_s^{(\hat{a},\hat{b})}, F_t^{(\hat{a},\hat{b})}) \\
&= F_k \cdot 1 = F_k.
\end{aligned}
$$

□

Observaciones

1. La condición $b \neq 0$ en la Definición 12 es de suma importancia, pués si $b = 0$ entonces la sucesión de Fibonacci se convierte en la sucesión nula y no podría ser parte de la Base de $C(a, b)$ mostrada en la Proposición 3.

2. Varias de las propiedades de la Sucesión de Fibonacci que aparecen en el trabajo pueden ser demostradas mediante otros métodos, por ejemplo, la igualdad de matrices y la fórmula que aparecen en la sección 2.2 pueden ser probadas por inducción matemática.

Bibliografía

[1] Dan Kalman, Robert Mena. “The Fibonacci Numbers”. Mathematics Magazine Vol.76 .N0.3 (2003).

[2] Kenneth Hoffman, Ray Kunze.*Linear Algebra*. Prentice Hall, inc., 1971.

[3] Karlheinz Spindler.*Abstract Algebra with Applications Vol.I: Vector Spaces and Groups*.Marcel Dekker,Inc. 1994.