ANILLOS DE HERMITE. LA RECTA PROYECTIVA

Astrid Liliana Contreras Mendoza

Trabajo de Grado para optar al título de Magister en Matemáticas

Directora

Claudia Inés Granados Pinzón

Doctora en Matemáticas

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Matemáticas

Maestría en Matemáticas

Bucaramanga

2021

Dedicatoria

A mi madre.

Agradecimientos

Agradezco especialmente a mi padre Jorge Alberto Contreras por brindarme la oportunidad de estudiar una carrera profesional y motivarme a continuar con mi formación académica.

Con profunda nostalgia, agradezco a mi madre Hilba Mendoza, por todas sus oraciones y sus todos sus esfuerzos para apoyarme en todo lo relacionado con mi vida personal, académica y profesional.

A mi hermana Elizabeth por su ayuda, su compañía y toda su preocupación en todos y cada uno de aquellos días díficiles.

Quiero agradecer a la profesora Claudia Inés Granados, por todo su cariño, su dedicación, su tiempo, sus consejos y enseñanzas las cuales fueron muy importantes para la realización de este trabajo.

A todos mis amigos y compañeros del posgrado, por los aprendizajes y colaboraciones compartidas. Agradezco especialmente a Jackson y Andrés, con quienes he compartido la mayor parte del proceso.

Por último, agradezco a quienes me hayan colaborado en algún aspecto antes y durante el desarrollo de este trabajo.

Tabla de Contenido

Resumen

Título: Anillos de Hermite. La recta proyectiva [*]

Autor: Astrid Liliana Contreras Mendoza [**]

Palabras Clave: Módulos libres, Anillos de Hermite, Fila unimodular, Recta proyectiva, Recta proyectiva dual.

Descripción: Los trabajos de Quillen y Suslin sobre la conjetura de la fila unimodular de Serre, abre el campo a los llamados por (Lam, 2010) anillos de Hermite. Por una parte se demuestra que los anillos locales, el producto directo de cuerpos y las $\mathbb{K}$-álgebras finitas son anillos de Hermite. Un problema abierto sobre este tipo de anillos, es la Conjetura de Hermite: si $\mathcal{R}$ es un anillo de Hermite, entonces $\mathcal{R}[x]$ es un anillo de Hermite. Para el caso en que el anillo tenga dimensión de Krull menor o igual a un entero dado se prueba que la conjetura es verdadera.

Por otra parte, la teoría estudiada sobre los espacios proyectivos tiene un enfoque algebraico, por ejemplo en (Doneddu, 1980) se definen los espacios proyectivos asociados a un espacio vectorial de dimensión finita sobre un cuerpo $\mathbb{K}$, este enfoque permite considerar la generalización de los espacios vectoriales a los $\mathcal{R}$-módulos libres. Se prueban resultados relacionados con puntos fuertemente independientes, referencias proyectivas y proyectividades algebraicas hasta llegar a demostrar el Teorema de Staudt para rectas proyectivas. Se demuestra que existe una relación biunívoca entre el espacio proyectivo y el espacio proyectivo dual y concluimos demostrando que la forma bilineal asociada a esta relación biunívoca determina una estructura simpléctica sobre el $\mathcal{A}$-módulo $\mathcal{A}^2$.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Directora: Claudia Inés Granados Pinzón, Doctora en Matemáticas.

Abstract

Title: Hermite Rings. The projective line. *

Author: Astrid Liliana Contreras Mendoza. **

Keywords: Free modules, Hermite Rings, Unimodular row, Projective line, Dual projective line.

Description: The works of Quillen and Suslin on the conjecture of the unimodular row of Serre, opens the field to the so called by (Lam, 2010) Hermite rings. On the one hand it is shown that the local rings, the direct product of fields and the $\mathbb{K}$-finite algebras are Hermite rings. An open problem about this type of rings is the Hermite Conjecture: if $\mathcal{R}$ is a Hermite ring, then $\mathcal{R}[x]$ is a Hermite ring. For the case in which the ring has a Krull dimension less than or equal to a given integer, the conjecture is proved to be true.

On the other hand, lhe theory studied on projective spaces has an algebraic approach, for example in (Doneddu, 1980) the projective spaces associated with a finite dimensional vector space on a field $\mathbb{K}$ are defined, this approach allows to consider the generalization of vector spaces to the $\mathcal{R}$-free modules. Results about strongly to independent points, projective references and algebraic projectivities are tested until Staudt's Theorem for projective lines is proven. It is shown that there is a one-to-one relationship between the projective space and the dual projective space and we conclude by showing that the bilinear form associated with this one-to-one relationship determines a symplectic structure on the $\mathcal{A}$-module $\mathcal{A}^2$.

---

* Bachelor Thesis

** Faculty of Sciences. School of Mathematics. Director by: Dr. Claudia Inés Granados Pinzón.

Introducción

En 1955, J.P. Serre se preguntaba si los módulos proyectivos finitamente generados eran libres sobre el anillo de polinomios $\mathbb{K}[x_1, \ldots, x_n]$ de n variables, con $\mathbb{K}$ cuerpo. Esta afirmación fue motivada, por el hecho de que existe una correspondencia biunívoca entre *vectores bundles algebraicos*[1] sobre una variedad afín y los módulos proyectivos finitamente generados sobre su anillo de coordenadas tal como se demuestra en (Serre, 1958), (Swan, 1962) y (Vaserstein, 1986). Resulta que los módulos proyectivos finitamente generados sobre el anillo $\mathbb{K}[x_1, \ldots, x_n]$ corresponden a vectores bundles algebraicos sobre el espacio afín $\mathbb{A}^n_{\mathbb{K}}$, donde los módulos libres corresponden a vectores bundles triviales.

Serre no había especulado sobre una posible solución de su problema. Sin embargo, suponía una respuesta positiva. Serre hizo algunos avances hacia la solución, en 1957 logró demostrar que todo módulo proyectivo generado finitamente sobre el anillo polinomios $\mathbb{K}[x_1, \ldots, x_n]$, era establemente libre. Con el tiempo este problema se conoció como "La Conjetura de Serre". Más

---

[1] Considere K como los números reales, los complejos o los cuaterniones. Un K-vector bundle ζ sobre un espacio topológico X consiste de,

- *a*) Un espacio topológico X(espacio base) y un espacio $E(\zeta)$ (espacio total),
- *b*) una aplicación continua $\pi : E(\zeta) \longrightarrow X$ (la proyección),
- *c*) para todo $x \in X$, la fibra $F_x(\zeta) = \pi^{-1}(x)$ tiene estructura de espacio vectorial de dimensión finita sobre K.

tarde, el interés en los módulos proyectivos y la Conjetura de Serre fue más acentuada por el desarrollo de dos áreas estrechamente relacionadas en matemáticas: álgebra homológica y teoría K-algebraica. Con motivaciones provenientes de estas dos áreas, la Conjetura de Serre entró en la década de 1960 como uno de los principales problemas abiertos en álgebra y geometría algebraica afín.

El problema permaneció abierto hasta 1976, cuando Daniel Quillen (Quillen, 1976) y Andrei Suslin (Suslin, 1976) dieron de forma independiente una respuesta afirmativa a este famoso problema y hoy en día es conocido como el Teorema de Quillen- Suslin. Poco tiempo después, se dispuso de algunas pruebas muy ingeniosas y más breves como la de Leonid Vaserstein usando la técnica de extender filas unimodulares a matrices invertibles, esta solución introdujo el estudio de filas unimodulares como un nuevo tema de investigación en álgebra conmutativa.

Por una parte, los trabajos de Quillen y Suslin sobre la conjetura de la fila unimodular de Serre, abre el campo a los llamados por Lam (Lam, 2010) anillos de Hermite, estos anillos serán la estructura algebraica de gran interés en este escrito.

Por otra parte, también nos interesa estudiar la geometría proyectiva sobre un anillo. La geometría proyectiva tiene sus inicios en el Siglo II cuando Ptolometo en su obra el Almagesto de una manera informal introduce la geometría proyectiva. En 1936 el matemático francés Desargues utiliza la proyección central, es decir la proyección desde un punto para probar resultados geométricos y especialmente para obtener propiedades de las cónicas, la proyección central no conserva ni distancias ni ángulos y por lo tanto desde ese entonces se desvincula la geometría de la métrica.

Más adelante Plüker en 1928, define las coordenadas homogéneas y esto permite hablar de coordenadas de una recta en el plano, sin embargo existían algunos objetos a los cuales se les desconocían sus coordenadas, estos objetos eran las rectas en el espacio tridimensional. Este problema fue resuelto aproximadamente 20 años después y se llegó a su solución por medio de álgebra lineal y desde ese entonces la geometría proyectiva se convierte en el lenguaje geométrico del álgebra y naturalmente se asocian los espacios proyectivos a los espacios vectoriales.

Este enfoque algebraico permite hacer en una genereralización, en lugar de asociar a los espacios proyectivos los espacios vectoriales se pueden asociar $\mathcal{R}$-módulos libres. Y es por esto, que en la actualidad estudiar la geometría proyectiva sobre un anillo es un problema abierto. Granados en (Granados Pinzón, 2015) hace un estudio inicial de la recta proyectiva sobre un anillo total de fracciones, sin embargo, el esfuerzo de muchos investigadores se centra en estudiarlo para cualquier anillo $\mathcal{R}$.

Este trabajo consta de tres capítulos, donde se presentan resultados conocidos del álgebra conmutativa, se estudian los anillos de Hermite y se define la recta proyectiva sobre un anillo.

El Capítulo 1 se divide en cuatro secciones, en la primera sección se presentan algunos conceptos básicos, ejemplos y resultados relacionados con módulos, en particular, los módulos finitamente generados, módulos proyectivos y módulos libres. En la segunda sección se definen las matrices elementales y se presentan resultados básicos sobre operaciones con matrices elementa-

les, en particular un resultado clásico conocido como Lema de Whitehead. En la tercera sección se define la resultante de dos polinomios y se prueban algunas propiedades bastante últiles para los capítulos posteriores. En la cuarta sección definimos la dimensión de Krull, se demuestran propiedades y lemas necesarios para probar que la dimensión de Krull de un anillo puede expresarse de manera recursiva a través del espectro de Zariski.

En el Capítulo 2 iniciamos definiendo los módulos establemente libres, presentando ejemplos y resultados que dan condiciones necesarias para determinar cuándo un módulo establemente libre es libre, lo interesante es su interpretación matricial en términos de filas unimodulares y los elementos complementables. Con esto, se introduce la definición de anillo de Hermite. Probamos algunos resultados que relacionan los anillos de Hermite con los anillos locales, el anillo de polinomios $\mathbb{K}[x_1, \ldots, x_n]$ con $\mathbb{K}$ cuerpo, las $\mathbb{K}$-álgebras finitas, entre otros. Un problema abierto destacado sobre este tipo de anillos, es la Conjetura de Hermite: si $\mathcal{R}$ es un anillo de Hermite, entonces $\mathcal{R}[x]$ es un anillo de Hermite. Finalizamos la sección probando la conjetura de Hermite para un anillo $\mathcal{R}$ con dimensión de Krull menor o igual a un entero dado.

Adicionalmente, el presente trabajo tiene el objetivo de estudiar la geometría proyectiva sobre un anillo $\mathcal{R}$. En el Capítulo 3, inicialmente de forma breve se estudian las $\mathbb{R}$-álgebras de dimensión dos y las métricas del plano. En (Doneddu, 1980) se definen los espacios proyectivos asociados a un espacio vectorial E de dimensión finita, entonces en lugar de considerar espacios vectoriales se considerarán $\mathcal{R}$-módulos y así se definen los espacios proyectivos asociados a $\mathcal{R}$. Es por esto, que se dedica una sección de este capítulo al estudio de los $\mathcal{R}$-módulos libres de rango dos. Se define el producto exterior, se muestran propiedades y las proposiciones que obtuvimos

como resultados de este trabajo. Luego, se define la recta proyectiva sobre un anillo $\mathcal{R}$, se presentan ejemplos y resultados relacionados con puntos fuertemente independientes, referencias proyectivas y proyectividades algebraicas hasta llegar a demostrar el Teorema de Staudt para rectas proyectivas. Finalizando el capítulo, se define la recta proyectiva dual sobre un anillo total de fracciones, se demuestra que existe una relación biunívoca entre el espacio proyectivo y el espacio proyectivo dual. Terminamos demostrando, que la forma bilineal asociada a esta relación biunívoca determina una estructura simpléctica sobre el $\mathcal{A}$-módulo $\mathcal{A}^2$.

1. Preliminares

En este capítulo, se establecen algunos conceptos y resultados del álgebra conmutativa que servirán como base para el desarrollo y comprensión de los capítulos posteriores. Siempre $\mathcal{R}$ denotará un anillo conmutativo con unidad.

1.1. Módulos

En esta sección se estudian propiedades y resultados de uno los objetos algebraicos fundamentales en este trabajo, los módulos.

Definición 1.1. Sean $(\mathcal{M}, +)$ un grupo abeliano y $\mathcal{R}$ un anillo. Se dice que $\mathcal{M}$ tiene una estructura de módulo a izquierda sobre $\mathcal{R}$, si se ha definido un producto entre elementos de $\mathcal{M}$ y de $\mathcal{R}$, es decir, una función

$$\mathcal{R} \times \mathcal{M} \longrightarrow \mathcal{M}$$

$$(r, \boldsymbol{m}) \longmapsto r \cdot \boldsymbol{m}$$

para el cual se cumplen las siguientes condiciones:

1. $r_1 \cdot (\boldsymbol{m} + \boldsymbol{n}) = r_1 \cdot \boldsymbol{m} + r_1 \cdot \boldsymbol{n}$,
2. $(r_1 + r_2) \cdot \boldsymbol{m} = r_1 \cdot \boldsymbol{m} + r_2 \cdot \boldsymbol{m}$,
3. $(r_1 r_2) \cdot \boldsymbol{m} = r_1 (r_2 \cdot \boldsymbol{m})$,
4. $1_{\mathcal{R}} \cdot \boldsymbol{m} = \boldsymbol{m}$,

con $\boldsymbol{m}, \boldsymbol{n} \in \mathcal{M}$ y $r_1, r_2, 1_{\mathcal{R}} \in \mathcal{R}$.

Observación 1.2. Si $\mathcal{R}$ es un anillo conmutativo y $\mathcal{M}$ es un $\mathcal{R}$-módulo a izquierda, entonces el producto

$$r \cdot \boldsymbol{m} = \boldsymbol{m} \cdot r, \text{ para } \boldsymbol{m} \in \mathcal{M}, r \in \mathcal{R},$$

convierte a $\mathcal{M}$ en un $\mathcal{R}$-módulo a derecha. En este caso, se dice que $\mathcal{M}$ es un $\mathcal{R}$-$\mathcal{R}$-bimódulo. De ahora en adelante, se escribe simplemente $\mathcal{M}$ un $\mathcal{R}$-módulo para referirse a el $\mathcal{R}$-$\mathcal{R}$-bimódulo $\mathcal{M}$.

A continuación se presentan algunos ejemplos de $\mathcal{R}$-módulos donde se denota por $\mathcal{I} = \langle x_1, ..., x_n \rangle$ al ideal generado por $x_1, ..., x_n \in \mathcal{R}$ y el anillo cociente de $\mathcal{R}$ sobre $\mathcal{I}$ por $\frac{\mathcal{R}}{\mathcal{I}}$.

Ejemplo 1.3.

1. Si $\mathcal{R}$ es un cuerpo, un $\mathcal{R}$-módulo es un $\mathcal{R}$-espacio vectorial.
2. Un $\mathbb{Z}$-módulo es un grupo abeliano.
3. Todo anillo $\mathcal{R}$ es un $\mathcal{R}$-módulo.
4. Sean $\mathcal{R}$ un anillo y $M_{n\times n}(\mathcal{R})$ el anillo de matrices de orden $n \times n$ con entradas en $\mathcal{R}$, $M_{n\times n}(\mathcal{R})$ es un $\mathcal{R}$-módulo.
5. Si $\mathcal{I}$ es un ideal de $\mathcal{R}$, $\frac{\mathcal{R}}{\mathcal{I}}$ es un $\mathcal{R}$-módulo, donde

$$\mathcal{R} \times \frac{\mathcal{R}}{\mathcal{I}} \longrightarrow \frac{\mathcal{R}}{\mathcal{I}}$$
$$(r, x + \mathcal{I}) \longmapsto rx + \mathcal{I}.$$

En particular, para todo $n \in \mathbb{N}$, $\frac{\mathbb{Z}}{\langle n \rangle}$ es un $\mathbb{Z}$-módulo.

Considere los $\mathcal{R}$-módulos $\mathcal{M}$ y $\mathcal{N}$, una función $f : \mathcal{M} \longmapsto \mathcal{N}$ es un homomorfismo de $\mathcal{R}$-módulos si para todos $\boldsymbol{m}, \boldsymbol{m}_1 \in \mathcal{M}$ y $r \in \mathcal{R}$ se tiene que,

1. $f(\boldsymbol{m} + \boldsymbol{m}_1) = f(\boldsymbol{m}) + f(\boldsymbol{m}_1)$,

2. $f(r\boldsymbol{m}) = rf(\boldsymbol{m})$.

De forma análoga, al caso de grupos o anillos se definen monomorfismo, epimorfismo e isomorfismo de $\mathcal{R}$-módulos. Además se puede definir el siguiente conjunto

$$Hom_{\mathcal{R}}(\mathcal{M},\mathcal{N}) = \{f : \mathcal{M} \longmapsto \mathcal{N} : f \text{ es un homomorfismo}\}.$$

Note que $Hom_{\mathcal{R}}(\mathcal{M},\mathcal{N})$ es un grupo abeliano con la suma usual de funciones.

Ejemplo 1.4. $Hom_{\mathcal{R}}(\mathcal{M},\mathcal{N})$ es un $\mathcal{R}$-módulo.

En efecto, considere

$$\mathcal{R} \times Hom_{\mathcal{R}}(\mathcal{M},\mathcal{N}) \longrightarrow Hom_{\mathcal{R}}(\mathcal{M},\mathcal{N})$$

$$(r, f) \longmapsto rf$$

donde

$$rf : \mathcal{M} \longrightarrow \mathcal{N}$$

$$\boldsymbol{m} \longmapsto rf(\boldsymbol{m}).$$

Definición 1.5. Sean $\mathcal{M}$ un $\mathcal{R}$-módulo y $\mathcal{N} \subseteq \mathcal{M}$. Se dice que $\mathcal{N}$ es un submódulo de $\mathcal{M}$, si $\mathcal{N}$ es subgrupo de $\mathcal{M}$ y para todos $r \in \mathcal{R}$, $n \in \mathcal{N}$, tenemos que $rn \in \mathcal{N}$.

Ejemplo 1.6. 1. Sea $\mathcal{R}$ un anillo. Los $\mathcal{R}$-submódulos de $\mathcal{R}$, son sus ideales.

2. Si $\mathcal{M}$ es un $\mathcal{R}$-módulo y $\{\mathcal{M}_i\}_{i\in I}$ es una familia de submódulos de $\mathcal{M}$. Entonces, $\bigcap_{i\in I} \mathcal{M}_i$ es un submódulo de $\mathcal{M}$.

3. Sean $\mathcal{M}_1$ y $\mathcal{M}_2$ submódulos de un $\mathcal{R}$-módulo $\mathcal{M}$. Entonces,

$$\mathcal{M}_1 + \mathcal{M}_2 = \{m_1 + m_2 \mid m_1 \in \mathcal{M}_1, m_2 \in \mathcal{M}_2\}$$

es submódulo de $\mathcal{M}$ llamado submódulo suma de $\mathcal{M}_1$ y $\mathcal{M}_2$.

4. Sea $\mathcal{M}$ un $\mathcal{R}$-módulo y $\emptyset \neq X \subseteq \mathcal{M}$. Entonces

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} \boldsymbol{x}_i r_i \mid \boldsymbol{x}_i \in X \text{ y } r_i \in \mathcal{R} \right\}.$$

es submódulo de $\mathcal{M}$ y se conoce como el submódulo generado por X. Además, si $\langle X \rangle = \mathcal{M}$ se dirá que X es un sistema de generadores para $\mathcal{M}$. Decimos que $\mathcal{M}$ es finitamente generado si existe un subconjunto finito $X \subseteq \mathcal{M}$ tal que $\langle X \rangle = \mathcal{M}$, en el caso de que $X = \{\boldsymbol{x}\}$, $\langle X \rangle$ se llama submódulo monógeno.

1.1.1. Módulos libres. Los conceptos de independencia y dependencia lineal para módulos libres es análogo al estudiado en espacios vectoriales.

Definición 1.7. Sean $\mathcal{M}$ un $\mathcal{R}$-módulo y $\emptyset \neq B \subseteq \mathcal{M}$, se dice que B es una base para $\mathcal{M}$ si B es linealmente independiente y $\langle B \rangle = \mathcal{M}$.

Definición 1.8. Sea $\mathcal{M}$ un $\mathcal{R}$-módulo, se dice que $\mathcal{M}$ es libre si posee al menos una base.

Note que $\{0\}$ es un módulo libre con base $\emptyset$ y que el anillo $\mathcal{R}$ también lo es con base $B = \{1_{\mathcal{R}}\}$.

Ejemplo 1.9.

1. Todo módulo sobre un anillo de división, es libre. En particular, el anillo de división $\mathbb{Q}$ es un $\mathbb{Q}$-módulo. Los únicos ideales de $\mathbb{Q}$ son $\{0\}$ y $\mathbb{Q}$, entonces lo únicos $\mathbb{Q}$-submódulos de $\mathbb{Q}$ son $\{0\}$ y $\mathbb{Q}$, los cuales son $\mathbb{Q}$-módulos libres.

2. Sean $\mathcal{M}$ y $\mathcal{N}$ módulos libres sobre $\mathcal{R}$ de bases finitas entonces $Hom_{\mathcal{R}}(\mathcal{M},\mathcal{N})$ es libre. En particular, si consideramos $\mathcal{M} = \mathcal{R}$, entonces $Hom_{\mathcal{R}}(\mathcal{R},\mathcal{N}) \cong \mathcal{N}$ es libre.

Aunque el concepto de base para módulos libres es análoga a la estudiada en espacios vectoriales, algunas propiedades de las bases de los espacios vectoriales no se conservan para módulos. En particular, no todo módulo posee una base, dos bases finitas pueden tener diferente número de elementos, y no todo submódulo de un módulo libre es libre.

El siguiente Ejemplo 1.10 es muy interesante, pues a partir de este concluimos que no todo módulo posee una base.

Ejemplo 1.10. El $\mathbb{Z}$-módulo $\mathbb{Q}$, no es libre. Suponga que $\emptyset \neq B \subset \mathbb{Q}$ es una base de $\mathbb{Q}$. Sea $x_0 \in B$

y considere $B_0 = B - \{x_0\}$, se tiene que $\mathbb{Q} = \langle B_0 \rangle$, para esto veamos que $x_0 \in \langle B_0 \rangle$. En efecto,

$$\frac{x_0}{2} = x_0 k_0 + \sum_{i=1}^{n} x_i k_i \text{ con } a_i \in B_0 \text{ y } k_0, k_i \in \mathbb{Z} \text{ para } 1 \leq i \leq n.$$

Luego, $x_0 = x_0(2k_0) + \sum_{i=1}^{n} x_i(2k_i)$, así

$$\begin{aligned} x_0 - x_0(2k_0) &= \sum_{i=1}^{n} x_i(2k_i), \\ x_0(1 - 2k_0) &= \sum_{i=1}^{n} x_i(2k_i), \\ x_0 m &= \sum_{i=1}^{n} x_i(2k_i), \end{aligned}$$

donde $m = 1 - 2k_0 \in \mathbb{Z}$ y $m \neq 0$. Consideremos ahora el racional $\frac{x_0}{m}$,

$$\begin{aligned} \frac{x_0}{m} &= x_0 k_0' + \sum_{i=1}^{t} y_i k_i' \text{ con } y_i \in B_0 \text{ y } k_i' \in \mathbb{Z} \text{ para } 1 \leq i \leq t, \\ x_0 &= x_0 m k_0' + \sum_{i=1}^{t} y_i m k_i', \\ x_0 &= \sum_{i=1}^{n} x_i(2k_0' k_i) + \sum_{i=1}^{t} y_i m k_i' \text{ con } x_i, y_i \in B_0, \end{aligned}$$

con lo cual $x_0 \in \langle B_0 \rangle$. De lo anterior se concluye que el $\mathbb{Z}$-módulo $\mathbb{Q}$, no es finitamente generado. Veamos ahora que no es libre, supongamos que lo es, entonces existen $k_1, k_2, \ldots, k_n \in \mathbb{Z}$ y $x_1, \ldots, x_n \in B_0$ tales que $x_0 + x_1 k_1 + \ldots + x_n k_n = 0$, donde $\{x_0, x_1, \ldots, x_n\}$ es linealmente dependiente, lo cual es contradictorio.

Ejemplo 1.11. No todo submódulo de un módulo libre, es libre. En efecto, $\frac{\mathbb{Z}}{\langle 4\rangle}$ es $\frac{\mathbb{Z}}{\langle 4\rangle}$-módulo libre con base $1_{\frac{\mathbb{Z}}{\langle 4\rangle}}$, ahora considere $\mathcal{N} = \{\overline{0}, \overline{2}\}$ submódulo de $\frac{\mathbb{Z}}{\langle 4\rangle}$. Note que $\overline{2}\cdot\overline{2} = \overline{0}$ con $\overline{2} \neq \overline{0}$, es decir, $\mathcal{N}$ es generado por un elemento linealmente dependiente, por lo cual no posee base, y por lo tanto $\mathcal{N}$ no es libre.

Definición 1.12. Decimos que un anillo $\mathcal{R}$ satisface la Propiedad de número de base invariante (IBN) si, para cualesquieras enteros $n, m \geq 0$,

$$\mathcal{R}^m \cong \mathcal{R}^n (\text{ como } \mathcal{R}\text{-módulos}) \text{ implica que } m = n.$$

Note que esto significa que para cualesquiera dos bases de $\mathcal{M}$ un $\mathcal{R}$-módulo finitamente generado libre, tienen el mismo número de elementos.

Definición 1.13. Sean $\mathcal{R}$ un anillo con IBN y $\mathcal{M}$ un $\mathcal{R}$-módulo finitamente generado libre. Para cualesquiera dos bases de $\mathcal{M}$, las bases tienen el mismo número de elementos. Este número común se define como el rango de $\mathcal{M}$.

Observación 1.14. Por ejemplo, un teorema básico en álgebra lineal dice que los anillos de división satisfacen IBN. Ahora bien, si $\mathcal{R}$ y $\mathcal{S}$ son anillos para los cuales existe un homomorfismo de anillos no nulos $\mathcal{R} \longrightarrow \mathcal{S}$, un argumento del producto tensorial muestra que, siempre que $\mathcal{S}$ satisface IBN, $\mathcal{R}$ también lo hace. De acuerdo con las observaciones anteriores, los anillos locales satisfacen IBN, y que los anillos conmutativos distintos de cero satisfacen IBN como es nuestro caso. En (Lezama, 1985) se puede consultar un estudio recopilativo sobre los anillos que satisfacen IBN para más profundidad en el tema.

El siguiente teorema es un resultado importante que relaciona los módulos libres con la suma directa interna de módulos. Solo enunciaremos el resultado ya que para su prueba son necesarios algunos preliminares sobre la suma directa interna y externa de módulos. Se denotará como $\mathcal{R}^{(I)}$ a la suma directa $\bigoplus_{i\in I}\mathcal{R}_i$ donde cada sumando es $\mathcal{R}$.

Teorema 1.15. *(Lezama, Teorema 7.2.5) Sea $\mathcal{M}$ un $\mathcal{R}$-módulo libre con base B. Entonces $\mathcal{M} \cong \mathcal{R}^{(B)}$.*

Observación 1.16. Sea $\mathcal{M}$ un $\mathcal{R}$-módulo libre con base B. Si la cardinalidad de B es igual a $n \geq 1$, es decir, B tiene n elementos. Entonces, $\mathcal{M} \cong \mathcal{R}^n$ y se dice $\mathcal{M}$ es libre de rango n. Además, $\mathcal{R}^n$ es libre con base canónica $\{e_1, e_2, \ldots, e_n\}$, $e_i = (0, 0, \ldots, 1, \ldots, 0)$ donde 1 está en la i-ésima posición.

Ejemplo 1.17. El $\mathcal{R}$-módulo $M_{m\times n}(\mathcal{R})$ es un $\mathcal{R}$-módulo libre de rango mn. En efecto, defino $f : M_{m\times n}(\mathcal{R}) \longrightarrow \mathcal{R}^{mn}$ tal que

$$f\left(\begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \alpha_{21} & \ldots & \alpha_{2n} \\ \ldots & \ddots & \ldots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{bmatrix}\right) \longmapsto (\alpha_{11}, \alpha_{12}, \ldots \alpha_{m-1n}, \alpha_{mn}).$$

Es fácil verificar que f un $\mathcal{R}$-isomorfismo. Luego, $M_{m\times n}(\mathcal{R}) \cong \mathcal{R}^{mn}$.

Ejemplo 1.18. Un caso más general del ítem 2 del Ejemplo 1.9. Por el Teorema 1.15, podemos considerar $\mathcal{M} \cong \mathcal{R}^m$ y $\mathcal{N} \cong \mathcal{R}^n$, puesto que $\mathcal{M}$ y $\mathcal{N}$ son $\mathcal{R}$-módulos libres. Veamos que

$Hom_{\mathcal{R}}(\mathcal{R}^m, \mathcal{R}^n)$ es libre. En efecto, sean $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ y $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ bases para $\mathcal{R}^m$ y $\mathcal{R}^n$ respectivamente. El $\mathcal{R}$-homomorfismo lineal

$$f : \mathcal{R}^m \longrightarrow \mathcal{R}^n,$$

queda determinado según a donde se envía cada $\boldsymbol{v}_i$, tenemos

$$f(\boldsymbol{v}_i) \longmapsto \sum_{j=1}^{n} \alpha_{ij} \boldsymbol{u}_j, \ \ donde \ \ \alpha_{ij} \in \mathcal{R}.$$

Note que cualquier conjunto de α_{ij} determina un $\mathcal{R}$-homomorfismo lineal que va de $\mathcal{R}^m$ a $\mathcal{R}^n$. En otras palabras, cada $\mathcal{R}$-homomorfismo lineal puede expresarse de manera única como una matriz $A_f \in M_{n\times m}(\mathcal{R})$ (que depende de la elección de las bases)

$$A_f = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ddots & \ldots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{bmatrix}$$

en la cual la i-ésima columna de A_f esta formada por las coordenadas de $f(\boldsymbol{v}_i)$ en la base $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$.

Veamos que A_f determina f, pues si $\boldsymbol{x} = \sum_{i=1}^{m} a_i \boldsymbol{v}_i$,

$$f(\boldsymbol{x}) = f\left(\sum_{i=1}^{m} a_i \boldsymbol{v}_i\right) = \sum_{i=1}^{m} a_i f(\boldsymbol{v}_i) = \sum_{i=1}^{m} a_i \sum_{j=1}^{n} \alpha_{ij} \boldsymbol{u}_j = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} \boldsymbol{u}_j a_i.$$

En particular, las coordenadas de $f(\boldsymbol{x})$ en la base $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$, están dadas por

$$A_f \begin{pmatrix} a_1 \\ a_2 \\ \cdots \\ a_m \end{pmatrix}.$$

Recíprocamente, si $M = (\alpha_{ij}) \in M_{n\times m}(\mathcal{R})$, existe $g : \mathcal{R}^m \longrightarrow \mathcal{R}^n$ un único $\mathcal{R}$-homomorfismo tal que $g(\boldsymbol{v}_i) \longmapsto \sum_{j=1}^{n} \alpha_{ij} \boldsymbol{u}_j, \ \ donde \ \ \alpha_{ij} \in \mathcal{R}$. Por lo anterior, existe una relación biunívoca entre $Hom_{\mathcal{R}}(\mathcal{R}^m, \mathcal{R}^n)$ y $M_{n\times m}(\mathcal{R})$ como $\mathcal{R}$-módulos. Luego, $Hom_{\mathcal{R}}(\mathcal{R}^m, \mathcal{R}^n) \cong M_{n\times m}(\mathcal{R}) \cong \mathcal{R}^{mn}$. Así, $Hom_{\mathcal{R}}(\mathcal{R}^m, \mathcal{R}^n)$ es un $\mathcal{R}$-módulo libre de rango mn.

Definición 1.19. Sea $\mathcal{N}$ un submódulo de un $\mathcal{R}$-módulo $\mathcal{M}$. Decimos que $\mathcal{N}$ es un sumando directo de $\mathcal{M}$ si existe un submódulo $\mathcal{L}$ de $\mathcal{M}$ tal que $\mathcal{M} = \mathcal{L} \oplus \mathcal{N}$.

Proposición 1.20. (Yengui, Proposición 2) Sean $\mathcal{R}$ un anillo, $\mathcal{M}$ un $\mathcal{R}$-módulo y $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathcal{M}$. Las siguientes afirmaciones son equivalentes:

1. El submódulo $\mathcal{N} = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \rangle$ de $\mathcal{M}$ es libre con base $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ y $\mathcal{N}$ es sumando directo de $\mathcal{M}$.

2. Existe una forma n-lineal alternada $\Phi : \mathcal{M}^n \longrightarrow \mathcal{R}$ tal que

$$\Phi(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = 1.$$

Demostración. $1 \Rightarrow 2$ Sean $\mathcal{M} \cong \mathcal{L} \oplus \mathcal{N}$ para algún submódulo $\mathcal{L}$ de $\mathcal{M}$ y $\pi : \mathcal{M} \cong \mathcal{L} \oplus \mathcal{N} \longrightarrow \mathcal{N}$ la proyección de $\mathcal{M}$ sobre $\mathcal{N}$. Para cada $\boldsymbol{u}_k \in \mathcal{M}$, $\pi(\boldsymbol{u}_k) = \boldsymbol{n}_k$ para todo $k \in \{1, \ldots, n\}$ donde $\boldsymbol{n}_k \in \mathcal{N}$ para todo k. Como $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ es una base para $\mathcal{N}$, $\boldsymbol{n}_k = \sum_{i=1}^n \lambda_{ki} \boldsymbol{v}_i$ con $\lambda_{ki} \in \mathcal{R}$ para todo $k \in \{1, \ldots, n\}$. Por lo tanto, $\pi(\boldsymbol{u}_k) = \sum_{i=1}^n \lambda_{ki} \boldsymbol{v}_i$. Considere ahora $\{\boldsymbol{v}_1^*, \boldsymbol{v}_2^*, \ldots, \boldsymbol{v}_n^*\}$ el dual de la base $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$. Note que $\boldsymbol{v}_j^*(\sum_{i=1}^n \lambda_{ki} \boldsymbol{v}_i) = \lambda_{kj}$ con $\lambda_{kj} \in \mathcal{R}$. Entonces defino

$$\begin{aligned} \Phi : \mathcal{M}^n &\longrightarrow \mathcal{R} \\ (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) &\longmapsto \sum_{f \in S_n} sgn(f) \boldsymbol{v}_1^*(\pi(\boldsymbol{u}_{f(1)})) \ldots \boldsymbol{v}_n^*(\pi(\boldsymbol{u}_{f(n)})) \end{aligned}$$

donde S_n es el grupo de permutaciones de n elementos. Φ es una forma n-bilineal alternada, pues Φ corresponde a $det(\boldsymbol{v}_j^*(\pi(\boldsymbol{u}_i))_{1 \leq i,j \leq n}))$. Note que

$$\begin{aligned} \Phi(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) &= \sum_{f \in S_n} sgn(f) \boldsymbol{v}_1^*(\pi(\boldsymbol{u}_{f(1)})) \ldots \boldsymbol{v}_n^*(\pi(\boldsymbol{u}_{f(n)})) \\ &= \sum_{f \in S_n} sgn(f) \boldsymbol{v}_1^* \left(\sum_{i=1}^n \lambda_{f(1)i} \boldsymbol{v}_i \right) \ldots \boldsymbol{v}_n^* \left(\sum_{i=1}^n \lambda_{f(n)i} \boldsymbol{v}_i \right). \end{aligned}$$

$\boldsymbol{v}_j^* \left(\sum_{i=1}^n \lambda_{f(i)i} \boldsymbol{v}_i \right) = \lambda_{f(i)j} = 0$ en todos los términos, menos cuando $j = i$, es decir, $\lambda_{f(i)i} \neq 0$ para

todo $i \in \{1, \ldots, n\}$. Luego,

$$\Phi(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) = det(\boldsymbol{v}_j^*(\pi(\boldsymbol{u}_i))_{1 \leq i,j \leq n})) = \sum_{f \in S_n} sgn(f) \lambda_{f(1)1} \lambda_{f(2)2} \ldots \lambda_{f(n)n}.$$

Si $\boldsymbol{v}_j^*(\boldsymbol{v}_{f(i)}) = \lambda_{f(i)j} = 1$, entonces $f(i) = j$ para todo $i, j \in \{1, \ldots, n\}$. Por lo tanto $f = Id$ y así,

$$\Phi(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \lambda_{f(1)1} \lambda_{f(2)2} \ldots \lambda_{f(n)n} = 1.$$

$2 \Rightarrow 1$ Considere el $\mathcal{R}$-morfismo lineal $f : \mathcal{M} \longrightarrow \mathcal{M}$ definido como

$$f(\boldsymbol{u}) = \sum_{j=1}^{n} \Phi(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{u}, \boldsymbol{v}_{j+1}, \ldots \boldsymbol{v}_n) \boldsymbol{v}_j.$$

Veamos que $f(\boldsymbol{v}_i) = \boldsymbol{v}_i$ para todo $1 \leq i \leq n$. En efecto,

$$f(\boldsymbol{v}_i) = \sum_{j=1}^{n} \Phi(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_i, \boldsymbol{v}_{j+1}, \ldots \boldsymbol{v}_n) \boldsymbol{v}_j = \sum_{j=1}^{n} (\boldsymbol{v}_j^*(\boldsymbol{v}_i)) \boldsymbol{v}_j,$$

note que $(\boldsymbol{v}_j^*(\boldsymbol{v}_i)) = 0$ para todos los términos, excepto para $j = i$, por lo tanto $f(\boldsymbol{v}_i) = \boldsymbol{v}_i$. Además, la $Im(f) \subseteq \mathcal{N} = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \rangle$. De ahí se deduce que $f^2 = f$, f es una proyección, $Im(f) = \mathcal{N}$ y $\mathcal{N}$ es sumando directo de $\mathcal{M}$. Así, $\mathcal{M} = \mathcal{N} \oplus Im(Id_{\mathcal{M}} - f)$.

Ahora, se demuestra que $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ es un conjunto linealmente independiente. Para esto, si $\boldsymbol{u} = \sum_{j=1}^{n} \lambda_j \boldsymbol{v}_j = 0$ con $\lambda_j \in \mathcal{R}$, entonces $\Phi(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{u}, \boldsymbol{v}_{j+1}, \ldots \boldsymbol{v}_n) = \lambda_j = 0$, para todo $1 \leq j \leq n$. □

1.1.2. Sucesiones exactas.

Definición 1.21. Sean $\{\mathcal{M}_i\}_{i\in\mathbb{Z}}$ una sucesión de $\mathcal{R}$-módulos y una sucesión de $\mathcal{R}$-homomorfismos $\{f_i : \mathcal{M}_i \longrightarrow \mathcal{M}_{i+1}\}_{i\in\mathbb{Z}}$. La sucesión (finita o infinita)

$$\ldots \xrightarrow{f_{i+2}} \mathcal{M}_{i+1} \xrightarrow{f_{i+1}} \mathcal{M}_i \xrightarrow{f_i} \mathcal{M}_{i-1} \xrightarrow{f_{i-1}} \ldots$$

es llamada exacta en el término $\mathcal{M}_i$ si cumple que $Im(f_{i+1}) = ker(f_i)$ para $i \in \mathbb{Z}$. Se dice que la sucesión es exacta, si es exacta en todos sus términos, es decir, $Im(f_{i+1}) = ker(f_i)$ para todo $i \in \mathbb{Z}$. Una sucesión exacta corta es una sucesión exacta de la forma

$$0 \longrightarrow \mathcal{M}' \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}'' \longrightarrow 0. \tag{1.1.1}$$

Proposición 1.22. (Anderson and Fuller, Proposición 3.12) Sean $\mathcal{M}, \mathcal{M}'$,$\mathcal{M}''$ $\mathcal{R}$-módulos y f, g $\mathcal{R}$-homomorfismos. Se cumple que:

1. La sucesión $0 \longrightarrow \mathcal{M}' \xrightarrow{f} \mathcal{M}$ es exacta si y sólo si f es $\mathcal{R}$-monomorfismo.
2. La sucesión $\mathcal{M} \xrightarrow{g} \mathcal{M}'' \longrightarrow 0$ es exacta si y sólo si g es $\mathcal{R}$-epimorfismo.
3. La sucesión $0 \longrightarrow \mathcal{M}' \xrightarrow{f} \mathcal{M} \longrightarrow 0$ es exacta si y sólo si f es $\mathcal{R}$-isomofismo.

Observación 1.23. En la sucesión exacta corta dada en la ecuación (1.1.1), note que $\mathcal{M}' \cong Im(f) = f(\mathcal{M}') \subseteq \mathcal{M}$. Entonces, $\mathcal{M}'$ es isomorfo a un submódulo de $\mathcal{M}$. Además,

$$\mathcal{M}'' \cong \frac{\mathcal{M}}{ker(g)} = \frac{\mathcal{M}}{Im(f)}.$$

Así, dados $\mathcal{M}$ y $\mathcal{N}$ dos $\mathcal{R}$-módulos, podemos construir una sucesión exacta corta

$$0 \longrightarrow \mathcal{N} \xrightarrow{i} \mathcal{M} \xrightarrow{\pi} \frac{\mathcal{M}}{\mathcal{N}} \longrightarrow 0$$

donde i es la inclusión y π es la proyección natural.

Ejemplo 1.24. La sucesión $0 \xrightarrow{j} \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \frac{\mathbb{Z}}{\langle 2\rangle} \xrightarrow{j} 0$ es exacta, con $j : 0 \longrightarrow \mathbb{Z}$ el $\mathbb{Z}$-homomorfismo nulo y f, g $\mathbb{Z}$-homomorfismos definidos de la siguiente manera:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$f(n) \longmapsto 2 \cdot n$$

y

$$g : \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{\langle 2\rangle}$$

$$g(n) \longmapsto \overline{n} \text{ mód } 2.$$

En efecto, como $Im(j) = \{0\} = ker(f)$, la sucesión es exacta para el primer término $\mathbb{Z}$. Ahora, puesto que $Im(f) = \langle 2\rangle = ker(g)$, la sucesión es exacta para el segundo término $\mathbb{Z}$. Finalmente, como $Im(g) = \frac{\mathbb{Z}}{\langle 2\rangle} = ker(j)$ y la sucesión es exacta para el término $\frac{\mathbb{Z}}{\langle 2\rangle}$.

Proposición 1.25. (Anderson and Fuller, Proposición 5.12) Dada un sucesión exacta corta

$$0 \longrightarrow \mathcal{A} \xrightarrow{f} \mathcal{B} \xrightarrow{g} \mathcal{M} \longrightarrow 0$$

de $\mathcal{R}$-módulos, las siguientes afirmaciones son equivalentes:

1. $Im(f)$ es sumando directo de $\mathcal{B}$,

2. Existe $g' : \mathcal{M} \longrightarrow \mathcal{B}$ un $\mathcal{R}$-homomorfismo tal que $g \circ g' = Id_{\mathcal{M}}$,

3. Existe $f' : \mathcal{B} \longrightarrow \mathcal{A}$ un $\mathcal{R}$-homomorfismo tal que $f' \circ f = Id_{\mathcal{A}}$.

Demostración. $1 \Rightarrow 2$ En efecto, considere $\mathcal{B} = Im(f) \oplus B_1$, donde B_1 es un submódulo de $\mathcal{B}$. Entonces, como la sucesión es exacta, $\mathcal{B} = ker(g) \oplus B_1$. Sea $g_1 = g|_{B_1}$, se tiene que

$$\mathcal{M} = g(\mathcal{B}) = g(ker(g) \oplus B_1) = g(B_1) = g_1(B_1),$$

entonces g_1 es un $\mathcal{R}$-epimorfismo. Además, $ker(g_1) \subseteq ker(g) \cap B_1 = 0$. Luego g_1 es un $\mathcal{R}$-isomorfismo de B_1 en $\mathcal{M}$ y se define $g' = g_1^{-1} : \mathcal{M} \longrightarrow \mathcal{B}$. Entonces, $g \circ g' = Id_{\mathcal{M}}$. $2 \Rightarrow 1$ Note que $\mathcal{B} = ker(g) \oplus g' \circ g(\mathcal{B})$. Si $b \in \mathcal{B}$, entonces $b = (b - g'g(b)) + g'g(b)$. Ahora,

$$g(b - g'g(b)) = g(b) - gg'g(b) = g(b) - Id_{\mathcal{M}}g(b) = g(b) - g(b) = 0$$

así, $b - g'g(b) \in ker(g)$. Si $a \in kerg \cap g'g(\mathcal{B})$ entonces $a = g'g(b)$ para algún $b \in \mathcal{B}$ y $g(a) = 0$. Luego,

$$0 = g(a) = g(g'g(b)) = g(b),$$

entonces $a = 0$ y así $\mathcal{B} = kerg \oplus g'g(\mathcal{B}) = Im(f) \oplus g'g(\mathcal{B})$.

$1 \Rightarrow 3$ Escribiendo $\mathcal{B} = Im(f) \oplus B_1$, donde B_1 es un submódulo de $\mathcal{B}$. Podemos definir

$f' : \mathcal{B} \longrightarrow \mathcal{A}$, como $\mathcal{B}$ es suma directa, $b = b_1 + b_2$ donde $b_1 \in Im(f)$ y $b_2 \in B_1$, como f es un $\mathcal{R}$-monomorfismo, existe un único $a \in \mathcal{A}$ tal que $f(a) = b$. Así defino, $f'(b) = a$. Note que f' es un $\mathcal{R}$-homomorfismo y para cada $a \in \mathcal{A}, f(a) \in Im(f)$ y se escribe $f(a) = f(a) + 0$, así

$$f'(f(a)) = f'(f(a)) + 0 = f'(b) = a,$$

luego, $f' \circ f = Id_{\mathcal{A}}$.

$3 \Rightarrow 1$ Supongamos que existe $f' : \mathcal{B} \longrightarrow \mathcal{A}$ tal que $f' \circ f = Id_{\mathcal{A}}$. Veamos que $\mathcal{B} = Im(f) \oplus ker(f')$. Para todo $b \in \mathcal{B}$, consideramos $b = f \circ f'(a)$. Tomando $a = b + c$, con $b \in Im(f)$ veamos que $c \in ker(f')$. En efecto,

$$f'(c) = f'(a-b) = f'(a) - f'(b) = f'(a) - f' \circ f \circ f'(a) = f'(a) - Id_{\mathcal{A}} \circ f(a) = 0.$$

Para probar que son suma directa, tomamos $y \in Im(f) \cap ker(f')$, como $b \in Im(f)$ existe $a \in \mathcal{A}$ tal que $f(a) = b$. Ahora, si $f'(a) = 0$, implica que $f' \circ f(a) = 0$ luego $a = 0$ y como f es $\mathcal{R}$-monomorfismo se concluye que $b = 0$. □

Definición 1.26. Decimos que una sucesión exacta corta

$$0 \longrightarrow \mathcal{A} \xrightarrow{f} \mathcal{B} \xrightarrow{g} \mathcal{M} \longrightarrow 0$$

se divide, si se cumple alguna (y por tanto todas) de las condiciones de la Proposición 1.25.

Observación 1.27. Si la sucesión anterior se divide entonces $\mathcal{B} = Im(f) \oplus B_1$, donde $B_1 \cong \mathcal{M}$, es decir, $\mathcal{B} \cong \mathcal{A} \oplus \mathcal{M}$.

Ejemplo 1.28. La sucesión del Ejemplo 1.24,

$$0 \xrightarrow{j} \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \frac{\mathbb{Z}}{\langle 2\rangle} \xrightarrow{j} 0$$

no se divide. Caso contrario, si consideramos la sucesión

$$0 \xrightarrow{j} \langle 2\rangle \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \frac{\mathbb{Z}}{\langle 2\rangle} \xrightarrow{j} 0$$

es exacta y se divide.

Definición 1.29. Sea $\mathcal{P}$ un $\mathcal{R}$-módulo, decimos que $\mathcal{P}$ es proyectivo. Si dado un $\mathcal{R}$-epimorfismo $g : \mathcal{M} \longrightarrow \mathcal{N}$ y un $\mathcal{R}$-homomorfismo $h : \mathcal{P} \longrightarrow \mathcal{N}$, entonces existe $h' : \mathcal{P} \longrightarrow \mathcal{M}$ tal que $h = g \circ h'$, es decir, el siguiente diagrama es conmutativo

$$\begin{array}{ccccc} & & \mathcal{P} & & \\ & \overset{h'}{\swarrow} & \downarrow h & & \\ \mathcal{M} & \xrightarrow{g} & \mathcal{N} & \longrightarrow & 0. \end{array}$$

Por ejemplo, si $\mathcal{P}$ es libre, entonces $\mathcal{P}$ es proyectivo. De hecho, si $\mathcal{P}$ es libre, siempre se puede completar el diagrama anterior por la propiedad universal de módulos libres. Lo contrario no se cumple, es decir, si $\mathcal{P}$ es proyectivo entonces no siempre $\mathcal{P}$ es libre. Para esto en el Ejemplo 1.32 se propone un contraejemplo, pero antes de verlo es necesaria la Proposición 1.30 que caracteriza los módulos proyectivos como sumando directo de $\mathcal{R}$-módulos libres y por sucesiones exactas cortas que se dividen.

Proposición 1.30. (Lam, Proposición 1.2) Las siguientes afirmaciones son equivalentes:

1. $\mathcal{P}$ es un $\mathcal{R}$-módulo proyectivo,

2. $\mathcal{P}$ es sumando directo de un $\mathcal{R}$-módulo libre,

3. Toda sucesión exacta corta

$$0 \longrightarrow \mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{P} \longrightarrow 0$$

se divide.

En otras palabras, $\mathcal{P}$ es un $\mathcal{R}$-módulo proyectivo si es submódulo de un $\mathcal{R}$-módulo libre $\mathcal{M}$ y existe un submódulo $\mathcal{N}$ de $\mathcal{M}$ tal que $\mathcal{P} \oplus \mathcal{N} = \mathcal{M}$. Note que $\mathcal{N}$ también será un $\mathcal{R}$-módulo proyectivo.

Ejemplo 1.31. 1. Las sumas directas y los sumandos directos de módulos proyectivos son proyectivos.

2. Considere los siguientes $\mathbb{Z}$-módulos, $\mathcal{M} = \frac{\mathbb{Z}}{\langle 4 \rangle}$, $\mathcal{N} = \frac{\mathbb{Z}}{\langle 2 \rangle}$ y $\mathcal{P} = \frac{\mathbb{Z}}{\langle 2 \rangle}$. Ahora,

$$\begin{array}{ccccc} & & & & \mathcal{P} \\ & & \overset{h'}{\swarrow} & & \downarrow h \\ \mathcal{M} & \xrightarrow{\pi} & \mathcal{N} & \longrightarrow & 0 \end{array}$$

si π es la proyección de $\mathcal{M} = \frac{\mathbb{Z}}{\langle 4 \rangle}$ en $\mathcal{N} = \frac{\mathbb{Z}}{\langle 2 \rangle}$ y si $h = Id_{\frac{\mathbb{Z}}{\langle 2 \rangle}}$ es la identidad de $\frac{\mathbb{Z}}{\langle 2 \rangle}$, no existe h' un $\mathbb{Z}$-homomorfismo $\mathcal{P}$ en $\mathcal{M}$ tal que $\pi \circ h' = h$. Luego, $\mathcal{P} = \frac{\mathbb{Z}}{\langle 2 \rangle}$ no es proyectivo. Caso contrario sucede si consideramos a $\mathcal{P} = \frac{\mathbb{Z}}{\langle 2 \rangle}$ como un $\frac{\mathbb{Z}}{\langle 2 \rangle}$-módulo, $\mathcal{P}$ es libre y por lo tanto es proyectivo.

Ejemplo 1.32. (Proyectivo no implica libre)

Sean $\mathcal{M} = \frac{\mathbb{Z}}{\langle 6\rangle}$, $\mathcal{N} = \frac{\mathbb{Z}}{\langle 2\rangle}$ y $\mathcal{P} = \frac{\mathbb{Z}}{\langle 3\rangle}$. Es fácil verificar que $\mathcal{M} \cong \mathcal{N} \bigoplus \mathcal{P}$ luego, $\mathcal{N}$ y $\mathcal{P}$ son $\frac{\mathbb{Z}}{\langle 6\rangle}$-módulos proyectivos por la Proposición 1.30, pero no pueden ser libres ya que $\mathcal{N}$ y $\mathcal{P}$ como $\frac{\mathbb{Z}}{\langle 6\rangle}$-módulos son generados por un elemento linealmente dependiente.

1.1.3. Ideales fraccionarios.

Definición 1.33. Sean $\mathcal{R}$ un anillo. Un elemento r en $\mathcal{R}$, es llamado no divisor de cero si $ar = 0$, entonces $a = 0$ para todo $a \in \mathcal{R}$. Tal elemento r también se dice que es regular en $\mathcal{R}$.

Ejemplo 1.34. Todo elemento invertible es regular.

El conjunto de elementos regulares en $\mathcal{R}$ denotado por $C_{\mathcal{R}}$ es un subconjunto multiplicativo y $1_{\mathcal{R}} \in C_{\mathcal{R}}$. La localización de $\mathcal{R}$ por $C_{\mathcal{R}}$ es un anillo conmutativo que denotaremos por $Q(\mathcal{R})$ y tiene la propiedad de que todo elemento regular, en $Q(\mathcal{R})$, es invertible en $Q(\mathcal{R})$, $Q(\mathcal{R})$ se conoce como el anillo total de fracciones de $\mathcal{R}$. Ahora, se estudiarán los $\mathcal{R}$-submódulos invertibles en una extensión $Q(\mathcal{R}) \supseteq \mathcal{R}$. Los $\mathcal{R}$-submódulos de $Q(\mathcal{R})$ son llamados ideales fraccionarios.

Sean $I, J \in Q(\mathcal{R})$ ideales fraccionarios, se definen

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \text{ y } n \in \mathbb{N} \right\} \text{ y}$$

$$I^{-1} = \{k \in Q(\mathcal{R}) : kI \subseteq \mathcal{R}\}.$$

A continuación se presenta una equivalencia entre los módulos proyectivos con los ideales fraccionarios.

Teorema 1.35. *(Lam, Teorema 2.17) Para todo $I \subseteq Q(\mathcal{R})$, las siguientes afirmaciones son equivalentes,*

1. *I es invertible, es decir $II^{-1} = \mathcal{R}$.*

2. *I es $\mathcal{R}$-módulo proyectivo y $I \cap C_{\mathcal{R}} \neq \emptyset$.*

Si se cumple 1 (o 2) por la equivalencia, entonces I es finitamente generado y libre si y sólo si $I = a\mathcal{R}$ para algún $a \in Q(\mathcal{R})$.

Escribimos $\mathfrak{M}(\mathcal{R})$ a la familia de $\mathcal{R}$-módulos finitamente generados y $\mathfrak{B}(\mathcal{R})$ la familia de $\mathcal{R}$-módulos proyectivos finitamente generados.

1.2. Operaciones con matrices elementales

Definición 1.36. Decimos que $M \in M_{n\times n}(\mathcal{R})$ es una matriz elemental si representa la adición de una fila o columna en otra, es decir, la matriz elemental $E_{i,j}(r)$ es la matriz correspondiente a la operación elemental de matrices $F_i \longrightarrow F_i + rF_j$. Estas pueden ser construidas tomando la matriz identidad y reemplazando uno de los elementos nulos por un valor no nulo.

Sea $r \in \mathcal{R}$, la matriz elemental se denota por $E_{i,j}(r)$ donde $i \neq j$ con $1 \leq i, j \leq n$, como la matriz $n \times n$ con unos en la diagonal, con r en la posición (i, j) y cero en el resto de las entradas.

Ejemplo 1.37. Sea $E \in M_{4\times 4}(\mathcal{R})$, se tiene que

$$E_{2,3}(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Observación 1.38. Se denota como $E_n(\mathcal{R})$ al grupo multiplicativo de las matrices elementales de orden $n \times n$, por $GL_n(\mathcal{R})$ al grupo de las matrices invertibles de orden $n \times n$ y $E_{n+m}(\mathcal{R})$ es el grupo de las matrices bloque que tienen la forma $\begin{pmatrix} I_m & 0 \\ 0 & I_n \end{pmatrix}$.

Como $\mathcal{R}$ es un anillo y $n \geq 2$ entonces $E_n(\mathcal{R})$ es subgrupo de $GL_n(\mathcal{R})$, y por lo tanto $E_n(\mathcal{R})$ es subgrupo de $SL_n(\mathcal{R})$.

Lema 1.39. Lema de Whitehead (Lam, Lema 5.1) Para $A, B \in GL_n(\mathcal{R})$, se tiene que

$$\begin{pmatrix} AB & 0 \\ 0 & I_n \end{pmatrix} \in \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cdot E_{2n}(\mathcal{R}).$$

Demostración. En efecto, se tiene que

$$\begin{pmatrix} AB & A \\ 0 & I_n \end{pmatrix} \cdot \begin{pmatrix} I_n & -B^{-1} \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & I_n \end{pmatrix}.$$

ya que

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cdot \begin{pmatrix} I_n & 0 \\ B^{-1} & I_n \end{pmatrix} = \begin{pmatrix} A & 0 \\ I_n & B \end{pmatrix}$$

$$\begin{pmatrix} A & 0 \\ I_n & B \end{pmatrix} \cdot \begin{pmatrix} I_n & -B \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} A & -AB \\ I_n & 0 \end{pmatrix}$$

$$\begin{pmatrix} A & -AB \\ I_n & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} = \begin{pmatrix} AB & A \\ 0 & I_n \end{pmatrix}$$

$$\begin{pmatrix} AB & A \\ 0 & I_n \end{pmatrix} \cdot \begin{pmatrix} I_n & -B^{-1} \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & I_n \end{pmatrix}.$$

□

El Lema 1.39 afirma que una matriz de la forma $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}$ con $A, A^{-1} \in GL_n(\mathcal{R})$ es equivalente a la matriz identidad por transformaciones elementales.

En (Liu and Li, 2018) se prueba que, para un anillo $\mathcal{R}$ y $n \geq 3$,

$$GL_n(\mathcal{R}[x]) = GL_n(\mathcal{R}) \cdot E_n(\mathcal{R}[x])$$

y como consecuencia de esto, se obtiene el siguiente resultado que será necesario en el siguiente capítulo.

Teorema 1.40. *(Liu and Li, Teorema 4.5) Sean $\mathcal{R}$ un anillo y $n \geq 3$. Entonces, para todo $v(x) \in GL_n(\mathcal{R}[x])$, $v(x)$ es congruente con $v(0)$ módulo $E_n(\mathcal{R}[x])$.*

1.3. La resultante

Definición 1.41. Sean $\mathcal{R}$ un anillo y $\mathcal{R}[x]$ el anillo de polinomios. Consideremos $f, g \in \mathcal{R}[x]$ polinomios de la siguiente forma,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad a_n \neq 0, a_i \in \mathcal{R},$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0, \qquad b_m \neq 0, b_i \in \mathcal{R}$$

de grados n, m respectivamente. Definimos la matriz de Sylvester de f, g denotada por $Syl_x(f, n, g, m)$ como,

$$Syl_x(f,n,g,m) = \underbrace{\begin{bmatrix} a_n & a_{n-1} & \ldots & a_1 & a_0 & & \\ & a_n & a_{n-1} & \ldots & a_1 & a_0 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & & \\ & b_m & b_{m-1} & \ldots & b_1 & b_0 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ & & & b_m & b_{m-1} & \ldots & b_1 & b_0 \end{bmatrix}}_{n+m} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \\ a \end{matrix}}\right\} n \end{matrix}.$$

Los espacios de esta matriz son rellenados con ceros. La matriz de Sylvester puede ser vista

como la matriz cuyas filas son las coordenadas de los polinomios

$$x^{m-1}f, x^{m-2}f, \ldots, xf, f, x^{n-1}g, , \ldots, xg, g$$

en la base

$$x^{m+n-1}, x^{m+n-2}, \ldots, x, 1.$$

Ejemplo 1.42. Sea $\mathcal{R} = \mathbb{Z}$ y consideremos $f, g \in \mathbb{Z}[x]$, definidos como,

$$f(x) = 6x^2 + x \text{ con } deg(f(x)) = 2 \text{ y } g(x) = 3x + 1 \text{ con } deg(g(x)) = 1.$$

Entonces, $Syl_x(f, 2, g, 1)$ es una matriz de orden 3×3. En efecto,

$$Syl_x(f, 2, g, 1) = \begin{pmatrix} 6 & 1 & 0 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}.$$

Definición 1.43. Sean $\mathcal{R}$ un anillo y $\mathcal{R}[x]$ su anillo de polinomios. Tomando f y g como en la Definición 1.41, llamamos la resultante de f y g, denotada por $Res_x(f, g)$, con $f \neq 0$ y $g \neq 0$, $n + m \geq 1$, como

$$Res_x(f, g) = det(Syl_x(f, n, g, m)).$$

Ejemplo 1.44. Sean $\mathcal{R} = \mathbb{Z}$, $f(x) = 6x^2 + x$ y $g(x) = 3x + 1$. Entonces por el Ejemplo 1.42, se

tiene que

$$Res_x(f,g) = det(Syl_x(f,2,g,1)) = \begin{vmatrix} 6 & 1 & 0 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{vmatrix} = 3.$$

Considerando f y g como en la Definición 1.43 y usando las propiedades del determinante, se tiene que

$$Res_x(f,g) = (-1)^{nm} Res_x(g,f), \tag{1.3.1}$$

$$Res_x(cf,kg) = c^n k^m Res_x(f,g) \; con \; c,k \in \mathcal{R}. \tag{1.3.2}$$

Proposición 1.45. (Yengui, Proposición 52) Si $n = deg(f) \geq 1$ y $m = deg(g) \geq 1$ entonces $Res_x(f,g) \in \langle f,g \rangle \cap \mathcal{R}$. Además se pueden calcular $h,l \in \mathcal{R}[x]$ con $deg(h) < m$ y $deg(l) < n$ tales que,

$$h(x)f(x) + l(x)g(x) = Res_x(f,g) \in \mathcal{R}.$$

Demostración. Consideremos la matriz de Sylvester de los polinomios f y g

$$Syl_x(f,g) = \begin{bmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & & \\ & a_n & a_{n-1} & \dots & a_1 & a_0 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ & & & b_m & b_{m-1} & \dots & b_1 & b_0 \end{bmatrix}.$$

Por la *expansión de Laplace*, la cual establece que el determinante de una matriz cuadrada de tamaño n puede ser calculado por medio de los cofactores de la siguiente forma, si $A = [b_{ij}]_{n\times n}$ Entonces

$$\begin{aligned} det(A) =& C_{1i}b_{1i} + C_{2i}b_{2i} + \ldots + C_{ni}b_{ni}, \\ =& C_{j1}b_{j1} + C_{j2}b_{j2} + \ldots + C_{jn}b_{jn}, \end{aligned}$$

donde $C_{ij} = (-1)^{i+j}|M_{ij}|$ con M_{ij} la submatriz de A eliminando la fila i-ésima y la columna j-ésima. Calculando los cofactores de la $(n+m)$-ésima columna de $Syl_x(f,n,g,m)$, y notándolos

por $S_i = Cof(Syl_x(f,n,g,m))_{i,n+m}$, tenemos que,

$$\sum_{i=1}^{n+m} S_i[Syl_x(f,n,g,m)]_{i,n+m} = Res_x(f,g) \quad y \tag{1.3.3}$$

$$\sum_{i=1}^{n+m} S_i[Syl_x(f,n,g,m)]_{i,j} = 0 \tag{1.3.4}$$

para $j \neq n+m$, con $[Syl_x(f,n,g,m)]_{i,j}$ la componente i,j de la matriz de Sylvester. Considerando la igualdad

$$Syl_x(f,n,g,m) \begin{bmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x^n \\ x^{n-1} \\ \vdots \\ x \\ 1 \end{bmatrix} = \begin{bmatrix} x^{m-1}f \\ x^{m-2}f \\ \vdots \\ f \\ x^{n-1}g \\ \vdots \\ xg \\ g \end{bmatrix} \tag{1.3.5}$$

y los siguientes polinomios derivados de ella

$$h(x) = S_1 x^{m-1} + S_2 x^{m-2} + \ldots + S_{m-1}x + S_m, \tag{1.3.6}$$

$$l(x) = S_{m+1} x^{n-1} + S_{m+2} x^{n-2} + \ldots + S_{m+n-1}x + S_{n+m}. \tag{1.3.7}$$

Se obtienen los términos x^i del vector de la ecuación (1.3.5) por los S_j obtenidos anteriormente. Entonces de (1.3.3), (1.3.4), (1.3.5), (1.3.6) y (1.3.7) resulta que

$$\begin{aligned}
h(x)f(x)+l(x)g(x) =& S_1 x^{m-1} f(x) + S_2 x^{m-2} f(x) + \ldots + S_{m-1} x f(x) + S_m f(x) + \\
&+ S_{m+1} x^{n-1} g(x) + S_{n+2} x^{n-2} g(x) + \ldots + S_{m+n} g(x) \\
&= \sum_{j=1}^{m+n} S_1 [Syl_x(f,g)]_{1,j} x^{m+n-j} + \sum_{j=1}^{m+n} S_2 [Syl_x(f,g)]_{2,j} x^{m+n-j} + \ldots \\
&+ \sum_{j=1}^{m+n} S_{m+n} [Syl_x(f,g)]_{m+n,j} x^{m+n-j} \\
&= \sum_{i=1}^{m+n} \sum_{j=1}^{m+n} S_i [Syl_x(f,g)]_{i,j} x^{m+n-j} \\
&= \sum_{i=1}^{m+n} \left(\sum_{j=1}^{m+n} S_i [Syl_x(f,g)]_{i,j} \right) x^{m+n-j} \\
&= \sum_{i=1}^{m+n} S_i [Syl_x(f,g)]_{i,m+n} = Res_x(f,g).
\end{aligned}$$

□

En el siguiente ejemplo calcularemos polinomios $h, l \in \mathbb{Z}[x]$ para los polinomios f, g del Ejemplo 1.42 siguiendo la prueba constructiva de la proposición anterior.

Ejemplo 1.46. Sean

$$f(x) = 6x^2 + x \text{ con } deg(f(x)) = 2 \text{ y } g(x) = 3x + 1 \text{ con } deg(g(x)) = 1.$$

Por la Proposición 1.3.3 existen $h(x), l(x) \in \mathcal{R}[x]$ con $deg(h(x)) < 1$ y $deg(l(x)) < 2$ tal que

$$Res_x(f,g) = h(x)f(x) + l(x)g(x).$$

Consideramos la matriz de Sylvester de los polinomios f y g

$$Syl_x(f,2,g,1) = \begin{pmatrix} 6 & 1 & 0 \\ 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}$$

y calculamos los cofactores de tercera columna y los denotamos por S_i para $i \in \{1,2,3\}$, obtenemos que

$$Res_x(f,g) = \sum_{i=1}^{3} [Syl_x(f,g)]_{i,3} S_i = 0\begin{vmatrix} 3 & 1 \\ 0 & 3 \end{vmatrix} - 0\begin{vmatrix} 6 & 1 \\ 0 & 3 \end{vmatrix} + 1\begin{vmatrix} 6 & 1 \\ 3 & 1 \end{vmatrix} = 3.$$

Así,

$$S_1 = (-1)^{1+3}\begin{vmatrix} 3 & 1 \\ 0 & 3 \end{vmatrix}, \quad S_2 = (-1)^{2+3}\begin{vmatrix} 6 & 1 \\ 0 & 3 \end{vmatrix} \quad \text{y} \quad S_3 = (-1)^{3+3}\begin{vmatrix} 6 & 1 \\ 0 & 3 \end{vmatrix}.$$

Luego, $h(x) = S_1x^0$ y $l(x) = S_2x + S_3x^0$. Calculado cada S_i obtenemos que

$$h(x) = 9 \text{ y } l(x) = -18x + 3$$

Finalmente, verificamos que

$$Res_x(f,g) = h(x)f(x) + l(x)g(x) = 9(6x^2 + x) + (-18x + 3)(3x + 1) = 3.$$

Corolario 1.47. (Lombardi and Quitté, Corolario 7.2) Sean f y g en $\mathcal{R}[x]$, $\mathcal{R} \subseteq L$ una extensión del anillo $\mathcal{R}$ y $a \in L$ tal que $f(a) = g(a) = 0$, entonces $Res_x(f,g) = 0$.

Demostración. Sea $\alpha = Res_x(f,g)$. Por la Proposición 1.45, existen $h(x)$ y $l(x)$ tales que

$$Res_x(f,g) = h(x)f(x) + l(x)g(x).$$

En particular, $\alpha = h(a)f(a) + l(a)g(a)$. Como $a \in L$ es una raíz de f y g, tenemos que $\alpha = 0$. □

Ahora se presentarán algunas propiedades que resultan de operar la resultante $Res_x(f,g)$ y que facilitarán los cálculos aritméticos y algebraicos del Capítulo dos.

Lema 1.48. (Lombardi and Quitté, Lema 7.3) Sean f y g polinomios en $\mathcal{R}[x]$ con f un polinomio mónico de grado n.

1. Si $\mathcal{M} = \frac{\mathcal{R}[x]}{\langle f \rangle}$ es un $\mathcal{R}$-módulo libre de grado n y μ_g es la multiplicación por la clase de g en $\mathcal{M}$, es decir, $\mu_g : \mathcal{M} \longrightarrow \mathcal{M}$ definido como $\mu_g(y) = gy$, entonces, $det(\mu_g) = Res_x(f,g)$.

2. Sea $h \in \mathcal{R}[x]$, entonces $Res_x(f,gh) = Res_x(f,g)Res_x(f,h)$ y $Res_x(f,g+fh) = Res_x(f,g)$.

Demostración. 1. Consideremos $g \in \mathcal{R}[x]$ con $deg(g) = m \geq 1$. Como el polinomio f es mónico, la matriz de Sylvester

$$Syl_x(f,g) = \begin{bmatrix} 1 & a_{n-1} & \dots & a_1 & a_0 & & & & \\ & 1 & a_{n-1} & \dots & a_1 & a_0 & & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ & & & 1 & a_{n-1} & \dots & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ & & & & b_m & b_{m-1} & \dots & b_1 & b_0 \end{bmatrix}$$

la podemos llevar a la matriz

$$S' = \begin{bmatrix} 1 & a_{n-1} & \dots & a_1 & a_0 & & \\ & 1 & a_{n-1} & \dots & a_1 & a_0 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ & & & 1 & a_{n-1} & \dots & a_1 & a_0 \\ 0 & \dots & 0 & & & & & \\ \vdots & \ddots & 0 & & & M_g & & \\ 0 & \dots & 0 & & & & & \end{bmatrix}$$

donde M_g es una matriz que contiene los residuos de dividir $x^{n-1}g, x^{n-2}g, \dots, xg$, g por el polinomio f, así la matriz M_g es la matriz de orden $n \times n$ que representa al endomorfismo μ_g sobre la base canónica de los polinomios. Luego,

$$Res_x(f,g) = det(Syl_x(f,g)) = det(S') = det(M_g) = det(\mu_g).$$

2. *a*) Para la primera igualdad, usamos el ítem anterior,

$Res_x(f,gh) = det(\mu_{gh})$ y como $\mu_{gh} = \mu_g \circ \mu_h$, entonces, por operaciones de operado-

res lineales y propiedades del determinante, tenemos que

$$Res_x(f, gh) = det(\mu_{gh}) = det(\mu_g)det(\mu_h) = Res_x(f, g)Res_x(f, h).$$

b) La segunda igualdad se prueba de manera análoga. En efecto,

$Res_x(f, g + fh) = det(\mu_{g+fh})$ y como $det(\mu_{g+fh}) = det(\mu_g)$ entonces, por operaciones de operadores lineales y propiedades del determinante, tenemos que

$$Res_x(f, g + fh) = det(\mu_{g+fh}) = det(\mu_g) = Res_x(f, g).$$

□

Para las siguientes proposiciones es importante tener en cuenta que $\mathbb{K}$ denotará un cuerpo y $\mathbb{K}^*$ denotará las unidades del cuerpo $\mathbb{K}$.

Proposición 1.49. (Yengui, Corolario 53) Sean f y g polinomios en $\mathbb{K}[x]$ de grado $n, m \geq 1$ respectivamente, con $Res_x(f, g) = 0$, entonces f y g tienen el máximo común divisor de grado mayor o igual a 1.

Demostración. Tenemos que $Res_x(f, g) = 0$, por la Proposición 1.45, existen $h, l \in \mathbb{K}[x]$ con $deg(h(x)) < m$ y $deg(l(x)) < n$ tales que

$$0 = Res_x(f, g) = h(x)f(x) + l(x)g(x),$$

así, $h(x)f(x) = -l(x)g(x)$. Note que el polinomio $h(x)f(x) = -l(x)g(x)$ tiene grado menor o igual $m+n$, luego el mínimo común múltiplo entre f y g tiene grado menor que $m+n$. Como $\mathbb{K}[x]$ es un dominio de integridad, entonces cumple la siguiente relación

$$m.c.m(f,g)m.c.d(f,g) = \alpha fg$$

con $\alpha \in \mathbb{K}^*$. Luego, $deg(m.c.d(f,g)) \leq 1$. □

Lema 1.50. (Lombardi and Quitté, Lema 7.5) Sean $f, g \in \mathbb{K}[x]$ con f mónico de grado n, entonces el ideal de eliminación $\mathcal{I} = \langle f, g\rangle \cap \mathcal{R}$ satisface $\mathcal{I}^n \subseteq \langle Res_x(f,g)\rangle \subseteq \mathcal{I}$. En particular,

1. $Res_x(f,g)$ es invertible si, y sólo si, $1 \in \langle f, g\rangle$.

2. $Res_x(f,g)$ no es divisor de cero si, y sólo si, $Ann(\mathcal{I}) = 0$, donde $Ann(\mathcal{I})$ es el anulador de $\mathcal{I}$.

3. $Res_x(f,g)$ es nilpotente si, y sólo si, $\mathcal{I}$ es nilpotente.

Demostración. Por la Proposición 1.45, existen $h(x), l(x) \in \mathbb{K}[x]$ tales que $Res_x(f,g) = h(x)f(x) + l(x)g(x)$. Consideramos $\mathcal{M} = \frac{\mathcal{R}[x]}{\langle f\rangle}$ y $1, \overline{x} \in \mathcal{M}$. Una base de $\mathcal{M}$ sobre $\mathcal{R}$ es $\{\overline{x}, \ldots, \overline{x}^{n-1}\}$. Note que la inclusión $\langle Res_x(f,g)\rangle \subseteq \mathcal{I}$ es clara. Veamos que $\mathcal{I}^n \subseteq \langle Res_x(f,g)\rangle$, en efecto, sea $\alpha_i \in \mathcal{I}$ para $1 \leq i \leq n$ con $\alpha_i = h_i(x)f(x) + l_i(x)g(x)$ donde $h_i(x), l_i(x) \in \mathbb{K}[x]$. Por el Lema 1.48, $\alpha_1, \alpha_2\overline{x}, \ldots, \alpha_n\overline{x}^{n-1} \in Im(\mu_g)$, donde μ_g es la multiplicación por la clase de g en $\mathcal{M}$, luego la

matriz

$$D = \begin{pmatrix} \alpha_1 & & & & \\ & \alpha_2 & & & \\ & & \alpha_3 & & \\ & & & \ddots & \\ & & & & \alpha_n \end{pmatrix} = GB$$

donde G es la matriz que representa a μ_g en la base canónica $\{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$ y

$$B = \begin{pmatrix} g_1 & 0 & \ldots & & 0 \\ 0 & g_2 & \ldots & & \vdots \\ \vdots & \vdots & \ddots & & 0 \\ 0 & 0 & 0 & \ldots & g_n \end{pmatrix}.$$

Por tanto,

$$\prod_{i=1}^{n} \alpha_i = det(D) = det(GB) = det(G)det(B) = Res_x(f,g)Det(B)$$

y así, $\prod_{i=1}^{n} \alpha_i \in \langle Res_x(f,g) \rangle$. □

1.4. Dimensión de Krull

Definición 1.51. Sea $\mathcal{R}$ un anillo, definimos la dimensión de Krull como el supremo de los enteros n tales que existe una cadena de ideales primos en $\mathcal{R}$, es decir, $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_n$ en $\mathcal{R}$. Por convención, si existe una cadena infinita de ideales en el anillo, entonces decimos que la dimensión de Krull del anillo es infinita.

Ejemplo 1.52.

1. La dimensión de Krull de un cuerpo es cero.

2. Para el anillo de enteros $\mathbb{Z}$ sus ideales primos son $\langle 0\rangle$ y $\langle \mathfrak{p}\rangle = \mathfrak{p}\mathbb{Z}$, para $\mathfrak{p} > 0$ entero primo. Por lo tanto las cadenas mas largas de ideales primos en $\mathbb{Z}$ son todas de la forma $\langle 0\rangle \subsetneq \langle \mathfrak{p}\rangle$ y así el anillo $\mathbb{Z}$ tiene dimensión de Krull igual a uno.

3. Un dominio de ideales principales que no sea cuerpo tiene dimensión de Krull igual a uno por el Teorema del ideal principal de Krull (Eisenbud, Teorema 10.1).

4. El anillo de polinomios en n indeterminadas $\mathbb{K}[x_1, \ldots, x_n]$ con $\mathbb{K}$ cuerpo, tiene dimensión de Krull igual a n. En particular, el anillo $\mathbb{C}[x]$ tiene dimensión de Krull igual a uno (Coquand and Lombardi, Corolario 4).

Definición 1.53. Sea $\mathcal{R}$ un anillo. Definimos el espectro de $\mathcal{R}$, $Spec(\mathcal{R})$, como el conjunto de todos los ideales primos de $\mathcal{R}$, es decir,

$$Spec(\mathcal{R}) = \{\mathfrak{p} \subseteq \mathcal{R} : \mathfrak{p} \text{ es un ideal primo de } \mathcal{R}\}.$$

Se introduce una topología en $Spec(\mathcal{R})$ asociando a cada subconjunto E de $\mathcal{R}$ el conjunto

$$V(E) = \{\mathfrak{p} \in Spec(\mathcal{R}) \mid \mathfrak{p} \supseteq E\}.$$

En particular, si $\mathcal{I} = \langle E \rangle$ es el ideal generado por los elementos de E, entonces $V(E) = V(\mathcal{I})$, por lo que de ahora en adelante nos restringimos a considerar sólo los conjuntos $V(\mathcal{I})$.

Proposición 1.54. (Elizondo, Lema 1.10) Sea $\mathcal{R}$ un anillo. Entonces,

1. $V(\mathcal{R}) = \emptyset$ y $V(0) = Spec(\mathcal{R})$,
2. Si $\mathcal{I}, \mathcal{J}$ son ideales de $\mathcal{R}$, entonces $V(\mathcal{I}\mathcal{J}) = V(\mathcal{I}) \cup V(\mathcal{J})$,
3. Sea $k \in \mathbb{N}$. Si $\mathcal{I}_k$ son ideales de $\mathcal{R}$, entonces $V\left(\bigcup_k \mathcal{I}_k\right) = V\left(\sum_k \mathcal{I}_k\right) = \bigcap_k V\left(\mathcal{I}_k\right)$,
4. Si $\mathcal{I} \subseteq \mathcal{J}$ son ideales de $\mathcal{R}$, entonces $V(\mathcal{I}) \supseteq V(\mathcal{J})$.

La topología definida por cerrados $V(\mathcal{I})$, donde $\mathcal{I}$ es cualquier ideal de $\mathcal{R}$, es llamada la topología de $Zariski$. El complemento de dichos conjuntos cerrados es

$$\bigcup_{a \in \mathcal{I}} \{\mathfrak{p} \in Spec(\mathcal{R}) \mid a \notin \mathfrak{p}\},$$

la base natural para estos abiertos son los conjuntos

$$D(a) = \{\mathfrak{p} \in Spec(\mathcal{R}) \mid a \notin \mathfrak{p}\}.$$

Los conjuntos $D(a)$, variando $a \in \mathcal{I}$, forman una base para la topología de $Spec(\mathcal{R})$.

Definición 1.55. Si $\mathcal{I} \subseteq \mathcal{R}$ es un ideal, su radical es el conjunto

$$\sqrt{\mathcal{I}} = \{a \in \mathcal{R} : a^n \in \mathcal{I} \text{ para algún entero } n \geq 1 \},$$

$\sqrt{\mathcal{I}}$ es un ideal de $\mathcal{R}$. Para el caso particular del ideal $0 \subseteq \mathcal{R}$, el radical $\sqrt{0}$ se llama nilradical del anillo $\mathcal{R}$.

Observación 1.56. Si $\mathcal{I} \subseteq \mathcal{R}$ es cualquier ideal, entonces $\sqrt{\mathcal{I}} = \bigcap_{\mathfrak{p} \supseteq \mathcal{I}} \mathfrak{p}$. En particular, $\sqrt{0} = \bigcap_{\mathfrak{p} \in Spec(\mathcal{R})}$.

A continuación se prueban las propiedades de la base de la topología de *Zariski* que son muy necesarias para el objetivo de la sección.

Proposición 1.57. (López Soria, Proposición 7.1) Sean $a, b \in \mathcal{R}$, entonces,

1. $D(1) = Spec(\mathcal{R})$,
2. $D(0) = \emptyset$,
3. $D(ab) = D(a) \cap D(b)$,
4. $D(a+b) \subseteq D(a) \cup D(b)$,
5. $D(b) = \emptyset$ si y sólo si b es nilpotente,
6. Si $Spec(\mathcal{R}) = D(b_1) \cup \ldots \cup D(b_n)$ entonces $\langle b_1, \ldots, b_n \rangle = \mathcal{R}$.

Demostración. 1. Puesto que ningún ideal primo contiene el elemento unidad, en particular para todo $a \in \mathcal{R}^*$, se tiene que $D(a) = Spec(\mathcal{R})$.

2. Note que $0 = \langle 0 \rangle_{\mathcal{R}} \subseteq \mathfrak{p}$, para todo $\mathfrak{p} \in Spec(\mathcal{R})$.

3. Veamos que $D(ab)$ esta contenido en $D(a) \cap D(b)$, y viceversa. Sea $\mathfrak{p} \in D(ab)$, $ab \notin \mathfrak{p}$, entonces $a \notin \mathfrak{p}$ y $b \notin \mathfrak{p}$, luego $\mathfrak{p} \in D(a) \cap D(b)$. Si $\mathfrak{p} \in D(a) \cap D(b)$, entonces $\mathfrak{p} \in D(a)$ y $\mathfrak{p} \in D(b)$, $a \notin \mathfrak{p}$ y $b \notin \mathfrak{p}$, en consecuencia $ab \notin \mathfrak{p}$, por lo tanto $\mathfrak{p} \in D(a) \cap D(b)$.

4. Sea $\mathfrak{p} \in D(a+b)$ entonces $a+b \notin \mathfrak{p}$, como $(\mathfrak{p}, +)$ es un subgrupo de $(\mathcal{R}, +)$, $a \notin \mathfrak{p}$ o $b \notin \mathfrak{p}$, luego $\mathfrak{p} \in D(a) \cup D(b)$.

5. Sea $b \in \mathfrak{p}$, para todo $\mathfrak{p} \in Spec(\mathcal{R})$ y como $\bigcap_{\mathfrak{p} \in Spec(\mathcal{R})} \mathfrak{p} = \sqrt{0}$, luego $b^n \in 0$ para algún $n \in \mathbb{Z}$, por lo tanto b es nilpotente. Recíprocamente, como b es nilpotente, tenemos que $b^m = 0$ para algún $m \in \mathbb{N}$, entonces

$$D(b^2) = D(bb) = D(b) \cap D(b) = D(b).$$

Repitiendo este proceso se obtiene que

$$D(b) = \underbrace{D(b) \cap \ldots \cap D(b)}_{m \quad veces} = D(b^m) = D(0) = \emptyset.$$

6. Como $Spec(\mathcal{R}) = D(b_1) \cup \ldots \cup D(b_n)$, calculando complementos, $\emptyset = (D(b_1))^c \cap \ldots \cap (D(b_n)^c = V(b_1) \cap \ldots \cap V(b_n)$. Ahora, por el item 3 de la Proposición 1.54 se tiene que $\emptyset = V\left(\sum_{i=1}^{n} \langle b_i \rangle\right)$,

es decir, $\sum_{i=1}^{n}\langle b_i\rangle = \mathcal{R}$, por lo que concluimos que $\langle b_1,\ldots,b_n\rangle = \mathcal{R}$.

□

Esta topología con las propiedades mostradas en la Proposición 1.57, genera el retículo distributivo $(L_z,\cup,\cap)$, con $L_z = \{D(a) \mid a \in \mathcal{R}\}$ y la inclusión como relación de orden.
Los lemas demostrados a continuación son afirmaciones que se encuentran en la prueba del Teorema 1.63 y que presentamos con detalle. Para esto, necesitaremos las siguientes propiedades y conceptos adicionales .

Definición 1.58. Sea $\mathcal{R}$ un anillo. Para $a \in \mathcal{R}$ definimos la frontera de a como el ideal generado por a y los elementos $b \in \mathcal{R}$ tales que ab es nilpotente o de manera equivalente $D(ab) = \emptyset$. Lo notaremos por $\mathcal{B}(a)$.

La siguiente proposición será de gran utilidad en la prueba del Teorema 1.63 y omitimos su demostración porque la demostración que conocemos usa teoría de retículos y se sale de los alcances de este trabajo.

Proposición 1.59. (Coquand et al., Teorema 8) Sea $\mathcal{R}$ un anillo. $\mathcal{R}$ tiene dimensión de Krull $\leq k$ si, y sólo si, para todo $a \in \mathcal{R}$ se tiene que $\frac{\mathcal{R}}{\mathcal{B}(a)}$ tiene dimensión de Krull $\leq k-1$.

Lema 1.60. Sea $b \in \mathcal{R}$ un elemento nilpotente, entonces $Spec(\mathcal{R}) = D(b_1)\cup\ldots\cup D(b_n)\cup D(b)$ implica que $Spec(\mathcal{R}) = D(b_1)\cup\ldots\cup D(b_n)$.

Demostración. Por la Propiedad 5 de la Proposición 1.57 como b un elemento nilpotente, $D(b) = \emptyset$.

Luego,

$$Spec(\mathcal{R}) = D(b_1) \cup \ldots \cup D(b_n) \cup D(b) = D(b_1) \cup \ldots \cup D(b_n) \cup \emptyset = D(b_1) \cup \ldots \cup D(b_n).$$

□

Lema 1.61. $D(a+b) \cup D(ab) = D(a) \cup D(b)$.

Demostración. Como el retículo $L_z = \{D(a) \mid a \in \mathcal{R}\}$ es distributivo, entonces

$$\begin{aligned} D(a+b) \cup D(ab) &= D(a+b) \cup (D(a) \cap D(b)) \\ &= (D(a+b) \cup D(a)) \cap (D(a+b) \cup D(b)) \end{aligned}$$

queda verificar que $D(a+b) \cup D(a) = D(a) \cup D(b)$.

Es claro que $D(a+b) \cup D(a) \subseteq D(a) \cup D(b)$ por la propiedad 4 de la base de la topología de Zariski. Para la otra probar la otra contencencia supongamos que no se cumple, es decir, existe $\mathfrak{p} \in D(a) \cup D(b)$ y $\mathfrak{p} \notin D(a+b) \cup D(a)$. Entonces $a+b \in \mathfrak{p}$ y $a \in \mathfrak{p}$, como $(\mathfrak{p}, +)$ es un subgrupo de $(\mathcal{R}, +)$ tenemos que $-a \in \mathfrak{p}$. Como $a+b, -a \in \mathfrak{p}$ entonces $b \in \mathfrak{p}$, luego $\mathfrak{p} \notin D(a)$ y $\mathfrak{p} \notin D(b)$, una contradicción, ya que $\mathfrak{p} \in D(a) \cup D(b)$. Luego $D(a) \cup D(b) \subseteq D(a+b) \cup D(a)$. Este resultado

es análogo para $D(a+b)\cup D(b)$, entonces,

$$(D(a+b)\cup D(a))\cap(D(a+b)\cup D(b)) = (D(a)\cup D(b))\cap(D(a)\cup D(b))$$
$$= D(a)\cup D(b).$$

□

Lema 1.62. Sean $a,b\in\mathcal{R}$ tales que ab un elemento nilpotente, entonces $Spec(\mathcal{R}) = D(b_1)\cup\ldots\cup D(b_n)\cup D(a)\cup D(b)$ implica que $Spec(\mathcal{R}) = D(b_1)\cup\ldots\cup D(b_n)\cup D(a+b)$.

Demostración. Por el Lema 1.61, $Spec(\mathcal{R}) = D(b_1)\cup\ldots\cup D(b_n)\cup D(a)\cup D(b) = D(b_1)\cup\ldots\cup D(b_n)\cup D(a+b)\cup D(ab)$ y por el Lema 1.60, se tiene que

$$D(b_1)\cup\ldots\cup D(b_n)\cup D(a+b)\cup D(ab) = D(b_1)\cup\ldots\cup D(b_n)\cup D(a+b).$$

□

Teorema 1.63. *(Yengui, Teorema 91) Si la dimensión de Krull de $\mathcal{R}$ es menor que n y $Spec(\mathcal{R}) = D(a)\cup D(b_1)\cup\ldots\cup D(b_n)$, entonces existen $x_1,x_2,\ldots x_n\in\mathcal{R}$ tales que*

$$Spec(\mathcal{R}) = D(b_1+ax_1)\cup\ldots\cup D(b_n+ax_n).$$

Demostración. Hacemos inducción sobre n. Si $n = 1$,

$$Spec(\mathcal{R}) = D(a) \cup D(b_1).$$

Entonces, por el ítem 6 de la Proposición 1.57, $\langle a, b_1 \rangle = \mathcal{R}$. Luego, $D(a + b_1) = Spec(\mathcal{R})$, con $x_1 = 1$.

Si $n > 1$, se consideran $\mathcal{B}(b_n)$ la frontera de b_n y el anillo $\frac{\mathcal{R}}{\mathcal{B}(b_n)}$ por la Proposición 1.59, $\frac{\mathcal{R}}{\mathcal{B}(b_n)}$ tiene dimensión de Krull igual a $n-1$, entonces por hipótesis de inducción, existen $\overline{x_1}, \ldots, \overline{x_{n-1}} \in \frac{\mathcal{R}}{\mathcal{B}(b_n)}$ tales que

$$Spec\left(\frac{\mathcal{R}}{\mathcal{B}(b_n)}\right) = D(\overline{b_1 + ax_1}) \cup \ldots \cup D(\overline{b_{n-1} + ax_{n-1}})$$

en $\frac{\mathcal{R}}{\mathcal{B}(b_n)}$. Luego existe $x_n \in \mathcal{R}$ tal que $D(b_n x_n) = \emptyset$ y

$$Spec(\mathcal{R}) = D(b_1 + ax_1) \cup \ldots \cup D(b_{n-1} + ax_{n-1}) \cup D(b_n + x_n) \cup D(b_n x_n),$$

por el Lema 1.61

$$Spec(\mathcal{R}) = D(b_1 + ax_1) \cup \ldots \cup D(b_{n-1} + ax_{n-1}) \cup D(b_n) \cup D(x_n),$$

dado que

$$Spec(\mathcal{R}) = D(b_1 + ax_1) \cup \ldots \cup D(b_{n-1} + ax_{n-1}) \cup D(b_n) \cup D(a).$$

Entonces, por la distributividad del retículo, haciendo

$$X = D(b_1 + ax_1) \cup \ldots \cup D(b_{n-1} + ax_{n-1}) \cup D(b_n),$$

se tiene que,

$$\begin{aligned}(X \cup D(x_n)) \cap (X \cup D(a)) &= X \cup (D(x_n) \cap D(a)).\\ &= X \cup D(ax_n).\end{aligned}$$

Finalmente por el Lema 1.60,

$$\begin{aligned}Spec(\mathcal{R}) &= D(b_1 + ax_1) \cup \ldots \cup D(b_{n-1} + ax_{n-1}) \cup D(b_n) \cup D(ax_n)\\ &= D(b_1 + ax_1) \cup \ldots \cup D(b_{n-1} + ax_{n-1}) \cup D(b_n + ax_n).\end{aligned}$$

□

2. Anillos de Hermite

Inicialmente se definen los módulos establemente libres, los cuales son la estructura algebraica de mayor interés en este capítulo. El problema principal consiste en determinar cuándo un módulo establemente libre es libre, se presenta una equivalencia con la teoría matricial bastante útil para estudiar propiedades de los módulos establemente libres y a partir de esto, se definen los anillos de Hermite. Se presentan algunos ejemplos interesantes de anillos de Hermite y la relación de este tipo de anillos con otros anillos. En particular no todo módulo establemente libre es libre, es decir, existen anillos que no son de Hermite, en el Ejemplo 2.33 se ilustra hasta ahora el único anillo que no es de Hermite. Encontrar anillos que no sean de Hermite es un problema abierto, pues no es una tarea fácil demostrarlo. Finalmente entramos en contexto con otro problema abierto muy famoso relacionado con este tipo de anillos, conocido como la Conjetura de Hermite 1, se presentan hasta ahora los resultados más cercanos acerca de esta conjetura.

2.1. Módulos establemente libres

Antes de definir los módulos establemente libres es necesario hacer la aclaración que $\mathcal{R}$ continúa siendo un anillo conmutativo con unidad.

Definición 2.1. Sean $\mathcal{R}$ un anillo y $\mathcal{M}$ un $\mathcal{R}$-módulo. Decimos que $\mathcal{M}$ es establemente libre de tipo n $(0 \leq n \leq \infty)$, si $\mathcal{M} \oplus \mathcal{R}^n$ es libre, es decir, $\mathcal{M} \oplus \mathcal{R}^n \cong \mathcal{R}^m$ para $n, m \geq 0$ apropiados. Esta definición permite concluir que $\mathcal{M}$ es isomorfo al kernel de un epimorfismo $f : \mathcal{R}^m \longrightarrow \mathcal{R}^n$.

Observación 2.2. El módulo $\mathcal{M}$ es proyectivo y si $n = 0$, $\mathcal{M}$ es libre.

Hay una buena razón por la que se quiere restringir n a un cardinal finito. De hecho si no imponemos la restricción, cualquier módulo proyectivo satisface la Definición 2.1. La prueba de esto es una famosa construcción de Eilenberg:

Sean $\mathcal{P} \oplus Q = E$ libre y $F = E \oplus E \oplus E \oplus \dots$ también libre. Entonces

$$\begin{aligned}
\mathcal{P} \oplus F \cong & \mathcal{P} \oplus E \oplus E \oplus E \oplus \dots \\
\cong & \mathcal{P} \oplus (Q \oplus \mathcal{P}) \oplus (Q \oplus \mathcal{P}) \oplus (Q \oplus \mathcal{P}) \oplus \dots \\
\cong & (Q \oplus \mathcal{P}) \oplus (Q \oplus \mathcal{P}) \oplus (Q \oplus \mathcal{P}) \oplus \dots \\
\cong & E \oplus E \oplus E \oplus \dots \\
\cong & F!.
\end{aligned}$$

Luego, $\mathcal{P} \oplus F$ es libre y por lo tanto $\mathcal{P}$ es establemente libre.

Proposición 2.3. (Lam, Proposición 4.2) Si $\mathcal{P}$ es establemente libre, pero no es finitamente generado, entonces $\mathcal{P}$ es libre.

Observación 2.4. Como se observó en la Proposición 2.3, no es necesario que $\mathcal{P}$ establemente libre, sea finitamente generado para ser libre. La Definición 2.1 es de interés en este trabajo principalmente en el caso que $\mathcal{M}$ es finitamente generado. Es por eso, que a partir de ahora limitaremos nuestra atención a $\mathcal{M} \in \mathfrak{M}(\mathcal{R})$.

Ejemplo 2.5. Todo módulo libre es establemente libre. En efecto, se tiene que $\mathcal{M}$ es libre, es decir, existe un conjunto finito $X \subseteq \mathcal{M}$ linealmente independiente tal que $\langle X \rangle = \mathcal{M}$. Como $\mathcal{M}$ es

finitamente generado entonces consideremos el $\mathcal{R}$-homomorfismo:

$$f : \mathcal{M} \longrightarrow \mathcal{R}^n$$

$$\boldsymbol{x}_i \longmapsto e_i$$

con $e_i = (0, \ldots, 1, \ldots, 0)$ donde 1 se encuentra en la posición i-ésima. Entonces f define un $\mathcal{R}$-isomorfismo de módulos, luego $\mathcal{M} \cong \mathcal{R}^n$. En consecuencia $\mathcal{M}$ es establemente libre, puesto que $\mathcal{M} \oplus 0 \cong \mathcal{R}^n$.

Es natural preguntarse si la recíproca es cierta, y la respuesta es que no. En realidad, no es un problema fácil encontrar módulos establemente libres que no sean libres. Para presentar el contraejemplo, es importante la siguiente observación.

Observación 2.6. Por la Definición 2.1, $\mathcal{M}$ es establemente libre de tipo n si $\mathcal{M}$ es isomorfo al kernel de un epimorfismo $f : \mathcal{R}^m \longrightarrow \mathcal{R}^n$. Si consideramos A, la matriz de tamaño $n \times m$ que denota a f, entonces A es invertible a derecha, es decir, existe C de tamaño $m \times n$ tal que $AC = I_m$. Cualquier matriz $A_{n\times m}$ define un $\mathcal{R}$-módulo finitamente generado establemente libre $\mathcal{M}$, de tipo n,

$$\mathcal{M} = \left\{ \alpha = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid \ A \cdot \alpha = 0 \right\},$$

el espacio solución de $A_{n\times m}$. De esta manera, el estudio de $\mathcal{R}$-módulos finitamente generados libres y establemente libres es equivalente a estudiar matrices rectangulares invertibles a derecha sobre $\mathcal{R}$.

Ejemplo 2.7. No todo módulo establemente libre, es libre. En efecto, considere

$$\mathcal{R} = \frac{\mathbb{R}[x,y,z]}{\langle x^2+y^2+z^2-1\rangle}$$

el anillo de polinomios reales sobre la 2-esfera. Y considere

$$T = \{(\overline{y_1},\overline{y_2},\overline{y_3}) \in \mathcal{R}^3 \ \mid \ \overline{x}_1\overline{y}_1+\overline{x}_2\overline{y}_2+\overline{x}_3\overline{y}_3 = 0\}.$$

Veamos que $T \oplus \mathcal{R} \cong \mathcal{R}^3$. En efecto, como $\mathcal{R}$ es un anillo, en $\mathcal{R}^3$ podemos considerar el producto escalar $\cdot : \mathcal{R}^3 \times \mathcal{R}^3 \longrightarrow \mathcal{R}$. Así, $(\overline{x},\overline{y},\overline{z})\cdot(\overline{x},\overline{y},\overline{z}) = \overline{x}^2+\overline{y}^2+\overline{z}^2 = 1$. Para todo $\boldsymbol{x} \in \mathcal{R}^3$, considero $r = \boldsymbol{x}\cdot(\overline{x},\overline{y},\overline{z}) \in \mathcal{R}$. Entonces

$$\begin{aligned}(\boldsymbol{x} - r(\overline{x},\overline{y},\overline{z}))\cdot(\overline{x},\overline{y},\overline{z}) &= \boldsymbol{x}\cdot(\overline{x},\overline{y},\overline{z}) - r(\overline{x},\overline{y},\overline{z})\cdot(\overline{x},\overline{y},\overline{z}) \\ &= r - r(1) = 0.\end{aligned}$$

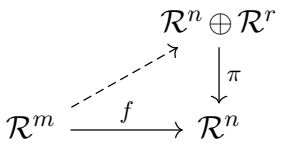
Luego, $(\boldsymbol{x} - r(\overline{x},\overline{y},\overline{z})) \in T$. Así, $\mathcal{R}^3 = T + \mathcal{R}(\overline{x},\overline{y},\overline{z})$. Veamos ahora que es suma directa, es decir. $\mathcal{R}(\overline{x},\overline{y},\overline{z}) \cap T = (0,0,0)$. Si $r(\overline{x},\overline{y},\overline{z}) \in T$, entonces

$$r(\overline{x},\overline{y},\overline{z})\cdot(\overline{x},\overline{y},\overline{z}) = r(1) = 0,$$

luego $r = 0$. Por lo tanto $\mathcal{R}^3 = T \oplus \mathcal{R}(\overline{x}, \overline{y}, \overline{z})$. Es fácil verificar que $\mathcal{R} \cong \mathcal{R}(\overline{x}, \overline{y}, \overline{z})$ por $f : r \longmapsto r(\overline{x}, \overline{y}, \overline{z})$, así $T \oplus \mathcal{R} \cong \mathcal{R}^3$ y T es un módulo establemente libre de rango 2 por la Observación 2.6, pero T no es libre. Para probar esto se usa un argumento topológico que se comentará con detalle a posteriori en el Ejemplo 2.33.

El siguiente resultado proporciona un criterio para determinar cuándo un $\mathcal{R}$-módulo $\mathcal{M}$ establemente libre, es libre.

Teorema 2.8. *(Lam, Proposición 4.3) Sean $f : \mathcal{R}^m \longrightarrow \mathcal{R}^n$ un $\mathcal{R}$-epimorfismo y $\mathcal{M} \cong ker\, f$. $\mathcal{M}$ es libre si, y sólo si, f se puede extender a un $\mathcal{R}$-isomorfismo $\hat{f} : \mathcal{R}^m \to \mathcal{R}^n \oplus \mathcal{R}^r$ tal que $\pi \circ \hat{f} = f$, donde $\pi : \mathcal{R}^n \oplus \mathcal{R}^r \to \mathcal{R}^n$ es la proyección sobre el primer factor,*



Demostración. Sea $\mathcal{M}$ un $\mathcal{R}$-módulo libre de rango r, entonces existe un $\mathcal{R}$-isomorfismo $g : \mathcal{M} \longrightarrow \mathcal{R}^r$ y como $\mathcal{M} \cong ker(f)$, $\mathcal{R}^m \cong \mathcal{N} \oplus \mathcal{M}$, dado que f es un $\mathcal{R}$-epimorfismo, entonces $f_0 = f|_{\mathcal{N}} : \mathcal{N} \longrightarrow \mathcal{R}^n$ es un isomorfismo. Luego $\hat{f} = f_0 \oplus g : \mathcal{R}^m \longrightarrow \mathcal{R}^n \oplus \mathcal{R}^r$ es el isomorfismo deseado.

Recíprocamente, suponga que existe $\hat{f}$, como $\pi \circ \hat{f} = f$, se tiene que $ker(f) \cong ker(\pi) = \mathcal{R}^r$.

□

En la situación anterior, en general $\mathcal{R}^m \cong \mathcal{R}^n \oplus \mathcal{R}^r$ no implica necesariamente que se cumple que $m = n + r$. Sin embargo, en nuestro caso como consideramos $\mathcal{R}$ anillo conmutativo no nulo, $\mathcal{R}$ satisface la IBN.

Ahora veamos la interpretación matricial del Teorema 2.8. Sea A la matriz de tamaño $n \times m$ que denota a f, y sea B la matriz de tamaño $(n+r) \times m$ que denota al isomorfismo $\hat{f}$, si este existe. La condición $\pi \circ \hat{f} = f$ nos dice que A es una submatriz de B, que consiste en sus primeras n filas. La condición de que $\hat{f}$ sea un isomorfismo quiere decir que B es una matriz invertible. Entonces por la observación anterior, el Teorema 2.8 puede ser enunciado de la siguiente manera:

Teorema 2.9. *(Teorema 2.8 Versión matricial) Para cualquier matriz A invertible de tamaño $n \times m$, el espacio solución (establemente libre) de A es libre si, y sólo si, A puede ser complementable a una matriz invertible añadiendo un número adecuado de filas.*

Demostración. Es claro por la Observación 2.6, pero para más detalles ver (Yengui, Proposición 18). □

Definición 2.10. Sea $\mathcal{M}$ un $\mathcal{R}$-módulo libre, en el caso donde $\mathcal{M} \cong \mathcal{R}^n$ se define el siguiente conjunto,

$$Um_n(\mathcal{R}) = \{(x_1, ..., x_n) \in \mathcal{R}^n | \langle x_1, ..., x_n \rangle = \mathcal{R}\}.$$

Los elementos de $Um_n(\mathcal{R})$ se denominan las filas unimodulares de longitud n sobre $\mathcal{R}$ (o $(x_1, \ldots, x_n)^t$ se llama el vector unimodular).

Observación 2.11. Por la Proposición 1.20, en el caso donde $n = 1$, se dice que $\boldsymbol{x}_1 \in \mathcal{M}$ es unimodular si existe una forma lineal $\Phi : \mathcal{M} \longmapsto \mathcal{R}$ tal que $\Phi(\boldsymbol{x}_1) = 1$. Por ejemplo, si $a_1, b_1, \ldots a_n, b_n \in \mathcal{R}$ con $a_1 b_1 + \ldots + a_n b_n = 1$, entonces $\boldsymbol{x} = (a_1, \ldots, a_n)$ es unimodular en $\mathcal{R}^n$.

La correspondencia lineal es

$$\Phi : \mathcal{R}^n \longrightarrow \mathcal{R}$$

$$(a_1, \ldots a_n) \longmapsto a_1 b_1 + \ldots + a_n b_n.$$

Definición 2.12. Si una fila unimodular sobre $\mathcal{R}$ se puede completar a matriz invertible, es decir, se puede escribir como la primera fila de una matriz invertible con entradas en $\mathcal{R}$, decimos que la fila es complementable sobre $\mathcal{R}$.

Ejemplo 2.13. Considerando $\mathcal{R} = \mathbb{Z}$, cada fila unimodular (a, b) de longitud 2 es complementable. De hecho, escribiendo $ac + bd = 1$, la matriz $\begin{pmatrix} a & b \\ -d & c \end{pmatrix}$ tiene determinante 1.

El siguiente resultado es consecuencia del Teorema 2.9 y será necesario para justificar el Ejemplo 2.15.

Teorema 2.14. *(Yengui, Teorema 25) Para todo anillo $\mathcal{R}$, cualquier $\mathcal{R}$-módulo establemente libre $\mathcal{P}$ de rango 1, es libre; es decir, $\mathcal{P} \cong \mathcal{R}$.*

Demostración. Sea $\mathcal{P}$ un $\mathcal{R}$-módulo establemente libre de rango 1, por la Definición 2.1, se cumple que $\mathcal{P} \oplus \mathcal{R}^{n-1} \cong \mathcal{R}^n$ para algún $n \geq 2$, representado como el espacio solución de una matriz invertible M de orden $(n-1) \times n$. Esto es, $\mathcal{P} \cong ker(M)$ y existe $N \in GL_{n\times(n-1)}(\mathcal{R})$ tal que $MN = I_{n-1}$. Probar que $\mathcal{R}$ es libre es equivalente a probar, por el Teorema 2.9, que M puede ser complementable. Sean $b_1, b_2, \ldots, b_n$ los menores maximales de la matriz M, estos son comaximales, es decir, $1 \in \langle b_1, b_2, \ldots, b_n \rangle$. En efecto, sea $\mathfrak{m}$ un ideal maximal de $\mathcal{R}$. Entonces considerando

$\frac{\mathcal{R}}{\mathfrak{m}}$, se obtiene que $\overline{MN} = I_{n-1}$. Como $\overline{M}$ es una matriz invertible y tiene rango $n-1$ se puede completar a una matriz $M_{\mathfrak{m}} \in GL_n(\frac{\mathcal{R}}{\mathfrak{m}})$. Luego $detM_{\mathfrak{m}} \neq \overline{0}$ y por lo tanto $\langle b_1, b_2, \ldots, b_n\rangle \nsubseteq \mathfrak{m}$. De forma que si $a_1b_1 + a_2b_2 + \ldots + a_nb_n = 1$ entonces M es complementable, es decir, agregando un número adecuado de filas a $[a_1, \ldots, a_n]$ se tiene que M tiene determinante uno. □

A partir de la definición de módulo establemente libre se deduce fácilmente que todo módulo establemente libre, es proyectivo. Lo contrario no es cierto, es decir, existen módulos proyectivos que no son establemente libres. Para ilustrar esto, basta con considerar un ideal no principal en un dominio de Dedekind. Los dominios de Dedekind son estructuras algebraicas ampliamente estudiadas en el álgebra abstracta, más específicamente en la teoría algebraica de números y el álgebra conmutativa se recomienda ver (Ríos, 2015) para más profundidad en el tema.

Ejemplo 2.15. Considere $\mathcal{R} = \mathbb{Z}[\sqrt{-5}]$ y $Q(\mathcal{R}) = \mathbb{Q}[\sqrt{-5}]$.

El ideal fraccionario $I = \langle 2, 1+\sqrt{-5}\rangle$, en el dominio de Dedekind $\mathbb{Z}[\sqrt{-5}]$, es un módulo proyectivo de rango 1 por el Teorema 1.35, pues $I = \langle 2, 1+\sqrt{-5}\rangle$ es un ideal invertible, su inverso es $J = \frac{1}{2}I = \langle 1, \frac{1+\sqrt{-5}}{2}\rangle$. En efecto,

$$\begin{aligned} IJ = \frac{1}{2}I^2 &= \frac{1}{2}(4, 2(1+\sqrt{-5}), 1+2\sqrt{-5}+(\sqrt{-5})^2) \\ &= (2, 1+\sqrt{-5}, \sqrt{-5}-2) = \mathcal{R}. \end{aligned}$$

De la ecuación $I^2 = 2\mathcal{R}$ se tiene que I no es ideal principal y por lo tanto no es libre. Si $I =$

$(x+y\sqrt{-5})\mathcal{R}$ donde $x, y \in \mathbb{Z}$, entonces $2 = \alpha(x+y\sqrt{-5})^2$ para algún $\alpha \in \mathcal{R}$. Sea

$$\begin{aligned} N: \quad & Q(\mathcal{R}) \longrightarrow \mathbb{Q} \\ & x+y\sqrt{-5} \longmapsto x^2+5y^2 \end{aligned}$$

una norma sobre el cuerpo $\mathbb{Q}$, se tiene que,

$$4 = N(\alpha)N(x+y\sqrt{-5})^2 = N(\alpha)(x^2+5y^2)^2.$$

Esto obliga a que (x, y) debe ser $(\pm 1, 0)$, lo cual es claramente imposible. Luego, no es establemente libre pues por el Teorema 2.14, los $\mathcal{R}$-módulos establemente libres de rango uno son libres.

Como se observa en el ejemplo anterior, no todo módulo proyectivo es establemente libre, entonces ¿Bajo qué condiciones un módulo proyectivo es establemente libre? Para responder esta pregunta, presentamos la siguiente definición.

Definición 2.16. Sea $\mathcal{M}$ un $\mathcal{R}$-módulo. Se dice que $\mathcal{M}$ tiene una resolución libre finita si existe una sucesión exacta

$$0 \longrightarrow F_n \longrightarrow \ldots \longrightarrow F_0 \longrightarrow \mathcal{M} \longrightarrow 0$$

tal que F_i es libre con base finita, es decir, $F_i \cong \mathcal{R}^{n_i}$ para algún $n_i \in \mathbb{N}$.

La condición para que un $\mathcal{R}$-módulo proyectivo $\mathcal{P}$ sea establemente libre es que $\mathcal{P}$ sea finitamente generado y tenga una resolución libre finita como se presenta en el siguiente resultado.

Teorema 2.17. *(Lezama, Teorema 5.1.6) Si $\mathcal{P}$ es un $\mathcal{R}$-módulo proyectivo finitamente generado con una resolución libre finita si y sólo si $\mathcal{P}$ es establemente libre.*

Demostración. Se prueba que $\mathcal{P}$ es establemente libre por inducción sobre n, para el caso $n = 0$ es claro. Suponga ahora $n \geq 1$, se tiene que $\mathcal{P}$ tiene una resolución libre finita

$$0 \longrightarrow F_n \longrightarrow \ldots \longrightarrow F_0 \xrightarrow{f} \mathcal{P} \longrightarrow 0.$$

Considere $\mathcal{P}_1 = ker(f)$, entonces

$$0 \longrightarrow \mathcal{P}_1 \longrightarrow F_0 \xrightarrow{f} \mathcal{P} \longrightarrow 0$$

es una sucesión exacta corta. Como $\mathcal{P}$ es proyectivo, por el Teorema 1.30, la sucesión se divide, así que $F_0 = \mathcal{P} \oplus \mathcal{P}_1$ y se tiene que $\mathcal{P}_1$ es proyectivo. Ahora, $\mathcal{P}_1$ tiene una resolución finita libre más pequeña que la resolución finita de $\mathcal{P}$

$$0 \longrightarrow F_n \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{f} \mathcal{P}_1 \longrightarrow 0$$

entonces por hipotesis de inducción, existe un $\mathcal{R}$-módulo libre F tal que $F \oplus \mathcal{P}_1$ es libre. Dado que $F_0 \oplus F$ es libre, entonces

$$F_0 \oplus F \cong \mathcal{P} \oplus (\mathcal{P}_1 \oplus F).$$

Luego, $\mathcal{P}$ es un $\mathcal{R}$-módulo establemente libre. Recíprocamente, si $\mathcal{P}$ es establemente libre, esto es equivale a que existe una sucesión exacta corta de la siguiente forma

$$0 \longrightarrow \mathcal{R}^m \longrightarrow \mathcal{R}^n \longrightarrow \mathcal{M} \longrightarrow 0$$

para $n, m \in \mathbb{N}$. Note que la sucesión es un resolución libre finita.

□

La siguiente afirmación da un criterio bastante útil para determinar la "libertad" de los módulos finitamente generados establemente libres sobre un anillo $\mathcal{R}$ en términos de filas unimodulares.

Proposición 2.18. (Yengui, Proposición 20) Sea $\mathcal{R}$ un anillo, entonces las siguientes afirmaciones son equivalentes:

1. Cualquier módulo finitamente generado establemente libre sobre $\mathcal{R}$, es libre.

2. Cualquier fila unimodular puede ser complementable a una matriz invertible (añadiendo un número adecuado de filas).

Demostración. Esto es consecuencia del Teorema 2.9. □

2.2. Anillos de Hermite

Definición 2.19. Sea $\mathcal{R}$ un anillo, decimos que $\mathcal{R}$ es un anillo de Hermite si todo módulo establemente libre sobre $\mathcal{R}$, es libre. Por la Proposición 2.18, equivale a que toda fila unimodular puede ser complementable a una matriz invertible.

Ejemplo 2.20.

1. El anillo de polinomios $\mathbb{K}[x_1, ..., x_n]$, con $\mathbb{K}$ cuerpo, es un ejemplo de anillo de Hermite por el Teorema de Quillen-Suslin.

2. Si todo $\mathcal{R}$-módulo $\mathcal{M}$ proyectivo finitamente generado con una resolución finita sobre $\mathcal{R}$ es libre, entonces $\mathcal{R}$ es un anillo de Hermite. En efecto, por el Ejemplo 2.17, probamos

que un $\mathcal{R}$-módulo $\mathcal{M}$ proyectivo finitamente generado con una resolución finita sobre $\mathcal{R}$ es establemente libre, luego todo $\mathcal{R}$-módulo $\mathcal{M}$ establemente libre, es libre, y así concluimos que $\mathcal{R}$ es un anillo de Hermite.

Observación 2.21. Sea $\mathcal{R}$ un anillo. Si $\alpha = (a_1, \ldots, a_n)$, $\beta = (b_1, \ldots, b_n) \in Um_n(\mathcal{R})$, filas unimodulares de longitud n en $\mathcal{R}$, escribimos $\alpha \sim \beta$ si existe $U \in GL_n(\mathcal{R})$ tal que $\alpha U = \beta$, es decir, α y β se conjugan bajo la acción de multiplicación a derecha de $GL_n(\mathcal{R})$. De manera más general, si G es cualquier subgrupo dado de $GL_n(\mathcal{R})$, escribimos $\sim_G$ para denotar la conjugación de filas unimodulares bajo la acción de G. Mediante un cálculo sencillo, vemos que en particular, para $\alpha \in Um_n(\mathcal{R})$, $\alpha \sim_G (1, 0, \ldots, 0)$ si y sólo si α es complementable a una matriz en G.
La relación $\sim$ establece una relación de equivalencia en $Um_n(\mathcal{R})$. Las clases de equivalencia de $Um_n(\mathcal{R})$ bajo la $\sim$ son solo las órbitas de la acción de $GL_n(\mathcal{R})$.

A continuación se presenta un resultado que caracteriza los anillos de Hermite en términos de las filas unimodulares y matrices invertibles. El Teorema 2.22 en su versión original se presenta con tres equivalencias, sin embargo el autor hace la observación que se cumple para los sistemas transpuestos, es por eso que este Teorema de caracterización que a continuación se presenta, tiene siete equivalencias.

Teorema 2.22. *Teorema de caracterización (Lezama, Teorema 5.3.2) Sea $\mathcal{R}$ un anillo. Las siguientes afirmaciones son equivalentes:*

1. *$\mathcal{R}$ es anillo de Hermite.*

2. *Cualquier vector unimodular v en $\mathcal{R}$ de tamaño $n \times 1$ puede ser complementado a una matriz invertible de $GL_n(\mathcal{R})$ añadiendo $n-1$ columnas.*

3. *Cualquier fila unimodular v en $\mathcal{R}$ de tamaño $1 \times n$ puede ser completado a una matriz invertible de $GL_n(\mathcal{R})$ añadiendo $n-1$ filas.*

4. *Dado un vector unimodular v en $\mathcal{R}$ de tamaño $n \times 1$ existe una matriz $U \in GL_n(\mathcal{R})$ tal que $Uv = (1, 0, ..., 0)^t$.*

5. *Dada una fila unimodular v en $\mathcal{R}$ de tamaño $1 \times n$ existe una matriz $U \in GL_n(\mathcal{R})$ tal que $vU = e_1$.*

6. *Dada una matriz unimodular M en $\mathcal{R}$ de tamaño $n \times m$ con $n \geq m$, existe una matriz $U \in GL_n(\mathcal{R})$ tal que,*
$$UM = \begin{pmatrix} I_t \\ \\ 0 \end{pmatrix}.$$

7. *Dada una matriz unimodular M en $\mathcal{R}$ de tamaño $m \times n$ con $n \geq m$, existe una matriz $U \in GL_n(\mathcal{R})$ tal que,*
$$MU = \begin{pmatrix} I_t & | & 0 \end{pmatrix}.$$

Demostración. Tenemos $2 \Leftrightarrow 3$, $4 \Leftrightarrow 5$ y $6 \Leftrightarrow 7$ por el simple hecho de transponer los sistemas. Veamos las demás equivalencias.

$1 \Rightarrow 2$ Sea $v = (v_1, \cdots, v_n)^t \in Um_n(\mathcal{R})$, entonces existe $u = (u_1, \cdots, u_n)$ tal que $u \cdot v^t = 1$.

Defino

$$f : \mathcal{R}^n \longrightarrow \mathcal{R}$$

$$e_i \longmapsto u_i$$

donde $\{e_1, \cdots, e_n\}$ es la base canónica de $\mathcal{R}^n$. Luego, f define un epimorfismo en el que $f(v) = 1$, luego existe $g : \mathcal{R} \longrightarrow \mathcal{R}^n$ un monomorfismo tal que $fg = I_{\mathcal{R}}$ y $\mathcal{R}^n = Im(g) \oplus ker(f)$. Se define $g(1) = v$, entonces $Im(g) \cong \mathcal{M}$ es libre con base $\{v\}$. Luego $\mathcal{M}^r \cong \mathcal{M} \oplus ker(f)$, así $ker(f)$ es establemente libre. Por hipótesis $ker(f)$ es libre de rango $n-1$, con base $\{x_1, \cdots, x_{n-1}\}$, entonces $(v \ \ x_1 \cdots x_{n-1}) \in GL_n(\mathcal{R})$.

$2 \Rightarrow 1$ Sea $\mathcal{M}$ un módulo establemente libre sobre $\mathcal{R}$, entonces existen enteros $p, q \geq 0$ tales que $\mathcal{R}^p \cong \mathcal{R}^q \oplus \mathcal{M}$. Es suficiente probar este hecho considerando el caso $q = 1$ ya que para $q > 1$ tenemos que $\mathcal{R}^q \oplus \mathcal{M} \cong \mathcal{R} \oplus (\mathcal{R}^{q-1} \oplus \mathcal{M})$ es libre, luego $\mathcal{R}^{q-1} \oplus \mathcal{M}$ es libre. Reiterando este procedimiento obtenemos que $\mathcal{H} \oplus \mathcal{M}$ es libre. Veamos para $q = 1$.

Sea $p \geq 1$ tal que $\mathcal{R}^p \cong \mathcal{R} \oplus \mathcal{M}$. Sean $\pi : \mathcal{R}^p \longrightarrow \mathcal{R}$ la proyección cuyo núcleo es isomorfo a $\mathcal{M}$ y $\{e_1, \ldots, e_p\}$ la base canónica de $\mathcal{R}^p$. Existe $\gamma : \mathcal{R} \longrightarrow \mathcal{R}^p$ tal que $\gamma \circ \pi = I_{\mathcal{R}}$. Así $\mathcal{R}^p = ker(\pi) \oplus Im(\gamma)$. Sea $\gamma(1) = v$, con $v = (v_1, \ldots, v_p) \in \mathcal{R}^p$, entonces $\pi(v) = 1 = v_1\pi(e_1) + \ldots + \pi(e_p)$, luego $v \in Um_p(\mathcal{R})$. Más aún, $\mathcal{R}^p \cong ker(\pi) \oplus \langle v \rangle$.

Por hipótesis, existe $U \in GL_p(\mathcal{R})$ tal que $Uv = e_1$. Sea $f : \mathcal{R}^p \longrightarrow \mathcal{R}^p$ el isomorfismo definido por la matriz U en la base canónica de $\mathcal{R}^p$, entonces $f(e_1) = v$ y $f(e_i) = v_i$ para $2 \leq i \leq p$ donde v_i es otra columna de U.

Basta probar que si $f(e_i) \in ker(\pi)$ para $p \geq i \geq 2$, entonces $f(e_i)$ es libre, luego M es libre. En efecto, sea $\hat{f}$ la restricción de f a $\langle e_2, \ldots, e_p \rangle$, es decir, $\hat{f} : \langle e_2, \ldots, e_p \rangle \longrightarrow ker(\pi)$. Queremos ver que $\hat{f}$ es una biyección. $\hat{f}$ es inyectiva por ser restricción de f, veamos ahora que $\hat{f}$ es sobre, sea $w \in \mathcal{R}^p$, existe $x \in \mathcal{R}^p$ tal que $f(x) = w$, $x = a_1e_1 + \beta$ donde $\beta = a_2e_2 + \ldots + a_ne_n$ luego $f(x) = f(a_1e_1 + \beta) = a_1f(e_1) + f(\beta) = a_1v + f(\beta) = w$, si $w \in ker(\pi)$ entonces $w - f(\beta) \in ker(\pi) \cap \langle v \rangle = 0$, así $w = \hat{f}(x)$, es decir, $\hat{f}$ es sobreyectiva.

Como f fue definida a partir de U, se necesita modificar U de tal manera que la primera columna sea v y las otras columnas sean $v_i \in ker(\pi)$, para $i \geq 2$. Sea $\pi(v_i) = b_i \in \mathcal{R}$ y defino $v_i' = v_i - b_iv$, entonces construimos la matriz V tal que la primera columna es v y las otras son la i-ésima fila de U menos b_iv, entonces $\pi(v_i') = \pi(v_i - b_iv) = \pi(v_i) - b_i\pi(v) = b_i - b_i = 0$. Luego $v_i' \in ker(\pi)$.

$2 \Leftrightarrow 4$ v puede ser complementado a una matriz V de $GL_n(\mathcal{R})$ si y sólo si, existe $U \in GL_n(\mathcal{R})$ tal que $Uv = e_1^t$ si y sólo si, $v = U^{-1}e_1^t$. Luego, $V = U^{-1}$.

$5 \Rightarrow 7$ Por inducción sobre m. Si $m = 1$ es claro, ya que se reduce al caso de que M es una fila unimodular. Supongamos que se cumple para $m - 1$ y demostremos para m. Sea M una matriz unimodular de tamaño $m \times n$, con $m \geq n$, entonces existe una matriz N tal que $MN = I_m$ entonces tenemos que la primera fila v de M es unimodular. Por 5 existe una matriz $U \in GL_n(\mathcal{R})$

tal que $vU = e_1$ y definamos

$$MU = \begin{pmatrix} e_1 \\ \\ M_1 \end{pmatrix},$$

donde M_1 es una matriz de tamaño $m-1 \times n$. Dado que $MN = I_m$, entonces, $MU(U^{-1}N) = I_m$, entonces MU es una matriz unimodular. Sea M_2 la matriz que resulta de quitar la primera columna de M_1, entonces M_2 es una matriz de tamaño $(n-1) \times (m-1)$, con $(n-1) \geq (m-1)$, por hipótesis de inducción existe $V \in GL_{n-1}(\mathcal{R})$ tal que $M_2V = (I_{m-1} \mid 0)$. Como

$$MU = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \\ \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \\ \vdots & \vdots & \ddots & \vdots \\ \\ \alpha_{(m-1)1} & \alpha_{(m-1)2} & \dots & \alpha_{(m-1)n} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \\ A & M_2 \end{pmatrix}.$$

Entonces, llamando $F = MU$ la matriz unimodular de tamaño $m \times n$, existe $W \in GL_{n\times n}(\mathcal{R})$ tal que

$$FW = \begin{pmatrix} 1 & 0 \\ \\ A & M_2 \end{pmatrix}_{m\times n} \begin{pmatrix} 1 & 0 \\ \\ 0 & V \end{pmatrix}_{n\times n} = \begin{pmatrix} 1 & 0 & 0 \\ \\ A & M_2V & 0 \end{pmatrix}_{m\times n} = \begin{pmatrix} 1 & 0 & 0 \\ \\ A & I_{m-1} & 0 \end{pmatrix},$$

queda eliminar A por operaciones elementales a la derecha, y Por lo tanto $FW = (I_m \mid 0)$.

$7 \Rightarrow 5$ Consideramos el caso $t = 1$, dada una fila unimodular de tamaño $1 \times n$, entonces por una matriz $U \in GL_n(\mathcal{R})$, tenemos que $\mathcal{M}U = (1, 0, \cdots, 0)$. □

En el resto de la sección, se estudiarán algunas relaciones de los anillos conmutativos con unidad y los anillos de Hermite dadas por (Granados Pinzón and Olaya León, 2020). Por ejemplo, los anillos locales, en particular, los cuerpos, el producto directo de anillos de Hermite, el producto directo de cuerpos y las $\mathbb{K}$-álgebras finitas son anillos de Hermite.

Proposición 2.23. (Granados Pinzón and Olaya León, Proposición 3.7) Sea $\mathcal{R}$ un anillo local, es decir, $\mathcal{R}$ tiene un único ideal maximal. Entonces, $\mathcal{R}$ es un anillo de Hermite.

Demostración. Sea $\mathfrak{m}$ el ideal maximal de $\mathcal{R}$. Para toda $(a_1, \ldots, a_n) \in \mathcal{R}^n$ fila unimodular, existen $x_1, \ldots, x_n \in \mathcal{R}$ tales que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$. Entonces $\langle x_1, \ldots, x_n \rangle \nsubseteq \mathfrak{m}$. Esto es, existe $i \in \{1, \ldots, n\}$ tal que $x_i \notin \mathfrak{m}$. Luego x_i es invertible, es decir, existe $x_i^{-1} \in \mathcal{R}$ tal que $x_i x_i^{-1} = 1$. Así, existe una matriz con determinante uno,

$$\begin{vmatrix} x_1 & x_2 & \ldots & x_{i-1} & x_i & x_{i+1} & \ldots & x_n \\ \lambda & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = \lambda x_i = 1,$$

donde $\lambda = x_i^{-1}$ para i impar, o $\lambda = -x_i^{-1}$, para i par. En consecuencia, $\mathcal{R}$ es un anillo de Hermite. □

Ejemplo 2.24. 1. Un cuerpo es un anillo de Hermite.

2. Sea $\mathcal{R}$ un anillo, $\mathfrak{p}$ un ideal primo de $\mathcal{R}$. Se llama al anillo $\mathcal{R}_{\mathfrak{p}}$ la localización de $\mathcal{R}$ por $\mathfrak{p}$. Entonces $\mathcal{R}_{\mathfrak{p}}$ es un anillo local, por lo tanto es un anillo de Hermite.

Para probar la Proposición 2.26 es necesario el lema y las siguientes definiciones. Se dice que $a \in \mathcal{R}$ es idempotente si y sólo si $a^2 = a$ y, dos idempotentes $e_1, e_2 \in \mathcal{R}$ se llaman ortogonales si $\{e_1, e_2\}$ es un conjunto ortogonal, esto es $e_1 e_2 = 0$.

Lema 2.25. Sean $e_1, \cdots, e_r \in \mathcal{R}$ idempotentes ortogonales y $\alpha_{i,j}^k \in \mathcal{R}$. Si $M = (\alpha_{i,j})_{1 \leq i,j \leq n}$, donde la componente (i,j) denotada por $[\alpha_{i,j}]_{1 \leq i,j \leq n}$ cumple

$$[\alpha_{i,j}]_{1 \leq i,j \leq n} = \sum_{k=1}^{r} \alpha_{i,j}^k e_k$$

entonces

$$det(M) = \sum_{k=1}^{r} det(\alpha_{i,j}^k) e_k.$$

Demostración. En efecto, sea

$$\begin{pmatrix} \alpha_{11} & \dots & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \dots & \dots & \alpha_{nn} \end{pmatrix} = \begin{pmatrix} \alpha_{11}^1 e_1 + \ldots + \alpha_{11}^r e_r & \dots & \dots & \alpha_{1n}^1 e_1 + \ldots + \alpha_{1n}^r e_r \\ \alpha_{21}^1 e_1 + \ldots + \alpha_{21}^r e_r & \dots & \dots & \alpha_{2n}^1 e_1 + \ldots + \alpha_{2n}^r e_r \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1}^1 e_1 + \ldots + \alpha_{n1}^r e_r & \dots & \dots & \alpha_{nn}^1 e_1 + \ldots + \alpha_{nn}^r e_r \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{11}^1 e_1 & \dots & \dots & \alpha_{1n}^1 e_1 \\ \alpha_{21}^1 e_1 & \dots & \dots & \alpha_{2n}^1 e_1 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1}^1 e_1 & \dots & \dots & \alpha_{nn}^1 e_1 \end{pmatrix} + \ldots + \begin{pmatrix} \alpha_{11}^r e_r & \dots & \dots & \alpha_{1n}^r e_r \\ \alpha_{21}^r e_r & \dots & \dots & \alpha_{2n}^r e_r \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1}^r e_r & \dots & \dots & \alpha_{nn}^r e_r \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{11} & \dots & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \dots & \dots & \alpha_{nn} \end{pmatrix} e_1 + \ldots + \begin{pmatrix} \alpha_{11} & \dots & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \dots & \dots & \alpha_{nn} \end{pmatrix} e_r$$

luego,

$$\begin{vmatrix} \alpha_{11} & \dots & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \dots & \dots & \alpha_{nn} \end{vmatrix} = \begin{vmatrix} \alpha_{11} & \dots & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \dots & \dots & \alpha_{nn} \end{vmatrix} e_1 + \ldots + \begin{vmatrix} \alpha_{11} & \dots & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \dots & \dots & \alpha_{nn} \end{vmatrix} e_r$$

así,

$$det(M) = \sum_{k=1}^{r} det(\alpha_{i,j}^{k}) e_k.$$

□

Proposición 2.26. (Granados Pinzón and Olaya León, Proposición 3.8) Sea $\{\mathcal{R}_i\}_{i\in I}$ una familia de anillos de Hermite, entonces $R = \prod_{i\in I} \mathcal{R}_i$ es un anillo de Hermite.

Demostración. Consideremos la proyección i-ésima, $\pi_i : R \longrightarrow \mathcal{R}_i$. Para toda fila unimodular $(a_1, \ldots, a_n) \in R^n$, existen $x_1, \ldots, x_n \in R$ tales que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$. Aplicando la proyección i-ésima tenemos que $\pi_i(a_1)\pi_i(x_1) + \pi_i(a_2)\pi_i(x_2) + \ldots + \pi_i(a_n)\pi_i(x_n) = 1$, entonces, $(\pi_i(a_1), \pi_i(a_2), \ldots, \pi_i(a_n))$ es una fila unimodular para todo $i \in I$.

Por otra parte, como $\mathcal{R}_i$ es un anillo de Hermite, existe una matriz invertible $M_i = (m_{i,j})_{1\leq i,j\leq n}$ con la primera fila $(\pi_i(a_1), \pi_i(a_2), \ldots, \pi_i(a_n))$ para todo $i \in I$ por lo tanto existe $M = (\alpha_{i,j})_{1\leq i,j\leq n}$ invertible con la primera fila $(a_1, \ldots, a_n)$. En efecto, definiendo $\alpha_{i,j}$ como $\pi_i(\alpha_{i,j}) = m_{i,j}^{i}$ para todo $i \in I$ y como π_i es un homomorfismo de anillos entonces, para todo $i \in I$,

$$\pi_i\left(\begin{array}{l} \\ det\begin{pmatrix} a_1 & \dots & a_n \\ \alpha_{21} & & \alpha_{2n} \\ \vdots & & \vdots \\ \alpha_{n1} & & \alpha_{nn} \end{pmatrix} \end{array}\right) = det\pi_i \begin{pmatrix} a_1 & \dots & a_n \\ \alpha_{21} & & \alpha_{2n} \\ \vdots & & \vdots \\ \alpha_{n1} & & \alpha_{nn} \end{pmatrix} = det \begin{pmatrix} \pi_i(a_1) & \dots & \pi_i(a_n) \\ m^i_{21} & & m^i_{2n} \\ \vdots & & \vdots \\ m^i_{n1} & & m^i_{nn} \end{pmatrix} = 1.$$

□

Corolario 2.27. Sea $\{\mathbb{K}_i\}_{i\in I}$ una familia de cuerpos. El producto directo de cuerpos $\prod_{i\in I}\mathbb{K}_i$ es un anillo de Hermite.

Demostración. Se sigue de la Proposición 2.26. □

Definición 2.28. $\mathcal{A}$ es una $\mathbb{K}$-álgebra finita, $\mathcal{A}$ si es una álgebra conmutativa con unidad y tiene dimensión finita como espacio vectorial sobre un cuerpo $\mathbb{K}$.

Ejemplo 2.29. Si consideramos una extensión de grado 2 de $\mathbb{R}$,

$$\mathcal{R} \cong \frac{\mathbb{R}[x]}{(x^2+bx+c)}$$

se pueden dar tres casos, estos según las raíces del polinomio de grados dos x^2+bx+c puede que este, tenga dos raíces imaginarias, dos raíces reales distintas o una raíz doble. Por esto se obtiene

que salvo isomorfismos, las tres álgebras de dimensión dos sobre $\mathbb{R}$ son,

$$\mathbb{C} \cong \frac{\mathbb{R}[x]}{(x^2+1)}, \ \mathbb{P} \cong \frac{\mathbb{R}[x]}{(x^2-1)} \text{ y } \mathbb{D} \cong \frac{\mathbb{R}[x]}{(x^2)}.$$

Es importante recordar que estas $\mathbb{R}$-álgebras no son isomorfas entre sí, pues $\mathbb{C}$ es un cuerpo, mientras $\mathbb{P}$ y $\mathbb{D}$ no lo son, $\mathbb{P}$ tiene divisores de cero y $\mathbb{D}$ además tiene elementos nilpotentes.

La siguiente proposición muestra una caracterización bastante útil de las $\mathbb{K}$-álgebras finitas a partir de anillos locales.

Proposición 2.30. (Granados-Pinzón and Olaya-León, Proposición 2.2) $\mathcal{A}$ es $\mathbb{K}$-álgebra finita si y sólo si $\mathcal{A}$ es suma directa de $\mathbb{K}$-álgebras finitas locales.

Proposición 2.31. Toda $\mathbb{K}$-álgebra finita es un anillo de Hermite.

Demostración. Sea $\mathcal{A}$ una $\mathbb{K}$-álgebra finita, por la Proposición 2.30, $\mathcal{A} = A_1 \times \ldots \times A_k$, donde los A_i son anillos locales para todo $i \in \{1, \ldots, k\}$, luego A_i son Anillos de Hermite para todo $i \in \{1, \ldots, k\}$ y por la Proposición 2.26, $\mathcal{A}$ es un anillo de Hermite. □

Hasta ahora, es natural preguntarse por el comportamiento de los anillos de Hermite con subanillos y con anillos cocientes, ¿Será que la propiedad de ser un anillo de Hermite se hereda para subanillos y cocientes? En la siguiente sección se dará una respuesta a la pregunta planteada.

2.2.1. Una fila unimodular que no es complementable. Antes de enunciar el Ejemplo 2.33 de un anillo que no es Hermite es importante recordar el siguiente resultado clásico de la geometría diferencial conocido con el Teorema de Hopf-Poincaré.

Teorema 2.32. *Teorema de Hopf-Poincaré (Etayo Gordejuela, Teorema 9.16) Sea $S^n \subseteq \mathbb{R}^{n+1}$ la esfera unidad de dimensión n centrada en el origen.*

1. *Si n es par, entonces S^n no admite ningún campo vectorial sin ceros.*

2. *Si n es impar, entonces S^n admite campos vectoriales sin ceros.*

Demostración La prueba de este resultado se puede consultar en (Etayo Gordejuela, Teorema 9.16).

En particular, el Teorema de Hopf-Poincaré dice que en S^2, todo campo vectorial se anula. Este hecho se usará en el siguiente ejemplo.

Ejemplo 2.33. Consideremos el anillo de polinomios reales sobre la 2-esfera S^2

$$\mathcal{R} = \mathcal{R}[\overline{x}, \overline{y}, \overline{z}] = \frac{\mathbb{R}[x, y, z]}{\langle x^2 + y^2 + z^2 - 1 \rangle},$$

entonces $(\bar{x}, \bar{y}, \bar{z}) \in \mathcal{R}^3$ es una fila unimodular pues $\bar{x}\bar{x} + \bar{y}\bar{y} + \bar{z}\bar{z} = 1$. Note que $(\bar{x}, \bar{y}, \bar{z})$ no es complementable. Para ello supongamos que $(\bar{x}, \bar{y}, \bar{z})$ es complementable, es decir que existe $A \in GL_3(\mathcal{R})$.

Sea

$$A = \begin{pmatrix} \bar{x} & \bar{y} & \bar{z} \\ f & g & h \\ f' & g' & h' \end{pmatrix},$$

entonces

$$\begin{aligned} det(A) &= f' \begin{vmatrix} \bar{y} & \bar{z} \\ g & h \end{vmatrix} - g' \begin{vmatrix} \bar{x} & \bar{z} \\ f & h \end{vmatrix} + h' \begin{vmatrix} \bar{x} & \bar{y} \\ f & g \end{vmatrix} \\ &= f'(\bar{y}h - \bar{z}g) - g'(\bar{x}h - f\bar{z}) + h'(\bar{x}g - \bar{y}f) \\ &= e \neq 0, \end{aligned}$$

donde las funciones $f, g, h, f', g', h', e, e^{-1}$ son expresiones polinómicas en S^2. Ahora, considere

$$\begin{aligned} \mathbf{\Gamma} : S^2 &\longrightarrow \mathbb{R}^3 \\ v &\longmapsto (f(v), g(v), h(v)). \end{aligned}$$

Note que $\mathbf{\Gamma}$ es un campo vectorial sobre S^2 que por el Teorema 2.32, se anula, es decir $(f(v), g(v), h(v)) = (0, 0, 0)$ para algún $v \in S^2$, lo cual es absurdo pues $det(A) = e \neq 0$.

Ahora, se responderán las preguntas planteadas al final de la sección anterior. En general un subanillo de un anillo de Hermite no es un anillo de Hermite y un cociente de un anillo de Hermite tampoco es Hermite. Por ejemplo, el anillo del Ejemplo 2.33 es un dominio entero por tanto su cuerpo de fracciones $Q(\mathcal{R})$ es anillo de Hermite, $\mathcal{R} \subseteq Q(\mathcal{R})$ y $\mathcal{R}$ no es Hermite. Además $\mathbb{R}[x, y, z]$ es un anillo de Hermite y $\mathcal{R} = \frac{\mathbb{R}[x,y,z]}{\langle x^2+y^2+z^2-1\rangle}$ no lo es.

2.3. Conjetura de Hermite

La conjetura de Hermite surge de los trabajos en el problema de Serre sobre módulos proyectivos, el cual fue resuelto por Quillen y Suslin de manera independiente (Lam, 2010). De este hecho ha surgido un gran interés en estudiar los módulos proyectivos y ha dado base para más conjeturas y problemas abiertos para estos módulos. Ahora es natural pensar bajo qué condiciones el anillo de polinomios es un anillo de Hermite, es decir, ¿Cuándo el anillo de polinomios $\mathcal{R}[x]$ es un anillo de Hermite?. Se probó en (Lam, 2010) que en particular para $\mathcal{R}$ cuerpo, $\mathcal{R}[x]$ es un anillo de Hermite, pero ¿si $\mathcal{R}$ es un anillo de Hermite, lo es su anillo de polinomios $\mathcal{R}[x]$? la respuesta a esa pregunta aún sigue siendo incierta y es lo que hoy en día se conoce como la conjetura de Hermite.

Conjetura 1. La Conjetura de Hermite

Las siguientes afirmaciones son equivalentes

1. Si $\mathcal{R}$ es un anillo de Hermite entonces, $\mathcal{R}[x]$ es un anillo de Hermite.

2. Si $v = (v_0(x), ..., v_n(x))$ es una fila unimodular con entradas en $\mathcal{R}[x]$ tal que $v(0) = (1, 0, ..., 0)$ puede ser complementado a una matriz de $GL_{n+1}(\mathcal{R})$ entonces v puede ser complementable

a una matriz en $GL_{n+1}(\mathcal{R}[x])$.

3. Dado $v(x) = (v_0(x), \ldots, v_n(x)) \in Um_{n+1}(\mathcal{R}[x])$, entonces existe $A \in GL_{n+1}(\mathcal{R}[x])$ tal que $Av(x)^t = (1, 0, \ldots, 0)^t$.

Mnif y Yengui presentan un algoritmo para complementar filas unimodulares sobre anillos noetherianos pero finalmente Yengui en (Yengui, 2008) prueba la conjetura en el caso en que $\mathcal{R}$ tiene dimensión de Krull menor o igual a uno. En esta sección se presenta la prueba la conjetura de Hermite en el caso en que $\mathcal{R}$ tiene dimensión de Krull menor o igual a un entero dado d, para esto se inicia demostrando algunos lemas necesarios y con base en los resultados presentados en el Capítulo 1 se llegará al resultado importante.

Lema 2.34. (Yengui, Proposición 56) Sean $\mathcal{R}$ un anillo y $f, g \in \mathcal{R}[x]$ con f un polinomio mónico, entonces

$$\langle f, g\rangle = \mathcal{R}[x] \Longleftrightarrow Res_x(f, g) \in \mathcal{R}^*.$$

Demostración. $\Rightarrow$) Por la Proposición 1.45, se tiene que $Res_x(f, g) \in \langle f, g\rangle \cap \mathcal{R}$, como $\langle f, g\rangle = \mathcal{R}[x]$, $Res_x(f, g) \in \mathcal{R}[x] \cap \mathcal{R} = \mathcal{R}$, así $Res_x(f, g) \in \mathcal{R}^*$.

$\Leftarrow$) Sean $u, v \in \mathcal{R}[x]$ tales que $uf + vg = 1$. Como f es mónico, por el Lema 1.48, tenemos que

$$Res_x(f, vg) = Res_x(f, v)Res_x(f, g) = Res_x(f, uf + vg) = Res_x(f, 1) = 1.$$

Luego, $1 \in \langle f, g\rangle$, así $\langle f, g\rangle = \mathcal{R}[x]$. □

Lema 2.35. (Yengui, Lema 182) Sea $\mathcal{R}$ un anillo e $\mathcal{I}$ un ideal de $\mathcal{R}[x]$ que contiene un polinomio mónico. Supongamos que $\mathcal{J}$ es un ideal de $\mathcal{R}$ tal que $\mathcal{I}+\mathcal{J}[x]=\mathcal{R}[x]$. Entonces $(\mathcal{I}\cap\mathcal{R})+\mathcal{J}=\mathcal{R}$.

Demostración. Sea $f\in\mathcal{I}$ un polinomio mónico. Se tiene que $\mathcal{I}+\mathcal{J}[x]=\mathcal{R}[x]$ luego existen $g\in\mathcal{I}$ y $h\in\mathcal{J}[x]$ tales que $g(x)+h(x)=1$.

Considerando el anillo $\frac{\mathcal{R}}{\mathcal{J}}[x]$ se tiene que este es generado por $\overline{f}$ y $\overline{g}$ con las clases tomadas módulo $\mathcal{J}[x]$, pueden ser tomadas de esta forma pues $\frac{\mathcal{R}[x]}{\mathcal{J}[x]}\cong\frac{\mathcal{R}}{\mathcal{J}}[x]$. Es decir,

$$\overline{f}(x)=f(x)+\mathcal{J}[x],$$

$$\overline{g}(x)=g(x)+\mathcal{J}[x],$$

con $f(x),g(x)\in\mathcal{I}$ y como $g(x)+h(x)=1$, entonces $\overline{1}=\overline{g}(x)$. Ahora, por el Lema 2.34, se tiene que, $Res_x(\overline{f},\overline{g})\in\left(\frac{\mathcal{R}}{\mathcal{J}}\right)^*$, con

$$\overline{f}(x)=\overline{1}x^n+\overline{a_{n-1}}x^{n-1}+\ldots+\overline{a_1}x+\overline{a_0},$$

$$\overline{g}(x)=\overline{b_m}x^m+\overline{b_{m-1}}x^{m-1}+\ldots+\overline{b_1}x+\overline{b_0}.$$

Entonces,

$$Res_x(\overline{f},\overline{g}) = \begin{bmatrix} \overline{a_n} & \overline{a_{n-1}} & \dots & \overline{a_1} & \overline{a_0} & & \\ & \overline{a_n} & \overline{a_{n-1}} & \dots & \overline{a_1} & \overline{a_0} & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ \overline{b_m} & \overline{b_{m-1}} & \dots & \overline{b_1} & \overline{b_0} & & \\ & \overline{b_m} & \overline{b_{m-1}} & \dots & \overline{b_1} & \overline{b_0} & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ & & & \overline{b_m} & \overline{b_{m-1}} & \dots & \overline{b_1} & \overline{b_0} \end{bmatrix} = \overline{Res_x(f,g)}$$

Luego, $\overline{Res_x(f,g)} \in \left(\frac{\mathcal{R}}{\mathcal{J}}\right)^*$. Entonces, $\langle\overline{Res_x(f,g)}\rangle = \left(\frac{\mathcal{R}}{\mathcal{J}}\right)$, por esto, $\langle Res_x(f,g)\rangle + \mathcal{J} = \mathcal{R}$ y como $Res_x(f,g) \in \mathcal{I} \cap \mathcal{R}$, $\langle Res_x(f,g)\rangle \subseteq \mathcal{I} \cap \mathcal{R}$ y se obtiene que $(\mathcal{I} \cap \mathcal{R}) + \mathcal{J} = \mathcal{R}$. □

Lema 2.36. (Yengui, Lema 183) Sean $\mathcal{R}$ un anillo y $f \in \mathcal{R}[x]$ de grado $n > 0$, tal que $f(0) \in \mathcal{R}^*$. Entonces para cualquier $g(x) \in \mathcal{R}[x]$ y $k \geq deg(g(x)) - deg(f(x)) + 1$, con $k \in \mathbb{N}$, existe $h_k(x) \in \mathcal{R}[x]$ con $deg(h_k(x)) < n$ tal que

$$g(x) \equiv x^k h_k(x) \text{ mód } \langle f(x)\rangle.$$

Demostración. Sean

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0.$$

Consideramos,

$$\begin{aligned} g(x) - b_0 a_0^{-1} f(x) &= (b_m x^m + \ldots + b_0) - (b_0 + (b_0 a_0^{-1}) a_1 x + \ldots + \\ &\quad + (b_0 + b_0 a_0^{-1}) a_n x^n) + a_{n-1} x^{n-1}, \\ &= x h_1(x), \end{aligned}$$

donde $h_1(x) = b^m x^{m-1} + \ldots + b_1 - b_0 a_0^{-1} a_n x^{n-1} - \ldots - b_0 a_0^{-1}$. Luego,

$$g(x) = x h_1(x) + b_0 a_0^{-1} f(x), \tag{2.3.1}$$

$$g(x) \equiv x h_1(x) \text{ mód } \langle f(x) \rangle. \tag{2.3.2}$$

con $deg(h_1(x)) < max(n, m)$. El siguiente paso análogo al anterior, se sigue que,

$$x h_2(x) = h_1(x) - (b_1 a_0^{-1} - b_0 (a_0^{-1})^2 a_1) f(x), \tag{2.3.3}$$

$$h_1(x) \equiv x h_2(x) \text{ mód } \langle f(x) \rangle. \tag{2.3.4}$$

Por las ecuaciones 2.3.2 y 2.3.4, se tiene

$$g(x) \equiv x^2 h_2(x) \text{ mód } \langle f(x) \rangle.$$

continuando con el proceso, el paso n se obtiene el resultado deseado

$$g(x) \equiv x^n h_n(x) \text{ mód } \langle f(x) \rangle.$$

□

Lema 2.37. (Yengui, Lema 184) Sean $k \in \mathbb{N}$, $\mathcal{R}$ un anillo con $f_1, \ldots, f_n \in \mathcal{R}[x]$ con grados $\leq k-1$ y f_{n+1} con grado k. Si los coeficientes de $f_1, \ldots, f_n$ generan el ideal $\mathcal{R}$, es decir, generan todo el anillo $\mathcal{R}$, entonces $\langle f_1, f_2, \ldots, f_n, f_{n+1} \rangle$ contiene un polinomio de grado $k-1$.

Demostración. Sean $\mathcal{A} = \langle f_i \mid 1 \leq i \leq n \rangle$ y $\mathcal{B}$ el ideal generado por los coeficientes de x^{k-1} de los polinomios de grado $\leq k-1$ de $\mathcal{A}$.

Se probará que $\mathcal{B} = \mathcal{R}$, más aún, vemos que todos los coeficientes de los f_i están en $\mathcal{B}$. En efecto, consideremos

$$f_i(x) = b_0 + b_1 x + \ldots + b_{k-1} x^{k-1}, \quad 1 \leq i \leq n,$$

$$f_{n+1}(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + x^k,$$

donde $b_{k-1} \in \mathcal{B}$. Sea

$$\begin{aligned} f_i' &= x f_i(x) - b_{k-1} x^{k-1} f_{n+1}(x) \\ &= b_0' + b_1' x + \ldots + b_{k-1}' x^{k-1}. \end{aligned}$$

Note que $f_i' \in \mathcal{A}$ y como $b_j' \equiv b_{j-1}$ mód $\langle b_{k-1} \rangle$ entonces $b_{k-1}' = b_{k-2} + a_{k-1}b_{k-1} \in \mathcal{B}$, luego $b_{k-2} \in \mathcal{B}$ y de manera general se obtiene que b_i pertenece a $\mathcal{B}$ para todo i, luego $\mathcal{B} = \mathcal{R}$.

Como $\mathcal{B}$ se construye con todos los coeficientes de los polinomios de $\mathcal{A}$ con grado menor o igual a $k-1$, entonces a partir de combinaciones de estos polinomios se puede generar un polinomio mónico de grado $k-1$. □

Lema 2.38. Lema de Suslin (Yengui, Teorema 57) Sea $\mathcal{R}$ un anillo. Si $(v_1, \ldots, v_n) \in Um_n(\mathcal{R}[x])$ donde v_1 es mónico y $n \geq 2$, entonces existen $A_1, \ldots A_p \in E_{n-1}(\mathcal{R}[x])$ tales que

$$\langle Res_x(v_1, \omega_1), \ldots, Res_x(v_1, \omega_p) \rangle = \mathcal{R}$$

donde $\omega_i = e_1 A_i(v_2, \ldots, v_n)^t$ con $e_1 = (1, 0, 0, \ldots, 0)$.

La demostración del Lema de Suslin 2.38 es constructiva, presenta un ingenioso algoritmo para calcular $A_1, \ldots A_p \in E_{n-1}(\mathcal{R}[x])$, por lo que consideramos más interesante presentar un caso en particular, para ilustrar el Lema de Suslin proponemos el siguiente ejemplo.

Ejemplo 2.39. Considere $\mathcal{R} = \mathbb{Z}$. Sea

$$V = (v_1, v_2, v_3)^t = (x^2 + 2x + 2, 3, 2x^2 + 11x - 3)^t \in Um_3(\mathbb{Z}[x]).$$

Note que si $U = (u_1, u_2, u_3) = (-2x + 2, -3x^2 + x - 1, x)$, entonces

$$UV = v_1u_1 + v_2u_2 + v_3u_3 = 1.$$

Observe que $deg(v_1) = 2$, mediante operaciones elementales se reduce el grado de los demás polinomios. En este caso,

$$E_{3,1}(-2)V^t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} x^2+2x+2 \\ 3 \\ 2x^2+11x-3 \end{pmatrix} = \begin{pmatrix} x^2+2x+2 \\ 3 \\ 7x-7 \end{pmatrix}.$$

Ahora, calculando $min_{1\leq i\leq 3}\{deg(v_i)\}$, es decir, $min_{1\leq i\leq 3}\{2,0,1\} = 0$ que corresponde al polinomio v_2. Considero a V en el anillo $\frac{\mathbb{Z}}{\langle 3\rangle}[x]$, esto es, $V = \begin{pmatrix} x^2+2x+2 \\ 0 \\ x+2 \end{pmatrix}$.

Entonces,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x^2+2x+2 \\ 0 \\ x+2 \end{pmatrix} = \begin{pmatrix} x^2+2x+2 \\ x+2 \\ x+2 \end{pmatrix} \text{ y } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x^2+2x+2 \\ 0 \\ x+2 \end{pmatrix} = \begin{pmatrix} x^2+2x+2 \\ 0 \\ x+2 \end{pmatrix}$$

Así, por el Lema de Suslin 2.38, se tiene que $A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Hallando ω_1 y ω_2 se tiene que

$$\begin{aligned}\omega_1 &= e_1 A_1(3, 2x^2+11x-3)\\ &= (1,0)\begin{pmatrix}1 & 1\\ \\ 0 & 1\end{pmatrix}(3, 2x^2+11x-3)\\ &= 2x^2+11x,\end{aligned}$$

$$\begin{aligned}\omega_2 &= e_1 A_2(3, 2x^2+11x-3)\\ &= (1,0)\begin{pmatrix}1 & 0\\ \\ 0 & 1\end{pmatrix}(3, 2x^2+11x-3)\\ &= 3.\end{aligned}$$

En consecuencia,

$$Res_x(v_1,\omega_1) = Res_x(x^2+2x+2, 2x^2+11x) = \begin{vmatrix}1 & 2 & 2 & 0\\ \\ 0 & 1 & 2 & 2\\ \\ 2 & 11 & 0 & 0\\ \\ 0 & 2 & 11 & 0\end{vmatrix} = 170, \qquad (2.3.5)$$

y

$$Res_x(v_1,\omega_2) = Res_x(x^2+2x+2,3) = \begin{vmatrix} 1 & 2 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{vmatrix} = 9. \tag{2.3.6}$$

Concluimos de las ecuaciones (2.3.5) y (2.3.6) que $\langle Res_x(v_1,\omega_1), Res_x(v_1,\omega_2)\rangle = \langle 170, 9\rangle = \mathbb{Z}$.

Corolario 2.40. Sea $\mathcal{R}$ un anillo. Si $n \geq 2$ y $(v_1,\ldots,v_n) \in Um_n(\mathcal{R}[x])$ donde v_1 es mónico entonces existe $E \in E_n(\mathcal{R})$ tal que $Ev^t = (1,0,\ldots,0)^t$.

Demostración. Es consecuencia del Lema 2.38 □

A continuación se probará el teorema del rango estable para un anillo $\mathcal{R}$ mediante los resultados del capítulo uno, en particular, usando la interpretación constructiva de la dimensión de Krull.

Teorema 2.41. *Teorema del Rango Estable(Yengui, Teorema 92) Sea $\mathcal{R}$ un anillo con dimensión de Krull $\leq d$, $n \geq d+1$ y $v^t = (v_0,v_1,\ldots,v_n) \in Um_{n+1}(\mathcal{R})$, entonces existe $E \in E_{n+1}(R)$ tal que*

$$Ev^t = (1,0,\ldots,0)^t.$$

Demostración. Por el Teorema 1.63 y la propiedad 6 de los abiertos básicos de la topología de

Zariski sobre $Spec(\mathcal{R})$, existen $x_1, x_2, \ldots, x_n$ tales que $1 \in \langle v_1 + x_1 v_0, \ldots, v_n + x_n v_0 \rangle$, entonces

$$E_{n+1,1}(x_n)...E_{2,1}(x_1)v = (v_0, v_1 + x_1 v_0, \ldots, v_n + x_n v_0)^t.$$

Como $1 \in \langle v_1 + x_1 v_0, \ldots, v_n + x_n v_0 \rangle$, se puede generar $-v_0$. Sean $b_1, b_2, \ldots, b_n \in \mathcal{R}$ los coeficientes para generarlo, así

$$\begin{pmatrix} 1 & b_1 & b_2 & \ldots & b_n \\ & 1 & & & \\ & & \ddots & & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 + x_1 v_0 \\ \vdots \\ v_n + x_n v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ v_1 + x_1 v_0 \\ \vdots \\ v_n + x_n v_0 \end{pmatrix}.$$

Ahora considerando $a_1, \ldots, a_n \in \mathcal{R}$ tales que generan a 1, se tiene que

$$\begin{pmatrix} 1 & a_1 & a_2 & \ldots & a_n \\ & 1 & & & \\ & & \ddots & & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 0 \\ v_1 + x_1 v_0 \\ \vdots \\ v_n + x_n v_0 \end{pmatrix} = \begin{pmatrix} 1 \\ v_1 + x_1 v_0 \\ \vdots \\ v_n + x_n v_0 \end{pmatrix}.$$

Ahora basta considerar las matrices elementales $E_{i+1,1}(-v_i - x_i v_0)$ para eliminar el resto de las entradas, es decir, para $i = 1$ se tiene

$$E_{2,1}(-v_1 - x_1v_0)\begin{pmatrix} 1 \\ v_1 + x_1v_0 \\ \vdots \\ v_n + x_nv_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ v_n + x_nv_0 \end{pmatrix},$$

esto para cada $i \in \{1, \ldots, n\}$ hasta obtener $(1, 0, \ldots, 0)^t$. □

Ahora el siguiente teorema, corresponde a la versión del rango estable para el anillo de polinomios $\mathcal{R}[x]$.

Teorema 2.42. *(Yengui, Teorema 192) Sea $\mathcal{R}$ un anillo con dimensión de Krull $\leq d$, $n \geq d+1$ y $v(x) = (v_0(x), v_1(x), \ldots, v_n(x)) \in Um_{n+1}(\mathcal{R}[x])$, entonces existe $E \in E_{n+1}(R[x])$ tal que*

$$Ev^t = (1, 0, \ldots, 0)^t.$$

Demostración. Por el Teorema de rango estable 2.41, para cualquier $v^t \in Um_{n+1}(\mathcal{R})$, existe $M \in E_{n+1}(\mathcal{R})$ tal que $Mv^t = (1, 0, \ldots, 0)^t$ entonces es suficiente probar que existe $E \in E_{n+1}(\mathcal{R}[x])$ tal que $Ev^t(x) = v(0)^t$.

Por el principio local-global de filas unimodulares sobre $\mathcal{R}[x]$ bajo la acción del grupo elemental $E_{n+1}(\mathcal{R}[x])$ con $n \geq 2$ (Apte et al., Teorema 4,7), se puede suponer que $\mathcal{R}$ es local. Al tener que

$\mathcal{R}$ se puede considerar un anillo local, se afirma que dado $x \in \mathcal{R}$,

$$\forall x \in \mathcal{R}, x \in \mathcal{R}^* \; o \; x \in Rad(\mathcal{R})$$

y más aún se supone que $\mathcal{R}$ es reducido. Sea N el número de elementos no nulos de los coeficientes de $v_0(x), \ldots, v_n(x)$. Se prueba el resultado deseado haciendo una doble inducción sobre N y d.

Para el caso $N = 1$ tenemos que el resultado es inmediato, ya que al tener que $v_i(x) = c$ es invertible, por el Lema de Whitehead 1.39, por operaciones elementales se puede llegar al vector v^t al vector e_1^t.

Para el caso $d = 0$, se tiene que $\mathcal{R}[x] \subseteq \mathcal{R}\langle x \rangle = \mathcal{R}(x)$ donde $\mathcal{R}\langle x \rangle = W^{-1}\mathcal{R}[x]$ con $W \subseteq \mathcal{R}[x]$ los polinomios mónicos de $\mathcal{R}[x]$ y $\mathcal{R}(x) = U^{-1}\mathcal{R}[x]$ con $U \subseteq \mathcal{R}[x]$ los polinomios unitarios. Así, $\mathcal{R}\langle x \rangle$ es un anillo local. Ahora,

$$\frac{v_0(x)k_0(x)}{1} + \ldots + \frac{v_n(x)k_n(x)}{1} = \frac{1}{1}$$

con $k_i(x) \in \mathcal{R}[x]$. Luego, $\frac{v_i(x)k_i(x)}{1} \in \mathcal{R}\langle x \rangle^*$, sin pérdida de generalidad $\frac{v_0(x)k_0(x)}{1} \in \mathcal{R}\langle x \rangle^*$, entonces

$$\frac{v_0(x)k_0(x)}{1}\frac{a(x)}{s(x)} = \frac{1}{1}.$$

Por lo anterior, existe $t(x) \in U$ tal que

$$v_0(x)k_0(x)a(x)t(x) = s(x)t(x)$$

Como $s(x), t(x) \in U$, $s(x)t(x) \in U$, así $v_0(x)$ divide a un polinomio mónico, luego su coeficiente principal es invertible en $\mathcal{R}$. Por el Lema de Whitehead 1.39 y el Corolario 2.40. se tiene el resultado deseado.

Haciendo inducción sobre N, se tiene que el vector $v^t(x)$ puede ser transformado por operaciones elementales en un vector con una entrada constante. Sea $N > 1$ y $d > 0$, denotemos por $m_0 = deg(v_0)$ y a el coeficiente principal de $v_0(x)$. Si $a \in \mathcal{R}^*$ el resultado se tiene por el Lema 2.38. Si $a \in Rad(\mathcal{R})$ por la hipótesis de inducción sobre N en el anillo $\frac{\mathcal{R}}{\langle a \rangle}$ podemos asumir que

$$v(x) \equiv (1, 0, \ldots, 0) \text{ mód } (a\mathcal{R}[x])^{n+1}.$$

Por el Lema 2.36 considerando un par $2k$ lo suficientemente grande, tenemos que

$$v_i(x) \equiv x^{2k}\omega_i \text{ mód } (\langle v_0(x) \rangle)$$

donde $deg(\omega_i) < m_0$ y $1 \leq i \leq n$.

Si $m_0 \leq 1$ entonces el resultado se tiene, ya que si $m_0 = 0$ esto es $v_0(x) = v_0(0)$, luego el problema está solucionado; Si $m_0 = 1$ entonces se obtiene que es de la forma $ax + v_0(0)$ y este es invertible, luego el teorema está resuelto. Ahora suponga que $m_0 \leq 2$. Sean $(c_0, c_1, \ldots, c_{m_0(n-1)})$

cada uno de los coeficientes de $1, x, \ldots, x^{m_0-1}$ en los polinomios $v_2(x), \ldots, v_n(x)$. Considere:

$$\mathcal{I} = \langle v_0(x), v_1(x) \rangle_{\mathcal{R}_a}$$

$$\mathcal{J} = \langle c_0, c_1, \ldots, c_{m_0(n-1)} \rangle_{\mathcal{R}_a}$$

donde $\mathcal{R}_a$ es la localización de $\mathcal{R}$ por el ideal generado por a. Entonces por el Lema 2.35 tenemos que $(\mathcal{I} \cap \mathcal{R}_a) + \mathcal{J} = \mathcal{R}_a$. En efecto, se puede obtener los polinomios $v_2(x), \ldots, v_n(x)$ en $\mathcal{J}[x]$ y con $\mathcal{I}$ se puede completar el vector unimodular, por ende construir el elemento 1, luego $\mathcal{I} + \mathcal{J}[x] = \mathcal{R}_a[x]$. Como $dim(\mathcal{R}_a) < 2d \leq m_0(n-1)$, entonces por el Teorema 2.41, existen $(x_0, x_1, \ldots, x_{m_0(n-1)})$ tales que

$$(x_0, x_1, \ldots, x_{m_0(n-1)}) \equiv (c_0, c_1, \ldots, c_{m_0(n-1)}) \; mod(\; \langle v_0(x), v_1(x) \rangle \cap \mathcal{R}),$$

con $x_0\mathcal{R}_a + x_1\mathcal{R}_a + \ldots + x_{m_0(n-1)})\mathcal{R}_a = \mathcal{R}_a$. Note que aunque se esta trabajando en el anillo cociente $\mathcal{R}_a[x]$, todas las operaciones elementales que han sido efectuadas en $\mathcal{R}[x]$.

Suponga que $c_0\mathcal{R}_a + c_1\mathcal{R}_a + \ldots + c_{m_0(n-1)})\mathcal{R}_a = \mathcal{R}_a$, por el Lema 2.38. Note que el ideal $\langle v_0, v_2, \ldots, v_n \rangle$ contiene un polinomio mónico $\omega(x)$ en $\mathcal{R}_a$ de grado $m_0 - 1$.

Denotemos el coeficiente de ω como ua^k donde $u \in \mathcal{R}^*$ y el de v_1 como b. Utilizando el Lema

2.37, se pueden hacer las siguientes transformaciones vía operaciones elementales

$$(v_0, v_2, \ldots, v_n) \longmapsto (v_0, a^{2k}v_1, \ldots, v_n)$$
$$\longmapsto (v_0, a^{2k}v_1 + (1 - a^{2k}u^{-1}b)w, \ldots, v_n).$$

Ahora $a^{2k}v_1 + (1 - a^{2k}u^{-1}b)w$ es unitario en $\mathcal{R}_a$. Entonces se puede asumir que v_1 es unitario en $\mathcal{R}_a$ y $deg(v_1) < m_0$.

Por el Lema 2.37, como a es invertible módulo $\langle v_0, v_1\rangle$, por operaciones elementales, $(v_0, v_1, v_2, \ldots, v_n)$ puede ser transformado en $(v_0, v_1, a^l v_2, \ldots, a^l v_n)$ para un $l \in \mathbb{N}$ adecuado. Luego se puede dividir todos los $a^l v_i$, para $2 \leq i \leq n$, por v_1, así se puede asumir que $deg(v_i) < m_0$.

Reiterando el proceso anterior, se puede reducir el grado de v_1 obteniendo el hecho de que al menos una entrada sea constante.

Sigue la prueba, ahora solo con inducción sobre $d > 0$, entonces considere que $v_1 = c \in \mathcal{R}$, tome $T = \frac{\mathcal{R}}{\mathfrak{B}(c)}$, entonces considere que $dim(T) \leq d - 1$ y $\bar{v^t} = (\bar{v^0}, \bar{v^1}, \ldots, \bar{v^n}) \in Um_n(T[x])$ se tiene que existe $E_1 \in E_n(\mathcal{R}[x])$ tal que

$$E_1(v_0, v_2, \ldots, v_n)^t = (1 + ch_0 + y_0h'_0, ch_2 + y_2h'_2, \ldots, ch_n + y_nh'_n)^t$$

donde $h_i, h' \in \mathcal{R}[x], y_i \in \mathcal{R}$, con $cy_i = 0$. Sea

$$E_2 = \begin{pmatrix} 1 & 0 \\ & \\ 0 & E_1 \end{pmatrix} \in E_{n+1}(\mathcal{R}[x])$$

y $v' = (v_1, v_0, v_2, \ldots, v_n)^t$, se tiene que

$$E_2 v' = (c, 1 + ch_0 + y_0 h'_0, ch_2 + y_2 h'_2, \ldots, ch_n + y_n h'_n)^t = v''.$$

Luego, si

$$\Gamma = E_{1,2}(c) E_{2,1}(-h_1) \ldots E_{n+1,1}(-h_n),$$

$$\Gamma v'' = (0, 1 + y_0 h'_0, y_2 h'_2, \ldots, y_n h'_n)^t.$$

Además con operaciones elementales podemos enviar a $\Gamma v''$ al vector $(1, 0, \ldots, 0)$. □

Corolario 2.43. Para cualquier anillo $\mathcal{R}$ de dimensión de Krull $\leq d$, todo módulo finitamente generado establemente libre sobre $\mathcal{R}[x]$ de rango menor que d, es libre.

Demostración. Por el Teorema 2.41, todo módulo finitamente generado establemente libre sobre $\mathcal{R}$ es libre. Falta probar que todo módulo establemente libre sobre $\mathcal{R}[x]$ es extendido de $\mathcal{R}$. En efecto, sea $v(x) = (v_0(x), \ldots, v_n(x)) \in \mathcal{R}[x]^{n+1}$ con $n \geq d+1$ una fila unimodular, por el Teorema

2.42, existe $A \in GL_{n+1}(\mathcal{R}[x]^{n+1})$ tal que

$$Av(x)^t = (1, 0, \ldots, 0).$$

□

Corolario 2.44. La conjetura de Hermite es verdadera para anillos de dimensión de Krull menor o igual a 1.

Ejemplo 2.45. El anillo de enteros $\mathbb{Z}$ tiene dimensión de Krull igual a 1 así que $\mathbb{Z}[x]$ es un anillo de Hermite. Un dominio de ideales principales DIP tiene dimensión Krull igual a 1, por lo tanto un DIP es un anillo de Hermite. En particular, $\mathbb{K}[x]$, con $\mathbb{K}$ cuerpo.

En (Yengui, 2015) consideran $\mathbb{F}_2$, el cuerpo con dos elementos, se desea presentar un contraejemplo a la conjetura del anillo de Hermite, pero tienen un nuevo obstáculo el cual consiste en probar esta nueva conjetura:

Conjetura 2. El vector unimodular $(x_1, x_2, x_3)^t$ no es complementable sobre el anillo

$$\mathbb{F}_2[x_1, x_2, x_3, y_2, y_3] = \frac{\mathbb{F}_2[X_1, X_2, X_3, Y_2, Y_3]}{\langle X_1^2 + X_2Y_2 + X_3Y_3 - 1\rangle}.$$

O más general:

Conjetura 3. Si $\mathbb{K}$ es un cuerpo entonces el vector unimodular $(x_1, x_2, x_3)^t$ no es complementable

sobre el anillo

$$\mathbb{K}[x_1, x_2, x_3, y_2, y_3] = \frac{\mathbb{K}[X_1, X_2, X_3, Y_2, Y_3]}{\langle X_1^2 + X_2Y_2 + X_3Y_3 - 1\rangle}.$$

Esta conjetura es verdadera en el caso donde $\mathbb{K} = \mathbb{R}$, como hemos probado en el Ejemplo 2.33.

3. Recta proyectiva sobre anillos

En el plano afín, cuando se habla de la intersección de curvas algebraicas, normalmente se hace preciso separar el caso finito del infinito. Es decir, discernimos cuando dos curvas se intersectan de cuando no lo hacen, e interpretamos este último caso diciendo "se intersectan en un punto al infinito". Luego, la pregunta es ¿Se puede construir a partir del plano afín un espacio en el que tal distinción no sea necesaria?, la respuesta es afirmativa, en los espacios proyectivos. A lo largo de esta sección, estudiaremos los espacios proyectivos definidos sobre un anillo $\mathcal{R}$. En este capítulo, como $\mathcal{R}$ denota un anillo conmutativo con unidad, $\mathcal{M}$ será un $\mathcal{R}$-módulo libre de rango dos.

3.1. $\mathbb{R}$-álgebras de dimensión dos y geometrías del plano

En esta sección se presenta una idea de lo que significa estudiar los tres tipos geometrías en el plano: euclídea, hiperbólica y degenerada o más conocidas como Möebius, Laguerre y Minkowski, respectivamente. Desarrollaremos una revisión bibliográfica sobre el importante trabajo que hizo Klein sobre las tres geometrías del plano, es un primer acercamiento a la geometría proyectiva que nos motiva para el estudio de las secciones siguientes. Para esto serán necesarios algunos conceptos y resultados preliminares.

Definición 3.1. Un plano euclídeo es un par $(\mathbb{A}, Q)$ donde $\mathbb{A}$ es un plano afín real asociado al $\mathbb{K}$-espacio vectorial V y Q es una forma cuadrática definida positiva.

Definición 3.2. En el plano, una aplicación conforme es una función que preserva ángulos. El

conjunto de las aplicaciones conformes forman un grupo con la composición de aplicaciones y se conoce como el grupo inversivo.

Definición 3.3. Sean V un $\mathbb{K}$-espacio vectorial y $\boldsymbol{v}, \boldsymbol{u} \in V$. Se dice que $\boldsymbol{v}, \boldsymbol{u}$ son vectores ortogonales si $Q(\boldsymbol{v}, \boldsymbol{u}) = 0$. Los vectores ortogonales a sí mismos se denominan isótropos.

Definición 3.4. Sean V un $\mathbb{K}$-espacio vectorial de dimensión 4 sobre $\mathbb{K}$, $\mathbb{P}(V)$ es el espacio proyectivo asociado a V y Q una forma cuadrática no nula. La imagen por la aplicación canónica π del conjunto de los vectores isótropos no nulos, $[\overline{Q}]$ recibe el nombre de cuádrica asociada a Q. En otras palabras,

$$[\overline{Q}] = \{\pi(\boldsymbol{v}) \in \mathbb{P}(V) \ \mid \ Q(\boldsymbol{v}, \boldsymbol{v}) = 0\}$$

donde π es la aplicación canónica.

Definición 3.5. Una cuádrica del plano proyectivo, se denomina cónica y se denotará por $[Q]$.

Observación 3.6. Si consideramos $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$ una base de V y $\boldsymbol{v} = x\boldsymbol{u}_1 + y\boldsymbol{u}_2 + z\boldsymbol{u}_3$, entonces

$$Q(\boldsymbol{v}, \boldsymbol{v}) = a_0x^2 + a_1y^2 + a_2z^2 + 2b_0yz + 2b_1zx + 2b_2xy \tag{3.1.1}$$

donde $a_i, b_i \in \mathbb{K}$ para $i \in \{0, 1, 2\}$. La ecuación (3.1.1) se conoce como la ecuación de la cónica $[Q]$. De lo anterior, es claro que una cuádrica $[\overline{Q}]$ es una clase de polinomios homogéneos de grado dos que tiene asociada una forma cuadrática Q.

Observación 3.7. Sean R una forma cuadrática y $[\overline{R}]$ la cuádrica asociada a la forma cuadrática R. R define la métrica; si elegimos una métrica en $(\mathbb{A}, R)$ podemos identificar como espacios

vectoriales a $\mathbb{A}$ con $\mathbb{R}^2$. Por ejemplo, si consideramos la forma cuadrática $R(x,y) = x^2 + y^2$ de direcciones isótropas $(i,1)$ y $(-i,1)$, es decir, $R(i,1) = R(-i,1) = 0$, podemos identificar a $\mathbb{C}$ con $\mathbb{R}^2$.

Existen trabajos sobre la relación entre los números complejos y la geometría euclidiana como por ejemplo (Schwerdtfeger, 1979) una buena referencia para conocer los detalles de esta relación. La construcción clásica se le atribuye principalmente a Klein, quien al plano euclídeo le asocia dos objetos geométricos que permiten representar el grupo inversivo como un grupo de matrices, estos dos objetos son, la $\mathbb{R}$-álgebra $\mathbb{C} \cong \frac{\mathbb{R}[x]}{\langle x^2+1\rangle}$ y la cuádrica $[\overline{R}]$. La construcción se basa esencialmente en las analogías entre la métrica $x^2 + y^2$, el ideal que define $\mathbb{C}$ en $\mathbb{R}[x]$, que es $\langle x^2 + 1\rangle$ y la ecuación de la esfera $x^2 + y^2 + z^2 = 1$. Una idea general de esta construcción se puede encontrar en (Franco, pág 38-40).

Klein en su artículo del Mathematische Annalen (Klein, 1985) consideró la posibilidad de repetir la construcción de la geometría euclídea, para la geometría hiperbólica y degenerada. En una secuencia de tres artículos (Franco, 2008a), (Franco, 2007) y (Franco, 2008b) se expone la traducción de estas construcciones publicadas por Klein, la idea es cambiar la $\mathbb{R}$-álgebra y la cuádrica $[\overline{Q}]$ que asociamos al plano métrico. La herramienta básica que conecta los tres objetos geométricos: plano métrico, $\mathbb{R}$-álgebra y cuadrática $[\overline{Q}]$ es la proyección estereográfica.

3.1.1. Planos métricos. La forma cuadrática Q, que define la métrica es un polinomio homogéneo de grado dos en $\mathbb{R}[x, y]$.

1. **Caso definido positivo**. Si la forma cuadrática es $R(x, y) = x^2 + y^2$, R tiene dos direcciones isótropas imaginarias, es decir, dos rectas imaginarias.

2. **Caso indefinido**. Si la forma cuadrática es $Q(x, y) = x^2 - y^2$, Q tiene dos direcciones isótropas reales, es decir, dos rectas reales.

3. **Caso degenerado**. Si la forma cuadrática es $T(x, y) = x^2$, T tiene una dirección isótropa real doble, es decir, una recta real doble.

Cada uno de los tres casos se corresponden con cada uno de los tres tipos de geometrías en el plano: euclídea, hiperbólica y degenerada.

3.1.2. $\mathbb{R}$-álgebras de dimensión dos. Desde el punto de vista del álgebra, existen tres tipos de extensiones de grado dos. En efecto, considere una extensión de grado dos de $\mathbb{R}$

$$\frac{\mathbb{R}[x]}{(x^2 + bx + c)},$$

se pueden dar tres casos, estos según las raíces del polinomio de grados dos

$$x^2 + bx + c.$$

Puede que este, tenga dos raíces imaginarias, dos raíces reales distintas o una raíz doble. Se prueba en (Franco, 2008a) que salvo isomorfismos, las tres álgebras de dimensión dos sobre $\mathbb{R}$ son :

$$\mathbb{C} \cong \frac{\mathbb{R}[x]}{\langle x^2+1\rangle},\ \mathbb{P} \cong \frac{\mathbb{R}[x]}{\langle x^2-1\rangle},\ \mathbb{D} \cong \frac{\mathbb{R}[x]}{\langle x^2\rangle}.$$

Definición 3.8. Llamamos:

1. Números complejos a

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

2. Números paracomplejos a

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

3. Números duales a

$$\mathbb{D} \cong \frac{\mathbb{R}[x]}{(x^2)} = \{a+kb \mid a,b \in \mathbb{R},\ k^2=0\}.$$

Identificando el plano con cada una de estas $\mathbb{R}$-álgebras, se obtiene una representación lineal del grupo inversivo, para cada uno de los tres tipos de métricas mencionadas anteriormente.

En (Franco, 2008b) se prueba que las rectas proyectivas sobre las $\mathbb{R}$-álgebras $\mathbb{C},\mathbb{P}$ y $\mathbb{D}$ tienen estructura de variedad diferenciable bidimensional y en (Franco, 2008a) que generan las tres geometrías clásicas del plano, Möebius, Laguerre y Minkowski, respectivamente.

Definición 3.9. Sean $\mathbb{K}$ una $\mathbb{R}$-álgebra de dimensión dos y $z \in \mathbb{K}$, llamamos conjugado de z en $\mathbb{K}$ a un $\overline{z} \in \mathbb{K}$ tal que $(x-z)(x-\overline{z}) = m_z$ donde m_z es el polinomio mínimo de z.

Se puede probar que el conjugado siempre existe y es único, en particular, sea $z = a + bi \in \mathbb{K} = \mathbb{C}, \mathbb{P}$ ó $\mathbb{D}$, el conjugado de z es $\overline{z} = a - bi$. Para cada tipo de $\mathbb{R}$-álgebra la correspondencia de conjugación es:

$$- : \mathbb{K} \longrightarrow \mathbb{K}$$

$$z \longmapsto \overline{z}.$$

Verifica:

1. $-$ es $\mathbb{R}$-lineal,
2. $\overline{1_{\mathbb{K}}} = 1_{\mathbb{K}}$,
3. $\overline{\overline{z}} = z$,
4. $z \cdot \overline{z} = |z|^2$ para todo $z \in \mathbb{K}$.

Note que un homomorfismo de $\mathbb{R}$-álgebras de dimensión dos, $\Phi : \mathbb{K} \longrightarrow \mathbb{K}$ queda unívocamente determinado por la imagen de un elemento cuyo polinomio mínimo sea el polinomio que define la extensión, que la imagen de ese elemento ha de seguir siendo una raíz de ese polinomio y que el homomorfismo será inyectivo si el polinomio mínimo de la imagen sigue siendo el polinomio que define la extensión. Por lo tanto los únicos homomorfismos de $\mathbb{R}$-álgebras, para cada caso son:

1. **Caso** $\mathbb{C}$, la identidad y la conjugación.

2. **Caso** $\mathbb{P}$, la identidad, la conjugación y las dos aplicaciones

$$\begin{aligned} \mathbb{P} &\longrightarrow \mathbb{P} \\ a+bj &\longmapsto a+bj \\ a+bj &\longmapsto a-bj. \end{aligned}$$

3. **Caso** $\mathbb{D}$, las infinitas aplicaciones

$$\begin{aligned} \mathbb{D} &\longrightarrow \mathbb{D} \\ a+bk &\longmapsto a+b\lambda k \end{aligned}$$

de los cuales son automorfismos sólo la identidad y la conjugación.

Proposición 3.10. (Franco, Proposición 7) En una $\mathbb{R}$-álgebra con unidad, de dimensión dos, se tiene que

1. z es divisor de cero si y sólo si z no es invertible.

2. Si z es divisor de cero, $zz' = 0$ con $z' \neq 0$ si y sólo si $z' = \lambda\bar{z}$ para $\lambda \in \mathbb{R}^*$.

3. Si z es invertible, entonces $z^{-1} = \frac{\bar{z}}{|z|^2}$.

Identificando el plano $\mathbb{R}^2$ como espacio vectorial con cada una de las $\mathbb{R}$-álgebras $\mathbb{C}, \mathbb{P}$ y $\mathbb{D}$, los divisores de cero son:

1. **Caso** $\mathbb{C}$, no hay divisores de cero. Viendo $\mathbb{C}$ como $\mathbb{R}^2$, son las dos rectas imaginarias dadas por $x^2+y^2=0$. Las únicas raíces son $\pm i$.

2. **Caso** $\mathbb{P}$, son las dos rectas $x^2-y^2=0$ que son las dos rectas que pasan por el origen y tiene pendientes ± 1. Además para que el producto de dos paracomplejos sea cero, el punto correspondiente a cada uno de ellos debe estar en una de esas dos rectas. Las raíces son ± 1 y $\pm j$.

3. **Caso** $\mathbb{D}$, es la recta doble $x^2=0$. Además para que el producto sea cero los dos puntos tienen que estar en esa recta. Hay infinitas raíces, que son λk con $\lambda \in \mathbb{R}$.

3.1.3. Cuádricas. De manera análoga a los planos métricos y las $\mathbb{R}$-álgebras, también existen tres tipo de cuádricas en el espacio proyectivo real $\mathbb{P}^3_{\mathbb{R}}$. Para exponer esto será necesario introducir de manera rápida algunos conceptos sobre cónicas y cuádricas. Sin embargo, para indagar más acerca de cónicas y cuádricas se recomienda ver (Doneddu, 1980) y (Franco, 2007).

Definición 3.11. Sean V un $\mathbb{K}$-espacio vectorial y $V^\perp$ el espacio ortogonal de V. Se dice que cuádrica $[\overline{Q}]$, es degenerada si $V^\perp \neq \{0\}$ o lo que es equivalente a que $\mathbb{P}(V^\perp) \neq \emptyset$.

Observación 3.12. Recordemos que toda forma cuadrática Q está asociada una forma bilineal que denotaremos por F_Q. Claramente esta forma bilineal F_Q estará también asociada a la cuádrica $[\overline{Q}]$. Dado un punto $P \in [\overline{Q}]$ se puede construir un hiperplano tangente a P respecto a la forma bilineal F_Q asociada a la cuádrica, es decir, $F_Q(S,P)=0$ para todo $S \in [\overline{Q}]$, denotaremos al hiperplano tangente por $P^\perp$.

Según como sea la intersección de una cuádrica $[\overline{Q}]$ con sus hiperplanos tangentes podemos determinar los tipos de cuádricas en el espacio proyectivo real $\mathbb{P}^3_{\mathbb{R}}$. La siguiente proposición caracteriza los tipos de cuádricas.

Proposición 3.13. (Franco, Proposición 3) Sean $[\overline{Q}] \in \mathbb{P}^3_{\mathbb{R}}$ una cuádrica no degenerada y $P \in [\overline{Q}]$. Entonces

1. $[\overline{Q}]$ es de tipo elíptico si $P^{\perp} \cap [\overline{Q}] = P, l_1, l_2$ son dos rectas imaginarias.

2. $[\overline{Q}]$ es de tipo hiperbólico si $P^{\perp} \cap [\overline{Q}] = \{r_1, r_2\}$, con r_1, r_2 rectas que se cortan en P.

3. $[\overline{Q}]$ es el cono real si $P^{\perp} \cap [\overline{Q}] = \{r_0\}$ con r_0 recta que pasa por P.

Definición 3.14. Sean $[\overline{Q}]$ una cuádrica no degenerada y H el hiperplano tangente en $\mathbb{P}(V)$. Llamaremos ciclos a las cuádricas $[C] \in \mathbb{P}(V)$, tales que $[C] \cap H \cap [\overline{Q}] = [\overline{Q}]$ o lo que es equivalente a las proyecciones estereográficas de secciones planas a la cuádrica.

Definición 3.15. Los ciclos no degenerados son proyecciones de secciones planas no tangentes y los ciclos degenerados se corresponden con secciones planas tangentes.

En (Franco, 2007) se ha estudiado la generalización de la proyección estereográfica a cuádricas generales, describiendo los ciclos en el plano eligiendo una referencia adecuada, los ciclos no degenerados son, según el tipo de cuádrica elegida:

1. Si $[\overline{Q}]$ es de tipo elíptico, los ciclos no degenerados son las rectas y circunferencias.

2. Si $[\overline{Q}]$ es de tipo hiperbólico, los ciclos no degenerados son rectas de pendientes distintas a ± 1 e hipérbolas con asíntotas de pendientes ± 1.

3. Si $[\overline{Q}]$ es el cono real, los ciclos no degenerados son rectas de pendientes distintas a infinito (rectas verticales) y parábolas con eje de pendiente infinita.

Para finalizar, se demuestra que las $\mathbb{R}$-álgebras $\mathbb{P}$ y $\mathbb{D}$ aunque pierden la estructura de cuerpo, queda suficiente estructura algebraica para poder definir una razón doble y mediante esta, podemos definir los ciclos. En lo que sigue la $\mathbb{R}$-álgebra $\mathbb{K}$ será $\mathbb{C}, \mathbb{P}$ ó $\mathbb{D}$. Empezamos definiendo la razón de cuatro puntos distintos en $\mathbb{K}$.

Definición 3.16. Dados $z_1, z_2, z_3, z_4 \in \mathbb{K}$, con $z_i = a_i + jb_i$ con $i \in \{1, 2, 3, 4\}$. Llamamos razón doble de esos cuatro puntos a:

$$[z_1, z_2, z_3, z_4] = \frac{(z_1 - z_4)(z_2 - z_3)}{(z_3 - z_1)(z_4 - z_2)},$$

siempre que ese cociente sea un elemento invertible de $\mathbb{K}$.

Identificando el plano $\mathbb{R}^2$ con cada una de las $\mathbb{R}$-álgebras $\mathbb{C}, \mathbb{P}$ y $\mathbb{D}$ como $\mathbb{K}$-espacios vectoriales, se tiene:

1. **Caso** $\mathbb{K} = \mathbb{C}$, la razón doble está definida si los cuatro puntos son distintos.

2. **Caso** $\mathbb{K} = \mathbb{P}$, la razón doble está definida siempre que no haya dos puntos que estén en las rectas de pendiente ± 1.

3. **Caso** $\mathbb{K} = \mathbb{D}$, la razón doble está definida siempre que dos puntos no estén en rectas paralelas al eje y.

Observación 3.17. Identificando el plano $\mathbb{R}^2$ con $\mathbb{K}$ como espacios vectoriales, tres puntos definen un único ciclo no degenerado siempre que se pueda definir su razón doble. Además, si consideramos otro punto $z \in \mathbb{K}$, si su razón doble está en $\mathbb{R}$ obtenemos una forma algebraica de definir los ciclos no degenerados.

Proposición 3.18. Sean z_1, z_2 y z_3 puntos de $\mathbb{R}^2$ tales que determinan un único ciclo no degenerado. Otro punto $z \in \mathbb{K}$ está en el ciclo definido por z_1, z_2 y z_3, si y sólo si $[z_1, z_2, z_3, z] \in \mathbb{R}$.

Demostración. La razón doble está definida precisamente porque los tres puntos definen un único ciclo no degenerado.

1. Si los tres puntos están alineados (el ciclo es una recta)

$$[z_1, z_2, z_3, z] = \frac{(z_1 - z)(z_2 - z_3)}{(z_3 - z_1)(z - z_2)} = \frac{\lambda(z_1 - z)(z_3 - z_1)}{(z_3 - z_1)(z - z_2)} \in \mathbb{R},$$

   si y sólo si z está en la recta $\{z_1, z_2, z_3\}$.

2. En otro caso, si los tres puntos no están alineados. Sea $z = x + y\sigma$, con $\sigma = i, j$ ó k según sea el caso. Calculemos la razón doble

$$[z_1, z_2, z_3, z] = \frac{((a_1 - x) + \sigma(b_1 - y))((a_2 - a_3) + \sigma(b_2) - b_3))}{((a_3 - a_1) + \sigma(b_3 - b_1))((x - a_2) + \sigma(y - b_2))},$$

   haciendo el producto, obtenemos que la razón doble se puede expresar como el cociente de

polinomios homogéneos en $\mathbb{K}[x, y]$

$$[z_1, z_2, z_3, z] = \frac{p_1(x,y) + \sigma p_2(x,y)}{p_3(x,y) + \sigma p_4(x,y)}$$

cada $p_i(x, y)$ está dada por

$$p_i(x, y) = \alpha_i x + \beta_i y + K$$

donde

$$\alpha_1 = a_3 - a_2, \quad \alpha_2 = b_3 - b_2, \quad \alpha_3 = a_3 - a_1, \quad \alpha_4 = b_3 - b_1,$$

$$\beta_1 = \sigma^2\alpha_4, \quad \beta_2 = \alpha_3, \quad \beta_3 = \sigma^2\alpha_2, \quad \beta_4 = \alpha_1.$$

K es un término constante que resulta de las sumas y diferencias entre los demás términos en los que no se factoriza ni x ni y. Ahora, para calcular la razón doble, multiplicamos el cociente por su polinomio conjugado. De esta forma,

$$[z_1, z_2, z_3, z] = \frac{(p_1(x,y) + \sigma p_2(x,y))(p_3(x,y) - \sigma p_4(x,y))}{p_3(x,y)^2 + \sigma^2 p_4(x,y)^2} \in \mathbb{R}$$

lo equivalente a

$$p_3(x,y)p_2(x,y) - p_1(x,y)p_4(x,y) = 0 \tag{3.1.2}$$

es decir, la parte imaginaria del polinomio debe ser cero. Note que la ecuación (3.1.2), es la

ecuación de una cónica. En efecto, sustituyendo

$$\begin{aligned} p_3(x,y)p_2(x,y) - p_1(x,y)p_4(x,y) =& (\alpha_2\alpha_3 - \alpha_1\alpha_4)x^2 + (\beta_2\beta_3 - \beta_1\beta_4)y^2 + \\ & (\alpha_3\beta_2 + \alpha_2\beta_3 - \alpha_1\beta_4 - \alpha_4\beta_1)xy + r(x,y) \\ & = (\alpha_2\alpha_3 - \alpha_1\alpha_4)x^2 + \sigma^2(\alpha_2\alpha_3 - \alpha_1\alpha_4)y^2 + r(x,y) \end{aligned}$$

siendo $r(x,y)$ un polinomio homogéneo de grado uno, y además

$$(\alpha_2\alpha_3 - \alpha_1\alpha_4) = (b_2 - b_3)(a_3 - a_1) - (a_3 - a_2)(b_3 - b_1) \neq 0,$$

pues si $(\alpha_2\alpha_3 - \alpha_1\alpha_4) = 0$ los puntos z_1, z_2 y z_3 estarían sobre la misma recta, y esto es absurdo, porque estamos considerando el caso en donde no lo están. Finalmente, la ecuación de la cónica es

$$(\alpha_2\alpha_3 - \alpha_1\alpha_4)x^2 + \sigma^2(\alpha_2\alpha_3 - \alpha_1\alpha_4)y^2 + r(x,y)$$

con $\sigma = i, j$ ó k según sea el caso.

Homogeneizando la ecuación de la cónica, veamos la intersección de la cónica con el infinito. Sean $[x,y,z]$ las coordenadas del punto (x,y,z) en la cónica descrita anteriormente. Veamos los casos,

- **Caso** $\mathbb{K} = \mathbb{C}$ $(i^2 = -1)$: $x^2 + y^2 = 0$. La intersección de la cónica con el infinito son los puntos $[0,1,i]$ y $[0,1,-i]$. En el plano euclídeo usual, la cónica es una circunferencia.

- **Caso** $\mathbb{K} = \mathbb{P}$ $(j^2 = 1)$: $x^2 - y^2 = 0$. La intersección de la cónica con el infinito son los puntos

$[0,1,1]$ y $[0,1,-1]$. En el plano euclídeo usual, la cónica es una hipérbola equilátera.

- **Caso** $\mathbb{K} = \mathbb{D}$ $(k^2 = 0)$: $x^2 = 0$. La intersección de la cónica con el infinito son los puntos dobles $[0,0,1]$ y entonces en la cónica en el plano euclídeo usual, es una parábola con eje de pendiente cero.

□

3.2. $\mathcal{R}$-módulos libres de rango dos

$\mathcal{M}$ un $\mathcal{R}$-módulo libre de rango 2, $\mathcal{M} \cong \mathcal{R}^2$.

Definición 3.19. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$ y $\boldsymbol{x}$,$\boldsymbol{y} \in \mathcal{M}$. Si $\boldsymbol{x} = x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2$ y $\boldsymbol{y} = y_1\boldsymbol{v}_1 + y_2\boldsymbol{v}_2$, definimos el producto exterior relativo a la base $\mathfrak{B}$ como

$$\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y} = \begin{vmatrix} x_1 & x_2 \\ \\ y_1 & y_2 \end{vmatrix} = x_1y_2 - x_2y_1 \in \mathcal{R}.$$

A continuación se presentarán algunas propiedades del producto exterior.

Proposición 3.20. (Granados Pinzón, pág 92) Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$ y $\mathbf{x}$,$\mathbf{y} \in \mathcal{M}$. Se cumple que:

1. $\wedge_{\mathfrak{B}}$ bilineal y antisimétrica, es decir, $\mathbf{x} \wedge_{\mathfrak{B}} \mathbf{y} = -\mathbf{y} \wedge_{\mathfrak{B}} \mathbf{x}$. Además $\mathbf{x} \wedge_{\mathfrak{B}} \mathbf{x} = 0$.

2. Si $\mathfrak{B}' = \{\boldsymbol{v}_1', \boldsymbol{v}_2'\}$ es otra base de $\mathcal{M}$ entonces,

$$\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y} = (\boldsymbol{x} \wedge_{\mathfrak{B}'} \boldsymbol{y})(\boldsymbol{v}_1' \wedge_{\mathfrak{B}} \boldsymbol{v}_2').$$

3. $\mathfrak{B}' = \{\boldsymbol{v}'_1, \boldsymbol{v}'_2\}$ es base de $\mathcal{M}$ si y sólo si $\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2 \in \mathcal{R}^*$.

Demostración. 1. Considere

$$\wedge_{\mathfrak{B}} : \mathcal{M} \times \mathcal{M} \longmapsto \mathcal{R}$$

$$(\boldsymbol{x},\boldsymbol{y}) \longmapsto \boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y}.$$

Sean $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z} \in \mathcal{M}$,

$$\wedge_{\mathfrak{B}}(\boldsymbol{x}+\boldsymbol{y},\boldsymbol{z}) = \begin{vmatrix} x_1+y_1 & x_2+y_2 \\ z_1 & z_2 \end{vmatrix} = \begin{vmatrix} x_1 & x_2 \\ z_1 & z_2 \end{vmatrix} + \begin{vmatrix} y_1 & y_2 \\ z_1 & z_2 \end{vmatrix} = \wedge_{\mathfrak{B}}(\boldsymbol{x},\boldsymbol{z}) + \wedge_{\mathfrak{B}}(\boldsymbol{y},\boldsymbol{z}),$$

$$\wedge_{\mathfrak{B}}(\alpha\boldsymbol{x},\boldsymbol{y}) = \begin{vmatrix} \alpha x_1 & \alpha x_2 \\ y_1 & y_2 \end{vmatrix} = \alpha x_1 y_2 - \alpha x_2 y_1 = \alpha(x_1 y_2 - x_2 y_1) = \alpha(\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y}).$$

Sean $\boldsymbol{x}$ y $\boldsymbol{y} \in \mathcal{M}$, se tiene que

$$-(\boldsymbol{y} \wedge_{\mathfrak{B}} \boldsymbol{x}) = -\begin{vmatrix} y_1 & y_2 \\ x_1 & x_2 \end{vmatrix} = -(x_2 y_1 - x_1 y_2) = x_1 y_2 - x_2 y_1 = \boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y},$$

$$\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{x} = \begin{vmatrix} x_1 & x_2 \\ x_1 & x_2 \end{vmatrix} = x_1 x_2 - x_1 x_2 = 0.$$

2. Sean $\boldsymbol{v}'_1 = v_{11}\boldsymbol{v}_1 + v_{12}\boldsymbol{v}_2$ y $\boldsymbol{v}'_2 = v_{21}\boldsymbol{v}_1 + v_{22}\boldsymbol{v}_2$. Ahora considere $\boldsymbol{x}$ y $\boldsymbol{y}$ en la base $\{\boldsymbol{v}'_1, \boldsymbol{v}'_2\}$,

$$\boldsymbol{x} = x_1\boldsymbol{v}'_1 + x_2\boldsymbol{v}'_2,$$

$$\boldsymbol{y} = y_1\boldsymbol{v}'_1 + y_2\boldsymbol{v}'_2.$$

Reemplazando $\boldsymbol{x}$ y $\boldsymbol{y}$ en la base $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ se tiene que

$$\boldsymbol{x} = x_1(v_{11}\boldsymbol{v}_1 + v_{12}\boldsymbol{v}_2) + x_2(v_{21}\boldsymbol{v}_1 + v_{22}\boldsymbol{v}_2),$$

$$\boldsymbol{y} = y_1(v_{11}\boldsymbol{v}_1 + v_{12}\boldsymbol{v}_2) + y_2(v_{21}\boldsymbol{v}_1 + v_{22}\boldsymbol{v}_2).$$

Así,

$$\boldsymbol{x} = (x_1v_{11} + x_2v_{21})\boldsymbol{v}_1 + (x_2v_{22} + x_1v_{12})\boldsymbol{v}_2,$$

$$\boldsymbol{y} = (y_1v_{11} + y_2v_{21})\boldsymbol{v}_1 + (y_2v_{22} + y_1v_{12})\boldsymbol{v}_2.$$

Luego,

$$\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y} = \begin{vmatrix} x_1v_{11} + x_2v_{21} & x_2v_{22} + x_1v_{12} \\ y_1v_{11} + y_2v_{21} & y_2v_{22} + y_1v_{12} \end{vmatrix} = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \begin{vmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{vmatrix}$$

$$= (\boldsymbol{x} \wedge_{\mathfrak{B}'} \boldsymbol{y})(\boldsymbol{v}_1 \wedge_{\mathfrak{B}} \boldsymbol{v}_2).$$

3. Veamos que si $\mathfrak{B}'$ es base de $\mathcal{M}$ entonces $\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2 \in \mathcal{R}^*$. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ y $\mathfrak{B}' = \{\boldsymbol{v}'_1, \boldsymbol{v}'_2\}$ bases de $\mathcal{M}$, por el item 2, se tiene que $\boldsymbol{v}_1 \wedge_{\mathfrak{B}} \boldsymbol{v}_2 = (\boldsymbol{v}_1 \wedge_{\mathfrak{B}'} \boldsymbol{v}_2)(\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2)$, note que las coordenadas de $\boldsymbol{v}_1$ y $\boldsymbol{v}_2$ en la base $\mathfrak{B}$, son $(1,0)$ y $(0,1)$ respectivamente. Así,

$$1 = \begin{vmatrix} 1 & 0 \\ \\ 0 & 1 \end{vmatrix} = \boldsymbol{v}_1 \wedge_{\mathfrak{B}} \boldsymbol{v}_2 = (\boldsymbol{v}_1 \wedge_{\mathfrak{B}'} \boldsymbol{v}_2)(\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2) \in \mathcal{R}^*.$$

Luego, $(\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2) \in \mathcal{R}^*$.

Veamos ahora que $\mathfrak{B}'$ es una base para $\mathcal{M}$. Sean $\boldsymbol{v}'_1 = x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2$ y $\boldsymbol{v}'_2 = y_1\boldsymbol{v}_1 + y_2\boldsymbol{v}_2$,

$$\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2 = \begin{vmatrix} x_1 & x_2 \\ \\ y_1 & y_2 \end{vmatrix} = x_1y_2 - x_2y_1 \in \mathcal{R}^*.$$

Luego, $\begin{pmatrix} x_1 & x_2 \\ \\ y_1 & y_2 \end{pmatrix}$ es invertible y por lo tanto, existe $\begin{pmatrix} x_1 & x_2 \\ \\ y_1 & y_2 \end{pmatrix}^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \\ \beta_1 & \beta_2 \end{pmatrix}$. Entonces $\boldsymbol{v}_1 = \alpha_1\boldsymbol{v}'_1 + \alpha_2\boldsymbol{v}'_2$ y $\boldsymbol{v}_2 = \beta_1\boldsymbol{v}'_1 + \beta_2\boldsymbol{v}'_2$. Puesto que $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ es base, entonces $\mathfrak{B}' = \{\boldsymbol{v}'_1, \boldsymbol{v}'_2\}$ es un conjunto generador de $\mathcal{M}$. Como la dimensión de $\mathcal{M}$ es dos, se sigue que $\{\boldsymbol{v}'_1, \boldsymbol{v}'_2\}$ es base de $\mathcal{M}$.

□

Proposición 3.21. (Granados Pinzón, Proposición 3.1.8) Sean $\mathcal{M}$ un $\mathcal{R}-$módulo libre de rango dos y $\mathfrak{B}$ una base para $\mathcal{M}$. Para todos los $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z} \in \mathcal{M}$ se tiene

$$(\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y})\boldsymbol{z} + (\boldsymbol{z} \wedge_{\mathfrak{B}} \boldsymbol{x})\boldsymbol{y} + (\boldsymbol{y} \wedge_{\mathfrak{B}} \boldsymbol{z})\boldsymbol{x} = 0.$$

Demostración. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ base de $\mathcal{M}$ y $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z} \in \mathcal{M}$,

$$\boldsymbol{x} = x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2, \quad \boldsymbol{y} = y_1\boldsymbol{v}_1 + y_2\boldsymbol{v}_2, \quad \boldsymbol{z} = z_1\boldsymbol{v}_1 + z_2\boldsymbol{v}_2,$$

entonces

$$(x_1y_2 - x_2y_1)(z_1\boldsymbol{v}_1 + z_2\boldsymbol{v}_2) + (z_1x_2 - z_2x_1)(y_1\boldsymbol{v}_1 + y_2\boldsymbol{v}_2) + (y_1z_2 - y_2z_1)(x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2) =$$

$$(x_1y_2z_1 - x_2y_1z_1 + x_2y_1z_1 - x_1y_1z_2 + x_1y_1z_2 - x_1y_2z_1)\boldsymbol{v}_1 + (x_1y_2z_2 - x_2y_1z_2 + x_2y_2z_1 -$$

$$x_1y_2z_2 + z_2y_1z_2 - x_2y_2z_1)\boldsymbol{v}_2 = 0.$$

□

Proposición 3.22. (Granados Pinzón, Proposición 3.1.9) Si $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ es una base de $\mathcal{M}$ entonces para todo $\boldsymbol{x} \in \mathcal{M}$, $\boldsymbol{x} = (\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{v}_2)\boldsymbol{v}_1 + (\boldsymbol{v}_1 \wedge_{\mathfrak{B}} \boldsymbol{x})\boldsymbol{v}_2$.

Demostración. Considere $\boldsymbol{y} = \boldsymbol{v}_1$ y $\boldsymbol{z} = \boldsymbol{v}_2$ entonces por el Teorema 3.21, obtenemos que $(\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{v}_1)\boldsymbol{v}_2 + (\boldsymbol{v}_2 \wedge_{\mathfrak{B}} \boldsymbol{x})\boldsymbol{v}_1 + (\boldsymbol{v}_1 \wedge_{\mathfrak{B}} \boldsymbol{v}_2)\boldsymbol{x} = 0$. Luego,

$$\boldsymbol{x} = (\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{v}_2)\boldsymbol{v}_1 + (\boldsymbol{v}_1 \wedge_{\mathfrak{B}} \boldsymbol{x})\boldsymbol{v}_2.$$

□

Definición 3.23. Sea $\mathcal{M}$ un $\mathcal{R}-$módulo libre de rango dos. Si $\boldsymbol{m} \in \mathcal{M}$ y $\mathcal{N}_1, \mathcal{N}_2$ son submódulos monógenos de $\mathcal{M}$, se definen los siguientes conjuntos

1. $I(\boldsymbol{m}) = \{\boldsymbol{m} \wedge \boldsymbol{y} : \boldsymbol{y} \in \mathcal{M}\}$,
2. $I(\mathcal{N}_1) = \{\boldsymbol{y} \wedge \boldsymbol{z} : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z} \in \mathcal{M}\}$,
3. $I(\mathcal{N}_1\mathcal{N}_2) = \{\boldsymbol{y} \wedge \boldsymbol{z} : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z} \in \mathcal{N}_2\}$.

Los conjuntos de la Definición 3.23 son ideales de $\mathcal{R}$ independientes de la base elegida asociada al producto exterior. Además si $\mathcal{N}_1$ es libre y $\{\boldsymbol{m}\}$ es una base de $\mathcal{N}_1$, entonces se sigue que $I(\boldsymbol{m}) = I(\mathcal{N}_1)$ como se demuestra a continuación.

Proposición 3.24.
1. $I(\boldsymbol{m}), I(\mathcal{N}_1)$ y $I(\mathcal{N}_1\mathcal{N}_2)$ son ideales de $\mathcal{R}$ independientes de la base elegida para definir el producto exterior.
2. Si $\mathcal{N}_1$ es libre y $\{\boldsymbol{m}\}$ es una base de $\mathcal{N}_1$ entonces $I(\boldsymbol{m}) = I(\mathcal{N}_1)$.

Demostración.
1. Es fácil verificar que $I(\boldsymbol{m}), I(\mathcal{N}_1)$ y $I(\mathcal{N}_1\mathcal{N}_2)$ son ideales de $\mathcal{R}$. Veamos que son independientes de la base elegida para definir el producto exterior. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ y $\mathfrak{B}' = \{\boldsymbol{v}'_1, \boldsymbol{v}'_2\}$ bases de $\mathcal{R}$. Por el ítem 2 de la Proposición 3.20,

$$\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y} = (\boldsymbol{x} \wedge_{\mathfrak{B}'} \boldsymbol{y})(\boldsymbol{v}'_1 \wedge_{\mathfrak{B}} \boldsymbol{v}'_2)$$

para todo $\boldsymbol{x},\boldsymbol{y} \in \mathcal{M}$, entonces

$$\begin{aligned}\{\boldsymbol{x} \wedge_{\mathfrak{B}} \boldsymbol{y} : \boldsymbol{y} \in \mathcal{M}\} &= \{\boldsymbol{x} \wedge_{\mathfrak{B}'} [(\boldsymbol{v}_1' \wedge_{\mathfrak{B}} \boldsymbol{v}_2')\boldsymbol{y}] : \boldsymbol{y} \in \mathcal{M}\} \\ &= \{\boldsymbol{x} \wedge_{\mathfrak{B}'} \boldsymbol{y}' : \boldsymbol{y}' \in \mathcal{M}\}, \\ \{\boldsymbol{y} \wedge_{\mathfrak{B}} \boldsymbol{z} : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z} \in \mathcal{M}\} &= \{\boldsymbol{y} \wedge_{\mathfrak{B}'} [(\boldsymbol{v}_1' \wedge_{\mathfrak{B}} \boldsymbol{v}_2')\boldsymbol{z}] : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z} \in \mathcal{M}\} \\ &= \{\boldsymbol{y} \wedge_{\mathfrak{B}'} \boldsymbol{z}' : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z}' \in \mathcal{M}\}\end{aligned}$$

y

$$\begin{aligned}\{\boldsymbol{y} \wedge_{\mathfrak{B}} \boldsymbol{z} : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z} \in \mathcal{N}_2\} &= \{\boldsymbol{y} \wedge_{\mathfrak{B}'} [(\boldsymbol{v}_1' \wedge_{\mathfrak{B}} \boldsymbol{v}_2')\boldsymbol{z}] : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z} \in \mathcal{N}_2\} \\ &= \{\boldsymbol{y} \wedge_{\mathfrak{B}'} \boldsymbol{z}' : \boldsymbol{y} \in \mathcal{N}_1 \text{ y } \boldsymbol{z}' \in \mathcal{N}_2\}.\end{aligned}$$

2. Como $\boldsymbol{m} \in \mathcal{N}_1$, $I(\boldsymbol{m}) \subset I(\mathcal{N}_1)$. Veamos que $I(\mathcal{N}_1) \subset I(\boldsymbol{m})$. En efecto, si $\boldsymbol{y} \wedge \boldsymbol{z} \in \mathcal{N}_1$ entonces $\boldsymbol{y} \in \mathcal{N}_1$, luego $\boldsymbol{y} = \lambda \boldsymbol{m}$ con $\lambda \in \mathcal{R}$ así, $\boldsymbol{y} \wedge \boldsymbol{z} = \lambda \boldsymbol{m} \wedge \boldsymbol{z} = \boldsymbol{m} \wedge \lambda \boldsymbol{z} \in I(\boldsymbol{m})$.

□

A continuación el Lema 3.25 presenta una equivalencia entre las definiciones de filas unimodulares y elementos complementables dadas en el Capítulo 2 y los conjuntos mencionados en la Definición 3.23 en términos del producto exterior.

Proposición 3.25. (Granados, Contreras) Sean $\mathcal{M}$ un $\mathcal{R}-$módulo libre de rango dos y $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$. Entonces

1. $\boldsymbol{m} \in \mathcal{M}$ es unimodular si y sólo si $I(\boldsymbol{m}) = \mathcal{R}$.

2. $\boldsymbol{m} \in \mathcal{M}$ es complementable si y sólo si existe $\boldsymbol{n} \in \mathcal{M}$ tal que $\{\boldsymbol{m}, \boldsymbol{n}\}$ es una base de $\mathcal{M}$.

Demostración. Sea $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$, entonces para $\boldsymbol{m} \in \mathcal{M}$ se tiene que $\boldsymbol{m} = m_1\boldsymbol{v}_1 + m_2\boldsymbol{v}_2$ con $m_1, m_2 \in \mathcal{R}$.

1. $\boldsymbol{m} = (m_1, m_2) \in Um_2(\mathcal{R})$ si y sólo si $\langle m_1, m_2 \rangle = \mathcal{R}$ esto es equivalente a $\boldsymbol{y} = (y_2, -y_1) \in \mathcal{M}$ tal que $(m_1, m_2) \cdot (y_2, -y_1) = 1$, es decir $m_1y_2 - m_2y_1 = 1$ si y sólo si $I(\boldsymbol{m}) = \mathcal{R}$.

2. $\boldsymbol{m} = (m_1, m_2)$ es complementable, esto es equivalente a que existe $A \in GL_2(\mathcal{R})$ con primera fila (m_1, m_2), si y sólo si existe $\boldsymbol{n} = (n_1, n_2) \in \mathcal{M}$ tal que $\begin{pmatrix} m_1 & m_2 \\ n_1 & n_2 \end{pmatrix}$ es invertible, es decir, $\begin{vmatrix} m_1 & m_2 \\ n_1 & n_2 \end{vmatrix} = \boldsymbol{m} \wedge \boldsymbol{n} \in \mathcal{R}^*$, el ítem 3 de la Proposición 3.20 $\{\boldsymbol{m}, \boldsymbol{n}\}$ es una base de $\mathcal{M}$.

□

Las equivalencias de la Proposición 3.25 nos motiva a definir los siguientes elementos.

Definición 3.26. Se dice que $\boldsymbol{m} \in \mathcal{M}$ es:

1. **Unimodular**, si $I(\boldsymbol{m}) = \mathcal{R}$.

2. **Semimodular**, si $I(\boldsymbol{m}) = \lambda\mathcal{R}$ con λ no divisor de cero.

3. **Complementable**, si existe $\boldsymbol{n} \in \mathcal{M}$ tal que $\{\boldsymbol{m}, \boldsymbol{n}\}$ es base de $\mathcal{M}$.

4. **Simplificable**, si existe $\lambda \in \mathcal{R}$ no divisor de cero y $\boldsymbol{n} \in \mathcal{M}$ complementable tal que $\boldsymbol{m} = \lambda \boldsymbol{n}$.

Ejemplo 3.27. 1. Considere el $\mathbb{Z}$-módulo, $\mathbb{Z}^2$. Entonces $(x, y) \in \mathbb{Z}^2$ es unimodular si y sólo si $x, y \in \mathbb{Z}$ son primos relativos. En este caso existen $x', y' \in \mathbb{Z}$ tales que $xx' + yy' = m.c.d(x, y) = 1$. En particular, la pareja $(3, 5) \in \mathbb{Z}^2$ es unimodular. Observe que $(3, 5) \in \mathbb{Z}^2$ también es complementable pues $\{(3, 5), (1, 2)\}$ forma una base de $\mathbb{Z}^2$. Note que $(1, 2)$ también es un elemento complementable.

2. Sea $\mathcal{R} = \mathbb{R}[x]$. El elemento $(1+x, x^2) \in \mathcal{R}^2$ es semimodular, pues $(2, 2x) \in \mathcal{R}^2$ tal que $I((1+x, x^2)) = \begin{vmatrix} 1+x & x^2 \\ 2 & 2x \end{vmatrix} = 2x$ y 2 no es divisor de cero. Note que $(1, x)$ es complementable y además $(2, 2x) = 2(1, x)$, por lo tanto el par $(2, 2x)$ es simplificable.

En el Ejemplo 3.27 se observa que existe una relación entre los elementos unimodulares y complementables, es decir, parece que unimodular implica ser complementable y viceversa, y lo mismo sucede para los elementos semimodulares y simplificables. Entonces podemos preguntarnos ¿Esto siempre ocurre? La respuesta es afirmativa y se prueba en la Proposición 3.28 y, en Proposición 3.29 se presentan algunas propiedades de estos elementos como resultados de este trabajo.

Proposición 3.28. (Granados, Contreras) Sea $\mathcal{M}$ un $\mathcal{R}-$módulo libre de rango dos. Entonces,

1. $\boldsymbol{m}$ es complementable si y sólo si $\boldsymbol{m}$ es unimodular.

2. $\boldsymbol{m}$ es simplificable si y sólo si $\boldsymbol{m}$ es semimodular.

Demostración. 1. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base para $\mathcal{M}$ y $\boldsymbol{m} \in \mathcal{M}$, esto es, $\boldsymbol{m} = m_1\boldsymbol{v}_1 + m_2\boldsymbol{v}_2$ con $m_1, m_2 \in \mathcal{R}$. $\boldsymbol{m} \in \mathcal{M}$ es complementable, si y sólo si, existe $\boldsymbol{n} \in \mathcal{M}$ tal que $\{\boldsymbol{m}, \boldsymbol{n}\}$ es base de $\mathcal{M}$, lo mismo que,

$$\begin{vmatrix} m_1 & m_2 \\ n_1 & n_2 \end{vmatrix} = m_1n_2 - m_2n_1 \in \mathcal{R}^*.$$

Luego, $I(\boldsymbol{m}) = I((m_1, m_2)) = \mathcal{R}$, esto equivalente a que $\boldsymbol{m}$ es unimodular.

2. $\boldsymbol{m} \in \mathcal{M}$ es simplificable, si y sólo, si existe $\lambda \in \mathcal{R}$ no divisor de cero y $\boldsymbol{n} \in \mathcal{M}$ complementable tal que $\boldsymbol{m} = \lambda\boldsymbol{n}$. Como $\boldsymbol{n}$ es complementable si y sólo si $\boldsymbol{n}$ es unimodular si y sólo si $I(\boldsymbol{n}) = \mathcal{R}$, así $I(\boldsymbol{m}) = I(\lambda\boldsymbol{n}) = \lambda I(\boldsymbol{n}) = \lambda\mathcal{R}$ si y sólo si $\boldsymbol{m}$ es semimodular.

□

Proposición 3.29. (Granados, Contreras) Sean $\lambda \in \mathcal{R}$ y $\boldsymbol{m} \in \mathcal{M}$. Entonces,

1. Si $\lambda\boldsymbol{m} = \boldsymbol{0}$ entonces $\lambda I(\boldsymbol{m}) = 0$. La recíproca se tiene si $\boldsymbol{m} \in \mathcal{M}$ es complementable.

2. $\lambda\boldsymbol{m} = \boldsymbol{0}$ con λ no divisor de cero, se tiene que $\boldsymbol{m} = \boldsymbol{0}$.

3. Si $\boldsymbol{m}$ es semimodular y $\lambda\boldsymbol{m} = \boldsymbol{0}$, $\lambda = 0$.

4. $\lambda\boldsymbol{m} = \boldsymbol{0}$ con $\lambda \neq 0$, $\boldsymbol{m} \neq \boldsymbol{0}$, implica que λ es divisor de cero y $\boldsymbol{m}$ no es semimodular.

Demostración. 1. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$ y $\boldsymbol{m} \in \mathcal{M}$, $\boldsymbol{m} = x\boldsymbol{v}_1 + y\boldsymbol{v}_2$. Si $\lambda\boldsymbol{m} = \lambda x\boldsymbol{v}_1 + \lambda y\boldsymbol{v}_2 = 0$, se obtiene que $\lambda x = \lambda y = 0$. Ahora, $I(\boldsymbol{m}) = xn_2 - yn_1$ para algún $\boldsymbol{n} =$

$(n_1, n_2) \in \mathcal{M}$. Luego, $\lambda I(\boldsymbol{m}) = \lambda x n_2 - \lambda y n_1 = 0$.

Recíprocamente, como $\boldsymbol{m}$ es un complementable, entonces por el ítem 1 de la Proposición 3.28, $\boldsymbol{m}$ es unimodular, por lo tanto $I(\boldsymbol{m}) = \mathcal{R}$. Ahora, si $\lambda I(\boldsymbol{m}) = 0$ entonces $\lambda\mathcal{R} = 0$ por lo tanto $\lambda = 0$ y concluimos que $\lambda\boldsymbol{m} = \mathbf{0}$.

2. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$ y $\boldsymbol{m} \in \mathcal{M}$, $\boldsymbol{m} = x\boldsymbol{v}_1 + y\boldsymbol{v}_2$. Si $\lambda\boldsymbol{m} = \lambda x\boldsymbol{v}_1 + \lambda y\boldsymbol{v}_2 = \mathbf{0}$. Como λ es no divisor de cero $x = y = 0$. así $\boldsymbol{m} = \mathbf{0}$.

3. Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$ y $\boldsymbol{m} \in \mathcal{M}$, $\boldsymbol{m} = x\boldsymbol{v}_1 + y\boldsymbol{v}_2$. Si $\lambda\boldsymbol{m} = \lambda x\boldsymbol{v}_1 + \lambda y\boldsymbol{v}_2 = \mathbf{0}$, $\lambda x = \lambda y = 0$. Como $\boldsymbol{m}$ es semimodular, $I(\boldsymbol{m}) = \mu\mathcal{R}$, donde $\mu \in \mathcal{R}$ es no divisor de cero. Ahora, por el item 1, $\lambda I(\boldsymbol{m}) = \lambda(\mu x' + \mu y') = 0$ donde $x', y' \in \mathcal{R}$. Así, $\mu(\lambda x') = \mu(\lambda y') = 0$, como μ es no divisor de cero, se concluye que $\lambda = 0$.

4. Si $\lambda\boldsymbol{m} = \mathbf{0}$, por el item 1, $\lambda I(\boldsymbol{m}) = 0$. Como $\lambda \neq 0$, entonces λ es divisor de cero y $\boldsymbol{m}$ no es semimodular, pues si lo fuera, $I(\boldsymbol{m}) = \mu\mathcal{R}$ con μ un no divisor de cero, por lo tanto $\lambda I(\boldsymbol{m}) = \lambda\mu\mathcal{R} \neq 0$ lo cual es una contradicción.

□

Proposición 3.30. (Granados, Contreras) Sea $\mathcal{M}$ un $\mathcal{R}-$módulo libre de rango dos. Sean $\boldsymbol{m} \in \mathcal{M}$ complementable y $\lambda \in \mathcal{R}$. Dado $\boldsymbol{n} = \lambda\boldsymbol{m}$, λ es invertible si y sólo si $I(\boldsymbol{m}) = I(\boldsymbol{n})$.

Demostración. Si λ es invertible entonces existe $\lambda^{-1} \in \mathcal{R}$ tal que $\lambda\lambda^{-1} = 1$. Como $\boldsymbol{n} = \lambda\boldsymbol{m}$ entonces $\lambda^{-1}\boldsymbol{n} = \lambda^{-1}\lambda\boldsymbol{m} = \boldsymbol{m}$. Luego, $I(\boldsymbol{m}) = I(\boldsymbol{n})$. Recíprocamente, sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ base de $\mathcal{M}$ y $\boldsymbol{m}, \boldsymbol{n} \in \mathcal{M}$ no nulos, entonces $\boldsymbol{m} = x\boldsymbol{v}_1 + y\boldsymbol{v}_2$ y $\boldsymbol{n} = x'\boldsymbol{v}_1 + y'\boldsymbol{v}_2$. Si $I(\boldsymbol{m}) = I(\boldsymbol{n})$, existe $\lambda \in \mathcal{R}$ tal

que $\boldsymbol{m} = \lambda \boldsymbol{n}$ es decir, $(x, y) = \lambda(x', y')$, como $\boldsymbol{m}$ es complementable por la Proposición 3.28 $\boldsymbol{m}$ es unimodular, entonces existen $a, b \in \mathcal{R}$ tales que $1 = xa + yb$, así $1 = \lambda x'a + \lambda y'b = \lambda(x'a + y'b)$, luego λ es invertible. □

Proposición 3.31. (Franco, Proposición 5.0.6) Sean $\mathcal{R}$ un anillo y $\mathcal{M}$ un $\mathcal{R}-$módulo libre de rango dos. Son equivalentes:

1. $\boldsymbol{m} = (x, y)$ es complementable,

2. Si existe $\lambda \in \mathcal{R}$ tal que $\lambda x = \lambda y = 0$, entonces, $\lambda = 0$.

Demostración. $1 \Rightarrow 2$ Sean $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{M}$ y $\boldsymbol{m} = x\boldsymbol{v}_1 + y\boldsymbol{v}_2$, como $\boldsymbol{m}$ es complementable, por la Proposición 3.28, se obtiene que $\boldsymbol{m}$ es unimodular, es decir, existen $\alpha, \beta \in \mathcal{R}$ tales que $x\alpha + y\beta = 1$. Así, $\lambda x\alpha + \lambda y\beta = \lambda$ y como $\lambda x = \lambda y = 0$, entonces $\lambda = 0$.

$2 \Rightarrow 1$ Suponga $\lambda \neq 0$ tal que $\lambda x = \lambda y = 0$, entonces $\boldsymbol{m} = x\boldsymbol{v}_1 + y\boldsymbol{v}_2$ no es complementable, pues dada cualquier $\boldsymbol{n} = x'\boldsymbol{v}_1 + y'\boldsymbol{v}_2 \in \mathcal{M}$ se tiene que $\begin{vmatrix} x & y \\ x' & y' \end{vmatrix} = xy' - yx'$ es divisor de cero ya que $\lambda(xy' - yx') = \lambda xy' - \lambda x'y = 0$. □

3.3. Recta proyectiva sobre un anillo

Considerando $\mathbb{K}$ un cuerpo, se introducen los espacios proyectivos asociados a un $\mathbb{K}$-espacio vectorial E de dimensión finita por ejemplo en (Doneddu, 1980) y (Aroca and Fernández, 2009) se define la siguiente relación de equivalencia en $E - \{0\}$

$$u \sim v \text{ si y sólo si existe } \lambda \in \mathbb{K}^* \text{ tal que } u = \lambda v$$

y con esto, se define el espacio proyectivo asociado al $\mathbb{K}$-espacio vectorial E como se presenta a continuación:

Definición 3.32. El espacio proyectivo asociado a E esta dado por $\frac{E-\{0\}}{\sim}$.

Se denota por $\mathbb{P}(E)$ y su dimensión está dada por

$$dim\mathbb{P}(E) = dim_{\mathbb{K}}(E) - 1.$$

Si $\mathbb{E}$ es un plano, es decir, $dim_{\mathbb{K}}(E) = 2$, el espacio $\mathbb{P}(\mathbb{E})$ es una recta y se conoce como la *recta proyectiva.*

En el Ejemplo 1.3 vimos que si $\mathbb{K}$ es un cuerpo, un $\mathbb{K}$-espacio vectorial tiene estructura de $\mathbb{K}$-módulo, entonces en lugar de considerar un cuerpo $\mathbb{K}$ puedo tomar $\mathcal{R}$ un anillo y definir los espacios proyectivos asociados a $\mathcal{R}$.

Dado que nuestro interés consiste en definir la recta proyectiva sobre un anillo $\mathcal{R}$, se considerará $\mathcal{M}$ un $\mathcal{R}$-módulo libre de rango dos. Para definir la recta proyectiva sobre un anillo $\mathcal{R}$, es

necesario definir una relación de equivalencia sobre los elementos complementables de $\mathcal{M}$. Sea

$$\mathcal{R}_0^2 = \{\boldsymbol{m} \in \mathcal{M} \mid \boldsymbol{m} \text{ es no complementable}\}.$$

Ejemplo 3.33. Considere $\mathcal{R} = \frac{\mathbb{Z}}{\langle 4\rangle}$. Note que los elementos no complementables de $\frac{\mathbb{Z}}{\langle 4\rangle}$ son

$$\mathcal{R}_0^2 = \{(\overline{0},\overline{0}),(\overline{0},\overline{2}),(\overline{2},\overline{0}),(\overline{2},\overline{2})\}.$$

Ahora se define la siguiente relación de equivalencia sobre $\mathcal{R}^2 - \mathcal{R}_0^2$

$$\boldsymbol{m} \sim \boldsymbol{n} \text{ si y sólo si existe } \lambda \in \mathcal{R}^* \text{ tal que } \boldsymbol{n} = \lambda \boldsymbol{m}.$$

Proposición 3.34. (Franco, Proposición 5.0.7) $\sim$ es una relación de equivalencia.

Demostración. Veamos ahora que $\sim$ define una relación de equivalencia

1. *Reflexiva.* Sea $\boldsymbol{m} \in \mathcal{M}$, $\boldsymbol{m} \sim \boldsymbol{m}$ existe $1 \in \mathcal{R}^*$ donde $\boldsymbol{m} = 1\boldsymbol{m}$.

2. *Simétrica.* $\boldsymbol{m} \sim \boldsymbol{n}$ existe $\lambda \in \mathcal{R}^*$ tal que $\boldsymbol{n} = \lambda \boldsymbol{m}$, entonces $\lambda^{-1}\boldsymbol{n} = \lambda^{-1}\lambda \boldsymbol{m}$, luego $\lambda^{-1}\boldsymbol{n} = \boldsymbol{m}$ y así $\boldsymbol{n} \sim \boldsymbol{m}$.

3. *Transitiva.* $\boldsymbol{m} \sim \boldsymbol{n}$ y $\boldsymbol{n} \sim \boldsymbol{x}$ existen $\lambda, \lambda' \in \mathcal{R}^*$ tales que $\boldsymbol{n} = \lambda \boldsymbol{m}$ y $\boldsymbol{x} = \lambda' \boldsymbol{n}$. Luego, $\boldsymbol{x} = \lambda' \boldsymbol{n} = \lambda'(\lambda \boldsymbol{m}) = (\lambda'\lambda)\boldsymbol{m}$ donde $\lambda'\lambda \in \mathcal{R}^*$ y se concluye que $\boldsymbol{m} \sim \boldsymbol{x}$.

□

Definición 3.35. Se llama la recta proyectiva asociada al anillo $\mathcal{R}$, al conjunto,

$$\mathbb{P}^1_{\mathcal{R}} = \frac{\mathcal{R}^2 - \mathcal{R}_0^2}{\sim}.$$

La Definición 3.35 de recta proyectiva está dada para cualquier anillo $\mathcal{R}$. Los elementos en $\mathbb{P}^1_{\mathcal{R}}$ son clases de equivalencia, que notaremos por $[a_0, a_1]$.

El siguiente ejemplo muestra cómo calcular la recta proyectiva de $\mathcal{R} = \frac{\mathbb{Z}}{\langle 4\rangle}$ a partir de la Definición 3.35.

Ejemplo 3.36. Considere $\mathcal{R} = \frac{\mathbb{Z}}{\langle 4\rangle} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Por el Ejemplo 3.33 se tiene que los elementos no complementables son,

$$\mathcal{R}_0^2 = \{(\overline{0},\overline{0}), (\overline{0},\overline{2}), (\overline{2},\overline{0}), (\overline{2},\overline{2})\}.$$

Luego,

$$\begin{aligned}\mathcal{R}^2 - \mathcal{R}_0^2 = \{&(\overline{0},\overline{1}), (\overline{0},\overline{3}), (\overline{1},\overline{0}), (\overline{1},\overline{1}), (\overline{1},\overline{2}), (\overline{1},\overline{3}),\\ &(\overline{2},\overline{1}), (\overline{2},\overline{3}), (\overline{3},\overline{0}), (\overline{3},\overline{1}), (\overline{3},\overline{2}), (\overline{3},\overline{3})\}\end{aligned}$$

Como los elementos $\{\overline{1}, \overline{3}\}$ son invertibles en $\frac{\mathbb{Z}}{\langle 4\rangle}$, entonces $(x, y) \sim (x', y')$, si y sólo si, existe $\lambda \in \{\overline{1}, \overline{3}\}$ tal que $(x, y) = \lambda(x', y')$. En particular, $(\overline{2}, \overline{3}) \sim (\overline{2}, \overline{1})$ pues, $\overline{3}(\overline{2}, \overline{1}) = (\overline{2}, \overline{3})$ y así

con cada $(x, y) \in \frac{\mathbb{Z}}{\langle 4\rangle}$. Por lo tanto se obtiene,

$$(\overline{0},\overline{1}) \sim (\overline{0},\overline{3});\ \ (\overline{2},\overline{1}) \sim (\overline{2},\overline{3});\ \ (\overline{1},\overline{0}) \sim (\overline{3},\overline{0});\ \ (\overline{1},\overline{2}) \sim (\overline{3},\overline{2});\ \ (\overline{1},\overline{1}) \sim (\overline{3},\overline{3});$$

y $(\overline{1},\overline{3}) \sim (\overline{3},\overline{1})$.

Así,

$$\mathbb{P}^1_{\frac{\mathbb{Z}}{\langle 4\rangle}} = \{[\overline{0},\overline{1}],[\overline{1},\overline{0}],[\overline{1},\overline{1}],[\overline{1},\overline{3}],[\overline{1},\overline{2}],[\overline{2},\overline{1}]\}.$$

3.4. Puntos fuertemente independientes

En esta sección se presentan definiciones y resultados referentes a las rectas proyectivas sobre anillos conmutativos con uno, en particular las rectas proyectivas sobre anillos totales de fracciones. Decimos que un anillo $\mathcal{R}$ es un anillo total de fracciones si sus elementos son invertibles o divisores de cero, para estudiar propiedades generales de los anillos totales de fracciones se recomienda ver (Granados Pinzón and Olaya León, 2020). A partir de este momento consideramos ahora al anillo $\mathcal{R}$ como un anillo total de fracciones.

Definición 3.37. Sean $A = [a_0, a_1], B = [b_0, b_1] \in \mathbb{P}^1_{\mathcal{R}}$, diremos que un par de puntos son fuertemente independientes, si

$$\begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix} \in \mathcal{R}^*.$$

Observación 3.38. La definición anterior es independiente del representante elegido. En efecto,

dados dos representantes distintos de A, $[a_0, a_1]$ y $[a'_0, a'_1]$, se tiene que $[a_0, a_1] = [a'_0, a'_1]$ ya que existe $\lambda \in \mathcal{R}^*$ tal que $(a_0, a_1) = \lambda(a'_0, a'_1)$. De forma análoga dados dos representantes distintos de B, $[b_0, b_1]$ y $[b'_0, b'_1]$, se tiene que $[b_0, b_1] = [b'_0, b'_1]$ ya que existe $\gamma \in \mathcal{R}^*$, $(b_0, b_1) = \gamma(b_0, b'_1)$. Luego,

$$\begin{vmatrix} a'_0 & a'_1 \\ b'_0 & b'_1 \end{vmatrix} = \begin{vmatrix} \lambda a_0 & \lambda a_1 \\ \gamma b_0 & \gamma b_1 \end{vmatrix} = \lambda\gamma a_0 b_1 - \lambda\gamma a_1 b_1 = \lambda\gamma(a_0 b_1 - a_1 b_1)$$

es invertible, ya que $(a_0 b_1 - a_1 b_1) \in \mathcal{R}^*$ y $\lambda\gamma \in \mathcal{R}^*$.

Proposición 3.39. (Franco, Proposición 5.1.2) Sean A y B fuertemente independientes entonces para todo $C \in \mathbb{P}^1_{\mathcal{R}}$ existen $\gamma_1, \gamma_2 \in \mathcal{R}$ tales que si $A = [a_0, a_1]$, $B = [b_0, b_1]$, $C = [c_0, c_1]$,

$$[c_0, c_1] = [\gamma_1 a_0 + \gamma_2 b_0, \gamma_1 a_1 + \gamma_2 b_1].$$

El par (γ_1, γ_2) es único salvo producto por unidades.

Demostración. Se prueba inicialmente existencia. Sean $A, B \in \mathbb{P}^1_{\mathcal{R}}$ fuertemente independientes entonces, por definición,

$$\begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix} \in \mathcal{R}^*.$$

Es decir, A y B generan a $\mathcal{R}^2$, por lo tanto existen $\lambda_1, \lambda_2 \in \mathcal{R}$ tales que,

$$(c_0, c_1) = \lambda_1(a_0, a_1) + \lambda_2(b_0, b_1)$$

$$(c_0, c_1) = (\lambda_1 a_0 + \lambda_2 b_0, \lambda_1 a_1 + \lambda_2 b_1).$$

Ahora, se prueba la unicidad de (λ_1, λ_2) salvo producto por unidades. Sean (λ_1, λ_2) y $(\gamma_1, \gamma_2) \in \mathbb{P}^1_{\mathcal{R}}$ tales que

$$[c_0, c_1] = [\lambda_1 a_0 + \lambda_2 b_0, \lambda_1 a_1 + \lambda_2 b_1] = [\gamma_1 a_0 + \gamma_2 b_0, \gamma_1 a_1 + \gamma_2 b_1].$$

Por tanto, existe $\alpha \in \mathcal{R}^*$ tal que $\lambda_1 a_0 + \lambda_2 b_0 = (\gamma_1 a_0 + \gamma_2 b_0)\alpha$ y $\lambda_1 a_1 + \lambda_2 b_1 = (\gamma_1 a_1 + \gamma_2 b_1)\alpha$, es decir,

$$a_0(\alpha\gamma_1 - \lambda_1) + b_0(\alpha\gamma_2 - \lambda_2) = 0,$$

$$a_1(\alpha\gamma_1 - \lambda_1) + b_1(\alpha\gamma_2 - \lambda_2) = 0.$$

Este sistema de ecuaciones tiene solución trivial cero, puesto que A y B son fuertemente independientes, entonces A y B son linealmente independientes, es decir,

$$(\alpha\gamma_1 - \lambda_1) = 0 \text{ y } (\alpha\gamma_2 - \lambda_2) = 0.$$

entonces, $\lambda_1 = \alpha\gamma_1$ y $\lambda_2 = \alpha\gamma_2$, luego $(\lambda_1, \lambda_2) = \alpha(\gamma_1, \gamma_2)$. □

Definición 3.40. Diremos que $A = [a_0, a_1]$, $B = [b_0, b_1]$, $C = [c_0, c_1] \in \mathbb{P}^1_{\mathcal{R}}$, forman una referencia proyectiva si A y B son fuertemente independientes y existen representantes de los tres puntos, (a_0, a_1) representante de A, (b_0, b_1) representante de B y (c_0, c_1) representante de C tales que,

$$(c_0, c_1) = (a_0, a_1) + (b_0, b_1).$$

Proposición 3.41. (Franco, Proposición 5.1.3) Sea $\mathcal{R}$ un anillo. Son equivalentes:

1. $\{A, B, C\}$ es una referencia proyectiva.

2. A y B son fuertemente independientes y existen γ_1, γ_2 invertibles tales que

$$(c_0, c_1) = \gamma_1(a_0, a_1) + \gamma_2(b_0, b_1).$$

3. $\{A, B\}$, $\{A, C\}$ Y $\{B, C\}$ son fuertemente independientes.

Demostración. $1 \Rightarrow 2$ Sea $\{A, B, C\}$ una referencia proyectiva, por definición,

$$(c_0, c_1) = (a_0, a_1) + (b_0, b_1)$$

donde claramente $\gamma_1 = \gamma_2 = 1$.

$2 \Rightarrow 1$ Sean A y B fuertemente independientes, por la Proposición 3.39 existen γ_1 y γ_2 invertibles

tales que

$$(c_0, c_1) = \gamma_1(a_0, a_1) + \gamma_2(b_0, b_1) = (\gamma_1 a_0, \gamma_1 a_1) + (\gamma_2 b_0, \gamma_2 b_1). \tag{3.4.1}$$

Así, existen representantes de los puntos A y B tales que se cumple la ecuación (3.4.1).

$2 \Rightarrow 3$ Por hipótesis, $\{A, B\}$ son fuertemente independientes, y existen γ_1, γ_2 invertibles tales que $(c_0, c_1) = \gamma_1(a_0, a_1) + \gamma_2(b_0, b_1)$, donde $A = [a_0, a_1]$, $B = [b_0, b_1]$ y $[c_0, c_1]$ veamos que A y C son fuertemente independientes.

$$\begin{vmatrix} a_0 & a_1 \\ c_0 & c_1 \end{vmatrix} = \begin{vmatrix} a_0 & a_1 \\ \gamma_1 a_0 + \gamma_2 b_0 & \gamma_1 a_1 + \gamma_2 b_1 \end{vmatrix} = \gamma_1 \begin{vmatrix} a_0 & a_1 \\ a_0 & a_1 \end{vmatrix} + \gamma_2 \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}$$

$$= a_0(\gamma_1 a_1 + \gamma_2 b_1) - a_1(\gamma_1 a_0 + \gamma_2 b_0)$$

$$= \gamma_1 a_0 a_1 + \gamma_2 a_0 b_1 - \gamma_1 a_0 a_1 - \gamma_2 a_1 b_0$$

$$= \gamma_2 a_0 b_1 - \gamma_2 a_1 b_0$$

$$= \gamma_2(a_0 b_1 - a_1 b_0) \in \mathcal{R}^*,$$

ya que γ_2 y $(a_0 b_1 - a_1 b_0)$ pertenecen a $\mathcal{R}^*$, por lo tanto A y C son fuertemente independientes. De manera análoga se prueba que B y C son fuertemente independientes. $3 \Rightarrow 2$ Sean A y B fuertemente independientes, entonces generan a $\mathcal{R}^2$, por lo tanto existen $\gamma_1, \gamma_2 \in \mathcal{R}$ tales que

$$(c_0, c_1) = \gamma_1(a_0, a_1) + \gamma_2(b_0, b_1). \tag{3.4.2}$$

Supongamos que γ_1 no es invertible, entonces γ_1 es divisor de cero, luego existe $\gamma' \neq 0$ tal que $\gamma_1\gamma' = 0$, así multiplicando la ecuación (3.4.2) por γ', se obtiene

$$\gamma'(c_0, c_1) = \gamma'\gamma_1(a_0, a_1) + \gamma'\gamma_2(b_0, b_1)] = \gamma'\gamma_2(b_0, b_1),$$

es decir, B esta en la clase de C, y esto contradice la hipótesis de que $\{B, C\}$ son fuertemente independientes. □

3.5. Proyectividades en $\mathbb{P}^1_{\mathcal{R}}$

Definición 3.42. Sea $M \in M_{2\times 2}(\mathcal{R})$, se define la correspondencia

$$\psi_M : \mathbb{P}^1_{\mathcal{R}} \longrightarrow \mathbb{P}^1_{\mathcal{R}}$$

$$[x_0, x_1] \longmapsto [y_0, y_1]$$

donde

$$\begin{pmatrix} y_0 \\ \\ y_1 \end{pmatrix} = M \begin{pmatrix} x_0 \\ \\ x_1 \end{pmatrix}.$$

Observación 3.43. Dos matrices inducen la misma correspondencia si y sólo si $M = \rho N$ con $\rho \in \mathcal{R}^*$.

Proposición 3.44. (Franco, Proposición 5.1.4) Sea $\mathcal{R}$ un anillo. Si $detM \in \mathcal{R}^*$ entonces la corres-

pondencia ψ_M es una aplicación bien definida.

Demostración. Sea $(x_0, x_1) \in \mathcal{R}^2 - \mathcal{R}_0^2$, si

$$\begin{pmatrix} y_0 \\ \\ y_1 \end{pmatrix} = M \begin{pmatrix} x_0 \\ \\ x_1 \end{pmatrix} \in \mathcal{R}_0^2$$

como $detM \in \mathcal{R}^*$, entonces existe $M^{-1} = \begin{pmatrix} a & b \\ \\ c & d \end{pmatrix}$ tal que

$$M^{-1} \begin{pmatrix} y_0 \\ \\ y_1 \end{pmatrix} = \begin{pmatrix} a & b \\ \\ c & d \end{pmatrix} \begin{pmatrix} y_0 \\ \\ y_1 \end{pmatrix} = \begin{pmatrix} ay_0 + by_1 \\ \\ cy_0 + dy_1 \end{pmatrix} = \begin{pmatrix} x_0 \\ \\ x_1 \end{pmatrix}.$$

Puesto que $(x_0, x_1) \in \mathcal{R}^2 - \mathcal{R}_0^2$, existen $\mu_0, \mu_1 \in \mathcal{R}$ tales que $\mu_0 x_0 + \mu_1 x_1 = 1$ y por lo tanto, reemplazamos a x_0 y x_1 obteniendo que

$$\mu_0(ay_0 + by_1) + \mu_1(cy_0 + dy_1) = 1,$$

$$y_0(a\mu_0 + c\mu_1) + y_1(b\mu_0 + d\mu_1) = 1,$$

entonces $(y_0, y_1) \in \mathcal{R}^2 - \mathcal{R}_0^2$.

Veamos ahora que la aplicación ψ_M no depende de la elección del representante. En efecto,

dados dos representantes distintos de $[x_0, x_1]$ y $[x'_0, x'_1]$, se tiene que $[x_0, x_1] = [x'_0, x'_1]$ si que existe $\lambda \in \mathcal{R}^*$ tal que $(x_0, x_1) = \lambda(x'_0, x'_1)$.

$$\begin{pmatrix} y_0 \\ \\ y_1 \end{pmatrix} = M \begin{pmatrix} x_0 \\ \\ x_1 \end{pmatrix} = M \begin{pmatrix} \lambda x'_0 \\ \\ \lambda x'_1 \end{pmatrix} = \lambda M \begin{pmatrix} x'_0 \\ \\ x'_1 \end{pmatrix} = N \begin{pmatrix} x'_0 \\ \\ x'_1 \end{pmatrix}$$

donde $\lambda M = N$ y $\lambda \in \mathcal{R}^*$, por lo tanto inducen la misma correspondencia. □

Proposición 3.45. (Franco, Proposición 5.1.2) Sea $\mathcal{R}$ un anillo. La aplicación ψ_M dada por una matriz M envía pares de puntos fuertemente independientes en pares fuertemente independientes si y sólo si $detM \in \mathcal{R}^*$.

Demostración. Sean $A = [a_0, a_1]$, $B = [b_0, b_1]$ puntos fuertemente independientes y $M = \begin{pmatrix} \alpha & \beta \\ \\ \gamma & \delta \end{pmatrix}$, donde $\psi_M(A)$ y $\psi_M(B)$ están dados por

$$\psi_M(A) = MA = \begin{pmatrix} \alpha & \beta \\ \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a_0 \\ \\ a_1 \end{pmatrix} = \begin{pmatrix} \alpha a_0 + \beta a_1 \\ \\ \gamma a_0 + \delta a_1 \end{pmatrix},$$

$$\psi_M(B) = MB = \begin{pmatrix} \alpha & \beta \\ \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} b_0 \\ \\ b_1 \end{pmatrix} = \begin{pmatrix} \alpha b_0 + \beta b_1 \\ \\ \gamma b_0 + \delta b_1 \end{pmatrix}.$$

$\psi_M(A)$ y $\psi_M(B)$ son fuertemente independientes si y sólo si

$$\psi_M(A)\wedge\psi_M(B)=\begin{vmatrix}\alpha a_0+\beta a_1 & \alpha b_0+\beta b_1\\ \gamma a_0+\delta a_1 & \gamma b_0+\delta b_1\end{vmatrix}=\begin{vmatrix}\alpha & \beta\\ \gamma & \delta\end{vmatrix}\begin{vmatrix}a_0 & b_0\\ a_1 & b_1\end{vmatrix}=detM\begin{vmatrix}a_0 & b_0\\ a_1 & b_1\end{vmatrix}\in\mathcal{R}^*.$$

Es decir, $\psi_M(A)\wedge\psi_M(B)\in\mathcal{R}^*$ si y sólo si $detM\in\mathcal{R}^*$, ya que $\begin{vmatrix}a_0 & b_0\\ a_1 & b_1\end{vmatrix}\in\mathcal{R}^*$. □

Proposición 3.46. (Franco, Proposición 5.1.6.) Sean $\mathcal{R}$ un anillo y $\{A,B,C\}$ una referencia proyectiva, entonces para todo $X\in\mathbb{P}^1_{\mathcal{R}}$ existen (α,β) únicos salvo producto por unidades tales que

$$(c_0,c_1)=(a_0,a_1)+(b_0,b_1),$$

$$(x_0,x_1)=\alpha(a_0,a_1)+\beta(b_0,b_1).$$

Demostración. La primera igualdad se da por definición de referencia proyectiva. En la segunda igualdad hacemos uso de la Proposición 3.41, es decir existen $\gamma_1,\gamma_2\in\mathcal{R}$ únicos, salvo producto por unidades, tales que

$$[x_0,x_1]=[\alpha a_0+\beta b_0,\alpha a_1+\beta b_1].$$

Luego, existe $\lambda \in \mathcal{R}^*$ tal que

$$(x_0, x_1) = \lambda(\gamma_1 a_0 + \gamma_2 b_0, \gamma_1 a_1 + \gamma_2 b_1),$$

$$(x_0, x_1) = \alpha(a_0, a_1) + \beta(b_0, b_1),$$

donde $\alpha = \lambda\gamma_1$ y $\beta = \lambda\gamma_2$. □

Definición 3.47. Si $\{A, B, C\}$ forman una referencia proyectiva, se define la razón doble de cuatro puntos $A, B, C, X \in \mathbb{P}^1_{\mathcal{R}}$ como

$$[A, B, C, X] = \frac{\beta}{\alpha}$$

siempre que α y β sean invertibles, donde $X = [\alpha, \beta]$ en la referencia proyectiva $\{A, B, C\}$.

Observación 3.48.

1. La razón doble está definida siempre que A, B, C, D sean fuertemente independientes dos a dos.

2. Sean $A, B, C, D \in \mathbb{P}^1_{\mathcal{R}}$, $A = [a_0, a_1]$, $B = [b_0, b_1]$, $C = [c_0, c_1]$ y $D = [d_0, d_1]$ las coordenadas de los puntos en alguna referencia de $\mathbb{P}^1_{\mathcal{R}}$. La razón doble de A, B, C y D es

$$[A, B, C, D] = \frac{\begin{vmatrix} a_0 & d_0 \\ a_1 & d_1 \end{vmatrix} \begin{vmatrix} b_0 & c_0 \\ b_1 & c_1 \end{vmatrix}}{\begin{vmatrix} a_0 & c_0 \\ a_1 & c_1 \end{vmatrix} \begin{vmatrix} b_0 & d_0 \\ b_1 & d_1 \end{vmatrix}}.$$

Proposición 3.49. (Franco, Proposición 10) Sean $\{A, B, C\}$ y $\{D, E, F\}$ dos referencias proyectivas, entonces existe una única proyectividad algebraica lineal (Id-semilineal) que transforma una referencia en la otra.

Demostración. Se prueba la existencia, sean $\{A, B, C\}$ y $\{D, E, F\}$ dos referencias proyectivas, donde $A = [a_0, a_1], B = [b_0, b_1], C = [c_0, c_1]$, $D = [d_0, d_1], E = [e_0, e_1]$ y $F = [f_0, f_1]$, tales que

$$(c_0, c_1) = (a_0, a_1) + (b_0, b_1),$$

$$(f_0, f_1) = (d_0, d_1) + (e_0, e_1).$$

Sean $M = \begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}$ y $N = \begin{pmatrix} d_0 & e_0 \\ d_1 & e_1 \end{pmatrix}$. Como A y B son fuertemente independientes, al igual que D y E, se tiene que $\begin{vmatrix} a_0 & b_0 \\ a_1 & b_1 \end{vmatrix} \in \mathcal{R}^*$ y $\begin{vmatrix} d_0 & e_0 \\ d_1 & e_1 \end{vmatrix} \in \mathcal{R}^*$.
Note que $det(NM^{-1}) \in \mathcal{R}^*$, luego por la Proposición 3.44, la aplicación $\psi_{NM^{-1}}$ está bien definida y además, envía una referencia en otra.

En efecto, se verifica que envía el punto A en el punto D,

$$\begin{aligned}\psi_{NM^{-1}}([a_0,a_1]) &= \frac{1}{a_0b_1-a_1b_0}\begin{pmatrix} d_0 & e_0 \\ d_1 & e_1\end{pmatrix}\begin{pmatrix} b_1 & -b_0 \\ -a_1 & a_0\end{pmatrix}\begin{pmatrix} a_0 \\ a_1\end{pmatrix} \\ &= \frac{1}{a_0b_1-a_1b_0}\begin{pmatrix} d_0 & e_0 \\ d_1 & e_1\end{pmatrix}\begin{pmatrix} b_1a_0 & -b_0a_1 \\ -a_1a_0 & a_0a_1\end{pmatrix} \\ &= \begin{pmatrix} d_0 & e_0 \\ d_1 & e_1\end{pmatrix}\begin{pmatrix} 1 \\ 0\end{pmatrix} = \begin{pmatrix} d_0 \\ d_1\end{pmatrix}.\end{aligned}$$

De manera análoga se prueba que a B lo envía a E y a C lo envía a F. Ahora, para probar la unicidad, sean ψ_{M_1} y ψ_{M_2} tales que envían referencias en referencias, entonces $M_1M_2^{-1}$ deja invariante los puntos de la referencia, luego se identifica con la identidad, salvo un invertible en $\mathcal{R}$, entonces $M_1 = M_2$. □

Definición 3.50. Sea Φ una correspondencia $\Phi : \mathbb{P}^1_{\mathcal{R}} \longrightarrow \mathbb{P}^1_{\mathcal{R}}$, decimos que Φ es una proyectividad algebraica τ-semilineal de $\mathbb{P}^1_{\mathcal{R}}$ si existen $M \in M_{2\times 2}(\mathcal{R})$ con $detM \in \mathcal{R}^*$ y un automorfismo de $\mathcal{R}$ llamado τ, tal que

$$\Phi([x,y]) = \psi_M([\tau(x),\tau(y)]).$$

Proposición 3.51. Sea $\Phi : \mathbb{P}^1_{\mathcal{R}} \longrightarrow \mathbb{P}^1_{\mathcal{R}}$ una proyectividad algebraica τ-semilineal, se tiene que

$$[\Phi(A),\Phi(B),\Phi(C),\Phi(D)] = \tau([A,B,C,D])$$

para todos los $A, B, C, D \in \mathbb{P}^1_{\mathcal{R}}$ fuertemente independientes dos a dos.

Demostración. Considere $\{A, B, C\}$ como una referencia proyectiva de $\mathbb{P}^1_{\mathcal{R}}$, y sea $[A, B, C, D] = \lambda$ entonces D tiene coordenadas $[1, \lambda]$ en la referencia, luego $\Phi(D)$ tendrá coordenadas $[1, \tau(\lambda)]$ en la referencia $\{\Phi(A), \Phi(B), \Phi(C)\}$, y por tanto

$$[\Phi(A), \Phi(B), \Phi(C), \Phi(D)] = \tau(\lambda).$$

□

Definición 3.52. Se dice que cuatro puntos $A, B, C, D \in \mathbb{P}^1_{\mathcal{R}}$ forman una cuaterna armónica en $\mathbb{P}^1_{\mathcal{R}}$, si

$$[A, B, C, D] = -1.$$

Ejemplo 3.53. 1. Para todos $\alpha, \beta \in \mathcal{R}$ con $\{\alpha, \beta\} \cap \{0, 1\} = \emptyset$ y $\alpha \neq \pm\beta$ y $2 \in \mathcal{R}^*$ se tiene que

$$\left[[1, \alpha], [1, \beta], [1, 0], [1, \frac{(\alpha + \beta)}{2}]\right] = -1.$$

En efecto,

$$\frac{\begin{vmatrix} 1 & 0 \\ \alpha & 1 \end{vmatrix} \begin{vmatrix} 1 & 1 \\ \beta & \frac{\alpha+\beta}{2} \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ \alpha & \frac{\alpha+\beta}{2} \end{vmatrix} \begin{vmatrix} 1 & 0 \\ \beta & 1 \end{vmatrix}} = \frac{1\left(\frac{\alpha}{2}+\frac{\beta}{2}-\beta\right)}{\left(\frac{\alpha}{2}+\frac{\beta}{2}-\frac{\alpha}{1}\right)1} = \frac{\frac{\alpha-\beta}{2}}{\frac{\beta-\alpha}{2}} = -1.$$

2. Para todo $\alpha \in \mathcal{R} - \{0,1\}$ y $2 \in \mathcal{R}^*$ se tiene que

$$\left[[1,0],[1,\alpha],[0,1],[1,\frac{\alpha}{2}]\right] = -1.$$

En efecto,

$$\frac{\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 1 \\ \alpha & \frac{\alpha}{2} \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ 0 & \frac{\alpha}{2} \end{vmatrix} \begin{vmatrix} 1 & 0 \\ \alpha & 1 \end{vmatrix}} = \frac{1\left(\frac{\alpha}{2}-\alpha\right)}{\frac{\alpha}{2}-1} = \frac{\frac{-\alpha}{2}}{\frac{\alpha}{2}} = -1.$$

3. Para todo $\alpha, \beta \in \mathcal{R} - \{0,1\}$ con $\alpha \neq \pm\beta$ y $2 \in \mathcal{R}^*$ se tiene que

$$[[1,\alpha],[1,\beta],[1,0],[\alpha+\beta,2\alpha\beta]] = -1.$$

En efecto,

$$\frac{\begin{vmatrix} 1 & 1 \\ \alpha & 0 \end{vmatrix}\begin{vmatrix} 1 & \alpha+\beta \\ \beta & 2\alpha\beta \end{vmatrix}}{\begin{vmatrix} 1 & \alpha+\beta \\ \alpha & 2\alpha\beta \end{vmatrix}\begin{vmatrix} 1 & 1 \\ \beta & 0 \end{vmatrix}} = \frac{-\alpha(2\alpha\beta-\alpha\beta-\beta^2)}{(2\alpha\beta-\alpha^2-\alpha\beta)(-\beta)} = \frac{-\alpha\beta(2\alpha-\alpha-\beta)}{-\alpha\beta(2\beta-\alpha-\beta)} = \frac{\alpha-\beta}{\beta-\alpha} = -1.$$

Definición 3.54. Sea Φ una correspondencia $\Phi : \mathbb{P}^1_{\mathcal{R}} \longrightarrow \mathbb{P}^1_{\mathcal{R}}$, decimos que Φ es una proyectividad de Staudt si Φ es biyectiva, transforma pares fuertemente independientes en pares fuertemente independientes y conserva cuaternas armónicas.

Teorema 3.55. *(Franco, Teorema 5.1.1) Sea $\mathcal{R}$ un anillo y $2 \in \mathcal{R}^*$. Φ es una proyectividad de Staudt si y sólo si es una proyectividad algebraica.*

Demostración. $\Leftarrow$) Inmediato.

$\Rightarrow$) Sea Φ una proyectividad de Staudt, y considere $R = \{A, B, C\}$ una referencia proyectiva en $\mathbb{P}^1_{\mathcal{R}}$. Por la Proposición 3.41, tenemos que A, B y C son fuertemente independientes dos a dos, entonces $\Phi(A), \Phi(B)$ y $\Phi(C)$ son fuertemente independientes dos a dos, es decir $R' = \{\Phi(A), \Phi(B), \Phi(C)\}$ es una referencia proyectiva.

Ahora para cada $\lambda \in \mathcal{R} - \{0, 1\}$, definimos $X_\lambda = [x, y]$ al único punto tal que

$$(x, y) = (a_0, a_1) + \lambda(b_0, b_1)$$

y $A = [a_0, a_1]$, $B = [b_0, b_1]$ y $C = [c_0, c_1]$. Como R es una referencia proyectiva, se tiene que

$$(c_0, c_1) = (a_0, a_1) + (b_0, b_1).$$

Luego, $X_\lambda = [1, \lambda]$, equivale a

$$[A, B, C, X_\lambda] = \lambda,$$

entonces, se define $\tau : \mathcal{R} \longrightarrow \mathcal{R}$, tal que $\tau(0) = 0, \tau(1) = 1$ y para $\lambda \notin \{0, 1\}$, se tiene que $\tau(\lambda) = [\Phi(A), \Phi(B), \Phi(C), \Phi(X_\lambda)]$. Para probar que Φ es una proyectividad algebraica, debemos demostrar que τ está bien definida, es inyectiva, sobreyectiva y que es homomorfismo de anillo. Para esto, vamos a dividir la prueba en varios pasos.

1. Veamos que τ está bien definida, sean $[x', y'] = \Phi(X_\lambda), [a'_0, a'_1] = \Phi(A), [b'_0, b'_1] = \Phi(B)$ y $[c'_0, c'_1] = \Phi(C)$, con $(a'_0, a'_1) + (b'_0, b'_1) = (c'_0, c'_1)$ si $\alpha, \beta \in \mathcal{R}$ con

$$(x', y') = \alpha(a'_0, a'_1) + \beta(b'_0, b'_1).$$

   Observe que $\alpha \neq 0$ porqué $\Phi(X_\lambda)$ y $\Phi(B)$ son fuertemente independientes, ya que Φ es una proyectividad de Staudt, X_λ y B son fuertemente independientes. Si α no es invertible, entonces α es divisor de cero, luego, existe $\alpha' \neq 0$ tal que $\alpha\alpha' = 0$, así

$$\alpha'(x', y') = \alpha'\alpha(a'_0, a'_1) + \alpha'\beta(b'_0, b'_1),$$
$$\alpha'(x', y') = \alpha'\beta(b'_0, b'_1).$$

Considere,

$$\alpha'\beta\begin{vmatrix} x' & y' \\ b'_0 & b'_1 \end{vmatrix} = \alpha'\begin{vmatrix} x' & y' \\ \beta b'_0 & \beta b'_1 \end{vmatrix}$$

$$= \alpha'(x'\beta b'_1 - y'\beta b'_0)$$

$$= x'\alpha' y' - y'\alpha' x' = 0.$$

Lo cual es absurdo, ya que $\Phi(X_\lambda)$ y $\Phi(B)$ son fuertemente independientes y $\alpha'\beta \neq 0$, porque $\Phi(X_\lambda) \in \mathbb{P}^1_{\mathcal{R}}$, así que tenemos que la razón doble de

$$[\Phi(A), \Phi(B), \Phi(C), \Phi(X_\lambda)] = \frac{\beta}{\alpha}$$

está bien definida.

2. τ es inyectiva. En efecto, sea $\tau(\lambda) = \tau(\mu)$, $[1, \tau(\lambda)] = [1, \tau(\mu)]$, luego $\Phi([1, \tau(\lambda)]) = \Phi([1, \tau(\mu)])$ y como Φ es biyectiva, $\lambda = \mu$.

3. τ es sobreyectiva, ya qué Φ lo es, al igual que τ es automorfismo de anillos.

4. τ es un homomorfismo de anillos. En efecto,

   a) $\tau(\frac{\alpha}{2}) = \frac{\tau(\alpha)}{2}$. Por el ítem 2 del Ejemplo 3.53, para $\alpha \neq 0, 1$, en la referencia R se tiene que

$$\left[[1,0],[1,\alpha],[0,1],\left[1,\frac{\alpha}{2}\right]\right]=-1,$$

y como Φ es una proyectividad de Staudt, entonces

$$\left[\Phi([1,0]),\Phi([1,\alpha]),\Phi([0,1]),\Phi\left(\left[1,\frac{\alpha}{2}\right]\right)\right]=-1.$$

En la referencia R', queda

$$\left[[1,0],[1,\tau(\alpha)],[0,1],\left[1,\tau\left(\frac{\alpha}{2}\right)\right]\right]=-1.$$

Esto es,

$$\frac{\begin{vmatrix}1 & 1\\ 0 & \tau\left(\frac{\alpha}{2}\right)\end{vmatrix}\begin{vmatrix}1 & 0\\ \tau(\alpha) & 1\end{vmatrix}}{\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix}\begin{vmatrix}1 & 1\\ \tau(\alpha) & \tau\left(\frac{\alpha}{2}\right)\end{vmatrix}}=\frac{\tau\left(\frac{\alpha}{2}\right)\cdot 1}{1\cdot\left(\tau\left(\frac{\alpha}{2}\right)-\tau(\alpha)\right)}=-1.$$

Luego,

$$\tau\left(\frac{\alpha}{2}\right) = \frac{\tau(\alpha)}{2}.$$

b) $\tau(\alpha+\beta) = \tau(\alpha)+\tau(\beta)$. Si $\alpha = \beta$, se aplica el ítem anterior. Sea $\alpha \neq \beta$, por el ítem 1 del Ejemplo 3.53, en la referencia R se tiene que

$$\left[[1,\alpha],[1,\beta],[0,1],\left[1,\frac{\alpha+\beta}{2}\right]\right] = -1.$$

Como Φ es una proyectividad de Staudt,

$$\left[\Phi([1,\alpha]),\Phi([1,\beta]),\Phi([0,1]),\Phi\left(\left[1,\frac{\alpha+\beta}{2}\right]\right)\right] = -1.$$

y así en la referencia R',

$$\left[[1,\tau(\alpha)],[1,\tau(\beta)],[0,1],\left[1,\tau\left(\frac{\alpha+\beta}{2}\right)\right]\right] = -1.$$

Esto es,

$$\frac{\begin{vmatrix} 1 & 1 \\ \tau(\alpha) & \tau\left(\frac{\alpha+\beta}{2}\right) \end{vmatrix}\begin{vmatrix} 1 & 0 \\ \tau(\beta) & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 0 \\ \tau(\alpha) & 1 \end{vmatrix}\begin{vmatrix} 1 & 1 \\ \tau(\beta) & \tau\left(\frac{\alpha+\beta}{2}\right) \end{vmatrix}} = \frac{\tau\left(\frac{\alpha+\beta}{2}\right)-\tau(\alpha)}{\tau\left(\frac{\alpha+\beta}{2}\right)-\tau(\beta)} = -1.$$

Luego,

$$\begin{aligned} \tau\left(\frac{\alpha+\beta}{2}\right)-\tau(\alpha) &= -\tau\left(\frac{\alpha+\beta}{2}\right)+\tau(\beta) \\ 2\tau\left(\frac{\alpha+\beta}{2}\right) &= \tau(\alpha)+\tau(\beta) \\ \tau(\alpha+\beta) &= \tau(\alpha)+\tau(\beta). \end{aligned}$$

c) $\tau(\alpha)^2 = (\tau(\alpha))^2$. Para $\alpha, \beta \in \mathcal{R} - \{\, 0, 1 \,\}$ con $\alpha \neq \pm\beta$, entonces por ítem 3 del Ejemplo 3.53, se tiene que

$$[[1,\alpha],[1,\beta],[1,0],[\alpha+\beta,2\alpha\beta]] = -1.$$

Considere $\beta = 1-\alpha$ y $\alpha \neq \frac{1}{2}$

$$[[1,\alpha],[1,1-\alpha],[1,0],[1,2\alpha(1-\alpha)]] = -1.$$

Aplicando Φ,

$$[[1,\tau(\alpha)],[1,\tau(1-\alpha)],[1,0],[1,\tau(2\alpha(1-\alpha))]] = -1.$$

Como $\tau\left(\frac{1}{2}\right) = \frac{1}{2}$ y como τ es inyectiva entonces para $\alpha \neq \frac{1}{2}$, se tiene que $\tau(\alpha) \neq \frac{1}{2}$, y razonando como antes para $\tau(\alpha)$,

$$[[1,\tau(\alpha)],[1,1-\tau(\alpha)],[1,0],[1,\tau(2\alpha(1-\alpha))]] =$$

$$[[1,\tau(\alpha)],[1,\tau(1-\alpha)],[1,0],[1,2\tau(\alpha)(1-\alpha))]] = -1.$$

Por lo tanto

$$\tau(2\alpha(1-\alpha)) = 2\tau(\alpha)(1-\tau(\alpha))$$

entonces $\tau(\alpha)^2 = (\tau(\alpha))^2$, en particular, $\tau\left(\left(\frac{1}{2}\right)^2\right) = \left(\tau\left(\frac{1}{2}\right)\right)^2$.

d) $\tau(\alpha\beta) = \tau(\alpha)\tau(\beta)$. Considere

$$\tau((\alpha+\beta)^2) = \tau(\alpha^2+2\alpha\beta+\beta^2) = \tau(\alpha^2)+\tau(2\alpha\beta)+\tau(\beta^2)$$

$$= \tau(\alpha^2)+2\tau(\alpha\beta)+\tau(\beta^2)$$

y

$$(\tau(\alpha+\beta))^2 = (\tau(\alpha)+\tau(\beta))^2 = \tau(\alpha)^2 + 2\tau(\alpha)\tau(\beta) + \tau(\beta)^2$$
$$= \tau(\alpha^2) + 2\tau(\alpha)\tau(\beta) + \tau(\beta^2).$$

Por el ítem anterior, $(\tau(\alpha+\beta))^2 = \tau((\alpha+\beta)^2)$, entonces se obtiene que

$$2\tau(\alpha\beta) = 2\tau(\alpha)\tau(\beta),$$

luego

$$\tau(\alpha\beta) = \tau(\alpha)\tau(\beta).$$

De esta manera, Φ es una proyectividad algebraica τ-semilineal que transforma la referencia R en R'.

□

3.6. Recta proyectiva dual

En esta sección se denota a $\mathcal{A}$ como un anillo conmutativo que es un anillo total de fracciones y el producto $\mathcal{A}^2 = \mathcal{A} \times \mathcal{A}$ será un $\mathcal{A}$-módulo libre bidimensional o de rango 2.

Lema 3.56. (Franco, Lema 5.2.1) Sean $\alpha_0, \alpha_1 \in \mathcal{A}$ se tiene que el conjunto

$$\mathcal{N} = \{(x_0, x_1) \in \mathcal{A}^2 : \alpha_0 x_0 + \alpha_1 x_1 = 0\}$$

es un submódulo unidimensional y complementable si y sólo si (α_0, α_1) es complementable en $\mathcal{A}^2$.

Demostración. Para probar que si $\mathcal{N}$ es un submódulo unidimensional y complementable entonces (α_0, α_1) es complementable en $\mathcal{A}^2$ lo haremos por reducción al absurdo. Se tiene que existen $\boldsymbol{v}, \boldsymbol{v'} \in \mathcal{A}$ tales que $\mathcal{N} = \langle \boldsymbol{v} \rangle$ y $\langle \boldsymbol{v}, \boldsymbol{v'} \rangle = \mathcal{A}^2$. Sea $\boldsymbol{v'} = (v'_0, v'_1)$, si $\alpha_0 v'_0 + \alpha_1 v'_1$ no fuera invertible, existirían $\lambda' \in \mathcal{A}$ y $\lambda \in \mathcal{A}$ tal que $\lambda' \boldsymbol{v'} \in \mathcal{N}$ y $\lambda' \boldsymbol{v'} = \lambda \boldsymbol{v}$ y $\boldsymbol{v}$ y $\boldsymbol{v'}$ no serían independientes, lo cual es absurdo.

($\Leftarrow$) Como (α_0, α_1) es complementable, $(-\alpha_1, \alpha_0) \in \mathcal{A}^2$ también es complementable y por lo tanto existe $(\mu_0, \mu_1) \in \mathcal{A}^2$ tal que $\{(-\alpha_1, \alpha_0), (\mu_0, \mu_1)\}$ es una base de $\mathcal{A}^2$. Veamos que $\mathcal{N} = \langle (-\alpha_1, \alpha_0) \rangle$.

En efecto, sea $\boldsymbol{m} = \lambda_1(-\alpha_1, \alpha_0) + \lambda_2(\mu_0, \mu_1) \in \mathcal{N}$.

$$\boldsymbol{m} = (-\lambda_1 \alpha_1 + \lambda_2 \mu_0, \lambda_1 \alpha_0 + \lambda_2 \mu_1) \in \mathcal{N}$$

$$\begin{aligned}
&\Leftrightarrow \quad \alpha_0(-\lambda_1\alpha_1+\lambda_2\mu_0)+\alpha_1(\lambda_1\alpha_0+\lambda_2\mu_1)=0\\
&\Leftrightarrow \quad \alpha_0\lambda_2\mu_0+\alpha_1\lambda_2\mu_1=0\\
&\Leftrightarrow \quad \lambda_2(\alpha_0\mu_0+\alpha_1\mu_1)=0 \Leftrightarrow \lambda_2=0.
\end{aligned}$$

□

Ahora, se define el siguiente conjunto:

$$(\mathcal{A}^2)^* = \{\Phi : \mathcal{A}\times\mathcal{A} \longrightarrow \mathcal{A} \text{ lineal} \mid ker\Phi \text{ es unidimensional y complementable}\}.$$

Note que, por el Lema 3.56, se tiene que

$$(\mathcal{A}^2)^* = \{\Phi : \mathcal{A}\times\mathcal{A} \to \mathcal{A} \mid \Phi(x_0,x_1)=\alpha_0x_0+\alpha_1x_1, (\alpha_0,\alpha_1) \text{ complementable}\}.$$

Se denotará a $(\mathcal{A}^2)^*$ como el dual del $\mathcal{A}$-módulo $\mathcal{A}^2$ y se espera no exista confusión con el conjunto de los elementos invertibles de $\mathcal{A}$, que es denotado por $\mathcal{A}^*$.

Proposición 3.57. (Franco, Proposición 5.2.1) Sean $\Phi_1, \Phi_2 \in (\mathcal{A}^2)^*$, se tiene que $ker\Phi_1 = ker\Phi_2$ si y sólo si existe, $\lambda \in \mathcal{A}^*$ tal que $\Phi_1 = \lambda\Phi_2$. Además se tiene que esa condición define una relación de equivalencia en $(\mathcal{A}^2)^*$.

Demostración. $\Rightarrow$) Sea $\boldsymbol{m} \in \mathcal{A}\times\mathcal{A}$ tal que el $ker\Phi_1 = ker\Phi_2 = \langle \boldsymbol{m}\rangle$, como $\Phi_1, \Phi_2 \in (\mathcal{A}^*)$ existe

$\boldsymbol{n} \in \mathcal{A}^2$ tal que $\langle \boldsymbol{m}, \boldsymbol{n} \rangle = \mathcal{A}^2$, se tiene que $\Phi_1(\boldsymbol{n}), \Phi_2(\boldsymbol{n}) \in \mathcal{A}^*$, supongamos que no es así, es decir, $\Phi_1(\boldsymbol{n})$ y $\Phi_2(\boldsymbol{n}) \notin \mathcal{A}^*$. Como $\mathcal{A}$ es anillo total de fracciones, entonces $\Phi_1(\boldsymbol{n}), \Phi_2(\boldsymbol{n})$ son divisores de cero, entonces existe $z \in \mathcal{A}$, $z \neq 0$, de tal forma que $z\Phi_1(\boldsymbol{n}) = \Phi_1(z\boldsymbol{n}) = 0$, luego $z\boldsymbol{n} \in ker\Phi_1$ por lo tanto $\boldsymbol{n} \in \langle \boldsymbol{m} \rangle$ y esto es absurdo. Luego, $\Phi_1(\boldsymbol{n}) \in \mathcal{A}^*$. Análogamente se prueba que $\Phi_2(\boldsymbol{n}) \in \mathcal{A}^*$. Veamos ahora que $\Phi_1 = \frac{\Phi_1(\boldsymbol{n})}{\Phi_2(\boldsymbol{n})}\Phi_2$. En efecto, como $\langle \boldsymbol{m}, \boldsymbol{n} \rangle = \mathcal{A}^2$ para todo $\boldsymbol{x} \in \mathcal{A}^2$ existen $\alpha_1, \alpha_2 \in \mathcal{A}$ tales que $\boldsymbol{x} = \alpha_1\boldsymbol{m} + \alpha_2\boldsymbol{n}$. Así,

$$\Phi_1(\boldsymbol{x}) = \alpha_1\Phi_1(\boldsymbol{m}) + \alpha_2\Phi_1(\boldsymbol{n}),$$

$$\Phi_2(\boldsymbol{x}) = \alpha_1\Phi_2(\boldsymbol{m}) + \alpha_2\Phi_2(\boldsymbol{n}),$$

como $ker\Phi_1 = ker\Phi_2 = \langle \boldsymbol{m} \rangle$, $\Phi_1(\boldsymbol{x}) = \alpha_2\Phi_1(\boldsymbol{n})$ y $\Phi_2(\boldsymbol{x}) = \alpha_2\Phi_2(\boldsymbol{n})$. Luego, $\Phi_1(\boldsymbol{x}) = \frac{\Phi_1(\boldsymbol{n})}{\Phi_2(\boldsymbol{n})}\Phi_2(\boldsymbol{x})$ para todo $\boldsymbol{x} \in \mathcal{A}^2$.

$\Leftarrow$) Si $\Phi_1 = \lambda\Phi_2$, con $\lambda \in \mathcal{A}^*$, entonces $ker\Phi_1 = ker\lambda\Phi_2 = ker\Phi_2$.

Ahora, vamos a demostrar la segunda parte de la proposición. Veamos ahora que $\sim$ define una relación de equivalencia

1. *Reflexiva*. Sea $\Phi_1 \in (\mathcal{A})^*$, $ker\Phi_1 = ker\Phi_1$, entonces $\Phi_1 \sim \Phi_1$.

2. *Simétrica.* Sean $\Phi_1, \Phi_2 \in (\mathcal{A})^*$. Si $\Phi_1 \sim \Phi_2$ entonces $ker\Phi_1 = ker\Phi_2$, luego, $\Phi_2 \sim \Phi_1$

3. *Transitiva*. Sean $\Phi_1, \Phi_2, \Phi_3 \in (\mathcal{A})^*$. Si $\Phi_1 \sim \Phi_2$ y $\Phi_2 \sim \Phi_3$, veamos que $\Phi_1 \sim \Phi_3$, en efecto,

$ker\Phi_1 = ker\Phi_2$ y $ker\Phi_2 = ker\Phi_3$, luego $ker\Phi_1 = ker\Phi_3$ y así $\Phi_1 \sim \Phi_3$.

Luego, por $1, 2$ y 3, concluimos que $\sim$ es una relación de equivalencia. □

Definición 3.58. Llamaremos recta proyectiva dual del anillo $\mathcal{A}$ al cociente

$$\mathbb{P}((\mathcal{A}^2)^*) = \frac{(\mathcal{A}^2)^*}{\sim}$$

donde $\Phi_1 \sim \Phi_2 \Leftrightarrow ker\Phi_1 = ker\Phi_2$.

A continuación se determina la recta proyectiva dual del anillo $\frac{\mathbb{Z}}{\langle 2\rangle}$.

Ejemplo 3.59. Considere $\frac{\mathbb{Z}}{\langle 2\rangle} = \{\overline{0}, \overline{1}\}$. Luego, $\frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 2\rangle} = \{(\overline{0},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{0}), (\overline{1},\overline{1})\}$ y los elementos complementables en $\frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 2\rangle}$ son $\{(\overline{0},\overline{1}), (\overline{1},\overline{0}), (\overline{1},\overline{1})\}$.

Ahora, se define

$$\left(\frac{\mathbb{Z}}{\langle 2\rangle}^2\right)^* = \left\{\Phi_{(\alpha_0,\alpha_1)} : \frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 2\rangle} \longmapsto \frac{\mathbb{Z}}{\langle 2\rangle} \;\mid\; \Phi_{(\alpha_0,\alpha_1)}(x_0, y_0) = \alpha_0 x_0 + \alpha_1 y_0\right\}$$

donde (α_0, α_1) es complementable. Luego, se tiene que $\left(\frac{\mathbb{Z}}{\langle 2\rangle}^2\right)^* = \{\Phi_{(\overline{0},\overline{1})}, \Phi_{(\overline{1},\overline{1})}, \Phi_{(\overline{1},\overline{0})}\}$ y la recta proyectiva dual de $\frac{\mathbb{Z}}{\langle 2\rangle}^2$ está dada por

$$\mathbb{P}\left(\left(\frac{\mathbb{Z}}{\langle 2\rangle}^2\right)^*\right) = \frac{\left(\frac{\mathbb{Z}}{\langle 2\rangle}^2\right)^*}{\sim}$$

donde $\Phi_{(\alpha_0,\alpha_1)} \sim \Phi_{(\alpha_0',\alpha_1')} \Leftrightarrow ker\Phi_{(\alpha_0,\alpha_1)} = ker\Phi_{(\alpha_0',\alpha_1')}$. Encontremos cada $ker\Phi_{(\alpha_0,\alpha_1)}$.

1. Si $(\alpha_0, \alpha_1) = (\overline{0}, \overline{1})$,

$$\Phi_{(\overline{0},\overline{1})} : \frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 2\rangle} \longrightarrow \frac{\mathbb{Z}}{\langle 2\rangle}$$
$$(x_0, x_1) \longmapsto \overline{0}x_0 + \overline{1}x_1 = x_1.$$

Así, $\Phi_{(\overline{0},\overline{1})}(\overline{0},\overline{0}) = \overline{0}$; $\Phi_{(\overline{0},\overline{1})}(\overline{0},\overline{1}) = \overline{1}$; $\Phi_{(\overline{0},\overline{1})}(\overline{1},\overline{0}) = \overline{0}$ y $\Phi_{(\overline{0},\overline{1})}(\overline{1},\overline{1}) = \overline{1}$.

Luego, $ker\Phi_{(\overline{0},\overline{1})} = \{(\overline{0},\overline{0}), (\overline{1},\overline{0})\} = \langle(\overline{1},\overline{0})\rangle$.

2. Si $(\alpha_0, \alpha_1) = (\overline{1}, \overline{0})$,

$$\Phi_{(\overline{1},\overline{0})} : \frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 2\rangle} \longrightarrow \frac{\mathbb{Z}}{\langle 2\rangle}$$
$$(x_0, x_1) \longmapsto \overline{1}x_0 + \overline{0}x_1 = x_0.$$

Así, $\Phi_{(\overline{1},\overline{0})}(\overline{0},\overline{0}) = \overline{0}$; $\Phi_{(\overline{1},\overline{0})}(\overline{0},\overline{1}) = \overline{0}$; $\Phi_{(\overline{1},\overline{0})}(\overline{1},\overline{0}) = \overline{1}$ y $\Phi_{(\overline{1},\overline{0})}(\overline{1},\overline{1}) = \overline{1}$.

Luego, $ker\Phi_{(\overline{1},\overline{0})} = \{(\overline{0},\overline{0}), (\overline{0},\overline{1})\} = \langle(\overline{0},\overline{1})\rangle$.

3. Si $(\alpha_0, \alpha_1) = (\overline{1}, \overline{1})$,

$$\Phi_{(\overline{1},\overline{1})} : \frac{\mathbb{Z}}{\langle 2\rangle} \times \frac{\mathbb{Z}}{\langle 2\rangle} \longrightarrow \frac{\mathbb{Z}}{\langle 2\rangle}$$
$$(x_0, x_1) \longmapsto \overline{1}x_0 + \overline{1}x_1$$

Así, $\Phi_{(\overline{1},\overline{1})}(\overline{0},\overline{0}) = \overline{0}$; $\Phi_{(\overline{1},\overline{1})}(\overline{0},\overline{1}) = \overline{1}$; $\Phi_{(\overline{1},\overline{1})}(\overline{1},\overline{0}) = \overline{1}$ y $\Phi_{(\overline{1},\overline{1})}(\overline{1},\overline{1}) = \overline{0}$.

Luego, $ker\Phi_{(\overline{1},\overline{1})} = \{(\overline{0},\overline{0}),(\overline{1},\overline{1})\} = \langle(\overline{1},\overline{1})\rangle$.

Por lo tanto, $\mathbb{P}\left(\left(\frac{\mathbb{Z}}{\langle 2\rangle}^2\right)^*\right) = \{[\Phi_{(\overline{0},\overline{1})}],[\Phi_{(\overline{1},\overline{1})}],[\Phi_{(\overline{1},\overline{0})}]\} = \{[\overline{0},\overline{1}]_{\mathbb{P}^*},[\overline{1},\overline{1}]_{\mathbb{P}^*},[\overline{1},\overline{0}]_{\mathbb{P}^*}\}$

Observación 3.60. Si (α_0,α_1) es complementable, entonces $(-\alpha_1,\alpha_0)$ también lo es. Además $(-\alpha_1,\alpha_0) \in ker\Phi_{(\alpha_0,\alpha_1)}$, pues

$$\Phi_{(\alpha_0,\alpha_1)}(-\alpha_1,\alpha_0) = -\alpha_0\alpha_1 + \alpha_1\alpha_0 = 0$$

y por la recíproca del Lema 3.56, se tiene que $ker\Phi_{(\alpha_0,\alpha_1)} = \langle(-\alpha_1,\alpha_0)\rangle$.

En (Franco, 2009) Mazuelas menciona rápidamente algunos de los resultados presentados a continuación, sin embargo, los detalles como demostraciones, observaciones y ejemplos hacen parte de los resultados de este trabajo. Antes de presentar la proposición que relaciona los espacios proyectivos duales con los espacios proyectivos, definimos el siguiente conjunto,

$$X = \{\mathcal{N} \in \mathcal{A}^2 \mid \mathcal{N} \text{ es submódulo unidimensional y complementable}\}.$$

Proposición 3.61. Sea

$$F : X \longrightarrow \mathbb{P}((\mathcal{A}^2)^*)$$

$$\mathcal{N} \longmapsto [\Phi]$$

donde $[\Phi] = [\alpha_0, \alpha_1]_{\mathbb{P}^*}$. F define una correspondencia biunívoca entre el conjunto de submódulos unidimensionales y complementables de $\mathcal{A}^2$ y el espacio proyectivo dual asociado a $\mathcal{A}$.

Demostración. Considere $\mathcal{N} = ker\Phi = \langle(-\alpha_1, \alpha_0)\rangle \in \mathcal{A}^2$ y denotaremos la clase de equivalencia de $\Phi \in \mathbb{P}((\mathcal{A}^2)^*)$ por $[\Phi] = [\alpha_0, \alpha_1]_{\mathbb{P}^*}$. Entonces,

1. F está bien definida y es inyectiva. En efecto, sean $\mathcal{M}, \mathcal{N} \in X$, con $\mathcal{M} = ker\Phi_1 = \langle(-\alpha_1, \alpha_0)\rangle$ y $\mathcal{N} = ker\Phi_2 = \langle(-\beta_1, \beta_0)\rangle$, entonces $F(\mathcal{M}) = F(\mathcal{N}) \Leftrightarrow [\Phi_1] = [\Phi_2] \Leftrightarrow$ existe $\lambda \in \mathcal{A}^*$ tal que $\Phi_1 = \lambda\Phi_2 \Leftrightarrow ker\Phi_1 = ker\Phi_2 \Leftrightarrow \mathcal{M} = \mathcal{N}$.

2. F es sobreyectiva. Sea $[\Phi] \in \mathbb{P}((\mathcal{A}^2)^*)$, veamos que existe $\mathcal{M} \in X$ tal que $F(\mathcal{M}) = [\Phi]$. En efecto, $[\Phi] = [\alpha_0, \alpha_1]_{\mathbb{P}^*}$, donde $\langle(\alpha_0, \alpha_1)\rangle = ker\Phi$ y $ker\Phi$ es un submódulo unidimensional y complementable, luego $ker\Phi = \mathcal{M} \in X$.

□

Proposición 3.62. Sea

$$G : X \longrightarrow \mathbb{P}^1_{\mathcal{A}}$$

$$\mathcal{N} \longmapsto [\alpha_0, \alpha_1]_{\mathbb{P}}.$$

G define una correspondencia biunívoca. Esto es, un submódulo unidimensional y complementable $\mathcal{N} \in \mathcal{A}^2, \mathcal{N} = \langle(\alpha_0, \alpha_1)\rangle$ puede ser representando biunívocamente mediante el punto $[\alpha_0, \alpha_1] \in \mathbb{P}^1_{\mathcal{A}}$

Demostración. 1. G está bien definida y es inyectiva. En efecto, sean $\mathcal{M},\mathcal{N} \in X$ tales que $\mathcal{M} = \langle(\alpha_0, \alpha_1)\rangle$ y $\mathcal{N} = \langle(\beta_0, \beta_1)\rangle$. $G(\mathcal{M}) = G(\mathcal{N}) \Leftrightarrow [\alpha_0, \alpha_1]_{\mathbb{P}} = [\beta_0, \beta_1]_{\mathbb{P}} \Leftrightarrow$ existe $\lambda \in \mathcal{A}^*$ tal que $(\alpha_0, \alpha_1) = \lambda(\beta_0, \beta_1)$, luego $\mathcal{M} \subset \mathcal{N}$. Análogo se cumple que $\mathcal{N} \subset \mathcal{M}$.

2. G es sobreyectiva. Sea $[\alpha_0, \alpha_1]_{\mathbb{P}} \in \mathbb{P}^1_{\mathcal{A}}$, veamos que existe $\mathcal{M} \in X$ tal que $G(\mathcal{M}) = [\alpha_0, \alpha_1]_{\mathbb{P}}$. En efecto, como $[\alpha_0, \alpha_1]_{\mathbb{P}}$, sabemos que $\langle(\alpha_0, \alpha_1)\rangle$ es un submódulo unidimensional y complementable, luego $\langle(\alpha_0, \alpha_1)\rangle = \mathcal{M} \in X$.

□

Por las Proposiciones 3.61 y 3.62 podemos establecer la siguiente relación entre los puntos de la recta proyectiva y los puntos de espacio proyectivo dual.

Proposición 3.63. Existe una correlación canónica (isomorfismo), conocida como la polaridad nula de tal forma que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} & & \mathbb{P}((\mathcal{A}^2)^*) \\ & \overset{\Gamma}{\nearrow} & \uparrow F \\ \mathbb{P}^1_{\mathcal{A}} & \xrightarrow{G^{-1}} & X \end{array}$$

donde $\Gamma = F \circ G^{-1}$.

Demostración. Considere Γ definida así:

$$\Gamma : \mathbb{P}^1_{\mathcal{A}} \longrightarrow \mathbb{P}((\mathcal{A}^2)^*)$$

$$[\alpha_0, \alpha_1]_{\mathbb{P}} \longmapsto [\alpha_0, \alpha_1]_{\mathbb{P}^*}.$$

1. Γ está bien definida. En efecto,

$$\begin{aligned}\Gamma([\alpha_0,\alpha_1]_{\mathbb{P}}) &= F\circ G^{-1}([\alpha_0,\alpha_1]_{\mathbb{P}})\\ &= F(\mathcal{M}); \quad \mathcal{M} = ker\Phi_{(\alpha_0,\alpha_1)} = \langle(-\alpha_1,\alpha_0)\rangle\\ &= [\Phi]\\ &= [\alpha_0,\alpha_1]_{\mathbb{P}^*}.\end{aligned}$$

2. Γ es biyección. Por las Proposiciones 3.61 y 3.62, tenemos que Γ es compuesta de biyecciones, por lo tanto es biyección.

□

En el Ejemplo 3.59 se observa que calcular el espacio proyectivo dual a partir de la definición suele ser un proceso bastante extenso según el anillo considerado. En el siguiente ejemplo usamos la polaridad nula Γ definida anteriormente para calcular de forma más corta los puntos del espacio proyectivo dual del anillo $\frac{\mathbb{Z}}{\langle 4\rangle}$.

Ejemplo 3.64. Considere $\mathcal{R} = \frac{\mathbb{Z}}{\langle 4\rangle} = \{\overline{0},\overline{1},\overline{2},\overline{3}\}$. Por el Ejemplo 3.33 se tiene que

$$\mathcal{R}_0^2 = \{(\overline{0},\overline{0}),(\overline{0},\overline{2}),(\overline{2},\overline{0}),(\overline{2},\overline{2})\}.$$

Luego,

$$\left(\frac{\mathbb{Z}}{\langle 4\rangle}^{2}\right)^{*} = \{\Phi_{(\overline{0},\overline{1})}, \Phi_{(\overline{0},\overline{3})}, \Phi_{(\overline{1},\overline{0})}, \Phi_{(\overline{1},\overline{1})}, \Phi_{(\overline{1},\overline{2})}, \Phi_{(\overline{1},\overline{3})},$$

$$\Phi_{(\overline{2},\overline{1})}, \Phi_{(\overline{2},\overline{3})}, \Phi_{(\overline{3},\overline{0})}, \Phi_{(\overline{3},\overline{1})}, \Phi_{(\overline{3},\overline{2})}, \Phi_{(\overline{3},\overline{3})}\},$$

por una parte, para calcular $\mathbb{P}\left(\left(\frac{\mathbb{Z}}{\langle 4\rangle}^{2}\right)^{*}\right)$ por definición es necesario calcular $ker\Phi_{(\alpha_0,\alpha_1)}$ para cada (α_0, α_1) complementable y calcular las clases de equivalencia según la relación de equivalencia dada por,

$$\Phi_{(\alpha_0,\alpha_1)} \sim \Phi_{(\alpha_0',\alpha_1')} \Leftrightarrow ker\Phi_{(\alpha_0,\alpha_1)} = ker\Phi_{(\alpha_0',\alpha_1')}.$$

Por otra parte, del Ejemplo 3.36 se tiene que,

$$\mathbb{P}^1_{\frac{\mathbb{Z}}{\langle 4\rangle}} = \{[\overline{0},\overline{1}]_{\mathbb{P}}, [\overline{1},\overline{0}]_{\mathbb{P}}, [\overline{1},\overline{1}]_{\mathbb{P}}, [\overline{1},\overline{3}]_{\mathbb{P}}, [\overline{1},\overline{2}]_{\mathbb{P}}, [\overline{2},\overline{1}]_{\mathbb{P}}\},$$

y por la Proposición 3.63 sabemos que existe Γ tal que

$$\Gamma : \mathbb{P}^1_{\frac{\mathbb{Z}}{\langle 4\rangle}} \longrightarrow \mathbb{P}\left(\left(\frac{\mathbb{Z}}{\langle 4\rangle}^{2}\right)^{*}\right)$$

$$[\alpha_0, \alpha_1]_{\mathbb{P}} \longmapsto [\alpha_0, \alpha_1]_{\mathbb{P}^*}.$$

Luego,

$$\begin{aligned}\mathbb{P}\left(\left(\frac{\mathbb{Z}}{\langle 4\rangle}^{2}\right)^{*}\right) =&\{[\Phi_{(\overline{0},\overline{1})}],[\Phi_{(\overline{1},\overline{0})}],[\Phi_{(\overline{1},\overline{1})}],[\Phi_{(\overline{1},\overline{2})}],[\Phi_{(\overline{1},\overline{3})}],[\Phi_{(\overline{2},\overline{1})}]\},\\ =&\{[\overline{0},\overline{1}]_{\mathbb{P}^*},[\overline{1},\overline{0}]_{\mathbb{P}^*},[\overline{1},\overline{1}]_{\mathbb{P}^*},[\overline{1},\overline{3}]_{\mathbb{P}^*},[\overline{1},\overline{2}]_{\mathbb{P}^*},[\overline{2},\overline{1}]_{\mathbb{P}^*}\}.\end{aligned}$$

Esta polaridad nula Γ, determina una estructura simpléctica sobre el $\mathcal{A}$-módulo $\mathcal{A}^2$. Para probar esto, es necesario mencionar la definición de estructura simpléctica.

Definición 3.65. Sean $\mathcal{A}^2$ un $\mathcal{A}$-módulo y $H : \mathcal{A}^2 \times \mathcal{A}^2 \to \mathcal{A}$ una forma bilineal, antisimétrica y no degenerada, se dice que el par $(\mathcal{A}^2, H)$ forma una estructura simpléctica.

La siguiente Proposición 3.66 es un resultado de este trabajo y será útil para definir la forma bilineal.

Proposición 3.66. (Granados, Contreras) Γ definida en la Proposición 3.63 es una proyectividad de Staudt.

Demostración. Por la Proposición 3.63, Γ es biyección. Queda por probar que envía cuaternas armónicas en cuaternas armónicas. En efecto, Sean $A = [0,1]_{\mathbb{P}}$, $B = [1,0]_{\mathbb{P}}$, $C = [1,1]_{\mathbb{P}}$ y $D = [-1,1]_{\mathbb{P}}$, entonces $\{A,B,C,D\}$ una cuaterna armónica en $\mathbb{P}^1_{\mathcal{A}}$. Ahora, $\Gamma([0,0]_{\mathbb{P}}) = [0,0]_{\mathbb{P}^*}$; $\Gamma([1,0]_{\mathbb{P}}) = [1,0]_{\mathbb{P}^*}$; $\Gamma([0,1]_{\mathbb{P}}) = [0,1]_{\mathbb{P}^*}$ y $\Gamma([-1,1]_{\mathbb{P}}) = [-1,1]_{\mathbb{P}^*}$.

Se obtiene que $A' = [0,1]_{\mathbb{P}^*}$, $B' = [1,0]_{\mathbb{P}^*}$, $C' = [1,1]_{\mathbb{P}^*}$ y $D' = [-1,1]_{\mathbb{P}^*}$, entonces $\{A',B',C',D'\}$ una cuaterna armónica en $\mathbb{P}((\mathcal{A}^2)^*)$. Por lo tanto Γ es una proyectividad de Staud. □

Observación 3.67. Si $f : \mathbb{P} \longrightarrow \mathbb{P}'$ es una proyectividad de Staudt y $dim(\mathbb{P}) = 1$ existen un automorfismo τ de anillos y un isomorfismo τ-semilineal Φ entre los espacios asociados, tales que $f = [\Phi]$.

Por la Proposición 3.66, se tiene que Γ es una proyectividad de Staudt y como $dim(\mathbb{P}^1_{\mathcal{A}}) = 1$ existe un automorfismo $\tau = Id_{\mathcal{A}}$ de anillos y un isomorfismo $\tau-$semilineal Φ definido de la siguiente manera,

$$\Phi : \mathcal{A}^2 \longrightarrow (\mathcal{A}^2)^*$$

$$(\alpha_0, \alpha_1) \longmapsto \Phi_{(\alpha_0,\alpha_1)},$$

tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathcal{A}^2 & \xleftarrow{\Phi} & (\mathcal{A}^2)^* \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{P}^1_{\mathcal{A}} & \xleftarrow{\Gamma} & \mathbb{P}((\mathcal{A}^2)^*) \end{array}$$

donde π_1 y π_2 son las aplicaciones canónicas y se cumple que $\Gamma = [\Phi]$.

Entonces, sean $\boldsymbol{m}, \boldsymbol{n} \in \mathcal{A}^2$ y $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base para $\mathcal{A}^2$, se define

$$H : \mathcal{A}^2 \times \mathcal{A}^2 \longrightarrow \mathcal{A}$$

$$(\boldsymbol{m}, \boldsymbol{n}) \longmapsto \Phi_{\boldsymbol{n}}(\boldsymbol{m}) = \boldsymbol{m} \wedge_{\mathfrak{B}} \boldsymbol{n}.$$

Proposición 3.68. Sean $\boldsymbol{m}, \boldsymbol{n} \in \mathcal{A}^2$ y $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base para $\mathcal{A}^2$, tal que $\boldsymbol{m} = \alpha_0\boldsymbol{v}_1 + \alpha_1\boldsymbol{v}_2$ y

$\boldsymbol{n} = \beta_0 \boldsymbol{v}_1 + \beta_1 \boldsymbol{v}_2$,

$$H : \mathcal{A}^2 \times \mathcal{A}^2 \longrightarrow \mathcal{A}$$

$$(\boldsymbol{m}, \boldsymbol{n}) \longmapsto \Phi_{\boldsymbol{n}}(\boldsymbol{m}) = \boldsymbol{m} \wedge_{\mathfrak{B}} \boldsymbol{n},$$

es una forma bilineal antisimétrica.

Demostración. Es claro por el ítem 1 de la Proposición 3.20. □

Observación 3.69. A toda forma bilineal se le puede asociar una matriz, en este caso para $\boldsymbol{m}, \boldsymbol{n} \in \mathcal{A}^2$ con $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ una base de $\mathcal{A}^2$, tal que $\boldsymbol{m} = \alpha_0 \boldsymbol{v}_1 + \alpha_1 \boldsymbol{v}_2$ y $\boldsymbol{n} = \beta_0 \boldsymbol{v}_1 + \beta_1 \boldsymbol{v}_2$, se tiene que,

$$\boldsymbol{m} \wedge_{\mathfrak{B}} \boldsymbol{n} = \alpha_0\beta_1 - \alpha_1\beta_0 = (\alpha_0, \alpha_1)^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (\beta_0, \beta_1) = \boldsymbol{m}^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \boldsymbol{n}.$$

Luego, la matriz asociada a la forma bilineal H es,

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Definición 3.70. Sea $A = [\alpha_0, \alpha_1] \in \mathbb{P}^1_{\mathcal{A}}$ y $B = [\beta_0, \beta_1] \in \mathbb{P}((\mathcal{A}^2)^*)$ decimos que son incidentes si $[\alpha_0, \alpha_1] = [\beta_0, \beta_1]$.

Definición 3.71. Una polaridad es una correlación $f : \mathbb{P}^1_{\mathcal{A}} \longrightarrow \mathbb{P}((\mathcal{A}^2)^*)$ cuya inversa esta dada por

$f^{-1} : \mathbb{P}((\mathcal{A}^2)^*) \longrightarrow \mathbb{P}^1_{\mathcal{A}}$ y corresponde a si misma, es decir se cumple que $A \in \mathbb{P}^1_{\mathcal{A}}$ y $B \in \mathbb{P}((\mathcal{A}^2)^*)$ son incidentes si y sólo sí $f^{-1}(B) \in \mathbb{P}^1_{\mathcal{A}}$ y $f(A) \in \mathbb{P}((\mathcal{A}^2)^*)$ son incidentes.

Proposición 3.72. (Franco, Proposición 5.2.3) Una forma bilineal no degenerada dada por una matriz $M \in M_{2\times 2}(\mathcal{A})$ define una polaridad si y sólo si existe $\lambda \in \mathcal{A}^*$ tal que $M = \lambda M^t$.

Demostración. Sea $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, M define una correlación con matriz $\begin{pmatrix} b & d \\ -a & -c \end{pmatrix}$ cuya correlación inversa viene dada por la matriz $\begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$, por lo tanto la forma bilineal define una polaridad si y sólo si existe un $\lambda \in \mathcal{A}^*$ tal que

$$M = \lambda M^t \Leftrightarrow \lambda \begin{pmatrix} b & d \\ a & c \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix} \Leftrightarrow -\lambda \begin{pmatrix} b & d \\ -a & -c \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

□

Proposición 3.73. (Franco, Proposición 5.2.2) Una correlación determinada por una forma bilineal es un isomorfismo entre $\mathbb{P}^1_{\mathcal{A}}$ y $\mathbb{P}((\mathcal{A}^2)^*)$ si y sólo si la forma bilineal es no degenerada.

Demostración. Considere,

$$\Gamma : \mathbb{P}^1_{\mathcal{A}} \longrightarrow \mathbb{P}((\mathcal{A}^2)^*)$$

$$[\alpha_0, \alpha_1]_{\mathbb{P}} \longmapsto [\alpha_0, \alpha_1]_{\mathbb{P}^*}$$

la correlación determinada por la forma bilineal H. Por la Proposición 3.63, Γ es un isomorfismo, veamos entonces que su forma bilineal H es no degenerada. En efecto, considere $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ la matriz asociada a la forma bilineal H. Note que

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (-1) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (-1)M^t,$$

por la Proposición 3.72 se concluye que H es una forma bilineal no degenerada.

Recíprocamente, dada una forma bilineal

$$\begin{aligned} f : \mathcal{A}^2 \times \mathcal{A}^2 &\longrightarrow \mathcal{A} \\ (\boldsymbol{m}, \boldsymbol{n}) &\longmapsto \boldsymbol{m}^t \begin{pmatrix} a & b \\ c & d \end{pmatrix} \boldsymbol{n}, \end{aligned}$$

f determina una correlación, por la Proposición 3.72 la matriz asociada a la correlación es $\begin{pmatrix} b & d \\ -a & -c \end{pmatrix}$,

luego

$$\hat{\Gamma} : \mathbb{P}^1_{\mathcal{A}} \longrightarrow \mathbb{P}((\mathcal{A}^2)^*)$$

$$[\alpha_0, \alpha_1] \longmapsto [\alpha_0 b + \alpha_1 d, -\alpha_0 a - \alpha_1 c],$$

$\hat{\Gamma}$ es un isomorfismo. □

Proposición 3.74. $(\mathcal{A}^2, H)$ forman una estructura simpléctica.

Demostración. Por la Proposición 3.68 tenemos que H es bilineal y antisimétrica y por la Proposición 3.73 se tiene que la forma bilineal H es no degenerada y así concluimos que $(\mathcal{A}^2, H)$ forman una estructura simpléctica. □

Referencias Bibliográficas

Anderson, F. W. and Fuller, K. R. (2012). *Rings and categories of modules*, volume 13. Springer Science & Business Media.

Apte, H., Chattopadhyay, P., and Rao, R. A. (2012). A local global theorem for extended ideals. *J. Ramanujan Math. Soc*, 27(1):1–20.

Aroca, J. and Fernández, M. (2009). *Geometría proyectiva*. Publicaciones Universidad de Valladolid.

Coquand, T. and Lombardi, H. (2005). A short proof for the krull dimension of a polynomial ring. *The American Mathematical Monthly*, 112(9):826–829.

Coquand, T., Lombardi, H., and Roy, M.-F. (2005). An elementary characterization of krull dimension. *From sets and types to topology and analysis*, 48:239–244.

Doneddu, A. (1980). *Complementos de la geometría algebraica*. Ed. Aguilar.

Eisenbud, D. (2013). *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media.

Elizondo, J. (2015). *Anillos, ideales y espectro primo*. México: Universidad Nacional Autónoma de México.

Etayo Gordejuela, F. (2016). Topología diferencial.

Franco, S. M. (2007). Proyecciones estereográficas y geométricas en el plano. *Boletín de la Sociedad Puig Adam de profesores de matemáticas*, (75):37–54.

Franco, S. M. (2008a). Interpretación proyectiva de las métricas del plano real. *Instituto Interuniversitario de estudios de Iberoamérica y Portugal*, page 109.

Franco, S. M. (2008b). Rectas proyectivas sobre $\mathbb{R}$-álgebras bidimensionales y cuádricas en el espacio proyectivo. *Boletín de la Sociedad Puig Adam de profesores de matemáticas*, (80):57–76.

Franco, S. M. (2009). *Interpretación proyectiva de las geometrías métricas, equiformes e inversivas*. PhD thesis, Universidad de Valladolid.

Granados-Pinzón, C. and Olaya-León, W. (2016). $\mathbb{K}$-álgebras finitas conmutativas con unidad. *Ingeniería y Ciencia*, 12(24):31–49.

Granados Pinzón, C. and Olaya León, W. (2020). Anillos totales de fracciones y anillos de hermite. *Ciencia en Desarrollo*, 11(2):125–134.

Granados Pinzón, C. I. (2015). *Álgebras finitas sobre un cuerpo: la recta proyectiva*. PhD thesis, Universidad de Valladolid.

Klein, F. (1985). über die sogenannte nicht-euklidische geometrie. In *Gauss und die Anfänge der nicht-euklidischen Geometrie*, pages 224–238. Springer.

Lam, T.-Y. (2010). *Serre's problem on projective modules*. Springer Science & Business Media.

Lam, T.-Y. (2012). *Lectures on modules and rings*, volume 189. Springer Science & Business Media.

Lezama, O. (1985). Anillos dimensionales. *Boletín de Matemáticas*, 19(3):194–220.

Lezama, O. (2011). Matrix and gröbner methods in homological algebra over commutative polynomial rings. *Lambert Academic Publ*.

Lezama, O. (2017). *Cuaderno N° 3 Módulos*. Universidad Nacional de Colombia.

Liu, J. and Li, D. (2018). The hermite ring conjecture and special linear groups for valuation rings. *arXiv preprint arXiv:1811.01230*.

Lombardi, H. and Quitté, C. (2015). *Commutative algebra: Constructive methods: Finite projective modules*, volume 20. Springer.

López Soria, D. (2016). Normalidad del espectro primo y retracción sobre el espectro maximal.

Quillen, D. (1976). Projective modules over polynomial rings. *Inventiones mathematicae*, 36(1):167–171.

Ríos, J. E. G. (2015). *El anillo de los enteros algebraicos y dominios de Dedekind*. PhD thesis, Universidad Industrial de Santander.

Schwerdtfeger, H. (1979). Geometry of complex numbers: Circle geometry moebius transformation.

Serre, J.-P. (1958). Modules projectifs et espaces fibrés à fibre vectorielle. *Séminaire Dubreil. Algèbre et théorie des nombres*, 11(2):1–18.

Suslin, A. (1976). Projective modules over polynomial rings are free. *Doklady Akademii nauk SSSR*, 229:1063–1066.

Swan, R. G. (1962). Vector bundles and projective modules. *Transactions of the American Mathematical Society*, 105(2):264–277.

Vaserstein, L. N. (1986). Vector bundles and projective modules. *Transactions of the American Mathematical Society*, 294(2):749–755.

Yengui, I. (2008). The hermite ring conjecture in dimension one. *Journal of Algebra*, 320(1):437–441.

Yengui, I. (2015). Projective modules over polynomial rings. In *Constructive Commutative Algebra*, pages 9–103. Springer.