Automorfismos Polinomiales y la Conjetura de Keller

Guillermo Mantilla

Departamento de Matemáticas
Universidad de los Andes
Apartado Aéreo 4976
Bogotá, Colombia

Índice general

Notación y ConvencionesII

Introducción **2**

1. Preliminares **5**
1.1. Extensiones integrales 5
1.1.1. Dimensión 6
1.2. Algebras afines 7
1.2.1. Correspondencia entre variedades y $\mathbb{K}$-álgebras 10
1.3. Grado de trascendencia 11

2. Primeras reducciones **13**
2.1. Empezando por los Campos 14
2.2. Subiendo a la Cerradura Algebraica 16
2.2.1. El caso Complejo implica inyectividad 17

3. Morfismos Inyectivos y el caso Complejo **20**
3.1. Morfismos entre Variedades de igual Dimensión 20
3.1.1. Morfismos Jacobianos 20
3.1.2. Morfismos Finitos y Morfismos Dominantes 22
3.2. Morfismos Inyectivos 23

4. Las Derivadas **28**
4.0.1. Núcleo de una Derivación 31
4.1. Derivaciones localmente Nilpotentes 31
4.1.1. Exponencial de una derivación localmente nilpotente 32
4.1.2. Derivaciones Localmente nilpotentes y anillos de Polinomios . . . 34

5. Condición del Jacobiano en el contexto Algebraico **39**
5.1. Ramificación 39
5.1.1. Ramificación en maximales 39
5.1.2. Condiciones totalmente Algebraicas 41

Bibliografía **46**

Notación y Convenciones

- Todos los anillos son conmutativos y tienen identidad, denotada por 1.
- Las letras $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ se reservan para los naturales, los enteros los racionales, los reales , los complejos y los enteros módulo p respectivamente.
- Sea R, un anillo $U(R)$ es el conjunto de elementos invertibles de R.
- Sea R, un dominio $Q(R)$ es su campo de fracciones.
- Sea R subanillo de un anillo S. Si $s \in S$, $R[s]$ es el mínimo subanillo de S que contiene a R y a s.
- Si R es un anillo, y J un ideal de R. $\sqrt{J} := \{r \in R : \text{existe} \quad n \quad \text{tal que} \quad r^n \in J\}$.
- Si $\mathbb{K}$ es un campo $\overline{\mathbb{K}}$ es una clausura algebraica de $\mathbb{K}$.
- Si $\mathbb{K}$ es un campo, $\mathbb{K}^* = \mathbb{K} \setminus 0$.
- Si W, es una variedad algebraica y $X \subset W$, $\overline{X}$ es la clausura de Zariski de X en W.
- Si R es un anillo y A una R-algebra, siempre se supondrá que el morfismo de R a A es inyectivo.

Agradecimientos

La redacción de este documento se realizó en el marco de un proyecto financiado por la Facultad de Ciencias de la Universidad de los Andes. La parte "Digitación" del documento se realizó por el asistente del proyecto Camilo Andrés Soler.

Introducción

En 1939 el matemático Aleman Ott-Heinrich Keller en su publicación titulada "Ganze Cremona-Transformationen" formuló una pregunta sobre funciones polinomiales de los enteros en si mismos, la idea central en la pregunta de Keller es tratar de caracterizar algebraicamente cuando una función polinomial es biyección con inversa polinomial. Esta pregunta se puede generalizar a dominios con campo de cocientes de característica cero y a esta generalización se le conoce como "Problema generalizado de Keller". El propósito central de este trabajo es exponer en forma clara, breve y con herramientas no sofisticadas del álgebra conmutativa los resultados actuales sobre la pregunta de Keller, que hasta el día de hoy es un problema abierto.

El problema de Keller es el siguiente:

Dados Sea $\mathbb{Z}[x_1, ..., x_n]$ el anillo de polinomios en n variables sobre $\mathbb{Z}$. Una *función polinomial* es una función $F = (f_1, ..., f_n) : \mathbb{Z}^n \to \mathbb{Z}^n$ de la forma

$$(a_1, ..., a_n) \mapsto (f_1(a_1, ..., a_n), ..., f_n(a_1, ..., a_n))$$

Donde cada f_i es un elemento de $\mathbb{Z}[x_1, ..., x_n]$. Una función polinomial F se dice *invertible* si existe una función polinomial $G : \mathbb{Z}^n \to \mathbb{Z}^n$ tal que $x_i = g_i(f_1, ..., f_n)$ para todo $1 \leq i \leq n$. Se verifica fácilmente que la noción de ser invertible es equivalente a la siguiente igualdad:

$$\mathbb{Z}[x_1, ..., x_n] = \mathbb{Z}[f_1, ..., f_n] \tag{1}$$

Respecto a la definición anterior surge la pregunta: ¿Existe algún método sencillo para saber cuando F es invertible?

Encontrar una condición necesaria es algo sencillo, ya que si F fuera invertible y si denotamos JF la matriz

$$(\frac{df_i}{dx_j})_{1 \leq i,j \leq n}$$

Utilizando la regla de la cadena obtendríamos que JF es invertible, que por supuesto es equivalente a que su determinante sea 1 o -1. Nótese que si cambiamos $\mathbb{Z}$, por un dominio arbitrario R (Problema generalizado de Keller), la conclusión sería entonces que $Det(JF)$ pertenece a las unidades de R. Ahora la pregunta es, ¿es ésta una condición suficiente?. Si pensamos primero en el caso en que la característica de R es $p > 0$ la respuesta es no. Tome $n = 1$ y $F(X) = X - X^p$ en este caso $Det(JF) = 1$, pero aquí todo el anillo primo va al cero.

Por lo anterior podemos asumir que la característica de R es cero. En este caso si $n = 1$ es fácil ver que la condición es suficiente, ya que si $F'(X) \in U(R)$, $F(X)$ es un polinomio lineal no constante con coeficiente líder unidad, por tanto invertible. Sin embargo el caso $n \geq 2$, es un problema abierto que tiene como caso particular la famosa Conjetura del Jacobiano:

Conjetura del Jacobiano. Sea $F : \mathbb{C}^n \to \mathbb{C}^n$ Polinomial. Si $Det(JF) \in \mathbb{C}^*$, entonces

$$\mathbb{C}[x_1, ..., x_n] = \mathbb{C}[f_1, ..., f_n]. \tag{2}$$

Pensando solamente en el caso complejo, la pregunta podría ser mas general, como por ejemplo, ¿que pasa si F fuera analítica?. Desafortunadamente en la función

$$F(x, y) = (e^x, ye^{-x})$$

$Det(JF) = 1$ y no es inyectiva. Peor aún se puede encontrar $F : \mathbb{C}^2 \to \mathbb{C}^2$ analítica en cada componente, inyectiva, con $Det(JF) = 1$, pero no sobreyectiva. Lo anterior como veremos en el capítulo tres es imposible para funciones polinomiales. Así, la conjetura del Jacobiano debe depender de propiedades específicas de los polinomios en característica cero.

A pesar de la sencillez de la pregunta hecha por Keller, por ahora no sea a podido dar alguna respuesta. Hasta el momento se han publicado varias pruebas que finalmente resultaron fallidas. El intento mas reciente se dio en enero de este año, cuando la profesora Carolyn Dean del departamento de Matemáticas de Michigan, después de siete años de trabajo en el caso $n = 2$, al parecer había encontrado una prueba libre de errores. Desafortunadamente al poco tiempo del gran anuncio se le encontró una falla a el argumento de Dean, que hasta hoy no se ha podido corregir.

En la literatura actual las referencias mas completas sobre el problema de Keller son: [B], [E], [W]. Todas estas reúnen los resultados mas recientes sobre el problema, desafortunadamente se utiliza un nivel de sofisticación no accequible al publico matemático general. En principio, en este trabajo se obtienen algunos de estos resultados con herramientas básicas del álgebra conmutativa.

En el primer capítulo se recuerdan algunos resultados del álgebra conmutativa y de la geometría algebraica afín que serán necesarios a lo largo de este trabajo. En el segundo capítulo, básicamente se reduce el problema de Keller a el caso de campos algebraicamente cerrados y allí se da un primer acercamiento al campo de los números complejos. En el tercer capítulo se estudian los morfismos entre variedades afines de igual dimensión, y con esto se logra el primer resultado; si el grado de F es menor o igual a dos la conjetura es cierta. También en este capítulo se verifica que la conjetura del Jacobiano y el problema de Keller son enunciados equivalentes. Ya para este punto la idea es utilizar la estructura analítica que tiene $\mathbb{C}$, sumándole a esto el estudio de las derivaciones que son similares la derivada usual sobre los complejos. Finalmente la condición $Det(JF) = 1$ se cambia por una condición algebraica equivalente y con esto se encuentra una prueba sencilla del Lema (5.8), que hasta el momento sólo se tenía gracias a que cierto módulo era plano, resultado que necesitaba una gran maquinaria.

En resumen este trabajo es auto contenido y permite una breve introducción a la conjetura del Jacobiano, con pruebas novedosas pero sencillas de algunos de los resultados mas relevantes sobre la misma.

Capítulo 1

Preliminares

1.1. Extensiones integrales

Proposición 1.1. *Sea R un subanillo de un dominio entero S, y supongamos que S es integral sobre R. Entonces S es campo si y solo si R es campo.*

Demostración.
($\Leftarrow$) Supongamos que R es campo. Sea $s \in S, \quad s \neq 0$. Entonces como s es integral sobre $R, \quad s$ es algebraico sobre $R. \quad R(s) = R[s] \subseteq S$ así el campo $R(s)$ esta contenido en S pero $s^{-1} \in R(s)$ así $s^{-1} \in R$.
($\Rightarrow$) Supongamos que S es campo. Sea $r \in R, \quad r \neq 0$ entonces $r^{-1} \in S$ y como S es integral sobre R existen $a_0, ..., a_{n-1}$ elementos de R tales que $(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + ... + a_0 = 0$. Multiplicado por r^{n-1} se ve que $r^{-1} = -(a_{n-1}) + ... + a_1 r^{n-2} + a_0 r^{n-1} \in R$. $\square$

Corolario 1.2. *Sea R un subanillo de un anillo S, y supongamos que S es integral sobre R. Sea $Q \in Spec(S)$ y $P := Q \cap R$. Entonces Q es maximal en S si y solo si P lo es en R.*

Demostración. R/P se puede ver como un subanillo de S/Q y dado que S es integral sobre R es fácil ver que S/Q es integral sobre R/P; ahora por el lema anterior R/P es campo si y solo si S/Q es campo. $\square$

Teorema 1.3. *(Lying-over)*

Sea R un subanillo de un anillo S, y supongamos que S es integral sobre R. Dado $P \in Spec(R)$, existe $Q \in Spec(S)$ tal que $Q \cap R = P$.

Demostración. Ver [AM] □

Teorema 1.4. *(Going-up)*

Sea R un subanillo de un anillo S, y supongamos que S es integral sobre R. Sean m, n naturales con $m < n$. Sea

$$P_0 \subsetneq P_1 \subsetneq, ..., \subsetneq P_{n-1} \subsetneq P_n$$

una cadena de ideales primos de R y supongamos que

$$Q_0 \subsetneq Q_1 \subsetneq, ..., \subsetneq Q_{m-1} \subsetneq Q_m$$

es una cadena de primos de S tal que $Q_i \cap R = P_i$, para todo $i = 0, ..., m$. Entonces es posible extender la ultima cadena por ideales primos $Q_{m+1}, ..., Q_n$ de S, de manera que $Q_i \cap R = P_i$

Demostración. Utilizando (1.3) inducctívamente se tiene el resultado. □

1.1.1. Dimensión

Definición 1.5. Sea R un anillo.

1. Una cadena

$$P_0 \subsetneq P_1 \subsetneq, ..., \subsetneq P_n$$

de primos de R se dice que tiene longitud n si esta compuesta por $n+1$ eslabones.

2. La dimensión de R, denotada por $dim(R)$, es definida como

$$Sup\{n \in \mathbb{N} : \text{existe cadena de primos de longitud n en } R\}$$

3. Dado $P \in Spec(R)$, la *altura* de P, denotada por $ht(P)$ se define como el supremo de la longitud de cadenas definimos:

$$P_0 \subsetneq P_1 \subsetneq, ..., \subsetneq P_{n-1} \subsetneq P_n = P.$$

Lema 1.6. *Sea R un anillo de dimensión finita y sea $P \in Spec(R)$. Entonces $ht(P) + dim(R/P) \leq dim(R)$.*

Demostración. Es claro de la correspondencia reticular entre $Spec(R/P)$ y los primos de R que contienen a P. □

Teorema 1.7. *Sea R un subanillo de un anillo R, y supongamos que S es integral sobre R. Entonces $dim(R) = dim(S)$*

Demostración. Es una consecuencia directa de (1.4). Para una demostración detallada ver [AM] capítulo 5. □

1.2. Algebras afines

Un polinomio $f \in \mathbb{K}[x_1, ...x_n]$ con coeficientes en un campo $\mathbb{K}$ define una función $f : \mathbb{K}^n \longrightarrow \mathbb{K}$; el valor de f en un punto $(a_1, ..., a_n) \in \mathbb{K}^n$ se obtiene sustituyendo a_i por x_i en f. La función definida por f se llama *función polinomial*. Si $\mathbb{K}$ es infinito, entonces la única función polinomial que se anula en todo $\mathbb{K}^n$ es el polinomio cero. Por esto si $\mathbb{K}$ es infinito distintos polinomios definen diferentes funciones. Así, $\mathbb{K}[x_1, ..., x_n]$ se puede ver como el anillo de funciones polinomiales sobre $\mathbb{K}^n$.

Dado un subconjunto $I \subseteq \mathbb{K}[x_1, ..., x_n]$, se define un *subconjunto algebraico o variedad algebraica* de $\mathbb{K}^n$ por:

$$\mathbb{Z}_{\mathbb{K}}(I) = \{(a_1, ..., a_n) \in \mathbb{K}^n : f(a_1, ..., a_n) = 0 \quad \text{para toda } f \in I\}.$$

Dada la definición de $\mathbb{Z}_{\mathbb{K}}(I)$, es claro que $\mathbb{Z}_{\mathbb{K}}(I) = \mathbb{Z}_{\mathbb{K}}(\langle I \rangle)$.

Si $V = \mathbb{Z}_{\mathbb{K}}(I)$ es un conjunto algebraico un *subconjunto algebraico* $W \subseteq V$ es un conjunto de la forma $W = \mathbb{Z}_{\mathbb{K}}(J)$ para algún ideal J.

Ahora dado $V \subseteq \mathbb{K}^n$, se define

$$I(V) = \{f \in \mathbb{K}[x_1, ..., x_n] : f(a_1, ..., a_n) = 0 \quad \text{para toda } (a_1, ..., a_n) \in V\}$$

Es claro que $I(V)$ es un ideal. Una *función regular* sobre V es por definición una función polinomial de $\mathbb{K}^n$ restringida V. Identificando polinomios si ellos coinciden sobre V, se obtiene el *anillo coordenado* $\mathbb{K}[V]$ de V. De la definición es claro que

$$\mathbb{K}[V] = \mathbb{K}[x_1, ..., x_n]/I(V).$$

Definición 1.8. Si R es un anillo y $J \subseteq R$ es un ideal, entonces el conjunto

$$rad(J) := \{f \in R : f^n \in I \quad \text{para algún } n \text{ natural}\}$$

se denomina el *radical de J*.

Es fácil ver que $rad(I)$ es un ideal que contiene a J. Un ideal I se llama *radical* si y solo si $I = rad(I)$. Por lo anterior, R/I es libre de nilpotentes $\Leftrightarrow$ I es radical. Es fácil ver que si $X \subseteq \mathbb{K}^n$, $I(X)$ es radical; de aquí se puede deducir que no toda imagen homomorfa de $\mathbb{K}[x_1, ..., x_n]$ es un anillo de coordenadas

Teorema 1.9. *(Ceros de Hilbert)*

Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Si $I \subseteq \mathbb{K}[x_1, ..., x_n]$ es un ideal, entonces

$$I(Z_{\mathbb{K}}(I)) = \sqrt{I}.$$

Así, las correspondencias $I \mapsto Z_{\mathbb{K}}(I)$ y $X \mapsto I(X)$ inducen una biyección entre las colecciones de subconjuntos algebraicos de $\mathbb{K}^n$ e ideales radicales de $\mathbb{K}[x_1, ..., x_n]$

Demostración. Ver [K] □

Definición 1.10. Un anillo se dice *reducido* si es libre de nilpotentes.

Corolario 1.11. *Si $\mathbb{K}$ es un campo algebraicamente cerrado y A es una $\mathbb{K}$-algebra entonces, $A = \mathbb{K}[V]$ para algún conjunto algebraico V si y solo si A es finitamente generada y reducida.*

Corolario 1.12. *Sea $\mathbb{K}$ un campo algebraicamente cerrado y sea $V \subseteq \mathbb{K}^n$ un subconjunto algebraico. Todo Maximal de $\mathbb{K}[V]$ es de la forma $M_P = \langle x_1 - a_1, ..., x_n - a_n\rangle / I(V)$ para algún $P = (a_1, ..., a_n) \in \mathbb{K}^n$. En particular, los puntos de V están en correspondencia biyectiva con los maximales de $\mathbb{K}[X]$.*

Demostración. Es suficiente ver el caso en el que $\mathbb{K}[X] = \mathbb{K}[x_1, ..., x_n]$, es decir cuando $X = \mathbb{K}^n$. Sea M maximal de $\mathbb{K}[x_1, ..., x_n] entonces \quad I(Z_{\mathbb{K}}(M)) = M$ ya que todo primo es radical. Sea $P \in Z_{\mathbb{K}}(M)$ entonces $I(P) \supseteq I(Z_{\mathbb{K}}(M)) = M$. Como M es maximal y $1 \notin I(P)$ se tiene que $I(P) = M$. Ahora, $\langle x_1 - a_1, ..., x_n - a_n\rangle \subseteq I(P)$ y es un maximal, entonces

$$\langle x_1 - a_1, ..., x_n - a_n\rangle = I(P) = M.$$

□

Teorema 1.13. *(Ceros de Hilbert versión algebraica).*
Sea $\mathbb{K}$ un campo y L una extensión de $\mathbb{K}$. Dados elementos $\alpha_1, ..., \alpha_n$ de L tales que $\mathbb{K}[\alpha_1, ..., \alpha_n]$ es un campo, entonces $\alpha_1, ..., \alpha_n$ son algebraicos sobre $\mathbb{K}$

Demostración. Ver [K]. □

Definición 1.14. Un anillo R se dice de *Jacobson* si para todo ideal $I \subseteq R$

$$\bigcap_{P \supseteq I} P = \bigcap_{M \supseteq I} M$$

$$P \in Spec(R) \quad M \in Max(R)$$

Lema 1.15. *Sea R un anillo y sea I un ideal propio de R, entonces:*

$$\sqrt{I} = \bigcap_{\substack{P \in Spec(R) \\ P \supseteq I}} P.$$

Demostración. □

Proposición 1.16. *Sea $\mathbb{K}$ un campo algebraicamente cerrado, A un anillo de coordenadas, entonces A es de Jacobson.*

Demostración. Es suficiente ver que $\mathbb{K}[x_1, ..., x_n]$ es de Jacobson. Sea $I \subseteq \mathbb{K}[x_1, ..., x_n]$ unideal y sea $V = Z_{\mathbb{K}}(I)$. entonces

$$V = \bigcup_{x \in V} \{x\}$$

$$I(V) = \bigcap_{x \in V} I(\{x\}) = \bigcap_{x \in V} M_x$$

$$\bigcap_{x \in V} M_x \supseteq \bigcap_{M \supseteq I} M$$

$$M \in Max(R)$$

$$I(V) = I(Z_{\mathbb{K}}(I)) = \sqrt{I}$$

Ahora,

$$\sqrt{I} = \bigcap_{\substack{P \in Spec(R) \\ P \supseteq I}} P.$$

$$\bigcap_{\substack{P \in Spec(R) \\ P \supseteq I}} P \supseteq \bigcap_{\substack{M \in Max(R) \\ M \supseteq I}} M.$$

La igualdad es inmediata ya que todo maximal es primo. □

1.2.1. Correspondencia entre variedades y $\mathbb{K}$-álgebras

Dadas $V \subseteq \mathbb{K}^n$ y $W \subseteq \mathbb{K}^m$, variedades algebraicas, la funciones mas naturales entre ellas son las restricciones polinomiales, tales funciones

$$F : V \longrightarrow W$$

son llamadas morfismos de variedades.

Todo morfismo $F : V \longrightarrow W$ de variedades induce

$$F^* : \mathbb{K}[W] \longrightarrow \mathbb{K}[V],$$

$$g \mapsto g \circ F$$

un homomorfismo de $\mathbb{K}$-algebras entre sus anillos de coordenadas.

Teorema 1.17. *Sean V y W variedades como antes. Dado $G : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$, homomorfismo de $\mathbb{K}$-algebras, existe un morfismo $F : V \longrightarrow W$. Tal que $F^* = G$.*

Demostración. Si $f_0 + I(V) = G(y_j + I(W))$ para $j = 1, ..., m$ donde $\mathbb{K}[W] = \mathbb{K}[y_1, ..., y_m]/I(W)$. Podemos construir la función polinomial

$$F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$$

$$(a_1, ..., a_n) \longmapsto (f_1(a_1, ..., a_n), ..., f_m(a_1, ..., a_n))$$

1. $F(V) \subseteq W$. Sea $a \in V$, para ver que $F(a) \in W$ es suficiente ver que $F(a) \in Z_{\mathbb{K}}(I(W))$.

2. Sea $h(y_1, ...y_m) \in I(W)$ entonces;

   $h(F(a)) = h(f_1(a), f_2(a), ..., f_m(a)) = \quad h(G_1(y_1)(a), G_2(y_2)(a), ..., G_m(y_m)(a)) = G(h)(a).$

   Dado que $h \in I(W)$, $\quad G(h) = 0$ en $\mathbb{K}[V]$; es decir, $G(h) \in I(V)$ y como $a \in V$, $G(h)(a) = 0$. Ahora es inmediato de la definición que $F^* = G$.

□

1.3. Grado de trascendencia

Para una explicación detallada de bases de trascendencia ver [Lan2]

Definición 1.18. Sean $\mathbb{K}_1, \mathbb{K}_2$ campos tales que $\mathbb{K}_1 \subseteq \mathbb{K}_2$; $trad_{\mathbb{K}_1}(\mathbb{K}_2)$ es el *grado de trascendencia* de $\mathbb{K}_2$ sobre $\mathbb{K}_1$. Este es el cardinal de cualquier base de trascendencia para $\mathbb{K}_2$ sobre $\mathbb{K}_1$.

Teorema 1.19. *Sea $\mathbb{K}$ un campo y A un dominio integral que es una $\mathbb{K}$-algebra finitamente generada. Entonces:*

1. *$dim(A) = Trad_{\mathbb{K}}(\mathbb{Q}(A))$.*

2. *Para todo $P \in Spec(A)$, $ht(P) + dim(A/P) = dim(A)$.*

Demostración. Ver [AM] o [K].

□

Capítulo 2

Primeras reducciones

Conjetura de Keller: Sea R un dominio de característica cero, y sean $f_1, f_2, ..., f_n$ elementos de $R[x_1, x_2, ..., x_n]$ tales que, haciendo $F := (f_1, f_2, ..., f_n)$

$$J(F) := (\frac{df_i}{dx_j})_{i,j} \tag{2.1}$$

es una Matriz invertible en $R[x_1, x_2, ..., x_n]$ o equivalentemente que su determinante es unidad de R; entonces

$$R[f_1, f_2, ..., f_n] = R[x_1, x_2...x_n]. \tag{2.2}$$

Observación 2.1. *Es claro que si $J(F)$ es una matriz invertible sobre $R[x_1, x_2, ..., x_n]$, $J(F)(a_1, a_2, ..., a_n)$ es una matriz invertible sobre R para todo $(a_1, a_2, ..., a_n) \in R^n$. No obstante, el converso no se tiene a menos que R sea un campo algebraicamente cerrado.*

Ejemplo 2.2. *Sea $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 + x$. Su derivada es invertible para todo valor en $\mathbb{R}$ pero su inversa no es polinomial.*

2.1. Empezando por los Campos

Evidentemente una motivación para la Conjetura de Keller es el teorema de la función inversa. Por esto en el estudio de la conjetura un punto inicial sería tratar de ver los polinomios como funciones sobre R y además, que propiedades como que $J(F)$ sea invertible dependan de sus valores sobre R como función polinomial. Desafortunadamente como vimos en el ejemplo anterior esto no siempre se tiene, por esto en este capítulo se desarrollan las primeras herramientas para llegar a los campos algebraicamente cerrados donde si podemos contar con estas ventajas.

Teorema 2.3. *Es suficiente probar la conjetura de Keller en el caso en que R es campo.*

Demostración. Podemos suponer que $f_i(0,....,0) = 0$ por medio de la sustitución $f^i = f_i$-$f_i(0,....,0)$. Entonces $f_i = r_{i1}x_1 + r_{i2}x_2, ..., +r_{in}x_n + P_i(x_1, x_2, ..., x_n)$. Donde los términos de P_i son de grado mayor o igual a 2, por lo tanto

$$(\frac{df_i}{dx_j})(0,....,0) = r_{ij}. \tag{2.3}$$

Si $A = (r_{ij})_{i,j}$ entonces $Det(J(f))$ evaluado en $(0, 0, ..., 0)$ es $Det(A)$, así por hipótesis A es una matriz invertible sobre R. Entonces haciendo el cambio de variable $\vec{Y} = A\vec{x}$ claramente

$$R[x_1, x_2.....x_n] = R[Y_1, Y_2.....Y_n].$$

Cada f_i ahora depende de $(Y_1, Y_2, ...Y_n)$ y por la regla de la cadena $(\frac{df_i}{dx_j})_{i,j}$ sigue cumpliendo las hipótesis, y $f_i = Y_i + P_i$ tiene sólo términos de grado mayor o igual a dos.

$$Si \quad \mathbb{K} = \mathbb{Q}(R), \quad \mathbb{K}[Y_1, Y_2.....Y_n] = \mathbb{K}[f_1, f_2..., f_n], \quad \text{y por tanto} \tag{2.4}$$

$$Y_i = \sum C_{j1,\ldots,jn} f_1^{j1} f_2^{j2} \cdots f_n^{jn}.$$

Mostremos que los $C_{j1,\ldots,jn}$ están en R. Para ver esto defina un buen orden sobre $\mathbb{N}^n$ de la manera siguiente. Primero sea $V = (a_1, a_2, \ldots a_n)$ un elemento de $\mathbb{N}^n$ entonces definimos $V_k = (a_1, a_2, \ldots a_k, 0 \ldots, 0)$ y la norma de V, $\|V\|_1 = \sum_{j=1}^{n} a_i$. Se define entonces el orden $V < W$ si ocurre alguna de las siguientes:

1. $\|V\| < \|W\|$

2. Existe k tal que $1 \leqq k < n$ con:

   a) $\|V_k\| < \|W_k\|$

   b) $\|V_j\| = \|W_j\|$, $n \geq j > k$

Se puede ver inductivamente que $<$ es un orden lineal. Si no ocurriera que $V < W$ y que $W < V$ entonces $\|V\| = \|W\|$; ahora, si $\|V_{n-1}\| < \|W_{n-1}\|$ entonces, como $\|V_n\| = \|W_n\|$, se tiene $V < W$. Análogamente se ve que $\|W_{n-1}\| < \|V_{n-1}\|$ no es posible. Así, inductívamente, es claro que $\|V_k\| = \|W_k\| \; \forall k$, $1 \leqq k \leqq n$ lo que claramente implica que $V = W$. Dado que solo existen finitas tuplas con una norma dada, el orden definido es un buen orden sobre $\mathbb{N}^n$.

Ahora, dado

$$Y_i = \sum C_{j1,\ldots,jn} f_1^{j1} f_2^{j2} \cdots f_n^{jn}$$

se mostrará por inducción en el orden definido que los $C_{j1}, \ldots, _{jn}$ están en R.

1. Caso base: $C_{0,\ldots,0} = 0$ que es un elemento de R.

2. Paso inductivo: Supongamos que todo $C_{j1}, \ldots, C_{jn} \in R$ para toda tupla $(j_1, \ldots, j_n) < (i_1, \ldots, i_n)$, donde $(i_1, \ldots, i_n)$ es una tupla fija. Como

$$Y_i = \sum_{(j_1,\ldots,j_n)<(i_1,\ldots,i_n)} C_{j1,\ldots,jn} f_1^{j1} f_2^{j2} \cdots f_n^{jn} + \sum_{(j_1,\ldots,j_n)\geq(i_1,\ldots,i_n)} C_{j1,\ldots,jn} f_1^{j1} f_2^{j2} \cdots f_n^{jn}$$

Entonces por hipótesis de inducción tendríamos que

$$\sum_{(j_1,...,j_n)\geq(i_1,...,i_n)} C_{j1,...,jn} f_1^{j1} f_2^{j2} \cdots f_n^{jn} \in R[Y_1,...,Y_n]$$

En este último polinomio, como $f_i = Y_i + ...$ cosas de grado grado mayor el monomio $Y_1^{i1}Y_2^{i2},...,Y_n^{in}$ aparece con coeficiente $C_{i1}, C_{i2}, ..., C_{in}$ por esto él esta en R.

Por lo anterior cada $Y_i \in R[f_1,...,f_n]$ y entonces $R[Y_1,...,Y_n] = R[f_1,...,f_n]$. □

2.2. Subiendo a la Cerradura Algebraica

En este punto ya estamos en capacidad de pasar al caso algebraicamente cerrado.

Teorema 2.4. *Es suficiente probar la conjetura de Keller en el caso en que $K := R$ es un campo algebraicamente cerrado.*

Demostración. Sea $\bar{K}$ una clausura algebraica de K. Sean $f_1,...,f_n$ elementos de $K[x_1,...,x_n]$ tales que $\bar{K}[f_1,...,f_n] = \bar{K}[x_1,...,x_n]$. Entonces existen $G_1,...,G_n \in \bar{K}[f_1,...,f_n]$ tales que

$$X_i = G_i(f_1,...,f_n).$$

Sea L una extensión finita de K que contenga todos los coeficientes de los G_i's y sea de Galois sobre K. Siempre puedo hallarse ya que K es perfecto.
$G = Gal(L/K)$ actua naturalmente sobre $L[X_1,...,X_n]$ de la siguiente forma. Dado $g \in G$, sea $\hat{g} : L[X_1,...,X_n] \to L[X_1,...,X_n]$ la extension natural del isomorfismo $g : L \to L$.

$$|G|X_i = \sum_{g\in G} X_i^{\hat{g}} = \sum_{g\in G} G_i^{\hat{g}}(f_1^{\hat{g}},...,f_n^{\hat{g}}) =$$
$$\sum_{g\in G} G_i^{\hat{g}}(f_1,...,f_n) = \sum(\sum_{g\in G}(C_{j1,...,jn})^g) f_1^{j1},...,f_n^{jn}.$$

Donde $G_i(Y_1,...,Y_n) = \sum C_{j1,...,jn}Y_1^{j1},...,Y_n^{jn}$. Obviamente $\sum_{g\in G}(C_{j1,...,jn})^g \in Fix(G) = K$ luego $|G|X_i \in K[f_1,...,f_n]$ y por tanto $X_i \in K[f_1,...,f_n]$ para todo $1 \leqq i \leqq n$, así $K[X_1,...,X_n] = K[f_1,...,f_n]$. □

2.2.1. El caso Complejo implica inyectividad

Por todo lo anterior supondremos de ahora en adelante que $f_1,...,f_n \in K[X_1,...,X_n]$, K es un campo algebraicamente cerrado de característica cero. $(f_1(\bar{0}),...,f_n(\bar{0})) = (0,...,0)$ y Det(J(F)) $\in K$. A los f_i´s les podemos asociar una función polinomial

$$F : K^n \to K^n$$

$$(x_1,...,x_n) \mapsto (f_1(x_1,...,x_n),...,f_n(x_1,...,x_n)),$$

un morfismo entre variedades irreducibles de la misma dimensión.

Lema 2.5. *F es un isomorfismo polinomial si y solo si $K[f_1,...,f_n] = K[x_1,...,x_n]$.*

Demostración. 1. Si $K[f_1,...,f_n] = K[x_1,...,x_n]$ para todo $1 \leqq i \leqq n$, existe $g_i \in K[x_1,...,x_n]$ tal que $x_i = g_i(f_1,...,f_n)$. Entonces

$$G : K^n \to K^n$$

$$(x_1,...,x_n) \mapsto (g_1(\bar{x}),...,g_n(\bar{x}))$$

es el morfismo inverso de $\bar{F}$.

2. Si $F : K^n \to K^n$ es un isomorfismo con inversa G definida por unos $g_i's$, las funciones polinomiales $g_i(f_1(X_1,...,X_n),...,f_n(X_1,...,X_n)) - X_i$ Tienen a K^n como su conjunto de ceros. Por el teorema de los ceros de Hilbert son la función cero así

$$K[f_1,...,f_n] = K[x_1,...,x_n].$$

□

Proposición 2.6. *Supongamos que la conjetura de Keller se cumple para $\mathbb{C}$. Si $F : K^n \to K^n$ como antes y K es algebraicamente cerrado de característica cero, entonces F es inyectivo.*

Demostración.

1. Sea K_0 el subcampo de K generado por los coeficientes de F; entonces $trad(K_0/\mathbb{Q}) < \aleph_0$ y por esto existen subcampo $\hat{\mathbb{K}_0}$ de $\mathbb{C}$ y un isomorfismo $\varphi : K_0 \longrightarrow \hat{\mathbb{K}_0}$ isomorfismo. Restringiendo F a K_0, la puedo ver como función de K_0^n en K_0^n y allí sigue cumpliendo que $Det(J(F)) \in K_0^*$. Ahora extendiendo φ de manera natural entre $K_0[x_1, ..., x_n]$ y $\hat{K_0}[x_1, ..., x_n]$; φ transforma a $F = (f_1, ..., f_n)$ en $\hat{F} = (\hat{f}_1, ..., \hat{f}_n)$, donde $\hat{f}_i = \varphi(f_i)$ y $\hat{F} := \varphi(F)$. Ahora $\hat{f}_i \in \mathbb{C}[x_1, ..., x_n]$ y $Det(J(\hat{F})) = \varphi(Det(J(F))) \in \hat{K_0^*} \subseteq \mathbb{C}^*$, entonces dado que estamos suponiendo que en $\mathbb{C}$ se cumple la conjetura de Keller, $\mathbb{C}[\hat{f}_1, ..., \hat{f}_n] = \mathbb{C}[x_1, ..., x_n]$. Por tanto existe $\hat{G} : \mathbb{C}^n \longrightarrow \mathbb{C}^n$, inversa polinomial para $\hat{F}$.

2. Sea K_2 un campo algebraicamente cerrado, $K \subseteq K_2$ y $trad(K_2/K) \geq trad(\mathbb{C}/\mathbb{Q})$. Sea $\hat{K}_1$ el subcampo de $\mathbb{C}$ generado $\hat{K}_0$ y los coeficientes de $\hat{G}$

$$\varphi^{-1} : \hat{K}_0 \longrightarrow K_0 \quad con \quad \hat{K}_0 \subseteq \mathbb{C} \quad K_0 \subseteq K_2$$

   Dado que K_2 tiene suficiente grado de transcendencia, φ^{-1} puede ser extendido a un isomorfismo $\psi : \mathbb{C} \longrightarrow K_2$. Si $K_1 := \psi(\hat{K}_1)$, entonces $K_0 \subseteq K_1 \subseteq K_2$. Ahora extendiendo a ψ de manera natural entre $\mathbb{C}[x_1, ..., x_n]$ y $\psi(\mathbb{C})[x_1, ..., x_n]$, ψ transforma a $\hat{G} = (\hat{g}_1, ..., \hat{g}_n)$ en $G := (g_1, ..., g_n)$, donde $g_i = \psi(\hat{g}_i)$ y $G = \psi(\hat{G})$.

   Dado esto $F : \psi(\mathbb{C})^n \to \psi(\mathbb{C})^n$ es isomorfismo polinomial con inverso G; Como $\psi(\mathbb{C})$ es algebraicamente cerrado $\psi(\mathbb{C})[f_1, ..., f_n] = \psi(\mathbb{C})[x_1, ..., x_n]$, y puesto que los coeficientes de F están en $\psi(\mathbb{C})$ esto último implica que $K_2[f_1, ..., f_n] = K_2[x_1, ..., x_n]$ lo cual es equivalente a que $F : K_2^n \to K_2^n$ es un isomorfismo, y como $K^n \subseteq K_2^n$ entonces $F : K^n \to K^n$ es inyectiva.

$$\begin{tikzcd}
 & K_2 & & \mathbb{C} \arrow[ll, tail, "\psi"'] \\
K \arrow[ur, hook] & & & \\
 & K_1 \arrow[ul, hook] & & \widehat{K}_1 \arrow[ll, tail, two heads, "\psi|_{\widehat{K}_1}"'] \arrow[uu, hook] \\
 & K_0 \arrow[u, hook] & & \widehat{K}_0 \arrow[ll, tail, two heads, "\psi^{-1}"'] \arrow[u, hook]
\end{tikzcd} \tag{2.5}$$

□

Capítulo 3

Morfismos Inyectivos y el caso Complejo

3.1. Morfismos entre Variedades de igual Dimensión

3.1.1. Morfismos Jacobianos

Sea $\mathbb{K}$ un campo algebraicamente cerrado de característica cero, y sea

$$F : \mathbb{K}^n \to \mathbb{K}^n$$

un morfismo tal que

1. $F(\bar{0}) = \bar{0}$

2. $Det(J(F)) \in \mathbb{K}^*$

se dice entonces que F cumple con la *Condición del Jacobiano.*

Conjetura 3.1. *Sea $\mathbb{K}$ un campo algebraicamente cerrado de característica cero, y sea*

$$F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$$

un morfismo que cumple la Condición del Jacobiano. Entonces F es un isomorfismo de variedades.

Teorema 3.2. *(Teorema Formal de la Función inversa) Sea* $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ *que cumple la condición del Jacobiano. Viendo a* F *como elemento de las series formales,* F *es invertible.*

Demostración. Una demostración muy sencilla de este hecho puede ser encontrada en [E], pg4. □

Para un morfismo F de $\mathbb{K}^n$ en $\mathbb{K}^n$, el homomorfismo de $\mathbb{K}$-algebras asociado es:

$$F^* : \mathbb{K}[W] \to \mathbb{K}[V] \qquad F^* : \mathbb{K}[y_1, ..., y_n] \mapsto \mathbb{K}[x_1, ..., x_n]$$
$$p(y_1, ..., y_n) \mapsto p(f_1, ..., f_n)$$

donde $V = W = \mathbb{K}^n$.

Lema 3.3. *Si* F *cumple la condición del Jacobiano entonces* F^* *es inyectivo.*

Demostración. Si $p(y_1, ..., y_n) \in Ker(F^*)$ es porque $p(f_1, ..., f_n) = 0$. Sea p un polinomio tal que $p(f_1, ..., f_n) \equiv 0$. Se probará por inducción en el grado de p que el polinomio es idénticamente nulo. Como $F(\bar{0}) = \bar{0}$, $p(0, ..., 0) = 0$, y como $p \circ F : \mathbb{K}^n \to \mathbb{K}$ es la función cero, su derivada es cero:

$$D(p \circ F) = D(p)(F) \cdot J(F) = (0, ..., 0). \tag{3.1}$$

$D(p)$ es el gradiente de p y en cada componente tiene un polinomio de grado menor que el de p, gracias a que $J(F)$ es invertible por hipótesis inductiva cada uno de estos polinomios es idénticamente nulo, y ya que estamos en característica cero p es un polinomio constante que se anula en cero, es decir $p \equiv 0$.

□

Corolario 3.4. *Si* F *cumple la condición del Jacobiano entonces los* $f_i^{'}s$ *son algebraicamente independientes sobre* $\mathbb{K}$.

3.1.2. Morfismos Finitos y Morfismos Dominantes

Lema 3.5. *Si $F : V \longrightarrow W$ es un morfismo de $\mathbb{K}$-variedades, entonces F^* es inyectivo $\iff$ $F^*(V)$ es denso en W; es decir, F es dominante.*

Demostración. Supongamos F dominante.
Sea $g \in \mathbb{K}[W]$ tal que $F^*(g) \equiv 0 \quad \Rightarrow \quad g \circ f = 0 \quad g \equiv 0$ en $F(V)$; como $F(V)$ es denso en W y g es continuo entonces $g \equiv 0$ en W.
Supongamos que $F(V)$ no es denso $C = \overline{F(V)}$ es un cerrado propio entonces existe g no cero en $\mathbb{K}[W]$ tal que $g(C) = 0 \quad F^*(g) = 0$, por tanto F^* no es inyectiva □

Corolario 3.6. *Si $F : \mathbb{K}^n \to \mathbb{K}^n$ cumple la condición del Jacobiano es un morfismo dominante.*

Proposición 3.7. *Sea $F : V \longrightarrow W$ un morfismo de variedades algebraicas tal que $\mathbb{K}[V]$ es un $F^*(\mathbb{K}[W])$-módulo finitamente generado, entonces:*

1. *F es finito a uno.*

2. *Si $V_1 \subseteq V$ es un cerrado, entonces $F(V_1)$ es cerrado de la misma dimensión.*

Demostración. Cambiando V por V_1 y W por $\overline{F(V_1)}$, $F : V_1 \longrightarrow \overline{F(V_1)}$ es denso; así $F^* : \mathbb{K}[\overline{F(V_1)}] \longrightarrow \mathbb{K}[V_1]$ es inyectivo. Entonces lo único que debemos mostrar es que F es sobreyectivo y que V y W tienen la misma dimensión.
Tenemos:

$$\mathbb{K}[W] \xrightarrow{F^*} \mathbb{K}[V]$$

y $\mathbb{K}[V]$ finitamente generado sobre $\mathbb{K}[W]$, por tanto es una extensión integral, entonces por el teorema 1.7, página 7, $dim(\mathbb{K}[W]) = dim(\mathbb{K}[V])$ y por tanto $dim(V) = dim(W)$. Ahora un punto $P \in W$ corresponde a un ideal maximal M_p de $\mathbb{K}[W]$ y por 1.12 éste es la restricción por F^* de algún maximal de $\mathbb{K}[V]$, es decir un q tal que $q \in V$, así $F(q) = p$ y F es sobre. Sea $p \in V$, $dim(p) = 0$, entonces $dim(F^*(p)) = 0$ y por tanto $F^{-1}(p)$ es finito. □

Corolario 3.8. *Sea $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ morfismo polinomial. Si $F^*(\mathbb{K}[y_1, ..., y_2]) = \mathbb{K}[f_1, ..., f_n]$ hace que $\mathbb{K}[x_1, ..., x_n]$ sea un $\mathbb{K}[f_1, ..., f_n]$-módulo finitamente generado, entonces F es sobreyectivo y finito a uno.*

Demostración. Por el lema anterior, si $\mathbb{K}[x_1, ..., x_n]$ es un $\mathbb{K}[f_1, ..., f_n]$-módulo finitamente generado, F es finito a uno y manda cerrados en cerrados. Pero ya que F es dominante, tenemos que F es sobre. □

Proposición 3.9. *F como antes, si $\mathbb{K}[x_1, ..., x_n]$ es integral sobre $\mathbb{K}[f_1, ..., f_n]$, entonces $\mathbb{K}[x_1, ..., x_n]$ es un $\mathbb{K}[f_1, ..., f_n]$-módulo finitamente generado.*

Demostración. Inmediato del hecho que $\mathbb{K}[f_1, ..., f_n][x_1, ..., x_m] = \mathbb{K}[x_1, ..., x_m]$. □

Definición 3.10. Sean $V, \quad W$ dos variedades irreducibles de igual dimensión y $F : V \longrightarrow W$ un morfismo dominante, entonces $F^* : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$ es un morfismo inyectivo de $\mathbb{K}$-algebras. Si identificamos a $\mathbb{K}[W]$ con su imagen por F^* tenemos que $\mathbb{K}[W] \subseteq \mathbb{K}[V]$ y entonces $\mathbb{K}(W) \subseteq \mathbb{K}(V)$. Ya que $trad(\mathbb{K}(V)/\mathbb{K}) = trad(\mathbb{K}(W)/\mathbb{K})$ la extensión $\mathbb{K}(W) \subseteq \mathbb{K}(V)$ es algebraica y dado que ambas son $\mathbb{K}$-algebras finitamente generadas la extensión es finita. El índice $d = [\mathbb{K}(W) : \mathbb{K}(V)]$ de esta extensión es llamado *el grado* de F.

Teorema 3.11. *Sea $\mathbb{K}$ un campo algebraicamente cerrado de característica cero y sean $V, \quad W$ $\mathbb{K}$-variedades algebraicas de igual dimensión si $F : V \longrightarrow W$ es un morfismo dominante, entonces existe U abierto no vacío de W tal que $|F^{-1}(P)| = [\mathbb{K}(V) : \mathbb{K}(W)]$ para toda $P \in U$.*

Demostración. Ver [Sha] o [MI]. □

3.2. Morfismos Inyectivos

Teorema 3.12. *Sea $V \subseteq \mathbb{K}^n$ una $\mathbb{K}$-variedad y $\varphi : V \longrightarrow V$ un morfismo inyectivo, entonces φ es sobreyectivo.*

Demostración. Sean $V = Z_{\mathbb{K}}(f_1, f_2, ..., f_m), \quad f_i \in \mathbb{K}[x_1, ..., x_n] := \mathbb{K}[\bar{x}]$.

1. φ es inyectiva si y solo si para todo $(a,b) \in V \times V$

$$g_1(a) - g_1(b) = g_2(a) - g_2(b)... = g_n(a) - g_n(b) = 0$$

implica que $\bar{a} = \bar{b}$, donde $\varphi = [g_1, ..., g_n]$.

Sea I el ideal de $\mathbb{K}[x_1, ..., x_n, y_1, ..., y_n] := \mathbb{K}[x, y]$ generado por

$f_1(\bar{x}), ..., f_m(\bar{x}), f_1(\bar{y}), .., f_m(\bar{y}), g_1(\bar{x}) - g_1(\bar{y}), ..., g_n(\bar{x}) - g_n(\bar{y})$

y $J = \langle x_1 - y_1, x_2 - y_2, ..., x_n - y_n \rangle$.

φ es inyectiva si y sólo si $Z_{\mathbb{K}}(I) \subseteq Z_{\mathbb{K}}(J)$ que por el teorema de los ceros ocurre si y sólo si $\sqrt{I} \supseteq \sqrt{J}$.

Ahora si $\sqrt{I} \supseteq \sqrt{J}$, $\sqrt{I} \supseteq J$, entonces para cada $i \in (1, ..., n)$ existe $m_i \in \mathbb{N}$ tal que $(x_i - y_i)^{m_i} \in I$; si $m = \underset{i}{Max}\{m_i\}$, tenemos que $(x_i - y_i)^m \in I$ para cada i, así para cada i existen a_{ij}, b_{ij}, c_{ij} en $\mathbb{C}[\bar{x}, \bar{y}]$ tales que

$$(x_i - y_i)^m = \sum_{j=1}^{n} a_{ij}(g_j(\bar{x}) - g_j(\bar{y})) + \sum_{j=1}^{m}(b_{ij} f_j(\bar{x})) + \sum_{j=1}^{m}(c_{ij} f_j(\bar{y})). \tag{3.2}$$

Por tanto si φ es inyectiva se cumple la ecuación(3.1). Pero si se cumple, claramente es inyectiva.

2. Si φ no fuera sobreyectiva existiría $\bar{c} \in V$ tal que

$$I_c = \langle g_1(\bar{x}) - c_1, g_2(\bar{x}) - c_2, ..., g_n(\bar{x}) - c_n, f_1(\bar{x}), ..., f_m(\bar{x}) \rangle \subseteq \mathbb{K}[x]$$

no tiene ceros en $\mathbb{K}^n$. De nuevo por el teorema de los ceros $I_c = \mathbb{K}[x]$, así que existen $p_j \in \mathbb{K}[x]$ tales que

$$1 = \sum_{j=1}^{n} p_j(g_j - c_j) + \sum_{j=1}^{m} q_j f_j \tag{3.3}$$

3. $\varphi(V) \subseteq V$

Si $\bar{a} \in V$ entonces $(g_1(\bar{a}), g_2(\bar{a}), ..., g_n(\bar{a})) \in V$; equivalentemente: $\bar{a} \in Z_{\mathbb{K}}(\langle f_1(\bar{x}), ..., f_m(\bar{x})\rangle = I$ entonces $\bar{a} \in Z_{\mathbb{K}}(\langle f_1(g_1(\bar{x}), ..., g_n(\bar{x})), ..., f_m(g_1(\bar{x}), ..., g_n(\bar{x}))\rangle = J)$, que igual que en (3.2) es equivalente a que existen $N \in \mathbb{N}$, y $P_{i,j} \in \mathbb{K}[\bar{x}]$ tales que

$$[f_i(g_1(\bar{x}), ..., g_n(\bar{x}))]^N = \sum_{j=1}^{m} P_{i,j} f_j(\bar{x}). \tag{3.4}$$

$\forall i \in (1, ..., m)$

Si $c_1, ..., c_s$ es el conjunto de numeros complejos que aparece como coeficientes de los polinomios en las ecuaciones (3.2),(3.3),(3.4), se define $A = \mathbb{Z}[c_1, ..., c_s]$ mínimo anillo contenido en $\mathbb{K}$ que contiene a $\mathbb{Z}$ y a los c_i.

Afirmación 3.13. *Existe M, ideal Maximal de A tal que $|A/M| < \aleph_0$.*

Supongamos la afirmación (3.13). Si $\Bbbk = A/M$ y si definimos $V_{\overline{\Bbbk}} = \langle x \in \overline{\Bbbk}^n | \bar{f}_1(x) = 0, ..., \bar{f_m}(x) = 0\rangle$ el conjunto de ceros en $\overline{\Bbbk}^n$, de las clases de los polinomios que definían a V (tiene sentido ya que $f_i(\bar{x}) \in A[\bar{x}]$) $V_{\overline{\Bbbk}}$ es una $\overline{\Bbbk}$-variedad. Si se restringe φ a $V_{\overline{\Bbbk}}$

$$\begin{aligned} \varphi_{\overline{\Bbbk}} : V_{\overline{\Bbbk}} &\to \overline{\Bbbk}^n \\ \bar{a} &\mapsto \varphi[\bar{a}]; \end{aligned}$$

donde $\varphi := [\bar{g_1}, \bar{g_2}, ..., \bar{g_n}]$ que esta bien definido ya que $g_i \in A[\bar{x}]$.
Pasando la ecuación (3.4) a $\overline{\Bbbk}[\bar{x}]$, indican que $\varphi_{\overline{\Bbbk}}(\mathbb{V}_{\overline{\Bbbk}}) \subseteq \mathbb{V}_{\overline{\Bbbk}}$; las ecuaciones (3.2),(3.3) vistas en $\overline{\Bbbk}[\bar{x}, \bar{y}]$ y $\overline{\Bbbk}[\bar{x}]$ respectivamente, indican que $\varphi_{\overline{\Bbbk}}$ es inyectiva pero no es sobre, lo cual es una contradicción, ya que $\mathbb{V}_{\overline{\Bbbk}}$ es un limite directo de conjuntos finitos.

Para ver la afirmación como $A = \mathbb{Z}[c_1, ..., c_s]$ es un cociente de $\mathbb{Z}[x_1, ..., x_s]$; es suficiente ver que para todo M Maximal en $\mathbb{Z}[x_1, ..., x_s]$, se tiene que $\mathbb{Z}[x_1, ..., x_s]/M$ es finito. □

Lema 3.14. *Sea M ideal Maximal de $\mathbb{Z}[x_1, ..., x_s]$ entonces $\mathbb{Z} \cap M \neq 0$.*

Demostración. Supongamos que $M \cap \mathbb{Z} = 0$, entonces podemos suponer que $\mathbb{Z}$ esta incluido en $\mathbb{Z}[x_1, ..., x_s]/M$. Si llamamos $\alpha_1, ..., \alpha_s$ las clases de $x_1, ..., x_s$ módulo M entonces el cociente es $\mathbb{Z}[\alpha_1, ..., \alpha_s] = \mathbb{Q}[\alpha_1, ..., \alpha_s]$, que al ser campo es igual a $\mathbb{Q}(\alpha_1, ..., \alpha_s)$. Por el teorema de los ceros de Hilbert $\alpha_1, \alpha_2, ..., \alpha_s$ son algebraicos sobre $\mathbb{Q}$; por tanto existen polinomios $P_i(x) \in \mathbb{Z}[x]$ tales que que $P_i(\alpha_i) = 0$. Si q_i es el coeficiente líder de cada P_i tenemos entonces que $\mathbb{Z}[\alpha_1, ..., \alpha_s]$ es una extensión entera de $\mathbb{Z}[1/q_1, ..., 1/q_s]$ por tanto de igual dimensión. Dado que $\mathbb{Z}[\alpha_1, ..., \alpha_n]$ es campo y $\mathbb{Z}[1/p_1, ..., 1/p_s]$ no lo es tenemos una contradicción. □

Corolario 3.15. *Para todo M ideal Maximal de $\mathbb{Z}[x_1, ..., x_s]$ se tiene que $|\mathbb{Z}[x_1, ..., x_s]/M| < \aleph_0$.*

Demostración. $M \cap \mathbb{Z} = \langle p \rangle$ para p primo. Si $f_1, ..., f_n \in \mathbb{Z}[x_1, ..., x_s]$ genera a M, tomando sus reducciones Módulo p,

$$\mathbb{Z}[x_1, ..., x_s]/M \cong \mathbb{Z}_p[x_1, ..., x_s]/\langle f_1, ..., f_n \rangle$$

que es un campo. De nuevo por el teorema de los ceros De Hilbert este último es de la forma $\mathbb{Z}_p[\alpha_1, ..., \alpha_s]$, donde cada α_i es algebraico sobre $\mathbb{Z}_p$ □

Teorema 3.16. *Sea $G : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ polinomial e inyectivo entonces G es un automorfismo polinomial.*

Demostración. Como es inyectivo entonces es sobre y por tanto dominante, luego

$$\hat{G} : \mathbb{K}[x_1, ..., x_n] \longrightarrow \mathbb{C}[x_1, ..., x_n]$$

es inyectivo. Ahora $\hat{G}(\mathbb{K}[x_1, ..., x_n]) = \mathbb{K}[g_1, ..., g_n]$ y por dimensiones tenemos entonces que $\mathbb{K}([x_1, ..., x_n)$ es algebraico sobre $\mathbb{K}(g_1, ..., g_n)$. Si $d = [\mathbb{K}(x_1, ..., x_n) : \mathbb{K}(g_1, ..., g_n)]$. Por 3.11 existe $U \subseteq \mathbb{K}^n$ denso tal que para toda $a \in U$ se tiene $|G^{-1}(a)| = d$, pero como G es inyectivo $d = 1$ y $\mathbb{K}(x_1, ..., x_n) := \mathbb{K}(g_1, ..., g_n)$. Por tanto para toda $i = 1, ..., n$ existen $h_i, f_i \in \mathbb{C}[\bar{y}]$ primos relativos tales que

$$x_i = f_i(g_1, ..., g_n)/h_i(g_1, ..., g_n).$$

Si $h_i \notin \mathbb{K}$ existe $(b_1^i, ..., b_n^i) \in \mathbb{K}^n$ tal que $h_i(b_1^i, ..., b_n^i) = 0$, como G es sobre existe $(a_1^i, ..., a_n^i) \in \mathbb{K}^n$ tal que $G(a_1^i, ..., a_n^i) = (b_1^i, ..., b_n^i)$. Como $x_i h_i(b_1^i, ..., b_n^i) = f_i(b_1^i, ..., b_n^i)$, tenemos que $Z_{\mathbb{K}}(h_i) \subseteq Z_{\mathbb{K}}(f_i)$. Por el teorema de los ceros existe m tal que $f_i^m = h_i q_i$ para $q_i \in \mathbb{K}[\bar{y}]$, lo cual es una contradicción ya que h_i, f_i son primos relativos. Por lo tanto $x_i \in \mathbb{K}[g_1, ..., g_n]$ para toda i, luego

$$\mathbb{K}[g_1, ..., g_n] = \mathbb{K}[x_1, ..., x_n].$$

□

Corolario 3.17. *Si la conjetura de Keller es válida en el caso complejo, entonces el caso general también es válido*

Demostración. El resultado se sigue de 2.6, página 18 y de 3.16. □

Proposición 3.18. *Sea $F : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ que cumple la condición del Jacobiano. Si el grado de F (máximo grado de sus componentes) es menor o igual a 2. Entonces F es invertible.*

Demostración. Por 2.6 es suficiente probar que F es inyectiva. Supongamos que $F(x) = F(y)$, para algunos $x, y \in \mathbb{K}^n$, $x \neq y$. Podemos asumir que $y = 0$, por medio de las siguientes sustituciones:

1. $\tilde{F}(X) = F(X + x) - F(x)$.

2. $\tilde{x} = x - y$.

Ahora si escribimos a $F = F_1 + F_2$ como suma de componentes homogéneas, para todo $t \in \mathbb{K}$ tenemos que,

$$F(xt) = tF_1(x) + t^2 F_2(x).$$

Derivando esta ecuación respecto a t

$$F_1(x) + 2tF_2(x) = JF(tx) \cdot x,$$

evaluando en $t = \frac{1}{2}$ obtenemos una contradicción.

□

Capítulo 4

Las Derivadas

Por lo que se a encontrado hasta este punto, el problema de Keller es una pregunta sobre derivadas en el anillo $A = \mathbb{C}[x_1, ..., x_n]$. Por esto el camino mas natural a seguir es estudiar anillos donde existan operadores con propiedades semejantes a las derivadas usuales sobre A. Donde, alguna propiedad semejante podría ser que todo elemento se vuelve cero al derivarlo cierto número de veces, o que se cumpla la regla de Leibniz.

Definición 4.1. Si A es una R-algebra via un morfismo $\phi : R \longrightarrow A$ una función elemento d de $Hom_R(A, A)$ (Homomorfismos de R-álgebras) es una R-*derivación* si satisface:

1. $d(fg) = fd(g) + gd(f)$

   Para todos f, g en A

2. $d \circ \phi = 0$

Por inducción fácilmente se ve que dada una derivación d, para todo n y para cada par f, g se tiene que:

$$d^n(fg) = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} d^k(f) d^{n-k}(g)$$

(donde d^k es composición k-veces).

Ejemplo: $A = R[x_1, ..., x_n]$ $\quad d := d_i$ derivada parcial usual es una *R-derivación.*

El conjunto de todas las *R-derivaciones* sobre A será notado por $Der_R(A)$. Si d, d' pertenecen a $Der_R(A)$ es fácil ver entonces que el *corchete de Lie*

$$[d, d'] := dd' - d'd$$

está también en $Der_R(A)$.

$Der_R(A)$ es naturalmente un A-módulo.

Lema 4.2. *Si X es un conjunto generador para una R-álgebra A y $d \in Der_R(A)$. Entonces d está completamente determinada por sus valores sobre X.*

Proposición 4.3. $A = R[X_1, ..., X_n]$ *entonces $Der_R R[\bar{X}]$ es un $R[\bar{X}]$-módulo libre con base $\{d_1, ..., d_n\}$*

Demostración.

1. Sea $d \in Der_R R[X]$. Definamos $d' := d - \sum d(X_i)d_i$ entonces $d'(X_i) = 0$ para cada i; así Por el lema anterior $d' = \sum_{i=1}^n d(X_i)d_i$

2. Si $\sum_{i=1}^n a_i d_i \equiv 0$ donde $a_i \in R[\bar{X}]$, aplicando esta derivación a cada X_j obtenemos que $a_j = 0$ para todo j.

□

Proposición 4.4. *Sea A un dominio y $d \in Der_{\mathbb{Z}}A$; dado $S \subseteq A$ multiplicativo, existe una única derivación $\tilde{d}$ sobre $S^{-1}A$ que extiende a d*

Demostración. 1. Existencia:

Definase $\tilde{d} : S^{-1}A \longrightarrow S^{-1}A$ como

$$\tilde{d}(a/s) := \frac{sd(a) - ad(s)}{s^2}$$

a) Veamos que $\tilde{d}$ esta bien definida.

$$\text{Si} \quad \frac{a}{s} = \frac{b}{t} \quad \text{existe} \quad \lambda \in S \quad \text{tal} \quad \text{que} \quad \lambda at = \lambda bs.$$

Aplicando la derivación d a la ecuación obtenemos

$$d(\lambda)at + \lambda td(a) + \lambda ad(t) = d(\lambda)bs + \lambda sd(b) + \lambda bd(s).$$

Multiplicando por λst obtenemos

$$\lambda^2 t^2 sd(a) + \lambda^2 stad(t) = \lambda^2 s^2 td(b) + \lambda^2 stbd(s)$$
$$\lambda^2 t^2 sd(a) + \lambda^2 s^2 bd(t) = \lambda^2 s^2 td(b) + \lambda^2 t^2 ad(s)$$
$$\lambda^2 [t^2(sd(a) - ad(s))] = \lambda^2 [s^2(td(b) - bd(t))].$$

Dado que $\lambda^2 \in S$ entonces $\tilde{d}(\frac{a}{s}) = \tilde{d}(\frac{b}{t})$. Claramente $\tilde{d}$ extiende a d

b) $\tilde{d}$ es derivación.

$$\begin{aligned}
\frac{b}{t}\tilde{d}(\frac{a}{s}) + \frac{a}{s}\tilde{d}(\frac{b}{t}) &= \frac{bsd(a) - bad(s)}{ts^2} + \frac{atd(b) - abd(t)}{st^2} \\
&= \frac{tbsd(a) - tbad(s) + satd(b) - sabd(t)}{s^2t^2} \\
&= \frac{satd(b) + stbd(a) - absd(t) - abtd(s)}{s^2t^2} \\
&= \frac{std(ab) - abd(st)}{s^2t^2} \\
&= \tilde{d}(\frac{a}{s}\frac{b}{t})
\end{aligned}$$

2. Unicidad:

   Ahora, sea d' una derivación sobre $S^{-1}A$ que extiende a d, entonces

$$d'(\frac{a}{s}) = \frac{d'(a)}{s} + ad'(\frac{1}{s})$$

$$0 = d'(1) = d'\frac{s}{s} = \frac{1}{s}d'(s) + sd'(\frac{1}{s})$$

   es decir $d'(\frac{1}{s}) = -\frac{1}{s^2}d'(s)$; por tanto, $d'(\frac{a}{s}) = \frac{d'(a)}{s} - \frac{a}{s^2 d'(s)} = \frac{sd(a)-ad(s)}{s^2}$

□

Proposición 4.5. *Sea $\mathbb{K}$ un campo de características cero, $\mathbb{K} \subseteq \mathbb{L}$ una extensión de campos de dimensión finita y d una derivación sobre $\mathbb{K}$. Entonces d puede extenderse de manera única a una derivación $\tilde{d}$ sobre $\mathbb{L}$.*

Demostración. $\mathbb{L} = \mathbb{K}[\alpha]$ para algún α algebraico sobre $\mathbb{K}$, como $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base para $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$, para algún n, es suficiente conocer el valor de $\tilde{d}(\alpha)$. Ahora, si $\alpha^n + a_{n-1}\alpha^{n-1}, ..., +a_0 = 0$, donde $X^n + a_{n-1}X^{n-1}+, ..., a_0$ es el polinomio minimal de α sobre $\mathbb{K}$, por las leyes de derivación $\tilde{d}(\alpha)$ debe ser:

$$-\frac{[d(a_{n-1})\alpha^{n-1} + d(a_{n-2})\alpha^{n-2} + ... + d(a_0)]}{[n\alpha^{n-1} + a_{n-1}(n-1)\alpha^{n-2} + ... + a_n]}.$$

□

4.0.1. Núcleo de una Derivación

Sea A un dominio de característica cero y $d : A \longrightarrow A$ una derivación sobre A. Se denota por A^d el núcleo de d. Se puede ver fácilmente que A^d es un sub-anillo de A (respectivamente un sub-campo de A, en el caso que A es campo), esta sub-estructura se llama el conjunto de constantes.

Lema 4.6. *Si A es un dominio tal que $\mathbb{Q} \subseteq A$, entonces A^d es íntegramente cerrado en A.*

Demostración. Sea $a \in A$ tal que a es integral sobre A^d. Existen entonces $c_0, ..., c_{n-1} \in A^d$ tal que $a^n + a^{n-1}c_{n-1}+, ..., +c_0 = 0$ tomando el n-minimal y aplicando d, obtenemos

$$[na^{n-1} + (n-1)c_{n-1}a^{n-2}+, ..., +c_1]d(a) = 0$$

Dada la escogencia de n, $d(a) = 0$. □

4.1. Derivaciones localmente Nilpotentes

De acá en adelante R siempre será una $\mathbb{Q}$-álgebra.

Definición 4.7. Dada una R-algebra A, un elemento d de $Der_R(A)$ se dice *localmente nilpotente* si para todo $a \in A$ existe n entero positivo tal que $d^n(a) = 0$.

4.1.1. Exponencial de una derivación localmente nilpotente

Dada $d \in Der_R(A)$ localmente nilpotente, podemos extender d a $\tilde{d}$ un elemento de $Der_R(A[X])$ definiendo $\tilde{d}(X) = 0$ y dado ésto definimos

$$\begin{aligned} exp(d) : A[X] &\longrightarrow A[X] \\ g &\mapsto \sum_{n=0}^{\infty} \frac{\tilde{d}^n(g)}{n!} X^n. \end{aligned}$$

$exp(d)$ esta bien definido ya que d es localmente nilpotente.

Proposición 4.8. *$exp(d)$ es un elemento de $HOM_R(A[X])$.*

Demostración. Claramente es R-lineal

$$\begin{aligned} exp(d)(f)exp(d)(g) &= \sum_{i=0}^{\infty} \tilde{d}^i(f) \frac{X^i}{i!} \sum_{j=0}^{\infty} \tilde{d}^j(f) \frac{X^j}{j!} \\ &= \sum_{n=0}^{\infty} (\sum_{k=0}^{n} \frac{1}{k!(n-k)!} \tilde{d}^k(f) \tilde{d}^{n-k}(g)) \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \tilde{d}^n(fg) X^n \\ &= exp(d)(fg) \end{aligned}$$

□

Note que para todo n: $exp(d)(X^n) = X^n$. Ahora, definimos

$$\begin{aligned} exp^*(d) : A[X] &\longrightarrow A[X] \\ g &\mapsto \sum_{n=0}^{\infty} \frac{\tilde{d}^{(n)}(g)(-1)^n}{n!} X^n \end{aligned}$$

Lema 4.9. *Si $\varphi = exp(d)$ y $\psi = exp^*(d)$, entonces $\psi \circ \varphi(a) = \varphi \circ \psi(a) = a$, Para todo $a \in A$.*

Demostración. Dado $a \in A$ el coeficiente de X^i en $\psi(d(a))$ es $\frac{d^{i+1}(a)(-1)^i}{i!}$, que es el coeficiente de X^i de $\tilde{d}(\psi(a))$, es decir $\tilde{d}$ y ψ conmutan; de igual forma lo hacen $\tilde{d}$ y φ por tanto para todo $a \in A \quad \psi \circ \varphi(a) = \varphi \circ \psi(a)$. Ahora, si n es el mínimo entero positivo tal que $d^n(a) \neq 0$

$$\begin{aligned}
\psi(\varphi(a)) &= \psi(\sum_{i=0}^{n} \frac{d^i(a)}{i!})X^i \\
&= \sum_{i=0}^{n} \psi[d^i(a)]\frac{X^i}{i!} \\
&= \sum_{i=0}^{n}[\sum_{j=0}^{n-i} d^j(d^i(a))(-1)^j \frac{X^j}{j!}]\frac{X^i}{i!} \\
&= \sum_{i=0}^{n}[\sum_{k=i}^{n} d^k(a)\frac{(-1)^{k-i}X^k}{(k-i)!i!}].
\end{aligned}$$

Ahora sea l fijo, $v \leq l \leq n$. Si $i \leq l$, en cada término de la suma grande el coeficiente de X^l es

$$\frac{d^l(a)(-1)^{l-i}}{(l-i)!i!}.$$

Por tanto la doble sumatoria es igual a

$$\begin{aligned}
\sum_{l=0}^{n}[\sum_{i=0}^{l} \frac{d^l(a)(-1)^{l-i}}{(l-i)!i!}]X^l = \\
a + \sum_{l=1}^{n} d^l(a)[\sum_{i=0}^{l} \frac{(-1)^{l-i}}{(l-i)!i!}]X^l = \\
a + \sum_{l=1}^{n} d^l(a)\frac{X^l}{l!}(1-1)^l = a.
\end{aligned}$$

□

Corolario 4.10. $\varphi : A[X] \longrightarrow A[X]$ *es un automorfismo con inverso* ψ.

Demostración. Sea $a_0 + a_1X+, ..., +a_mX^m \in A[X]$

$\psi(a_0 + a_1X+, ..., +a_mX^m) = \psi(a_0) + \psi(a_1)X+, ..., +\psi(a_m)X^m \quad y$

$\varphi(\psi(a_0 + a_1X+, ..., +a_mX^m)) = \varphi(\psi(a_0)) + \varphi(\psi(a_1))X+, ..., +\varphi(\psi(a_m))X^m =$

$a_0 + a_1X+, ..., +a_mX^m$. □

dado por $\varphi_a := \Pi_a \circ \varphi$

4.1.2. Derivaciones Localmente nilpotentes y anillos de Polinomios

Para cada $a \in A$ se define

$$\Pi_a : A[X] \longrightarrow A[X]$$

$$g \mapsto g(a)$$

$$y \qquad \varphi_a : A[X] \longrightarrow A[X]$$

Lema 4.11. *Sea d una derivación localmente nilpotente sobre A y s un elemento arbitrario de A; se tiene entonces que para cada a en A:*

$$a = \sum_{i=0}^{\infty} \varphi_{-s}(d^i(a))\frac{s^i}{i!}.$$

Demostración. Dado $a \in A$. Entonces $\varphi(a) \in A[X]$

$$a = \psi(\varphi(a)) = \sum_{i=0}^{\infty} \psi(d^i(a))\frac{s^i}{i!}$$

aplicando Π_s y notando que $\Pi_s(a) = a$ y $\Pi_s \circ \psi = \varphi_{-s}$ se obtiene el resultado. □

Definición 4.12. Un elemento $s \in A$ se llama *corte para d* si $d(s) = 1$

Afirmación 4.13. *Un corte s para d siempre es trascendente sobre A^d.*

Demostración. Supongamos que $\sum_{i=1}^{N} a_1 s^i = 0$ con $a_i \in A$ y N mínimo. Aplicando d se puede ver que cada $a_i = 0$. □

Teorema 4.14. *Sea d una derivación localmente nilpotente sobre A y $s \in A$ un corte para d. Entonces $A = A^d[s]$ y $d = \frac{d}{ds}$ sobre A.*

Demostración. Sea $a \in A$

$$d(\varphi_{-s}(a)) = d(\sum \frac{(-1)^i}{i!})d^i(a)s^i) =$$

$$\sum[\frac{(-1)^i}{i!}(d^{i+1}(a)s^i + d^i(a)d(s^i))] =$$

$$\sum \frac{(-1)^i}{i!}(d^{i+1}(a)s^i + id^i(a)s^{i-1}) = 0$$

Por tanto $\varphi_{-s}(a) \in A^d$, para todo $a \in A$. Entonces por el lema anterior todo elemento de A es un polinomio en s con coeficientes en A^d. □

Dada una derivación localmente nilpotente sobre A, si $d \not\equiv 0$ entonces existe $a \in A$ tal que $d(a) \neq 0$. Sea n el mínimo entero positivo tal que $d^{n+1}(a) = 0$ y sea $p = d^{n-1}(a)$, entonces $q = d(p) \neq 0$ y $d^2(p) = 0$ ($q \in A^d$). El elemento p es llamado un *pre-corte* para d.

Sea $\tilde{A} := A[q^{-1}]$ entonces la derivación d puede ser extendida de manera única $d : \tilde{A} \longrightarrow \tilde{A}$ que seguiremos llamando igual por comodidad, y esta nueva d es localmente nilpotente sobre $\tilde{A}$. Ahora, $s = \frac{p}{q}$ es un corte para d sobre $\tilde{A}$. Por las construcciones hechas es sencillo verificar que

$$\tilde{A}^d = A^d[q^{-1}] \tag{4.1}$$

Por tanto de 4.14 obtenemos que

$$\tilde{A} = A^d[q^{-1}][s] \tag{4.2}$$

y d es $\frac{d}{ds}$ sobre $\tilde{A}$.

Dado que $q \in A^d$ y que $\mathbb{Q}(A) = \mathbb{Q}(\tilde{A})$ tenemos que

$$\mathbb{Q}(A) = \mathbb{Q}(A^d)(s) \tag{4.3}$$

con s trascendente sobre $\mathbb{Q}(A)$.

Note que $A \cap \mathbb{Q}(A^d) = A^d$

Teorema 4.15. *Sea A una $\mathbb{C}$-álgebra y $A \subset B$ extension integral. Si d es una derivación sobre B tal que $d(A) \subseteq A$ y su restricción sobre A tiene anillo de constantes $\mathbb{C}$, y además es localmente nilpotente, entonces d es localmente nilpotente sobre B.*

Demostración.

Si $d \equiv 0$ sobre A no hay nada que probar.

1. Se notará d también a la restricción a A. Como A^d es campo, en este caso tenemos que $A = \tilde{A}$ así, por 4.2 obtenemos que $A = \mathbb{C}[X]$ con X trascendente sobre $\mathbb{C}$ y $d = \frac{d}{dX}$ sobre A.

2. Sea $b \in B$. Como b es integro sobre $\mathbb{C}[X]$, es algebraico sobre $\mathbb{C}(X)$, derivando la ecuación que verifica esto último es fácil ver que $d(b) \in \mathbb{C}(X, b)$ y tambien $d^i(b)$ para todo i entero positivo.

$$B_0 := \mathbb{C}[X][b, d(b), d^2(b)...]$$

Si $\mathcal{C}$ es la clausura integral de $\mathbb{C}[X]$ en $\mathbb{C}(X, b)$ como $[\mathbb{C}(X, b) : \mathbb{C}(X)]$ es finito y $\mathbb{C}[X]$ es Noetheriano, $\mathcal{C}$ es un $\mathbb{C}[X]$-modulo finitamente generado, por tanto B_0, también lo es.

Ahora, es suficiente ver que d es localmente nilpotente sobre B_0, cuyo campo de cocientes $\mathbb{C}(X, b)$ es extensión finita de $\mathbb{C}(X)$. Lo anterior es una consecuencia inmediata de la siguiente proposición tomando $B = B_0$ y $L = \mathbb{C}(X, b)$.

□

Proposición 4.16. *Dada una extension de campos finita $\mathbb{C}(X) \subseteq L$ y un subanillo B de L tal que $\mathbb{C}[X] \subseteq B$, sea d la única extension de $\frac{d}{dX}$ a L y supongamos que $d(B) \subseteq B$. Si B es un $\mathbb{C}[X]$-módulo finitamente generado entonces $B = \mathbb{C}[X]$.*

Demostración. Sea $b \in B$, como B es finito sobre $\mathbb{C}[X]$, b debe satisfacer una ecuación diferencial de la forma

$$\frac{d^n}{dX}(b) + a_{n-1}(X)\frac{d^{n-1}}{d^{n-1}X}(b) +, ..., + a_0(X)b = 0$$

Se sabe por la teoría de ecuaciones diferenciales lineales en una variable compleja, que b es analítica donde los $a_i(X)$ son analíticos, pero $a_i(X) \in \mathbb{C}[X]$ por tanto b es una función entera y algebraica sobre $\mathbb{C}(X)$, y esto último implica que b es un polinomio. ver [E1]. □

Dados elementos $f_1, f_2, ..., f_n$ en $\mathbb{C}[x_1, ..., x_n]$ tales que $F = (f_1, ..., f_n)$ cumple $Det(JF) \in \mathbb{C}^*$ y $F(\bar{0}) = \bar{0}$, podemos definir las derivaciones $(\frac{d}{df_1}, ..., \frac{d}{df_n})$ en términos de $(\frac{d}{dx_1}, ..., \frac{d}{dx_n})$. Gracias a la regla de la cadena tenemos:

$$\frac{df_1}{dx_i}\frac{d}{df_1} + \frac{df_2}{dx_i}\frac{d}{df_2} + ... + \frac{df_n}{dx_i}\frac{d}{df_n} = \frac{d}{dx_i} \tag{4.4}$$

esto para todo $1 \leq i \leq n$. Ahora estas ecuaciones son equivalentes a

$$(\frac{d}{df_1}, ..., \frac{d}{df_n}) \cdot JF = (\frac{d}{dx_1}, ..., \frac{d}{dx_n}) \tag{4.5}$$

y dado que JF es invertible

$$(\frac{d}{df_1}, ..., \frac{d}{df_n}) = (\frac{d}{dx_1}, ..., \frac{d}{dx_n})(JF)^{-1}$$

que dá cada $\frac{d}{df_i}$ en términos de los $\frac{d}{dx_j}$.

Proposición 4.17. *Dada $F = (f_1, ..., f_n)$ con $f_i \in \mathbb{C}[x_1, ..., x_n]$ y $det(JF) \in \mathbb{C}^*$. Entonces $\mathbb{C}[f_1, ..., f_n] = \mathbb{C}[x_1, ..., x_n]$ si y sólo si $\frac{d}{df_i}$ es localmente nilpotente para cada i.*

Demostración. Si $\mathbb{C}[f_1, ..., f_n] = \mathbb{C}[x_1, ..., x_n]$, es obvio.
Ahora, sea $g \in \mathbb{C}[x_1, ..., x_n]$. Como $\frac{d}{df_i}$ es localmente nilpotente $(\frac{d}{df_i})^{m_i} g = 0$ para algún m_i entero positivo. Por 3.2 puedo suponer que $g \in \mathbb{C}\big[[f_1, ..., f_n]\big]$ pero dado que $(\frac{d}{df_i})^{m_i} g = 0$, el grado de g en F_i es menor que $m_i - 1$, así $g \in \mathbb{C}[f_1, ..., f_n]$. □

Teorema 4.18. *Dado $F = [f_1, ..., f_n] \in \mathbb{C}[x_1, ..., x_n]^n$ tal que $det(JF) \in \mathbb{C}^*$, entonces las siguientes son equivalentes:*

1. $\mathbb{C}[x_1, ..., x_n] = \mathbb{C}[f_1, ..., f_n]$.

2. $\mathbb{C}[f_1, ..., f_n] \subseteq \mathbb{C}[x_1, ..., x_n]$ *es extensión entera.*

Demostración. Obviamente 1) implica 2).
Ahora, cada $\frac{d}{df_i}$ es claramente nilpotente sobre $\mathbb{C}[f_1, ..., f_n]$. Por (4.15), página 35, cada $\frac{d}{df_i}$ es localmente nilpotente y así el resultado se sigue de la proposición anterior. □

Lema 4.19. *Sean $A \subseteq B$ dominios enteros de característica cero, con campos de cocientes $\mathbb{Q}(A)$ y $\mathbb{Q}(B)$, tales que:*

- $\mathbb{Q}(B) : \mathbb{Q}(A)$ *es una extensión de Galois finita.*

- $B \cap \mathbb{Q}(A) = A$.

Sea d una derivación sobre $\mathbb{Q}(B)$ tal que $d(\mathbb{Q}(A)) \subseteq \mathbb{Q}(A)$ y $d(B) \subseteq B$. Si B es integralmente cerrado, entonces $d(C) \subseteq C$ donde C es la clausura integral de A en $\mathbb{Q}(B)$.

Demostración.

1. Sea $G := Gal\big(\mathbb{Q}(B)/\mathbb{Q}(A)\big)$ y $g \in G$. Dado que $d(\mathbb{Q}(A)) \subseteq \mathbb{Q}(A)$, la derivación gdg^{-1} coincide con la derivación d sobre $\mathbb{Q}(A)$ y así por 4.5 $gd = dg$ para todo g en G.

2. Sea $g \in G$ es claro que $g(C) \subset C$.

3. Dado que B es integralmente cerrado $C \subset B$.

4. Sea $g \in G$ entonces $gd(C) = dg(C) \subset d(C) \subset d(B) \subset B$.

5. Sea $c \in C$, y sea $P(X) := \prod_{g \in G}(X - g(d(c)))$. Dado que los coeficientes de $P(X)$ son invariantes por G, tenemos que $P(X) \in Q(A)[X]$. Mas aun de 4) obtenemos que $P(X) \in B[X]$, entonces $P(X) \in Q(A)[X] \cap B[X] = A[X]$. Dado que $d(c)$ es un cero de $P(X)$, que es mónico $d(c) \in C$, como c era arbitrario $d(C) \subset C$.

$\square$

Capítulo 5

Condición del Jacobiano en el contexto Algebraico

5.1. Ramificación

Definición 5.1. Sea $A \subseteq B$ una extensión de anillos; la extension se dice *No Ramificada* si para cada q, ideal primo de B, se tienen las siguientes propiedades:

1. $\langle q \cap A \rangle B_q = \langle q \rangle B_q$.

2. $[\frac{B_q}{\langle q \rangle} : \frac{A_{A \cap q}}{\langle A \cap q \rangle}] < \aleph_0$.

3. La extensión de campos reciduales es separable.

5.1.1. Ramificación en maximales

Definición 5.2. Dados A, B como en la definición anterior, la extensión se dice *No Ramificada para Maximales*, si las condiciones anteriores sólo se exigen para q maximal de B.

Proposición 5.3. *Sea $B = \mathbb{C}[x_1, ..., x_n]$ y $A = \mathbb{C}[f_1, ..., f_n]$ con $f_i \in B$ y $F = (f_1, ..., f_n)$ que cumplen la hipótesis Jacobiana. Entonces $A \subseteq B$ es No Ramificada para Maximales.*

Demostración.

1. Sea $M \in Max(B)$. Existe $(a_1, ..., a_n) \in \mathbb{C}^n$ tal que $M = \langle x_1 - a_1, ..., x_2 - a_2 \rangle$. Si $g_i := f_i(x_1, ..., x_n) - f_i(a_1, ..., a_n)$ claramente $g_i(a_1, ..., a_n) = 0$. Así, por el teorema de los ceros de Hilbert cada $f_i \in M$; por tanto $\langle g_1, ..., g_n \rangle = N \subseteq A \cap M$. Pero dado que N es Maximal de A obtenemos que $N = A \cap M$.

2. $B_M / \langle M \rangle = A_N / \langle N \rangle = \mathbb{C}$. Por tanto lo único a verificar es que $\langle N \rangle B_M = \langle M \rangle B_M$. Por simplicidad los llamaremos N_M y M_M respectivamente.

   Tomando la expansión de Taylor de cada f_i alrededor del punto $(a_1, ..., a_n)$ obtenemos

$$\begin{bmatrix} f_1(x_1, ..., x_n) & - & f_1(a_1, ..., a_n) \\ & . & \\ & . & \\ & . & \\ f_n(x_1, ..., x_n) & - & f_n(a_1, ..., a_n) \end{bmatrix} = J(F)(\bar{a}) \begin{bmatrix} x_1 & - & a_1 \\ & . & \\ & . & \\ & . & \\ x_n & - & a_n \end{bmatrix}$$

   módulo M^2. Localizando en M obtenemos

$$\begin{bmatrix} f_1(x_1, ..., x_n) & - & f_1(a_1, ..., a_n) \\ & . & \\ & . & \\ & . & \\ f_n(x_1, ..., x_n) & - & f_n(a_1, ..., a_n) \end{bmatrix} = J(F)(\bar{a}) \begin{bmatrix} x_1 & - & a_1 \\ & . & \\ & . & \\ & . & \\ x_n & - & a_n \end{bmatrix}$$

   módulo M_M^2. Dado que $\{x_1 - a_1, ..., x_n - a_n\}$ forma una base de $\mathbb{C}$-espacio vectorial para M_M / M_M^2 y como $J(F)(\bar{a}) \in GL_n(\mathbb{C})$, $\{f_1(\bar{x}) - f_1(\bar{a}), ..., f_n(\bar{x}) - f_n(\bar{a})\}$ también es un base para este espacio vectorial. Así por (el Lema de Nakayama [AM]), $\{f_1(\bar{x}) - f_1(\bar{a}), ..., f_n(\bar{x}) - f_n(\bar{a})\}$ genera M_M; es decir, $N_M = M_M$.

$\square$

Lema 5.4. *Si* $B = \mathbb{C}[x_1, ..., x_n]$*,* $A = \mathbb{C}[f_1, ..., f_n]$ *con* $f_i \in \mathbb{C}[x_1, ..., x_n]$ *y* $A \subseteq B$ *es No Ramificada para Maximales,* F *cumple la hipótesis Jacobiana.*

Demostración. Dado que $\mathbb{C}$ es algebraicamente cerrado es suficiente ver que $det(JF(\bar{a})) \in \mathbb{C}^*$ para todo $\vec{a} \in \mathbb{C}^n$. Sea $\vec{a} = (a_1, ..., a_n)$ elemento de $\mathbb{C}^n$. Como en la demostración de la proposición anterior,

$$\begin{bmatrix} f_1(\bar{x}) & - & f_1(\bar{a}) \\ & . & \\ & . & \\ & . & \\ f_n(\bar{x}) & - & f_n(\bar{a}) \end{bmatrix} = J(F)(\bar{a}) \begin{bmatrix} x_1 & - & a_1 \\ & . & \\ & . & \\ & . & \\ x_n & - & a_n \end{bmatrix}$$

módulo M_M^2. Que la extensión No Ramifique para Maximales implica que las dos tuplas forman una base para M_M/M_M^2 y la igualdad Matricial sólo dice que $JF(\bar{a})$ es la matriz de cambio de base, por tanto invertible. Dado que $\bar{a}$ es arbitrario se tiene el resultado. □

5.1.2. Condiciones totalmente Algebraicas

Teorema 5.5. *Si* $B = \mathbb{C}[x_1, ..., x_n]$*,* $\quad A = \mathbb{C}[f_1, ..., f_n]$ *con* $f_i \in B$*, entonces* $A \subseteq B$ *es No Ramificada para Maximales si y sólo si es No Ramificada.*

Demostración. Sea $q \in Spec(B)$

1. Dado que B es de Jacobson

$$q = \bigcap_{M \geq q} M \qquad\qquad \text{donde cada } M \in Max(B).$$

Nótese que si $q \subseteq M$ entonces $B_M \subseteq B_q$, mas aún

$$B_q = \bigcup_{N \supseteq q} B_N \qquad\qquad \text{donde cada } N \in Max(B).$$

Ahora, $\langle q\cap A\rangle B_q = \langle q\cap A\rangle \bigcup_{N\supseteq q} B_N$ pero,

$$\begin{aligned}\langle q\cap A\rangle \bigcup_{N\supseteq q} B_N &\supseteq \bigcup_{N\supseteq q}\langle q\cap A\rangle B_N\\ \bigcup_{N\supseteq q}\langle q\cap A\rangle B_N &= \bigcup_{N\supseteq q}\langle \bigcap_{M\supseteq q} A\cap M\rangle B_N\\ &= \bigcup_{N\supseteq q}\bigcap_{M\supseteq q}\langle A\cap M\rangle B_N.\end{aligned}$$

Sean M, N elementos diferentes de $Max(B)$. Por lo visto anteriormente, $A\cap M$ y $A\cap N$ son elementos de $Max(A)$; por tanto, si no ocurriera que $A\cap M\subseteq N$ se tendría que $\langle A\cap M\rangle B_N = B_N$. Si $A\cap M\subseteq N$ entonces por maximalidad $\langle A\cap M\rangle B_N = \langle A\cap N\rangle B_N$. Dado el razonamiento anterior tenemos que

$$\bigcap_{M\supseteq q}\langle A\cap M\rangle B_N = \langle A\cap N\rangle B_N = \langle N\rangle B_N,$$

ya que la extensión es no ramificada para maximales. En conclusión obtuvimos

$$\langle q\cap A\rangle B_q \supseteq \bigcup_{N\supseteq q}\langle N\rangle B_N. \tag{5.1}$$

Ahora, $\langle q\rangle B_q = \langle q\rangle \bigcup_{M\supseteq q} B_M$ que claramente contiene a $\bigcup_{M\supseteq q}\langle q\rangle B_M$. Sea $\lambda\in \langle q\rangle \bigcup_{M\supseteq q} B_M$ entonces $\lambda = \sum_{j=1}^{m}\frac{f_j}{g_j}$ donde para cada j, $f_j\in q$ y cada $g_j\notin M_j$, donde M_j es un elemento de $Max(B)$ tal que $q\subseteq M_j$. Si g es el mínimo común múltiplo de los $g_j's$, $\lambda = \frac{h}{g}$ donde $h\in q$. Es fácil ver que existe $M\in Max(B)$ con $q\subseteq M$ tal que $g\notin M$, de no ser así, $g\in q$ lo que contradice que $\lambda\in\langle q\rangle B_q$; por tanto $\lambda\in\langle q\rangle B_M$. Ahora,

$$\begin{aligned}\langle q\rangle B_q &= \bigcup_{M\supseteq q}\langle q\rangle B_M\\ &= \bigcup_{M\supseteq q}\langle \bigcap_{N\supseteq q} N\rangle M\\ &= \bigcup_{M\supseteq q}\bigcap_{N\supseteq q}\langle N\rangle B_M.\end{aligned}$$

Si $N\neq M$, $\langle N\rangle B_M = B_M$ y por tanto

$$\bigcap_{N\supseteq q}\langle N\rangle B_M = \langle M\rangle B_M$$

y así,

$$\langle q\rangle B_q = \bigcup_{M\supseteq q} \langle M\rangle B_M$$

que por (5.1) equivale a

$$\langle q\rangle B_q \subseteq \langle q\cap A\rangle B_q$$

lo cual evidentemente significa que

$$\langle A\cap q\rangle B_q = \langle q\rangle B_q.$$

2. Sea $p = A\cap q$. Verificar que la extensión $B_q/\langle q\rangle : A_p/\langle p\rangle$ es finita es verificar que la extension $\mathbb{Q}(B/q) : \mathbb{Q}(A/p)$ es finita; lo cual a su vez es equivalente a verificar que $trad_{\mathbb{C}}(\mathbb{Q}(B/q)) = trad_{\mathbb{C}}(\mathbb{Q}(A/p))$, equivalente a verificar que $dim(B/q) = dim(A/p)$.

- Sea C la clausura integral de A en B. Dado que $dim(A) = dim(B)$ y que ambas son $\mathbb{C}$-algebras finitamente generadas $\mathbb{Q}(B) : \mathbb{Q}(A)$, es una extensión finita, en particular algebraica, de donde fácilmente se deduce que $\mathbb{Q}(B) = \mathbb{Q}(C)$.
- Ahora $p_1 := q\cap C$ es un ideal primo en C y $P = p_1\cap C$. Dado que la extensión $A\subseteq C$ es integral es fácil ver que $A/p \subseteq C/p_1$ todavía es integral, de donde se deduce que $\mathbb{Q}(C/p_1)$ es algebraico sobre $\mathbb{Q}(A/p)$.
- Ahora, $C\subseteq B\subseteq \mathbb{Q}(C) = \mathbb{Q}(A)$ por lo tanto, B se obtiene de C adjuntando elementos de $\mathbb{Q}(C)$ del tipo $\frac{c_1}{c_2}$, c_1, $c_2\in C$ y no tienen factores en común,ya que B es $D.F.U.$ Como B es dominio todos los denominadores forman un subconjunto multiplicativo de C y a su vez de B. Si S es este conjunto, entonces $C\subseteq B\subseteq S^{-1}B = S^{-1}C$ y q es un ideal tal que $q\cap S = \varnothing$,

ya que si no fuera no fuera así q no sería propio en B. De lo anterior se deduce que q proviene de un ideal primo $S^{-1}q$ de $S^{-1}B$. Entonces $C/p_1 \subseteq B/q \subseteq S^{-1}B/S^{-1}q = S^{-1}C/S^{-1}\tilde{q}$, donde $S^{-1}\tilde{q} \cap C = q$, y por consiguiente $S^{-1}\tilde{q} \cap C = p_1$ de donde $\tilde{q} = p_1$.

- Es fácil ver que $\mathbb{Q}(S^{-1}C/S^{-1}\tilde{q}) = \mathbb{Q}(S^{-1}C/S^{-1}P_1)$, entonces $\mathbb{Q}(B/q) = \mathbb{Q}(C/p_1)$ que es extensión finita de $\mathbb{Q}(A/p)$.

□

Corolario 5.6. *Dados $B = \mathbb{C}[x_1, ..., x_n]$, $A = \mathbb{C}[f_1, ..., f_n]$, $F = (f_1, ..., f_n)$ y $det(JF) \in \mathbb{C}^*$. Entonces para todo $q \in Spec(B)$, si $p = A \cap q$ se tiene $ht(p) = ht(q)$.*

Demostración. Por el teorema anterior la extensión es no ramificada, entonces

$$dim(A/p) = dim(B/q)$$

o equivalentemente

$$dim(A) - ht(p) = dim(B) - ht(q)$$

es decir, $n - ht(p) = n - ht(q)$. □

Lema 5.7. *Sea R un dominio de factorización única y sean f, g elementos de R no unidades y no cero. Entonces las siguientes son equivalentes:*

1. *f, g no son primos relativos*

2. *Existe $p \in Spec(R)$ tal que $\langle f, g\rangle \subseteq p$ y $ht(p) = 1$.*

Demostración. Si f, g no son primos relativos existe $\pi \in R$ irreducible tal que $\langle f, g\rangle \subseteq \langle \pi \rangle$, claramente $ht(\langle \pi \rangle) = 1$. Supongamos que existe $p \in Spec(R)$ tal que $ht(p) = 1$ y $\langle f, g\rangle \subseteq P$, veamos que P es principal. Sea $\pi \in p \setminus 0$, como R es $D.F.U.$, $x = \pi_1^{\alpha_1} ... \pi_n^{\alpha_n}$ donde cada π_i es irreducible, como p es primo existe π_i tal que $\pi_i \subseteq p \Rightarrow \langle \pi_i \rangle \subseteq P$ como $ht(p) = 1 \Rightarrow \langle \pi_i \rangle = p$. □

Lema 5.8. *Sean $B = \mathbb{C}[x_1, ..., x_n]$, $A = \mathbb{C}[f_1, ..., f_n]$, $F = (f_1, ..., f_n)$ y $Det(JF) \in \mathbb{C}^*$. Entonces $\mathbb{Q}(A) \cap B = A$.*

Demostración. Sean h, g elementos de A primos relativos con g no cero. Si $\frac{h}{g} \in B$; entonces existe $r \in B$ tal que $h = rg$ es decir, g divide a h y por lo tanto en B no son primos relativos; por esto existe $q \in Spec(B)$ tal que $h \in q$, $g \in q$ y $ht(q) = 1$. Si $p = A \cap q$, $ht(P) = 1$ y $\langle h, g\rangle \subseteq p$ lo que contradice que h y g eran primos relativos en A. Así alguno debe ser unidad, pero para que $\frac{h}{g}$ esté en B debe ser g □

Corolario 5.9. *Sean* $B = \mathbb{C}[x_1, ..., x_n]$, $A = \mathbb{C}[f_1, ..., f_n]$, $F = (f_1, ..., f_n)$ *y* $Det(JF) \in \mathbb{C}^*$. *Si* $\mathbb{Q}(A) = \mathbb{Q}(B)$, *entonces* $A = B$.

Corolario 5.10. *Sean* $B = \mathbb{C}[x_1, ..., x_n]$, $A = \mathbb{C}[f_1, ..., f_n]$, $F = (f_1, ..., f_n)$ *y* $Det(JF) \in \mathbb{C}^*$. *Si* $\mathbb{Q}(B)$ *es una extensión de Galois de* $\mathbb{Q}(A)$ *entonces* $A = B$.

Demostración. Sean C la clausura entera de A en $\mathbb{Q}(B)$, y sea $D = \frac{d}{df_i}$.
Por el lema 4.19 tenemos que $\frac{d}{df_i}(C) \subseteq C$, así por el teorema 4.15 $\frac{d}{df_i}$ es localmente nilpotente sobre C para toda $1 \leq i \leq n$.
Entonces argumentando como en 4.17 tenemos que $C \subseteq A$, es decir $A = C$. Dado que $\mathbb{Q}(B)$ es algebraico sobre $\mathbb{Q}(A)$, $\mathbb{Q}(B) = \mathbb{Q}(C) = \mathbb{Q}(A)$ por tanto $A = B$

□

Bibliografía

[AM] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[AX] J. Ax,*The elementary theory of finite fields*, Ann. Math. 88(1968), pp 239-271.

[B] H.Bass, E.H.Connel and D,Wright, *The Jacobian conjecture*, BULL.A.M.S., 7(2)(1982), 287-330.

[E] A.van den essen,*Polynomial Automorphisms and the Jacobian conjecture*,Basel; Boston; Berlin: Birkhäuser 2000.

[E1] A.van den essen,*Differential Structure of Etale Extensions of Polynomial Algebras* Springer-Verlag, New york, 1989, Proceedings of a Microprogram Held, June 15-July 2, 1987. .

[H] Hartshorne, Robim. *Algebraic Geometry.* Springer, 1977.

[K] Kunz, Ernest. *Introduction to conmutative algebra and algebraic geometry.* Birkhäuser, 1985.

[Lan] Lang, Serge. *Introduction to algebraic geometry.* Interscience publishers 1958.

[Lan2] S.Lang, *Algebra* Addison-Wesley 1971

[MI] J.S Milne, *Algebraic Geometry.*

[Sha] Shafarevich, Igor. *Basic algebraic geometry.* Springer-Verlag, 1974.

[W] S. Wang,*on the Jacobian conjecture*, J. Algebra,65(1980),453-494.