Álgebra de Diferencias

Andrés Goens

23 de abril de 2013

1. Introducción

Acerca mio: Yo soy un estudiante salvadoreño de matemática. Tengo una licenciatura en física y otra en matemática de la universidad de Aquisgrán "RWTH Aachen University". Ahora estoy por terminar la maestría en matemática en la misma universidad, y escribo mi tésis en el área de álgebra de diferencias, las bases de la cual quiero compartir en este artículo.

El álgebra de diferencias es una rama pequeña de las matemáticas, cuyo origen está cercanamente relacionado con el del álgebra diferencial, rama más grande con la que comparte mucha similitud. Es una rama relativamente nueva a su vez, [falta reseña histórica]

Para dar una primera idea del objeto de estudio de álgebra de diferencias, veremos un par de ejemplos de equaciones de diferencias. Probablemente uno de los ejemplos mejor conocidos es la secuencia de Fibonacci $1, 1, 2, 3, 5, 8, 13, \ldots$ que se puede ver como una solución de la siguiente ecuación recursiva:

$$a_0 = 1, a_1 = 1 \tag{1}$$

$$a_n = a_{n-1} + a_{n-2}, n \geq 2 \tag{2}$$

Otro ejemplo que probablemente también conozca cualquier matemático o físico es la ecuación funcional de la función Gamma:

$$\Gamma(x+1) = x\Gamma(x) \tag{3}$$

Es un resultado clásico del análisis complejo que cualquier función que cumpla esta ecuación es un múltiplo de la función Γ, a la que se le considera una generalización del factorial:

$$\Gamma(x) = \int_0^\infty \frac{t^x}{t} e^{-t} dt$$

Estos dos son ejemplos notables de ecuaciones de diferencias. En el álgebra de diferencias no se busca, sin embargo, encontrar soluciones de estas ecuaciones de manera "explicita", como lo son los números explicitos en la secuencia de Fibonacci, o la representación integral de la función Γ. El álgebra de diferencias investiga, más bien, la estructura que tienen dichas ecuaciones, y en sí, la existencia de tales.

1.1. Requisitos para este artículo

Este artículo pretende presentar lo más básico de la teoría del álgebra de diferencias, la cual en muchos aspectos se basa en geometría algebráica. Aunque conocimiento de geometría algebráica sería de mucha ayuda para entender este artículo, traté de escribirlo de tal manera que no sea necesaria. Sin embargo, conocimientos básicos de álgebra, como anillos, ideales, etc. y cierta madurez matemática probablemente sean verdaderamente indispensables para comprender este artículo. Para aquel lector que tenga interés en leerlo, pero tenga alguna laguna de conocimiento en el álgebra básica, recomiendo consultar el texto de Lang: [2]. Para aquellos que quieran buscar algo más específico de álgebra comutativa o geometría algebráica, recomiendo los textos de Eisenbud [3] o Hartshorne [4]. El contenido de álgebra de diferencias de este artículo esta basado las bases de mi tésis, aún en desarrollo, que a su vez están fuertemente basadas en los apuntes de la ponencia en álgebra de diferencias en el invierno 2012/13 de Michael Wibmer, [1].

2. Bases del Álgebra de Diferencias

Definición 2.1. Sea R un anillo comutativo (en este artículo, todos los anillos van a ser asociativos y unitales), y sea $\sigma : R \to R$ un endomorfismo de anillos en R. Entonces llamamos al par (R, σ) un anillo de diferencias, o un anillo σ. Por "abuso de notación" diremos que R es un anillo σ para referirnos al par, y si R' es otro anillo σ usaremos siempre la notación σ para el endomorfismo de R'; esto no debería causar confusión, puesto que se podrá inferir del contexto de que endomorfísmo se esta hablando

Definición 2.2. Sean R, R' anillos σ y sea $\varphi : R \to R'$ un morfismo de anillos. Decimos que φ es un morfismo de anillos σ si

$$\sigma(\varphi(r)) = \varphi(\sigma(r)) \text{ para todo } r \in R$$

Ejemplo 2.3. Hay un sinfin de ejemplos de anillos σ. Un par de los más importantes son los siguientes:

- Cualquier anillo R es un anillo σ con $\sigma = \mathrm{Id}_R$, a este le llamamos un anillo σ constante
- El cuerpo de las funciones meromórfas $\mathbb{C} \to \mathbb{C}$, que denotaremos con $\mathcal{M}$, es un anillo σ con $\sigma(f)(x) = f(x+1) \forall x \in \mathbb{C}$.
- Las secuencias de números en $\mathbb{Z}$, que denominaremos $\mathrm{Seq}(\mathbb{Z})$ forman un anillo σ con la operación de "correr" sus términos hacia la izquierda:

$$\sigma : (a_n)_{n\in\mathbb{N}} \mapsto (a_{n+1})_{n\in\mathbb{N}}$$

Definición 2.4. Sea R un anillo σ. Si R es un cuerpo, llamamos al par (R, σ) también un cuerpo σ. Si k es un cuerpo σ, A una k-álgebra que (como anillo) es un anillo σ y cumple: $\sigma(ar) = \sigma(a)\sigma(r)$, entonces llamamos a A un álgebra $k - \sigma$.

Ejemplo 2.5. Un ejemplo adicional, que por su generalidad es de especial importancia, son los llamados anillos polinomiales σ: Sea k un cuerpo. Consideremos el anillo de polynomios $R := k[y, \sigma(y), \sigma^2(y), \ldots]$, dónde $y, \sigma(y), \sigma^2(y), \ldots$ son por el momento simplemente nombres de variables (álgebraicamente independientes). A este anillo lo podemos hacer un álgebra $k-\sigma$ definiendo

$$\sigma : R \to R, y \mapsto \sigma(y), \sigma^{n-1}(y) \mapsto \sigma^n(y) \text{ para todo } n > 1$$

Extendendiolo de la manera obvia k-linearmente. Denotamos este anillo de polinomios σ con $k\{y\}$. De forma análoga podemos definir un anillo de polinomio σ sobre muchas variables: $k\{y_1, \ldots, y_n\}$.

Definición 2.6.
- Si S es un anillo σ y $R \leq S$ un subanillo de S, decimos que R es un subanillo σ, si $(R, \sigma_{|R})$ es un anillo σ, es decir, si la imagen de $\sigma_{|R}$ esta contenida en R.
- Si $I \trianglelefteq R$ es un ideal y subanillo σ se le llama ideal σ. No es dificil convencerse que esto define una estructura σ del anillo factorial canonica:

$$\sigma : R/I \to R/I, a + I \mapsto \sigma(a) + I$$

Definición 2.7. A un álgebra $k - \sigma$ A se le llama finitamente σ generada, si existen elementos $f_1, \ldots, f_n$ tales, que $A = k[f_1, f_2, \ldots, f_n, \sigma(f_1), \ldots, \sigma(f_n), \sigma^2(f_1), \ldots]$.

Comentario 2.8. Si A es un álgebra $k - \sigma$, σ generada por $f_1, \ldots, f_n$, entonces tenemos un epimorfismo de álgebras $k - \sigma$ canónico del anillo de polinomios σ, $k\{y_1, \ldots, y_n\}$ a A: $y_i \mapsto f_i, i = 1, \ldots, n$. Vemos entonces que los anillos de polinomios σ son objetos libres en la categoría de álgebras $k-\sigma$. Denotamos por esto al álgebra σ generada por $f_1, \ldots, f_n$ con $k\{f_1, \ldots, f_n\}$.

Definición 2.9. Si el Núcleo (Kernel) I del epimorfismo mencionado en el Comentario 2.8 es a su vez finitamente σ generada, por $r_1, \ldots, r_m$ digamos, entonces decimos que el álgebra A es finitamente σ presentada

Comentario 2.10. En las condiciones de la definicion anterior, por el teorema de homomorfismos tenemos $A \cong k\{y_1, \ldots, y_n\}/(r_1, \ldots, r_m)$. Nótese también que los conceptos finitamente σ generado y finitamente σ presentado son verdaderamente diferentes: a diferencia del caso de anillos polinomiales comunes, no tenemos el teorema de bases de Hilbert, lo que quiere decir que $k\{y_1, \ldots, y_n\}$ no es Noetheriano. En particular, a pesar de ser finitamente σ generada el álgebra, el ideal I puede no serlo.

Ejemplo 2.11. Sea k un cuerpo σ y sea $I \trianglelefteq_\sigma k\{y\}$ el ideal σ generado por $y\sigma(y), y\sigma^2(y), y\sigma^3(y), \ldots$, es decir $I = [y\sigma^i(y) \mid i \in \mathbb{N}_{\geq 1}]$. Entonces el anillo σ $R := k\{y\}/I$ (con $\sigma(r + I) := \sigma(r) + I$) es finitamente σ generado: $R = k\{y + I\}$, pero no finitamente σ-prestentado, pues I no es finitamente σ generado.

Comentario 2.12. Así como las ecuaciones algebráicas regulares se "reducen" al buscar soluciones de un polinomio, las ecuaciones de diferencias las podemos expresar como la búsqueda de soluciones para polinomios σ. Entiéndase aquí un homomorfismo como el del Comentario 2.8.

Ejemplo 2.13. Ahora podemos expresar los dos ejemplos de la introducción en el lenguaje del álgebra de diferencias: La secuencia de Fibonacci es una solución del polinomio $\sigma^2(y) + \sigma(y) - y$ en el anillo σ Seq($\mathbb{Z}$): esta es precisamente la relación de recurrencia $a_{n+2} + a_{n+1} = a_n$. De la misma manera, la función Γ es la solución del polinomio $\sigma(y) - zy$, adonde el coeficiente z es la función $z \mapsto z$, un elemento del cuerpo $\mathbb{C}(x)$ de funciones racionales.

3. Ideales de Diferencias

Sea $\mathfrak{a} \trianglelefteq_\sigma R$ un ideal σ de R.

- Llamamos a $\mathfrak{a}$ un ideal σ mezclado, si para cualesquiera $f, g \in R$ con $fg \in \mathfrak{a}$ implica que $f\sigma(g) \in \mathfrak{a}$.
- A $\mathfrak{a}$ le llamamos perfecto, si $\sigma^{i_1}(f) \cdots \sigma^{i_n}(f) \in \mathfrak{a}$ implica que $f \in \mathfrak{a}$, donde $n \in \mathbb{N}_{\geq 1}, i_j \in \mathbb{N}_{\geq 0}$ para todo $j \in \{1, \ldots, n\}$.
- $\mathfrak{a}$ se llama reflexivo, si $\sigma(a) \in \mathfrak{a}$ implica que $a \in \mathfrak{a}$.
- $\mathfrak{a}$ se llama σ-primo, si $\mathfrak{a}$ es un ideal primo y un ideal σ reflexivo.

Comentario 3.1. Es fácil ver de sus definiciones que los ideal σes σ-primos son perfectos, los ideal σes perfectos son mezclados, radicales y reflexivos. Los ideal σes, primos (como ideal únicamente) también son mezclados, pero no necesariamente perfectos. Nótese que hay una diferencia ente un ideal σ σ-primo y un ideal σ primo: el primero debe necesariamente ser reflexivo, lo cual no es el caso para el segundo. Estos dos tipos de ideal σes estan relacionados de cerca con los ideal σes perfectos y mezclados respectivamente.

Lemma 3.2. Sea $\varphi : R \to S$ un morfismo of anillos σ y sea $\mathfrak{a} \trianglelefteq_\sigma S$ un ideal σ. Entonces $\varphi^{-1}(\mathfrak{a}) \trianglelefteq_\sigma R$ es un ideal σ. De forma similar, si $\mathfrak{a}$ es un ideal σ mezclado, también lo es $\varphi^{-1}(\mathfrak{a})$. Lo mismo es cierto de los σ ideales perfectos y reflexivos.

Proof. Ya que $\mathfrak{a} \trianglelefteq S$ es un ideal, también lo es $\mathfrak{b} := \varphi^{-1}(\mathfrak{a}) \trianglelefteq R$. Sea $b \in \mathfrak{b}$. Entonces $\varphi(b) =: a \in \mathfrak{a}$ por definition. Ya que $\mathfrak{a} \trianglelefteq_\sigma S$ es un ideal σ, $\sigma(a) \in \mathfrak{a}$, y ya que φ es un morfismo σ, implica que $\sigma(a) = \sigma(\varphi(b)) = \varphi(\sigma(b)) \in \mathfrak{a}$. Por tanto, $\sigma(b) \in \mathfrak{b}$, que a su vez implica que $\mathfrak{b}$ es un ideal σ. Ahora, sea $\mathfrak{a}$ un ideal σ mezclado y $fg \in \mathfrak{b}$. Por definición de $\mathfrak{b}$, esto significa que $\varphi(fg) = \varphi(f)\varphi(g) \in \mathfrak{a}$. Ya que $\mathfrak{a}$ es mezclado, esto a su vez implica que $\varphi(f)\sigma\varphi(g) = \varphi(f)\varphi(\sigma(g)) \in \mathfrak{a}$, lo cual significa que $f\sigma(g) \in \mathfrak{b}$, por lo que $\mathfrak{b}$ también es mezclado. Este resultado para ideales de diferencias perfectos y reflexivos es analogo. □

Comentario 3.3. Sea R un anillo σ y $\mathfrak{a} \trianglelefteq_\sigma R$ un ideal σ. Podemos definir una estructura canonica de anillo σ en el anillo de cocientes $R/\mathfrak{a}$ via $\sigma(r + \mathfrak{a}) := \sigma(r) + \mathfrak{a}$. Esto está bien definido y, en especial, hace al epimorfismo de anillos canónico $\tau : R \to R/\mathfrak{a}$ un morfismo de anillos σ.

Proposición 3.4. Sea R un anillo σ y $\mathfrak{a} \trianglelefteq_\sigma R$ un ideal σ. Entonces existe una biyección entre los conjuntos $\{\mathfrak{b} \trianglelefteq_\sigma R/\mathfrak{a}\}$ y $\{\mathfrak{a} \trianglelefteq_\sigma \mathfrak{b} \trianglelefteq_\sigma R\}$, la cual esta dada por la funcion inducida por el encaje canónico como en el Lemma 3.2. Esto sigue siendo cierto si restringimos ambos conjuntos a los ideales σ que sean radicales, mezclados, primos, σ primos o perfectos.

Comentario 3.5. Sea R un anillo σ, y $F \subseteq R$ un subconjunto de R. Cualquier intersección de ideales σ mezclados y radicales que contengan a F, también es un ideal σ mezclado y radical, que por supuesto contiene a F. Esto significa que existe un ideal σ radical y mezclado mínimo (con respecto a la inclusión) que contiene a F; la intersección de todo dicho ideal.

$$\bigcap_{\substack{\mathfrak{b} \trianglelefteq_\sigma R, \\ \mathfrak{b} \text{ mezclado y rad.}}} \mathfrak{b}$$

Demostración. Sea I un conjunto índice, y sean $\mathfrak{a}_i \trianglelefteq_\sigma R$ para todo $i \in I$ ideales σ radicales y mezclados. Además, sea $\mathfrak{b} := \bigcap_{i\in I} \mathfrak{a}_i$ la intersección de estos. Si $a \in \mathfrak{a}_i$ para todo $i \in I$, entonces $\sigma(a) \in \mathfrak{a}_i$ para todo $i \in I$, ya que cada $\mathfrak{a}_i$ es un ideal σ. Esto implica que $\sigma(a) \in \mathfrak{b}$. Argumentos análogos demuestran las otras dos propiedades. □

Definición 3.6. Al ideal σ $\mathfrak{a}$ del Comentario 3.5 se llama la clausura radical y mezclada de F, y se le denota por $\{F\}_m$.

Comentario 3.7. Sea R un anillo σ, $\mathfrak{a} \trianglelefteq_\sigma R$ un ideal σ. Para tratar de encontrar $\{\mathfrak{a}\}_m$ es tentable definir $\mathfrak{a}' := \{f\sigma(g) \mid fg \in \mathfrak{a}\}$. Un ejemplo sencillo nos muestra que esto no basta, ya que $\mathfrak{a}'$ no es un ideal en general: Sea $R = k\{y_1, y_2, y_3\}$ con un cuerpo σ constante k, y $\mathfrak{a} = [y_1y_2, y_2y_3] \trianglelefteq_\sigma R$. Entonces no existen $f, g \in R$ tales que $f\sigma(g) = \sigma(y_2)y_3 + \sigma(y_1)y_2 \in \{\mathfrak{a}\}_m$ y $fg \in \mathfrak{a}$. Si tomamos el ideal σ generado por $\mathfrak{a}'$, $[\mathfrak{a}']$, no tenemos ninguna garantía que este siga siendo mezclado. De hecho, en el mismo ejemplo, $y_1\sigma^2(y_2) \notin [\mathfrak{a}']$, a pesar que $y_1\sigma(y_2) \in \mathfrak{a}'$. Podríamos repetir este proceso, pero esto nos dejaría sin $y_1\sigma^3(y_2)$ out, y así sucesivamente. Pero la unión de todos los conjuntos obtenidos así, si funciona, como lo veremos en el siguiente Lemma:

Lemma 3.8. Sea R un a anillo σ y $\mathfrak{a}$ un ideal σ mezclado. Entonces el radical de $\mathfrak{a}$, $\sqrt{\mathfrak{a}}$, también es mezclado. Sean $f, g \in R$ tales, que $fg \in \sqrt{\mathfrak{a}}$. Por definición existe un $n \in \mathbb{N}_{\geq 1}$ tal, que $f^n g^n = (fg)^n \in \mathfrak{a}$. Ya que $\mathfrak{a}$ es mezclado, esto implica que $f^n\sigma(g^n) = f^n\sigma(g)^n = (f\sigma(g))^n \in \mathfrak{a}$. Pero esto implica que $f\sigma(g) \in \sqrt{\mathfrak{a}}$, que era lo que debía mostrarse.

Lemma 3.9. Sea R un anillo σ y $F \subseteq R$. Además, sea $F' := \{f\sigma(g) \mid fg \in F\}$ como en el Commentario 3.7, y sea $F^{\{1\}} := [F]'$, $F^{\{n\}} := [F^{\{n-1\}}]'$. Entonces

$$\{F\}_m = \sqrt{\cup_{n=1}^{\infty} F^{\{n\}}} \tag{4}$$

Esta manera de obtener $\{F\}_m$ se le llama proceso de mezcla ("suffling process") y tiene un análogo para ideales σ perfectos.

Demostración. Sea $\mathfrak{a} := \bigcup_{n=1}^{\infty} F^{\{n\}}$. Es obvio de la construcción que $\mathfrak{a}$ es un ideal σ mezclado, y que $F \subseteq \mathfrak{a}$. Por inducción en los pasos iterativos $F^{\{n\}}$ obtenemos que para cada ideal σ mezclado $\mathfrak{b}$ que contiene a F, $F^{\{n\}} \subseteq \mathfrak{b}$. Por tanto, $\mathfrak{a}$ es el ideal σ mezclado más pequeño que contiene a F. Por el Lemma 3.8 sabemos que $\sqrt{\mathfrak{a}}$ sigue siendo mezclado, lo cual a su vez demuestra que $\sqrt{a}$ es, de hecho, el ideal σ radical y mezclado más pequeño que contiene a F. □

En la geometría algebráica, al tratar con variedades afinas, el enfoque moderno es el de definir una topología en el espectro del anillo, la topología de Zariski. A continuación haremos una generalización de este principio para el caso de anillos σ. El lector que no este familiarizado con este concepto no debe preocuparse, pues lo que sigue en este artículo no requiere dicho conocimiento, sólo que tal vez le costará más entender el porqué de estas construcciones. No obstante, para la demostración del teorema principal de este artículo, el Teorema 3.15, vamos a hacer uso de un par de resultados del álgebra comutativa que sólo se repetirán en el siguiente lemma. Al lector que no los conozca, y quiera saber más, se le sugiere consultar cualquier texto básico de álgebra comutativa o geometría algebráica, como [3] ó [4].

Lemma 3.10. Sea R be un anillo (comutativo, unital, asociativo) ring. Entonces:

- Si $R \leq S$ es un sobreanillo de R, y $\mathfrak{p}$ un ideal primo mínimo de R, entonces existe un ideal primo mínimo $\mathfrak{q}$ de S tal, que $\mathfrak{p} = \mathfrak{q} \cap R$
- Cada ideal radical de R es la intersección de ideales primos. Si R is noetheriano, entonces esta intersección es finita.
- Si R es noetheriano y $\mathfrak{p} \trianglelefteq R$ es un ideal primo mínimo de R, entonces existe un elemento $a \in R$ tal, que $\mathfrak{p}$ es el ideal aniquilador de a, es decir $\mathfrak{p} = \mathrm{Ann}(a) = \{r \in R \mid ra = 0\}$.

Proposición 3.11. Sea R un anillo σ finitamente σ generado por $\mathbb{Z}$, es decir, para el cual exista un conjunto finito $A \subseteq R$ de tal manera que cada $f \in R$ pueda ser escrito como una combinación $\mathbb{Z}$-linear (finita) de potencias de σ de elementos en A: Existe un $n \in \mathbb{N}_{\geq 1} : f \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)]$. Entonces, cada ideal σ radical y mezclado σ es la intersección de ideales de diferencias primos.

Proof. Sea $\mathfrak{a} \trianglelefteq_\sigma R$ un ideal σ mezclado y radical. Por la Proposición 3.4 existe una biyección entre los ideales primos de R que contienen a $\mathfrak{a}$ y los de $R/\mathfrak{a}$. Por consiguiente podemos asumir sin pérdida de la generalidad, que $\mathfrak{a} = [0] \trianglelefteq_\sigma R$, reemplazando R por $R/\mathfrak{a}$. Esto quiere decir que basta con demostrar que el ideal cero $[0]$ de un anillo σ bien-mezclado y reducido es la intersección de todos sus ideales $-s$ que son primos. Nótese que esta asunción no cambia el hecho que R sea finitamente σ generado por $\mathbb{Z}$. Sea pues $f \in R$ tal, que $f \notin \mathfrak{q}$ para todo $\mathfrak{q} \trianglelefteq_\sigma R$ primo. Aseveramos que f entonces tiene que ser 0. Si asumimos que este no es el caso, es decir, $f \neq 0$, entonces por la asunción de R, existe un $n \in \mathbb{N}$ tal, que $f \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)]$. Ahora usamos el caso especial para ideales (algebráicos): Puesto que $\mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)]$ es

noetheriano y reducido, $(0) \trianglelefteq R$ es la intersección de todos los ideales primos de R. En particular, existen ideales primo que no contienen a f. Sea $\mathfrak{q}_0 \trianglelefteq R$ uno de dichos ideales, mínimo con respecto a la inclusión. Es decir, $f \notin \mathfrak{q}_0$. Ya que $f \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)] \subset \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+1}(A)]$, nuevamente por el Lemma 3.10, podemos encontrar un $\mathfrak{q}_1 \trianglelefteq \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+1}(A)]$ tal, que $\mathfrak{q}_1 \cap \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)] = \mathfrak{q}_0$. Prosiguiendo inductivamente encontramos una cadena de ideales primos mínimos $\mathfrak{q}_i, i \in \mathbb{N}$, $\mathfrak{q}_i \trianglelefteq \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)]$, con $\mathfrak{q}_{i+1} \cap \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)] = \mathfrak{q}_i$ para todo $i \in \mathbb{N}$. Entonces $\mathfrak{q} := \bigcup_{i=0}^{\infty} \mathfrak{q}_i$ es un ideal primo de R, que cumple que $f \notin \mathfrak{q}$. De hecho, $\mathfrak{q}$ is incluso un ideal σ de R: Sea $a \in \mathfrak{q}$. Queremos demostrar que $\sigma(a) \in \mathfrak{q}$. Por la construcción de $\mathfrak{q}$ existe un $i \in \mathbb{N}$ tal, que $a \in \mathfrak{q}_{i-1} \subseteq \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i-1}(A)]$, lo que a su vez implica que $\sigma(a) \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)]$. El Lemma 3.10 dice entonces, que existe un $h \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)]$ tal, que $\mathfrak{q}_i = \mathrm{Ann}(h)$. Esto implica que $ah = 0$, y puesto que R es bien-mezclado, esto implica también que $\sigma(a)h = 0$, por tanto, $\sigma(a) \in \mathfrak{q}_i \subseteq \mathfrak{q}$. Pero esto significa que $\mathfrak{q}$ es un ideal σ y primo de R que no contiene a f, que contradice la asunción acerca de f, por lo que tiene que ser que $f = 0$. □

Para demostrar el caso general necesitamos otra herramienta todavía: el concepto de filtros.

Definición 3.12. Sea U un conjunto, y sea $F \subseteq \mathrm{Pot}(U)$, dónde $\mathrm{Pot}(U)$ denota el conjunto potencia de U. Entonces se le llama a F un filto si satisface los siguientes axiomas:

- $U \in F$ y $\emptyset \notin F$
- Si $V, W \subseteq U$ con $V \subseteq W$ y $V \in F$ entonces también tiene que ser $W \in F$
- Para $V_1, \ldots, V_n \in F$ tiene que cumplirse que

$$\bigcap_{i=1}^{n} V_i \in F$$

Un filtro F se llama ultrafiltro, si para cualquier $V \subseteq U$ se cumple que $V \in F$ o $U \backslash V \in F$. Nótese que los axiomas primero y tercero juntos implican que no pueden ambos serlo.

Comentario 3.13. Sea U un conjunto. Entonces, el conjunto de filtros sobre U está ordenado inductivamente por inclusión. Por el Lemma de Zorn para cada filtro F sobre U debe haber un filtro máximo G con respecto a la inclusión, tal que $F \subseteq G$. La maximalidad del filtro G implica que G será un

ultrafiltro, ya que en caso contrario podríamos encontrar un filtro en el que G este propiamente incluido al añadir uno de los conjuntos que contradicen la propiedad del ultrafiltro.

La razón por la que este concepto es útil en este contexto es la siguiente:

Lemma 3.14. Sea R un anillo σ, y sea M el conjunto de todos los subanillos σ de R que son finitamente σ-generados sobre $\mathbb{Z}$. Para cualquier subconjunto fijo $F \subseteq R$, consideraremos el conjunto $M_F := \{T \subseteq M \mid \{S \in M \mid F \subseteq S\} \subseteq T\} \subseteq \mathrm{Pot}(M)$.

Entonces,

$$\mathcal{F} := \bigcup_{F \subseteq R \text{ finito}} M_F$$

define un filtro sobre M. Si $\mathcal{G}$ es un ultrafiltro que contiene a $\mathcal{F}$, y $P := \prod_{S \in M} S$ con operaciones definidas en cada componente, entonces el ultrafiltro $\mathcal{G}$ define una relación de equivalencia en P via $(g_s)_{S \in M} \sim (h_s)_{S \in M} :\Leftrightarrow \{S \in M \mid g_s = h_s\} \in \mathcal{G}$. El conjunto de clases de equivalencia, $P/\mathcal{G} := P/\sim$, tiene una estructura natural como anillo σ structure y se le llama ultraproducto.

Demostración. $\mathcal{F}$ es un filtro, puesto que: Para $F \subseteq R$ finito: $[F] \in \{S \in M \mid F \subseteq S\} \neq \emptyset$, y ya que $T \supseteq \{S \in M \mid F \subseteq S\}$ para todo $T \in M_F$, $\emptyset \notin M_F$ (Nótese que $[\emptyset] = (0)$). Que $M \in M_F$ para cualquier $F \subseteq R$ es obvio, al igual que que $T \subseteq U, T \in M_F$, $U \in M_F$. Sólo necesitamos demostrar entonces que para $U, T \in \mathcal{F} : U \cap T \in \mathcal{F}$. Sea $u, t \subseteq R$ finito, tal que $U \in M_u, T \in M_t$. $u \cup t \subseteq R$ también sea finito y que se cumpla que $\{S \in M \mid u \cup t \subseteq S\} \subseteq \{S \in M \mid u \subseteq S\} \subseteq U$, y de forma similar para T. Esto significa que $U \cap T \in M_{u \cup t} \subseteq \mathcal{F}$, lo que concluye la demostración que $\mathcal{F}$ es un filtro. Ahora, consideremos un ultrafiltro $\mathcal{G} \supseteq \mathcal{F}$ y definamos $\sim$ on P como antes. Esta es una relación de equivalencia: Sea $f \sim g, g \sim h$ para $f, g, h \in P$. Esto significa que $\{S \in M \mid f_s = g_s\} \in \mathcal{G}, \{S \in M \mid g_s = h_s\} \in \mathcal{G}$. Pero entonces $\{S \in M \mid f_s = g_s\} \cap \{S \in M \mid g_s = h_s\} \subseteq \{S \in M \mid f_s = h_s\} \in \mathcal{G}$, ya que $\mathcal{G}$ es un filtro. La reflexividad es una consecuencia del hecho que $M \in \mathcal{G}$, y la simetría es obvia. Solo falta entonces demostrar que tenemos una estructura bien definida de anillo σ en $P/\sim$. Considere $f, f' \in P$ con $f \sim f'$. Sabemos que para todo $S \in M$ con $f_S = f'_S$: $\sigma(f)_S = \sigma(f')_S$. Pero entonces $\{S \in M \mid \sigma(f)_S = \sigma(f')_S\} \supseteq \{S \in M \mid f_S = f'_S\} \in \mathcal{G}$ por asunción, y ya que $\mathcal{G}$ es un filtro, esto significa que $\{S \in M \mid \sigma(f)_S = \sigma(f')_S\} \in \mathcal{G}$, por tanto $\sigma(f) \sim \sigma(f')$. Que $+, \cdot$ también están bien definidas se demuestra de una manera similar. □

Ahora demostraremos el caso general de la Proposition 3.11.

Teorema 3.15. Sea R un anillo σ, y $F \subseteq R$ be un subconjunto de R. Entonces,

$$\{F\}_m = \bigcap_{\substack{F \subseteq \mathfrak{p} \trianglelefteq_\sigma R \\ \mathfrak{p} \text{ primo}}} \mathfrak{p}$$

En especial, cada ideal σ de R mezclado y radical es la intersección de ideales de diferencia primos.

Proof. Basta con mostrar que cada ideal σ radicar y mezclado es la intersección de ideales σ y primos. Puesto que un ideal σ que sea primo también es radical y mezclado, es claro que $\{F\}_m \subseteq \mathfrak{p}$ para cada $\mathfrak{p} \trianglelefteq_\sigma R$ primo con $F \subseteq \mathfrak{p}$, lo que nos da la representación

$$\{F\}_m = \bigcap_{\substack{F \subseteq \mathfrak{p} \trianglelefteq_\sigma R \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}$$

Ahora, por el mismo argumento que en la Proposición 3.11, es suficiente demostrar en el caso que R sea bien-mezclado y reducido, que la intersección de todos los ideal σ y primos es $[0]$. Sea $0 \neq f \in R$. Vamos a construir un ideal σ y primo que no contenga a f:

Sea $P/\mathcal{G}$ el anillo de diferencias como en el Lemma 3.14. Considere la función $\varphi : R \to P/\mathcal{G}, g \mapsto (g_S)_{S \in M}$ con $(g_S) = g$ para todo $S \in M$ con $g \in S$. Ya que $\{S \in M \mid g \in S\} \in M_g$ (con M_g también como en el Lemma 3.14), todos los (g_S) así estan en la misma clase respecto a $\sim$, independientemente de los g_s para $g \notin S$. Por este hecho no es dificil ver que φ is un de anillos σ bien definido. Con la proposición 3.11 sabemos que para cada $S \in M$ existe un ideal primo σ $\mathfrak{p}_S \trianglelefteq_\sigma S$ tal que $f \notin S$. Definimos $\mathfrak{p} \trianglelefteq_\sigma P/\mathcal{G}$ como el conjunto de todas las clases de equivalencia de elementos $(g_s)_{S \in M}$ tales, que $\{S \in M \mid g_s \in \mathfrak{p}_S\} \in \mathcal{G}$. Para $[(g_s)_{S \in M}]_\sim, [(h_s)_{S \in M}]_\sim \in \mathfrak{p}$ es $\mathcal{G} \ni \{S \in M \mid g_s \in \mathfrak{p}_S\} \cap \{S \in M \mid h_s \in \mathfrak{p}_S\} \subseteq \{S \in M \mid g_s + h_s \in \mathfrak{p}_S\} \in \mathcal{G}$, ya que $\mathcal{G}$ es un filtro. Argumentos similares para $\sigma(g), gh$ para $h \in P/\mathcal{G}$ demustran que $\mathfrak{p}$ en efecto es un ideal σ. Más aún, $\mathfrak{p}$ también es primo ya que $\mathcal{G}$ es un ultrafiltro: Sean $g, h \in P$ con $\{S \in M \mid g_S h_S \in \mathfrak{p}_S\} \in \mathcal{G}$. Si $[g]_\sim \notin \mathfrak{p}$, entonces $V := \{S \in M \mid g_S \in \mathfrak{p}_S\} \notin \mathcal{G}$. Ya que $\mathcal{G}$ es un ultrafiltro, esto significa que $M \backslash V \in \mathcal{G}$. Pero $\mathcal{G} \ni (M \backslash V) \cap \{S \in M \mid g_S h_S \in \mathfrak{p}_S\} \subseteq \{S \in M \mid h_S \in \mathfrak{p}_S\} \in \mathcal{G}$, lo que significa que $[h]_\sim \in \mathfrak{p}$. Pero la pre-imágen de un ideal primo, $\varphi^{-1}(\mathfrak{p}) \trianglelefteq_\sigma R$ también es prima, al igual que un ideal de diferencias. Por construcción, $[\varphi(f)]_\sim \notin \mathfrak{p}$, lo que significa que $f \notin \varphi^{-1}(\mathfrak{p})$, como deseado. Esto concluye la demostración. □

4. Un Análogo de la Topología de Zariski

Para finalizar este artículo, veremos como podemos definir una topología en analogía a la topología de Zariski para un anillo σ.

Definición 4.1. Sea R un anillo σ. Definimos al conjunto de todos los ideales de diferencia primos como σ-Spec$(R) := \{\mathfrak{p} \trianglelefteq_\sigma R \mid \mathfrak{p} \text{ primo } \}$. De forma similar, definimos el conjunto de los ideales σ-primos como $\text{Spec}^\sigma(R) := \{\mathfrak{p} \trianglelefteq_\sigma R \mid \mathfrak{p} \ \sigma\text{-primo } \}$.

Comentario 4.2. En general puede ocurrir que tanto $\text{Spec}^\sigma(R)$, como σ-Spec$(R) = \emptyset$. Por ejemplo, sea R un anillo σ y considere el anillo σ $R \oplus R$, con $\sigma((r,s)) := (\sigma(s), \sigma(r))$. Este anillo no tiene ideales de diferencias primos: Sea $\mathfrak{p} \trianglelefteq R$ primo. Entonces $0 = (1,0)(0,1) \in \mathfrak{p}$, lo que significa que $(1,0) \in \mathfrak{p}$ o $(0,1) \in \mathfrak{p}$. Pero entonces $R \oplus 0 \subseteq \mathfrak{p}$ o $0 \oplus R \subseteq \mathfrak{p}$. Si asumimos que $\mathfrak{p}$ es un ideal σ, entonces lo anteriormente concluido implica que $R \oplus R \subseteq \mathfrak{p}$, lo cual no puede ocurrir por la definición de ideales primos.

En la geometría algebráica se define usalmente una topología en $\text{Spec}(R) = \{\mathfrak{p} \trianglelefteq R \mid p \text{ primo}\}$, llamada la topología de Zariski. Esto tiene un análogo en $\text{Spec}^\sigma(R)$, llamada usualmente la topología de Cohn. Aquí vamos a hacer otra definición análoga a las dos anteriores, en σ-Spec(R), y que es la topología "correcta" para trabajar con ideales de diferencias mezclados (por el Teorema 3.15, por ejemplo).

Definición 4.3. Sea R un anillo σ y $F \subseteq R$ un subconjunto de R. Entonces definimos $\mathcal{V}_m(F) := \{\mathfrak{p} \in \sigma\text{-Spec}(R) \mid F \subseteq \mathfrak{p}\}$.

Lemma 4.4. Sea R un anillo σ. Entonces tenemos:

a) $\mathcal{V}_m((0)) = \sigma$-Spec$(R)$, y $\mathcal{V}_m(R) = \emptyset$.

b) Para cualesquiera dos ideales $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ tenemos $\mathcal{V}_m(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b}) = \mathcal{V}_m(\mathfrak{a} \cap \mathfrak{b})$

c) Para cualquier familia de ideales $(\mathfrak{a}_i)_{i \in I}$ para un conjunto índice I, tenemos $\cap_{i \in I} \mathcal{V}_m(\mathfrak{a}_i) = \mathcal{V}_m(\sum_{i \in I} \mathfrak{a}_i)$

Proof. a) Es claro que $(0) \subseteq \mathfrak{p}$ para todo $\mathfrak{p} \in \sigma$-Spec(R), al igual que $R \not\subseteq \mathfrak{p}$ para todo $\mathfrak{p} \in \sigma$-Spec(R).

b) Sean $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ dos ideales en R. Entonces $\mathcal{V}_m(\mathfrak{a}) \cup \mathcal{V}_m(\mathfrak{b}) \subseteq \mathcal{V}_m(\mathfrak{a} \cap \mathfrak{b})$, ya que para $\mathfrak{p} \trianglelefteq_\sigma R$ primo, $\mathfrak{a} \subseteq \mathfrak{p}$ implica que $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, y similarmente para $\mathfrak{b}$. Por el otro lado, sea $\mathfrak{p} \trianglelefteq_\sigma R$ primo con $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, y $\mathfrak{a} \not\subseteq \mathfrak{p}$ (en caso contrario $\mathfrak{p} \in \mathcal{V}_m(\mathfrak{a})$ y hemos terminado). Entonces existe un

$f \in \mathfrak{a}$, $f \notin \mathfrak{p}$. Para cualquier $g \in \mathfrak{b}$, esto implica que $fg \in \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$. Ya que $\mathfrak{p}$ es primo, esto significa que $g \in \mathfrak{p}$, por tanto $\mathfrak{b} \subseteq \mathfrak{p}$, lo que concluye la demostración.

c) Sea $(\mathfrak{a}_i)_{i \in I}$ una familia de ideales de R. Entonces $\mathfrak{p} \in \cap_{i \in I} \mathcal{V}_m(\mathfrak{a}_i) \Leftrightarrow \mathfrak{a}_i \subseteq \mathfrak{p}$ para todo $i \in I \Leftrightarrow \mathfrak{p} \in \mathcal{V}_m(\sum_{i \in I} \mathfrak{a}_i)$.

□

Comentario 4.5. Ya que para un anillo σ, calquier ideal σ y primo es radical y mezclado, se cumple que para cualquier $F \subseteq R$, y cualquier ideal σ y primo $\mathfrak{p} \trianglelefteq_\sigma R$ con $F \subseteq \mathfrak{p}$: $(F) \subseteq [F] \subseteq \{F\}_m \subseteq \mathfrak{p}$. In especial, esto significa que $\mathcal{V}_m(F) = \mathcal{V}_m((F)) = \mathcal{V}_m([F]) = \mathcal{V}_m(\{F\}_m)$.

Definición 4.6. Sea R un anillo σ. Definimos una topología en σ-Spec(R) al definir que $A \subseteq \sigma$-Spec(R) es cerrado $:\Leftrightarrow A = \mathcal{V}_m(\mathfrak{a})$ para un ideal $\mathfrak{a} \trianglelefteq R$, o de forma equivalente, definiendo a un conjunto abierto si es el complemento de un conjunto de la forma $\mathcal{V}_m(\mathfrak{a})$. Esto es una topología bien definida gracias al Lemma 4.4. Definimos para $f \in R$: σ-$D(f) := \sigma$-Spec$(R) \backslash \mathcal{V}_m(f)$. Por el Comentario 4.5, σ-$D(f)$ es el complemento de un conjunto cerrado, y por consiguiente, abierto. Llamamos a los conjuntos de la forma σ-$D(f) \subseteq \sigma$-Spec(R) subconjuntos básicos abiertos de σ-Spec(R).

Con estas definiciones ya podemos empezar a trabajar con aspectos geométricos en álgebra de diferencias, y el lector que conozca la geometría algebráica apreciará por que estamos ya en un my buen camino. Desafortunadamente hasta aquí se limita este artículo, pero al lector interesado le recomiendo, si desea informarse más acerca del tema, que consulte los textos [5] ó [6].

5. Bibliografía

[1] Wibmer, Michael *Algebraic Difference Equations (Lecture Notes)*, Disponible en línea: `http://www.algebra.rwth-aachen.de/de/Mitarbeiter/Wibmer/Algebraic%20difference%20equations.pdf`

[2] Serge Lang, *Algebra*, Revised Third Edition, Springer, 2005

[3] Eisenbud, David *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, 1995

[4] Hartshorne, Robin *Algebric Geometry*, Springer, 1977

[5] Cohn, Richard *Difference Algebra*, Interscience Publishers, 1965

[6] Levin, Alexander *Difference Algebra*, Springer, 2008