UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIAS MATEMÁTICAS

FACULTAD DE CIENCIAS

ÁLGEBRA REAL Y SINGULARIDADES

T E S I S

QUE PARA OBTENER EL GRADO ACADÉMICO DE
MAESTRO EN CIENCIAS (MATEMÁTICAS)

P R E S E N T A

ENRIQUE ANDRADE SOLÍS

DIRECTOR DE TESIS: DR. ALBERTO LEÓN KUSHNER SCHNUR

MÉXICO D. F. NOVIEMBRE 2006

AGRADECIMIENTOS

Deseo expresar mi agradecimiento al Dr Alberto León Kushner Schnur por sugerirme el tema de tesis, por su acertada dirección, su infinita paciencia, generosidad y apoyo constante durante la elaboración de este trabajo.

Agradezco también a los miembros del jurado:

M en C José Antonio Gómez Ortega
Dr Alberto León Kushner Schnur
Dr Enrique Javier Elizondo Huerta
Dra Shirley Bromberg
Dra Adriana Ortiz Rodríguez
Dr Santiago López de Medrano Sánchez
Dr Jawad Snoussi

por sus acertados y oportunos comentarios vertidos al revisar este trabajo de tesis.

A Leonor, la compañera de mi vida, pues su apoyo ha sido para mi un estimulo constante.

Esta tesis fue posible gracias al apoyo del proyecto IN110803-3 *foliaciones geométricas y singularidades* PAPIIT.

ÍNDICE

INTRODUCCIÓN.

Uno de los objetivos de este trabajo es hacer un poco de geometría algebraica en el anillo local real de gérmenes en cero de funciones reales de variable vectorial suaves. Para ello se introducen algunos conceptos y resultados tales como germen de conjunto analítico real, coherencia de conjuntos analíticos, ideal de Malgrange, etc. En esta dirección se tiene el lema de Artin-Rees en el anillo local de gérmenes en cero de funciones suaves.

Es bien conocido que en el proceso de completación, el lema de Artin-Rees se utiliza para simplificar expresiones en las cuales se ven involucrados anillos noetherianos y sus ideales. En el caso de determinación de gérmenes, es también necesario llevar a cabo simplificaciones "similares" en las cuales se ven involucrados el álgebra local real de gérmenes en cero y sus ideales. Dado que el anillo local de gérmenes en cero no es un anillo noetheriano, no es posible usar el lema de Artin-Rees por lo que se hace necesario establecer un análogo de este resultado para el caso del anillo local de gérmenes en cero.

Como serán necesarios los conceptos y resultados del álgebra real, este trabajo se ha dividido en dos partes. La primera parte es una revisión de los seis primeros capítulos de las notas de T. Y. Lam; *An introduction to real algebra* dadas como un curso en la Sexta Escuela Latinoamericana de Matemáticas en Oaxtepec Morelos en el verano de 1982.[†)]

Los primeros tres capítulos de este trabajo constituyen esta primera parte. En el primer capítulo se desarrollan las diversas nociones de realidad para anillos conmutativos con unitario (anillos reales, semireales y locales reales). Parte de la información fue obtenida de [1], [4], [5], [7], [12], [15]y [16]; también, dado que en los últimos resultados de la primera sección (lema 1.1.31. y teorema 1.1.32.) y algunos de la segunda (corolario 1.2.23. y observación 1.2.34.) se hace uso de anillos locales regulares, se dedica el apéndice A para presentar los conceptos y resultados necesarios para la demostración de estas afirmaciones. Las referencias utilizadas aquí fueron [1], [7] y [12].

En el segundo capítulo se desarrolla la teoría de Artin y Schreier para anillos, tomando como base la de campos y se da el análogo del espectro primo de Zariski; "el espectro real de un anillo". Las referencias consultadas aquí son [2], [4], [15] y [16].

Es en el capítulo tres donde se ve la teoría de Artin-Lang para álgebras afines y sus campos de funciones y se proporcionan las versiones del teorema de los ceros de Hilbert al caso real. Aquí se da un breve repaso de teoría de campos y formas cuadráticas. Las referencias consultadas son: [1], [4], [11], [12], [13], [15] y [16].

La segunda parte de este trabajo está basada en los dos artículos *Finite determination on algebraic sets* de León Kushner y *Finite relative determination and relative stability* de León Kushner y Brasil Terra; ver las referencias [8] y [9]. Esta segunda parte, la constituye el cuarto y último capítulo de este trabajo. Aquí, se da la versión del lema de Artin-Rees del álgebra conmutativa (ver proposición 4.1.25.) al caso del anillo local real de gérmenes en cero (ver teorema 4.2.18.). Para esta segunda parte se han escrito

[†)] Estas notas aparecieron después como un artículo en la revista Rocky Mountain en 1984 (ver referencia [10].)

los tres apéndices restantes (B, C y D). Las referencias consultadas son [1], [3], [6], [14], [17], [18], [19] y [20].

1. ANILLOS REALES, SEMIREALES Y LOCALES REALES.

INTRODUCCIÓN

Se empieza este capítulo introduciendo el concepto de nivel de un anillo. Se exponen algunas propiedades y resultados importantes para el nivel de anillos; por ejemplo, el criterio global-local. En términos de este concepto se establecen las diversas nociones de realidad para anillos (anillo real, semireal y local real). En forma similar se dan algunas de las propiedades y se establecen algunos resultados sobre anillos reales, semireales, y locales reales. Aquí, como a lo largo de este trabajo, la palabra anillo significa anillo conmutativo con unitario y homomorfismo significa homomorfismo de anillos que lleva 1 a 1.

1.1. EL CONCEPTO DE NIVEL DE ANILLOS.

Sea A un anillo y S un subconjunto de A que satisface [†)]
1° Si a y b son elementos de S, entonces $ab \in S$.
2° $1 \in S$.

A tales subconjuntos se les denominan **conjuntos multiplicativamente cerrados** en A o también **conjuntos multiplicativos** en A. Si S es un conjunto multiplicativamente cerrado en A, entonces puede suceder que $0 \in S$. Un conjunto S en A que satisface

i) S es multiplicativamente cerrado en A.
ii) $0 \notin S$.

se denomina **sistema multiplicativo** en A.[‡)] Obviamente, todo sistema multiplicativo S en A es un conjunto multiplicativamente cerrado en A, pero no recíprocamente. A continuación se dan algunos ejemplos de conjuntos multiplicativamente cerrados y sistemas multiplicativos en A.

EJEMPLO 1.1.1. Si A es un dominio entero, entonces $A\backslash\{0\}$ es un sistema multiplicativo en A.

EJEMPLO 1.1.2. Si A es un anillo y P es un ideal primo de A, entonces $S=A\backslash P$ es un sistema multiplicativo en A

Más generalmente.

EJEMPLO 1.1.3. Sea A un anillo y $(P_j)_{j\in I}$ una familia de ideales primos de A, entonces $S=A\backslash\bigcup_{j\in I} P_j$ es un sistema multiplicativo en A.

[†)] S dotado de la operación de multiplicación del anillo A.
[‡)] Un sistema multiplicativo S en A es un subsemigrupo $(S , \cdot)$ de $(A , \cdot)$.

EJEMPLO 1.1.4. Sea A un anillo y S el conjunto de elementos no divisores de cero de A, entonces S es un sistema multiplicativo en A.

Si A es un anillo; se denota por $\sum \mathbf{A^2}$ el conjunto de sumas finitas de cuadrados en A, es decir,

$$\sum \mathbf{A^2} := \{ \sum_{i=1}^{n} a_i^{\,2} \mid a_i \in \mathrm{A} \}.$$

EJEMPLO 1.1.5. Sea A un anillo y S un subconjunto de A tal que $\mathrm{S}=\{1+\sum_{i=1}^{n} a_i^{\,2} \mid a_i \in \mathrm{A}\}$, entonces

a) S es un conjunto multiplicativamente cerrado en A.

b) Si además $-1 \notin \sum \mathbf{A^2}$, S es un sistema multiplicativo en A.

a) Es claro que $1 \in \mathrm{S}$. Si $a, b \in \mathrm{S}$, con $a=1+\sum_{i=1}^{n} a_i^{\,2}$ y $b=1+\sum_{j=1}^{m} b_j^{\,2}$, $a_i, b_j \in \mathrm{A}$; $i \in \{1, 2, ..., n\}$, $j \in \{1, 2, ..., m\}$, entonces

$$ab=(1+\sum_{i=1}^{n} a_i^{\,2})(1+\sum_{j=1}^{m} b_j^{\,2})$$

$$=1+\sum_{k=1}^{\tilde{n}} c_k^{\,2}$$

Luego, $ab \in \mathrm{S}$ y S es un conjunto multiplicativamente cerrado en A. b) Si $-1 \notin \sum \mathbf{A^2}$, entonces

$$1+\sum_{i=1}^{n} a_i^{\,2} \neq 0;$$

esto es, $0 \notin \mathrm{S}$. □

DEFINICIÓN 1.1.6. El **nivel** de un anillo A, escrito como *s*(A) viene dado por

$$s(\mathrm{A}) := \begin{cases} \min \left\{ k \in \mathbb{N} \,\middle|\, a_1^2 + \cdots + a_k^2 = -1, \ \text{con} \ \ a_i \in \mathrm{A}, \ \ i \in \{1, 2, ..., k\} \right\} \\ \infty \qquad\qquad \text{si} \ -1 \notin \sum \mathrm{A}^2 \end{cases}$$

es decir, el nivel de A es el menor número natural *k* tal que -1 puede escribirse como una suma de *k* cuadrados en A, o ∞ si -1 no se puede escribir como una suma finita de cuadrados. Con relación a la notación de nivel de un anillo A, la letra "*s*" en el símbolo *s*(A) proviene (como de costumbre) de la palabra alemana "*stufe*" que significa precisamente nivel. El concepto de nivel para anillos puede extenderse a ideales de anillos, es decir,

DEFINICIÓN 1.1.7. Sea A un anillo e *I* un ideal de A. El **nivel** de *I*, escrito *s*(*I*) es el nivel del anillo A/*I*, esto es, *s*(*I*)=*s*(A/*I*).

A continuación se establecen algunas propiedades para el nivel de anillos e ideales de anillos.

OBSERVACIÓN 1.1.8. Sean A, B anillos y $f:A\to B$ un homomorfismo de anillos. Si $s(A)<\infty$, entonces $s(B)<\infty$. De hecho, $s(B)\leq s(A)$.

DEMOSTRACIÓN

Es inmediata ya que $f(-1_A)=-1_B$. □

Si A es un anillo y S es un sistema multiplicativo en A, se puede definir una relación ~ en A×S como: $(a,s) \sim (b,t) \Leftrightarrow$ existe $u\in S$ con $u(ta-sb)=0$ para $(a , s), (b , t)\in A\times S$. Es sencillo verificar que ~ es una relación de equivalencia. Se denota la clase de equivalencia de la relación ~ que contiene (a,s) por $\overline{(a,s)}$ o también por $[a/s]$; y el conjunto de todas las clases de equivalencia de ~ como $S^{-1}A$. En el conjunto $S^{-1}A$ se pueden definir las operaciones de suma y multiplicación:

$$\overline{(a,s)}+\overline{(b,t)} := \overline{(at+bs,st)}$$
$$\overline{(a,s)}\cdot\overline{(b,t)} := \overline{(ab,st)}$$

para cada $\overline{(a,s)}$, $\overline{(b,t)}\in S^{-1}A$. Estas operaciones están bien definidas y el conjunto $S^{-1}A$ es dotado con una estructura de anillo, donde $\overline{(0,1)}$ y $\overline{(1,1)}$ son los elementos cero e identidad multiplicativo respectivamente, es decir, $(S^{-1}A ,+ ,\cdot)$ es un anillo denominado **anillo de cocientes** de A con respecto a S.

Si A es un anillo, se puede considerar la función $\varphi:A\to S^{-1}A$, $\varphi(a)=\overline{(a,1)}$, donde S es un sistema multiplicativo en A. φ satisface:

i) φ es un homomorfismo.

ii) $Ker(\varphi)=\{a\in A \mid \text{existe } s\in S \text{ con } sa=0\}$.

iii) Todo elemento de φ(S) es una unidad en $S^{-1}A$.

En efecto, que φ es un homomorfismo es inmediato, φ es llamado el **homomorfimo natural**. Por otro lado, $a\in Ker(\varphi)$ si y sólo si $\varphi(a)=\overline{(a,1)}=\overline{(0,1)}$; esto es equivalente a: existe $t\in S$ tal que $t(a\cdot 1-1\cdot 0)=0$. Finalmente, si $s\in S$, entonces $\varphi(s)=\overline{(s,1)}$ y su inverso es $\overline{(1,s)}$.

Si A es un dominio entero y $S=A\setminus\{0\}$; para $a, b\in A$, $s, t\in S$ se tiene que, existe $u\in S$ con $u(ta-sb)=0$ lo cual es equivalente a $ta-sb=0$. En este caso, $S^{-1}A$ construido del dominio entero A, es un campo denominado **campo de cocientes** del dominio entero A y se denota como $qf(A)$. El homomorfismo natural $\varphi:A\to S^{-1}A$ es una función inyectiva que encaja A como un subanillo del campo de cocientes. En el caso particular en que $S=A\setminus P$, con P un ideal primo de A, se tiene que, el anillo de cocientes $S^{-1}A$ es denotado como A_P y se denomina **localización** de A en P. Este anillo de cocientes tiene un único ideal maximal $PA_P:=\{\overline{(a,s)}\in A_P \mid a\in P, s\in S\}$. A los anillos A que poseen un único ideal maximal m se les denomina **anillos locales** y al campo $F=A/m$, **campo residual** de A. Así, la localización A_P es un anillo local con ideal maximal PA_P y A_P/PA_P es su campo residual.

OBSERVACIÓN 1.1.9. Sea A un anillo, S un sistema multiplicativo en A y $S^{-1}A$ el anillo de cocientes de A. Si $s(A)<\infty$, entonces $s(S^{-1}A)<\infty$.

DEMOSTRACIÓN

Se sigue directamente de la observación 1.1.8. □

OBSERVACIÓN 1.1.10. Sea A un dominio entero con campo de cocientes F. Si $s(A)<\infty$, entonces $s(F)<\infty$.

DEMOSTRACIÓN

Es un caso particular de la observación 1.1.9. □

EJEMPLO 1.1.11. Los anillos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ tienen nivel infinito. Esto es claro porque -1 no puede ser escrito como una suma finita de cuadrados en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ respectivamente.

EJEMPLO 1.1.12. El anillo $\mathbb{C}$ de números complejos tiene nivel igual a 1; esto es,

$$-1=i^2+0^2+\cdots+0^2.$$

EJEMPLO 1.1.13. El anillo $A=\mathbb{R}[x_1,\ldots,x_n]/\langle x_1^2+\cdots+x_n^2\rangle$ tiene nivel infinito.

En efecto, sea $\varphi:A\to\mathbb{R}$; $\varphi(\overline{f(x_1,\ldots,x_n)})=f(0,\ldots,0)$; claramente φ es un homomorfismo de anillos bien definido. Por la observación 1.1.8., se sigue que $s(A)=\infty$.

EJEMPLO 1.1.14. Sea $A=\mathbb{R}[x_1,\ldots,x_n]/\langle 1+x_1^2+\cdots+x_n^2\rangle$, entonces $s(A)=n$.

Supóngase que $s(A)<n$, luego

$$-\bar{1}=\overline{f_1(x)^2+\cdots+f_{n-1}(x)^2}$$

con $f_j(x)\in\mathbb{R}[x_1,\ldots,x_n]$, $j\in\{1,2,\ldots,n\text{-}1\}$. De esta forma existe $g\in\mathbb{R}[x_1,\ldots,x_n]$ tal que

$$-1=f_1(x)^2+\cdots+f_{n-1}(x)^2+g(x)(1+x_1^2+\cdots+x_n^2) \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Ahora, considérese los polinomios $f_j(x)$, $j\in\{1,2,\ldots,n\text{-}1\}$ en el anillo $\mathbb{C}[x_1,\ldots,x_n]$, entonces

$$f_j(ix)=P_j(x)+iQ_j(x) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

donde $P_j(x)$ y $Q_j(x)$ son polinomios reales pares e impares respectivamente, con $j\in\{1,\ldots,n\text{-}1\}$, e $i=\sqrt{-1}$. Sustituyendo (2) en (1) se obtiene

$$-1=\big(P_1(x)+iQ_1(x)\big)^2+\cdots+\big(P_{n-1}(x)+iQ_{n-1}(x)\big)^2+\big(Reg(ix)+iImg(ix)\big)\big(1+(ix_1)^2+\cdots+(ix_n)^2\big)$$

$$-1=\sum_{j=1}^{n-1}\big(P_j(x)^2-Q_j(x)^2+2iP_j(x)Q_j(x)\big)+\big(Reg(ix)+iImg(ix)\big)(1-x_1^2-\cdots-x_n^2)$$

$$-1=\sum_{j=1}^{n-1}\left(P_j(x)^2-Q_j(x)^2\right)+Reg(ix)(1-x_1^2-\cdots-x_n^2)+i\left[2\sum_{j=1}^{n-1}P_j(x)\,Q_j(x)+Img(ix)(1-x_1^2-\cdots-x_n^2)\right].$$

Comparando la parte real, se tiene que

$$-1=\sum_{j=1}^{n}\left(P_j(x)^2-Q_j(x)^2\right)+Reg(ix)(1-x_1^2-\cdots-x_n^2)\qquad\qquad(3)$$

Ahora, considérese la función continua $F:\mathbb{R}^n\to\mathbb{R}^{n-1}$; $F(x)=(Q_1(x),\ldots,Q_{n-1}(x))$; por el teorema de Borsuk-Ulam[†)] F colapsa un par de puntos antípodas en la esfera $S^{n-1}\subsetneq\mathbb{R}^n$, esto es, $F(a)=F(-a)$ para algún $a\in S^{n-1}$. Como $Q_j(x)$ son funciones impares, $Q_j(-x)=-Q_j(x)$ para cada índice $j\in\{1,2,\ldots,n-1\}$, se sigue que $F(-a)=-F(a)$; luego $F(a)=0$. Así, sustituyendo a en (3) se obtiene

$$-1=\sum_{j=1}^{n-1}\left(P_j(a)^2-Q_j(a)^2\right)+Reg(ia)(1-a_1^2-\cdots-a_n^2)$$

con $Q_j(a)=0$, para cada $j\in\{1,2,\ldots,n-1\}$ y $1-a_1^2-\cdots-a_n^2=0$. Entonces

$$-1=\sum_{j=1}^{n-1}P_j(a)^2\in\mathbb{R}$$

pero esto último es una contradicción. Por lo tanto se concluye que $s(A)=n$.

EJEMPLO 1.1.15. Sea $A=\mathbb{R}[x_1,\ldots,x_n]/\langle x_1^2+\cdots+x_n^2\rangle$ y $F=qf(A)$ el campo de cocientes de A. Entonces $s(F)<\infty$. De hecho se asegura que $s(F)\le n-1$.

En efecto, se desea encontrar funciones f_i, h_i con $i=1,2,\ldots,n-1$ tal que

$$-\bar{1}=\overline{\left(\frac{f_1}{h_1}\right)^2}+\overline{\left(\frac{f_2}{h_2}\right)^2}+\cdots+\overline{\left(\frac{f_{n-1}}{h_{n-1}}\right)^2}$$

entonces

$$-\bar{1}=\frac{\overline{(f_1^2h_2^2\cdots h_{n-1}^2+h_1^2f_2^2\cdots h_{n-1}^2+\cdots+h_1^2h_2^2\cdots f_{n-1}^2)}}{\overline{(h_1^2h_2^2\cdots h_{n-1}^2)}}$$

y

$$\overline{-h_1^2h_2^2\cdots h_{n-1}^2}=\overline{f_1^2h_2^2\cdots h_{n-1}^2+h_1^2f_2^2\cdots h_{n-1}^2+\cdots+h_1^2h_2^2\cdots f_{n-1}^2},$$

luego se tiene la igualdad

$$h_1^2h_2^2\cdots h_{n-1}^2+f_1^2h_2^2\cdots h_{n-1}^2+h_1^2f_2^2\cdots h_{n-1}^2+\cdots+h_1^2h_2^2\cdots f_{n-1}^2=p(x)(x_1^2+\cdots+x_n^2).$$

con $p(x)\in\mathbb{R}[x_1,\ldots,x_n]$. Si se sustituyen $h_1=x_1$, $h_2=x_1,\ldots,h_{n-1}=x_1$, $f_1=x_2$, $f_2=x_3,\ldots,f_{n-1}=x_n$ y $p(x)=(x_1^2)^{n-2}=x_1^2\cdots x_1^2$ ($(n-2)$-veces), se satisface la igualdad en la expresión anterior y se obtiene que, $s(qf(A))\le n-1$.

De los resultados de este ejemplo y del ejemplo 1.1.13., se observa que existen anillos A cuyo nivel es infinito y en cambio el nivel de su campo de cocientes $qf(A)$ es

---

[†)] **TEOREMA** (*Borsuk-Ulam*) Dada una aplicación continua $f:S^{n+1}\to\mathbb{R}^{n+1}$, existe un punto $x\in S^{n+1}$ tal que $f(x)=f(-x)$.

finito. De esta forma, el recíproco de 1.1.8. es falso en general. Se pasa ahora a establecer algunos resultados y definiciones.

Sea V un conjunto no vacío; se dice que una relación $\leq$ en V es un **orden parcial** en V si la relación es

i) **reflexiva** ($u \leq u$ para cada $u \in V$).

ii) **antisimétrica** ($u \leq v$ y $v \leq u$ entonces $u = v$, $u, v \in V$).

iii) **transitiva** ($u \leq v$ y $v \leq w$, entonces $u \leq w$ para cada $u, v, w \in V$).

Si $\leq$ es un orden parcial en V, se dice que $(V, \leq)$ es un **conjunto parcialmente ordenado**. Sea $(V, \leq)$ un conjunto parcialmente ordenado, se dice que $(V, \leq)$ es un **conjunto totalmente ordenado** si también se cumple:

iv) Para u y v elementos de V, $u \leq v$ o $v \leq u$ (comparación de elementos).

y la relación $\leq$ se denomina un **orden total** en V.

Se observa que cada subconjunto U de un conjunto parcialmente ordenado $(V, \leq)$ también es un conjunto parcialmente ordenado por la relación $\leq$. Sea U un subconjunto no vacío del conjunto parcialmente ordenado $(V, \leq)$, un elemento $v \in V$ es una **cota superior** de U si $u \leq v$ para cada $u \in U$, y un elemento $m \in V$ es un **elemento maximal** de $(V, \leq)$ si no existe $v \in V$ con $m < v$.[†)]

Con estos conceptos introducidos se puede ahora enunciar el lema de Zorn.

LEMA DE ZORN. Sea $(V, \leq)$ un conjunto no vacío parcialmente ordenado el cual tiene la propiedad de que todo subconjunto no vacío totalmente ordenado U de V tiene una cota superior en V. Entonces V tiene al menos un elemento maximal.

Como una aplicación del lema de Zorn se tiene el siguiente resultado.

PROPOSICIÓN 1.1.16. Sea A un anillo, entonces A tiene al menos un ideal maximal.

DEMOSTRACIÓN

Sea I_A la familia de todos los ideales propios de A. Como el ideal cero está en I_A, entonces $I_A \neq \varnothing$ e $(I_A, \subseteq)$ es un conjunto parcialmente ordenado. Sea I un subconjunto no vacío totalmente ordenado de I_A y considérese el conjunto $J = \bigcup_{I \in I} I$. Claramente J es un ideal propio de A y una cota superior de I en I_A.[‡)] Por el lema de Zorn, el conjunto parcialmente ordenado $(I_A, \subseteq)$ tiene al menos un elemento maximal, es decir, A tiene al menos un ideal maximal. □

Como una consecuencia de la proposición anterior, se tiene el siguiente

---

[†)] Si $(V, \leq)$ es un conjunto parcialmente ordenado, entonces para $u, v \in V$ se escribe $u < v$ si $u \leq v$ y $u \neq v$.

[‡)] Es claro que J es un subconjunto no vacío de I con la propiedad de que $ab \in J$ para cada $b \in J$ y $a \in A$. También si $a, b \in J$, existen ideales I_1, I_2 en I con $a \in I_1$ y $b \in I_2$. Dado que I está totalmente ordenado respecto a la inclusión se sigue que $I_1 \subseteq I_2$ o $I_2 \subseteq I_1$; de esta forma, $a+b$ está ya sea en I_1 o en I_2. Luego J es un ideal de A.

COROLARIO 1.1.17. Sea I un ideal propio de un anillo A, entonces existe un ideal maximal m de A tal que $I \subseteq m$.

DEMOSTRACIÓN

La demostración es similar a la de 1.1.16., con I_A la familia de ideales propios que contienen a I. □

Después de haber establecido algunas definiciones y probado algunos resultados acerca del concepto de orden, se pasa a establecer el siguiente lema que se deduce del lema de Zorn; el cual será útil en la demostración del primer resultado importante en esta sección.

LEMA 1.1.18. Sea A un anillo, S un sistema multiplicativo en A, I un ideal de A tal que $I \cap S = \emptyset$ y $\mathcal{J}$ la familia de ideales J de A con $I \subseteq J$, donde $J \cap S = \emptyset$. Entonces $\mathcal{J}$ tiene al menos un elemento maximal P que es un ideal primo de A. Si además, S satisface que $S + \sum \mathbf{A^2} \subseteq S$, se sigue que $s(qf(A/P)) = \infty$.

DEMOSTRACIÓN

Como $I \in \mathcal{J}$, entonces $\mathcal{J} \neq \emptyset$. Sea $\mathcal{J}$ un subconjunto no vacío totalmente ordenado de $\mathcal{J}$ y considérese $\mathcal{I} = \bigcup_{J \in \mathcal{J}} J$, entonces $\mathcal{I}$ es un ideal en A con la propiedad de que $I \subseteq \mathcal{I}$ e $\mathcal{I} \cap S = \emptyset$. Claramente $\mathcal{I}$ es una cota superior para $\mathcal{J}$ en $\mathcal{J}$. Por el lema de Zorn se sigue que $\mathcal{J}$ tiene al menos un elemento maximal P. P es un ideal propio de A ya que $P \cap S = \emptyset$ y $1 \in S$. Sean $a \notin P$, $b \notin P$; entonces $P \subseteq P + \langle a \rangle$ y $P \subseteq P + \langle b \rangle$; por la maximalidad de P se tiene que $(P + \langle a \rangle) \cap S \neq \emptyset$, y $(P + \langle b \rangle) \cap S \neq \emptyset$, luego existen elementos s, $s' \in S$, r, $r' \in A$ y p, $p' \in P$ tal que $s = p + ra$ y $s' = p' + r'b$, entonces $ss' = pp' + r'pb + rp'a + rr'ab$. Dado que $ss' \in S$ y $pp' + r'pb + rp'a \in P$, se sigue que $ab \notin P$; luego P es un ideal primo de A. Ahora, supóngase que $s(qf(A/P)) < \infty$, entonces

$$[-1] = ([a_1]/[b_1])^2 + \cdots + ([a_n]/[b_n])^2$$

$$[-1] = \sum_{i=1}^{n} [c_i]^2 / \prod_{i=1}^{n} [b_i]^2$$

con $[c_i]^2 = [b_1]^2 \cdots [a_i]^2 \cdots [b_n]^2$, donde $[a_i]^2$ está en la i-ésima posición, $i \in \{1, 2, \ldots, n\}$. Así, se tiene que

$$\sum_{i=1}^{n} c_i^{\,2} + \prod_{i=1}^{n} b_i^{\,2} \in P.$$

Sea $c_{n+1} = \prod_{i=1}^{n} b_i$, entonces $\sum_{i=1}^{n+1} c_i^{\,2} \in P$ pero $c_{n+1}^{\,2} \notin P$. Por la maximalidad del ideal P, $(P + \langle c_{n+1} \rangle) \cap S \neq \emptyset$; luego, existen $s \in S$, $a \in A$ y $p \in P$ tal que $s = p + ac_{n+1}$ y $s - ac_{n+1} \in P$, entonces $s^2 - a^2 c_{n+1}^{\,2} \in P$. Como $\sum_{i=1}^{n+1} a^2 c_i^2 \in P$, se sigue que

$$s^2\text{-}a^2c_{n+1}{}^2=a^2c_1{}^2+a^2c_2{}^2+\cdots+a^2c_n{}^2+s^2\text{-}a^2c_1{}^2\text{-}\cdots\text{-}a^2c_n{}^2\text{-}a^2c_{n+1}{}^2$$

$$a^2c_1{}^2+a^2c_2{}^2+\cdots+a^2c_n{}^2+s^2\text{-}a^2(c_1{}^2+c_2{}^2+\cdots+c_{n+1}{}^2)\in P.$$

De este modo,

$$a^2c_1{}^2+a^2c_2{}^2+\cdots+a^2c_n{}^2+s^2\in P;$$

también, como $a^2c_1{}^2+a^2c_2{}^2+\cdots+a^2c_n{}^2+s^2\in S+\sum\mathbf{A^2}\subseteq S$ se tiene que $S\cap P\neq\varnothing$ lo cual es una contradicción. Por lo tanto $s(qf(A/P))=\infty$. □

TEOREMA 1.1.19. Sea A un anillo. Entonces s(A)=∞, si y sólo si existe un ideal primo *P* de A con $s\big(qf(A/P)\big)=\infty$.

DEMOSTRACIÓN (⇒)

Sea $S=\{1+\sum_{i=1}^{n}a_i^{\,2}\mid a_i\in A\}\subsetneq A$. Como -1 no puede escribirse como una suma finita de cuadrados en A, se tiene que S es un sistema multiplicativo en A (ver ejemplo 1.1.5.) y $S+\sum\mathbf{A^2}\subseteq S$. Por el lema 1.1.18. se obtiene que $s(qf(A/P))=\infty$.

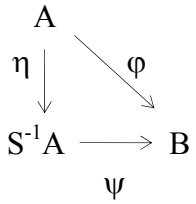
(⇐)

La condición suficiente se sigue de la observación 1.1.8. □

PROPOSICIÓN 1.1.20. Sea A un anillo, S un sistema multiplicativo en A y φ:A→B un homomorfismo de A en un anillo B que satisface: todo elemento de φ(S) es una unidad en B. Entonces existe un único homomorfismo ψ:S^{-1}A→B tal que ψ∘η=φ con η:A→S^{-1}A el homomorfismo natural.

DEMOSTRACIÓN

Defínase ψ:S^{-1}A→B; $\psi(\overline{(a,s)})=\varphi(a)\varphi(s)^{-1}$. Si $\overline{(a,s)}=\overline{(b,t)}$, con a, $b\in A$, y s, $t\in S$, entonces existe $u\in S$ tal que $u(at\text{-}sb)=0$. Luego



$$\varphi(u(at\text{-}sb))=\varphi(0)=0$$
$$\varphi(u)[\varphi(t)\varphi(a)\text{-}\varphi(s)\varphi(b)]=0.$$

Como φ(*u*) es una unidad en B, se sigue que $\varphi(a)\varphi(s)^{-1}=\varphi(b)\varphi(t)^{-1}$; así, se tiene que

$$\psi(\overline{(a,s)})=\psi(\overline{(b,t)})$$

y ψ está bien definida. Por otro lado, ψ es un homomorfismo. En efecto,

$$\begin{aligned}\psi(\overline{(a,s)}+\overline{(b,t)})&=\psi(\overline{(at+bs,st)})\\&=\varphi(at+bs)\varphi(st)^{-1}\\&=[\varphi(a)\varphi(t)+\varphi(b)\varphi(s)]\varphi(s)^{-1}\varphi(t)^{-1}\\&=\varphi(a)\varphi(s)^{-1}+\varphi(b)\varphi(t)^{-1}\\&=\psi(\overline{(a,s)})+\psi(\overline{(b,t)}).\end{aligned}$$

$$\psi(\overline{(a,s)}\ \overline{(b,t)})=\psi(\overline{(ab,st)})$$
$$=\varphi(ab)\varphi(st)^{-1}$$
$$=\varphi(a)\varphi(b)\varphi(s)^{-1}\varphi(t)^{-1}$$
$$=\psi(\overline{(a,s)})\psi(\overline{(b,t)}).$$

También se tiene que, para toda $a\in A$, el diagrama anterior conmuta, es decir,

$$\psi\circ\eta(a)=\psi(\overline{(a,1)})=\varphi(a)\varphi(1)^{-1}=\varphi(a).$$

Finalmente, se probará la unicidad de ψ. Supóngase que $\psi':S^{-1}A\to B$ es otro homomorfismo de anillos tal que $\psi'\circ\eta=\varphi$. Ya que ψ' es un homomorfismo de anillos, se tiene que

$$\psi'(\overline{(a,s)})=\psi'(\overline{(a,1)})\psi'(\overline{(1,s)}).$$

Como

$$\psi'(\overline{(a,1)})=\varphi(a)\varphi(1)^{-1}=\varphi(a) \text{ y } \psi'(\overline{(1,s)})=\varphi(1)\varphi(s)^{-1}=\varphi(s)^{-1}$$

se sigue que

$$\psi'(\overline{(a,s)})=\varphi(a)\varphi(1)^{-1}\varphi(1)\varphi(s)^{-1}=\varphi(a)\varphi(s)^{-1}=\psi(\overline{(a,s)})$$

Por lo tanto, ψ es único. □

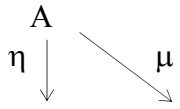
PROPOSICIÓN 1.1.21. Sea A un anillo, S un sistema multiplicativo en A, $\eta:A\to S^{-1}A$ el homomorfismo natural y $\mu:A\to B$ un homomorfismo de A en un anillo B que satisface:

a) Los elementos de $\mu(S)$ son unidades en B.

b) $Ker(\mu):=\{a\in A \mid \text{existe } t\in S \text{ con } ta=0\}$.

c) Todo elemento de B puede escribirse como $\mu(a)\mu(s)^{-1}$ para $a\in A$, $s\in S$.

Entonces existe un único isomorfismo $\psi:S^{-1}A\to B$ tal que $\psi\circ\eta=\mu$.

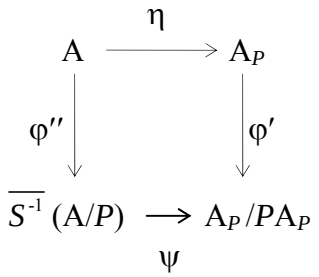


DEMOSTRACIÓN

Por la proposición 1.1.20., existe un único homomorfimo $\psi:S^{-1}A\to B$ tal que $\psi\circ\eta=\mu$. De c) se sigue directamente que ψ es supra-yectiva. Supóngase que $\overline{(a,s)}\in Ker(\psi)$ para $a\in A$, $s\in S$, entonces $\psi(\overline{(a,s)})=\mu(a)\mu(s)^{-1}=0_B$, es decir, $\mu(a)=0$; de esta forma, $a\in Ker(\mu)$. Utilizando b) se tiene que existe $t\in S$ con $ta=0$, luego $\overline{(a,s)}=\overline{(0,1)}$ en $S^{-1}A$. Por lo tanto ψ es inyectiva. □

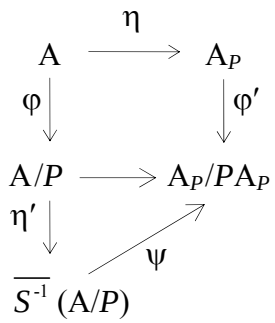
Como una aplicación de la proposición anterior, se prueba la siguiente

OBSERVACIÓN 1.1.22. Sea A un anillo, *P* un ideal primo de A, $S=A\setminus P$ y $\varphi:A\to A/P$ el homomorfismo canónico. Entonces el campo de cocientes del dominio A/P es isomorfo isomorfo al campo residual A_P/PA_P, es decir $qf(A/P)\cong A_P/PA_P$ donde $qf(A/P)=\overline{S^{-1}}(A/P)$ es el campo de cocientes del dominio entero A/P



DEMOSTRACIÓN

Es claro que $\overline{S}=\varphi(S)$ es un sistema multiplicativo en A/P, con $\overline{S}=\{s+P \mid s\in S\}$. Defínase la función $\mu: A/P \to A_P/PA_P$, $\mu(a+P)=\eta(a)+PA_P$, μ está bien definida porque η está bien definida; así, μ es un homomorfismo y el primer diagrama conmuta. Resta mostrar que μ satisface las condiciones de la proposición 1.1.21..



a) Los elementos de $\eta(S)$ son unidades en A_P y como $\eta(S)\cap PA_P=\varnothing$, los elementos de $\varphi'(\eta(S))$ son unidades en A_P/PA_P. Luego, los elementos de $\mu(\varphi(S))=\mu(\overline{S})$ son unidades en A_P/PA_P μ

b) El núcleo de φ' es PA_P y el núcleo de $\mu\circ\varphi=\varphi'\circ\eta$ es $\eta^{-1}(PA_P\cap\eta(A)) = \{a\in A \mid sa\in I$ para alguna $s\in S\}$. Así, el núcleo de μ es $\eta^{-1}(PA_P\cap\eta(A))/I$ que es precisamente el conjunto $\{\overline{a}\in(A/P)|$ existe $\overline{s}\in\overline{S}$, $\overline{s}\,\overline{a}=\overline{0}\}$

c) Finalmente, se tiene que todo elemento de A_P/PA_P puede escribirse en la forma

$$\begin{aligned}\varphi'(\eta(a)\eta(s)^{-1}) &= \varphi'(\eta(a))\varphi'(\eta(s)^{-1})^{-1}\\ &= \mu(\varphi(a))\mu(\varphi(s))^{-1}\\ &= \mu(a+P)\mu(s+P)^{-1}.\end{aligned}$$

Así, se concluye que $qf(A/P)\cong A_P/PA_P$. □

Como una consecuencia del teorema 1.1.19., se tiene uno de los resultados principales en este capítulo, el así llamado criterio global-local para el nivel de un anillo.

TEOREMA 1.1.23. (*Criterio Global-Local*) Sea A un anillo. Entonces $s(A)=\infty$ si y sólo si existe un ideal maximal m de A con $s(A_m)=\infty$.

DEMOSTRACIÓN ($\Rightarrow$)

Por el teorema 1.1.19., se sigue que existe un ideal primo P del anillo A con $s(qf(A/P))=\infty$. Como $qf(A/P)\cong A_P/PA_P$, entonces $s(A_P/PA_P)=\infty$. Nuevamente, por el teorema 1.1.19., se tiene que $s(A_P)=\infty$. Por el corolario 1.1.17., se sigue que existe un ideal maximal m de A tal que $P\subseteq m$. Considérese la localización A_m y defínase la función $\varphi: A_m \to A_P$; $\varphi([a/s])=\overline{(a,s)}$. Claramente φ está bien definida y es un homomorfismo. Como $s(A_P)=\infty$, de la observación 1.1.8., se sigue que $s(A_m)=\infty$.

($\Leftarrow$)

Es la demostración de la observación 1.1.9. □

Si A es un dominio entero con campo de cocientes F ($=qf(A)$), entonces se sabe que $s(F)\leq s(A)$; en particular $s(A)<\infty \Rightarrow s(F)<\infty$ (ver observaciones 1.1.9 y 1.1.10). Pero el recíproco no es cierto en general, es decir, existen campos de cocientes F de un dominio entero A con $s(F)<\infty$ tal que $s(A)=\infty$. Como un ejemplo se tiene el dominio entero

$A_n=\mathbb{R}[x_1,\ldots,x_n]/\langle x_1^2+\cdots+x_n^2\rangle$ con $n\geq 2$ del ejemplo 1.1.13. (para $n=1$; $A=\mathbb{R}[x]/\langle x^2\rangle$ no es un dominio entero) donde $s(A_n)=\infty$ y sin embargo $s(F)<\infty$ (ver ejemplo 1.1.15.). ¿Qué condiciones debe cumplir un anillo A para que se satisfaga $s(F)<\infty \Rightarrow s(A)<\infty$?. Antes de responder esto, se demostrarán los siguientes

LEMA 1.1.24. Sea A un anillo. Entonces $a\in A$ es una unidad de A si y sólo si para cada ideal maximal m de A, $a\notin m$.

DEMOSTRACIÓN

Es inmediata. □

LEMA 1.1.25. A es un anillo local si y sólo si el conjunto de no unidades de A es un ideal de A.

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que A es un anillo local con ideal maximal m. Por el lema anterior, m es precisamente el conjunto de no unidades de A.

($\Leftarrow$)

Supóngase que el conjunto de no unidades de A es un ideal I de A. Como $0\in I$, 0 es una no unidad de A e I es un ideal propio de A. Por la proposición 1.1.16., existe al menos un ideal maximal m de A. Por el lema 1.1.24., m consiste de no unidades de A y $m\subseteq I\subsetneq A$. Como m es un ideal maximal de A, se tiene que $m=I$. Luego, todo ideal maximal de A será igual a I. De esta forma, A es un anillo local y el único ideal maximal de A es precisamente el conjunto de no unidades de A. □

Se dice que un dominio entero A con campo de cocientes F es un **anillo de valoración** si para cada $x\in F\setminus\{0\}$, se tiene que $x\in A$ o $x^{-1}\in A$. Los anillos de valoración también son anillos locales, es decir,

LEMA 1.1.26. Sea A un anillo de valoración con campo de cocientes $F=qf(A)$, entonces A es un anillo local.

DEMOSTRACIÓN

Sea m el conjunto de no unidades de A, entonces $x\in m$ si y sólo si $x=0$ o $x^{-1}\notin A$. Si $a\in A$ y $x\in m$, se tendrá que $ax\in m$ (de lo contrario $(ax)^{-1}\in A$ y $x^{-1}=a(ax)^{-1}\in A$). Sean $x, y\in m$ con $x\neq 0$, $y\neq 0$; entonces $xy^{-1}\in A$ o $x^{-1}y\in A$. Si $xy^{-1}\in A$, entonces $x+y=(1+xy^{-1})y\in A_m\subseteq m$. Si $x^{-1}y\in A$ se tiene que $x+y\in m$. por lo tanto m es un ideal y por el lema 1.1.25., A es un anillo local. □

Para anillos de valoración se tiene el siguiente

LEMA 1.1.27. Sea A un anillo de valoración con campo de cocientes F y $\{x_1,\ldots,x_n\}$ un subconjunto en A con $x_i\neq 0$ para cada $i\in\{1,2,\ldots,n\}$. Entonces existe $i_0\in\{1,\ldots,n\}$ tal que

$x_i / x_{i_0} \in$A; para todo $i \in \{1,\ldots,n\}$.

DEMOSTRACIÓN

Escójase primero a x_i para i fija y fórmese los cocientes $x_1/x_i,\ldots, x_n/x_i$, $i \in \{1,\ldots,n\}$. Sean

$$X_i=\{(x_j/x_i) \mid (x_j/x_i)\in A \text{ con } j\in\{1,\ldots,n\}\} \text{ y}$$
$$Y_i=\{(x_j/x_i) \mid (x_j/x_i)\notin A \text{ con } j\in\{1,\ldots,n\}\}.$$

Sea i_0 tal que $\#(X_{i_0})=\max\{\#(X_1),\ldots,\#(X_n)\}$ †) Se afirma que $\#(X_{i_0})=n(\#(X_{i_0})\geq 1$ ya que $1\in X_{i_0}$. Supóngase que $\#(X_{i_0})=k<n$, es decir, en F existen k cocientes que pertenecen a A y n-k cocientes que no están en A. Se ordenan los cocientes x_1/x_{i_0}, x_2/x_{i_0} ,…, x_n/x_{i_0} de tal forma que primero aparezcan los k cocientes que están en A y después los n-k cocientes que no pertenecen al anillo A. Reindicando, se obtiene que y_1/x_{i_0}, y_2/x_{i_0} ,…, y_k/x_{i_0}, y_{k+1}/x_{i_0} ,…, y_n/x_{i_0} donde $y_1, y_2,\ldots, y_k$ son los numeradores de los k cocientes que están en A e $y_{k+1},\ldots, y_n$ los numeradores de los n-k cocientes que no están en A. Como $y_{k+1}/x_{i_0} \notin$A y A es un anillo de valoración, se sigue que $x_{i_0}/y_{k+1}\in$A. Así, $y_m/y_{k+1}\in$A con $m\in\{1, 2,\ldots, k\}$ ya que $y_m/y_{k+1}=(y_m/x_{i_0})(x_{i_0}/y_{k+1})$. Pero también $y_{k+1}/y_{k+1}\in$A; luego $\#(X_{i_0})=k+1$ lo cual contradice la elección de $k<n$. Por lo tanto, se concluye que $\#(X_{i_0})=n$, es decir, x_1/x_{i_0}, x_2/x_{i_0} ,…, $x_n/x_{i_0} \in$A. □

PROPOSICIÓN 1.1.28. Sea A un anillo de valoración con campo de cocientes F. Entonces s(F)=s(A) ya sea que s(F)<∞ o s(F)=∞.

DEMOSTRACIÓN

Supóngase que s(F)<∞, esto significa que

$$-\bar{1}=\left(\frac{\bar{b}_1}{\bar{c}_1}\right)^2+\cdots+\left(\frac{\bar{b}_n}{\bar{c}_n}\right)^2,$$

esto es,

$$-\bar{1}=\sum_{i=1}^{n}\bar{a}_i^{\,2}\Big/\prod_{i=1}^{n}\bar{c}_i^{\,2}$$

con $\bar{a}_i^{\,2}=\bar{c}_1^{\,2}\bar{c}_2^{\,2}\cdots\bar{b}_i^{\,2}\cdots\bar{c}_n^{\,2}$; luego $\prod_{i=1}^{n}\bar{c}_i^{\,2}(-\bar{1})=\sum_{i=1}^{n}\bar{a}_i^{\,2}$. Sí $\bar{a}_0^{\,2}=\prod_{i=1}^{n}\bar{c}_i^{\,2}$, entonces $\bar{a}_0^{\,2}+\sum_{i=1}^{n}\bar{a}_i^{\,2}=\bar{0}$. Por el lema anterior, se puede suponer (sin perdida de generalidad) que $a_1/a_0,\ldots,a_n/a_0\in$A. Así,

$$-1=(a_1/a_0)^2+\cdots+(a_n/a_0)^2$$

†) $\#(X_i)$ denota el número de elementos de X_i

Por lo tanto -1 es una suma finita de cuadrados en A, esto significa que, $s(A)\leq s(F)$. La igualdad $s(F)=s(A)$, se sigue de 1.1.8. o 1.1.10.. □

Se observa de la proposición anterior que $s(A)<\infty$ si y sólo si $s(F)<\infty$.

Un dominio entero A es un **dominio Prüfer** si para cada ideal maximal m de A, la localización A_m es un anillo de valoración. Para anillos Prüfer se tiene el siguiente

COROLARIO 1.1.29. Sea A un dominio Prüfer con campo de cocientes F. Entonces $s(A)<\infty$ si y sólo si $s(F)<\infty$.

DEMOSTRACIÓN ($\Rightarrow$)

Es directa de las observaciones 1.1.8. y 1.1.10.

($\Leftarrow$)

Supóngase que $s(F)<\infty$. Como A es un dominio Prüfer, entonces para cada ideal maximal m en A, A_m es un anillo de valoración con campo de cocientes $F_m=qf(A_m)$. Por la proposición 1.1.28., se tiene que $s(A_m)=s(F_m)$. Sea $\varphi:A\rightarrow A_m$, el homomorfismo natural; dado que $s(F_m)<\infty$ para cada ideal maximal m si y sólo si $s(A_m)<\infty$, para todo ideal m, entonces $s(A)<\infty$. □

Sea A un anillo y $P_0,\ldots,P_n$ ideales primos de A. Una expresión de la forma $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ es una **cadena** de ideales primos de A. Su **longitud** se define como el número de ideales en la cadena menos 1; y es un entero no negativo o ∞. La **dimensión de un anillo** A, escrita $dim(A)$ se define como el supremo de longitudes de todas las cadenas de ideales primos de A. Al igual que la longitud de una cadena, la dimensión es un número entero no negativo o ∞. También se define la **altura** de un ideal primo P, denotada $ht_A(P)$ como el supremo de las longitudes de cadenas $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ de ideales primos de A con $P_n=P$. Al igual que la longitud o la dimensión, la altura es un número entero no negativo o ∞. Se dice que un anillo A es **noetheriano** si equivalentemente se satisface que: todo ideal I de A es finitamente generado, toda familia de ideales de A tiene un elemento maximal (ahí) (*condición maximal*) o toda cadena ascendente de ideales de A es estacionaria (*condición de cadena ascendente*).[†)]

Sea (A, m) un anillo local noetheriano con campo residual $K=A/m$. Por la proposición A.4. (ver apéndice A), el K-espacio vectorial m/m^2 tiene dimensión finita y en este caso $dim(A)\leq dim_K(m/m^2)$. Los anillos para los cuales se da la igualdad anterior, serán de importancia aquí, es decir,

DEFINICIÓN 1.1.30. Un anillo local noetheriano (A, m) es un **anillo local regular** si $dim(A)=dim_K(m/m^2)$.

[†)] La **condición de cadena ascendente** establece que si $(I_i)_{i\in\mathbb{N}}$ es una familia de ideales de A tal que $I_1\subseteq I_2\subseteq\cdots I_i\subseteq I_{i+1}\subseteq\cdots$ entonces existe $k\in\mathbb{N}$ tal que $I_k=I_{k+i}$ para todo $i\in\mathbb{N}$.

Si (A, m) es un anillo local regular de dimensión d, se dice que un **sistema regular de parámetros para A** es un conjunto de d elementos que generan a m. Para más información acerca de anillos locales regulares se recomienda consultar el apéndice A. Con respecto al concepto de nivel de un anillo local regular, se tiene el siguiente

LEMA 1.1.31. Sea (A, m) un dominio entero local regular con campo de cocientes F, entonces $s(A/m)\leq s(F)$.

DEMOSTRACIÓN (por inducción sobre $dim(A)=d$)

Si d=1, por la proposición A.32., A es un anillo de valoración discreta, luego A es un anillo de valoración de una valoración discreta v de F. Por 1.1.28., se tiene que $s(A)=s(F)$ y de 1.1.8., se sigue que $s(A/m)\leq s(A)=s(F)$. Supóngase que $d>1$ y que el lema es cierto para todo anillo local regular de dimensión $< d$. Sea $\{x_1,\ldots,x_d\}$ un sistema regular de parámetros para A. Eligiendo un elemento $p\in\{x_1,\ldots,x_d\}$, se considera el anillo local noetheriano $\overline{A}=A/<p>$ con $\overline{m}=m/<p>$ su ideal maximal. Por la observación A.30., $\overline{A}$ es un anillo local regular de dimensión d-1 con campo residual $\overline{A}/\overline{m}=(A/<p>)/(m/<p>)\cong A/m$. Por la hipótesis de inducción, se tiene que $s(\overline{A}/\overline{m})=s(A/m)\leq s(qf(A/<p>))$. Dado que $qf(A/<p>)\cong A_{<p>}/<p>A_{<p>}$ (véase 1.1.22.), $ht_{A<p>}(<p>A_{<p>})=ht_A(<p>)$ (ver A.3.) y como $<p>$ es un ideal primo minimal de sí mismo, por el teorema A.21., se sigue que $ht_A(<p>)\leq 1$; luego $ht_A(<p>)=1$. Nuevamente por la proposición A.32., la localización $A_{<p>}$ es un anillo de valoración discreta y por tanto un anillo de valoración de una valoración discreta v del campo F. Por 1.1.28., se tiene que $s(A_{<p>})=s(F)$ y de la observación 1.1.8., se tiene que $s(A/m)\leq s(qf(A/<p>))=s(A_{<p>}/<p>A_{<p>})\leq s(A_{<p>})=s(F)$.[†)] □

Se dice que un anillo A es **regular** si A es noetheriano y las localizaciones A_m de A en todos los ideales maximales m de A son anillos locales regulares. A continuación, se enuncia el último resultado de esta sección.

TEOREMA 1.1.32. Sea A un dominio regular con campo de cocientes F. Entonces $s(A)<\infty$ si y sólo si $s(F)<\infty$.

DEMOSTRACIÓN

($\Rightarrow$) Ver 1.1.10..

($\Leftarrow$)

Sea P un ideal primo de A y considérese el dominio entero A/P. Como $s(F)=s(qf(A_P))<\infty$ (ver la nota de pie de pagina) y dado que $qf(A/P)\cong A_P/PA_P$ (ver observación 1.1.22.), por el lema anterior, se tiene que $s(A_P/PA_P)\leq s(qf(A_P))<\infty$. Luego por el teorema 1.1.19., se sigue que $s(A)<\infty$. □

[†)] Se sabe que si P es un ideal primo de un dominio entero A con $F=qf(A)$ su campo de cocientes y A_P es la localización de A en P, entonces $F\cong qf(A_P)$.

1.2. ANILLOS REALES, SEMIREALES Y LOCALES REALES.

En la sección anterior se comentó que existen anillos A para los cuales -1 no puede ser escrito como la suma de n cuadrados en A, para cualquier $n\in\mathbb{N}$. Ejemplos de tales anillos son: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc. Esto motiva la siguiente definición.

DEFINICIÓN 1.2.1. Un anillo A es **semireal** si $s(A)=\infty$.

Si I es un ideal de un anillo A, también se puede introducir la noción de semirealidad para I, es decir.

DEFINICIÓN 1.2.2. Sea A un anillo e I un ideal de A. Se dice que I es un **ideal semireal** si el anillo A/I es semireal.

En términos de la noción de semirealidad se pueden rescribir algunos de los resultados establecidos en la sección anterior referentes al concepto de nivel. Por ejemplo; las observaciones 1.1.8., 1.1.9. y 1.1.10. se escriben como:

OBSERVACIÓN 1.2.3. Sean A, B anillos y $\varphi:A\to B$ un homomorfismo de anillos. Si B es semireal, entonces A es semireal.

OBSERVACIÓN 1.2.4. Sea A un anillo y $S^{-1}A$ el anillo de cocientes de A con respecto a un sistema multiplicativo S en A. Si $S^{-1}A$ es semireal, entonces A es semireal.

OBSERVACIÓN 1.2.5. Si A es un anillo con campo de cocientes F y F es semireal, entonces A es semireal.

También se pueden rescribir los resultados importantes tales como los teoremas 1.1.19. y 1.1.23., proposición 1.1.28., corolario 1.1.29., lema 1.1.31. y teorema 1.1.32. Por ejemplo el teorema 1.1.19. se escribe como

TEOREMA 1.2.6. Sea A un anillo. Entonces A es semireal si y sólo si existe un ideal primo P en A con campo de cocientes $qf(A/P)$ semireal.

Sea K un subcampo del campo de los números reales, entonces si $x_1, x_2,\ldots, x_n\in K$ son tales que $\sum_{i=1}^{n} x_i^2 = 0$ con $n\in\mathbb{N}$, entonces $x_i=0$ para cada $i\in\{1, 2,\ldots,n\}$. Aquellos anillos que satisfacen una propiedad similar serán de gran importancia, es decir.

DEFINICIÓN 1.2.7. Un anillo A es **real** si siempre que $\sum_{i=1}^{n} a_i^2 = 0$ con $a_i\in A$ implica que $a_i=0$ para cada $i\in\{1,2,\ldots,n\}$.

EJEMPLO 1.2.8. Los anillos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son anillos reales.

Un ejemplo interesante de un anillo real viene dado por el siguiente

EJEMPLO 1.2.9. El anillo $\mathbb{Z}_{<p>}$ es un anillo real.

En efecto, sea

$$\mathbb{Z}_{<p>}=\{\overline{(m,n)} \mid m\in\mathbb{Z},\ n\in\mathbb{Z}\setminus<p> \text{ y } (p\ ,\ n)=1\}$$

Si

$$\overline{(m_1,n_1)^2}+\overline{(m_2,n_2)^2}+\cdots+\overline{(m_k,n_k)^2}=\overline{(0,1)}$$

con $m_1, m_2,\ldots, m_k\in\mathbb{Z}$; $n_1, n_2,\ldots, n_k\in\mathbb{Z}\setminus<p>$, entonces

$$\overline{(m_1^2,n_1^2)}+\overline{(m_2^2,n_2^2)}+\cdots+\overline{(m_k^2,n_k^2)}=\overline{(0,1)}$$

$$\overline{(m_1^2n_2^2\cdots n_k^2+n_1^2m_2^2\cdots n_k^2+\cdots+n_1^2n_2^2\cdots m_k^2,\ n_1^2n_2^2\cdots n_k^2)}=\overline{(0,1)}$$

$$(m_1n_2\cdots n_k)^2+(n_1m_2\cdots n_k)^2+\cdots+(n_1n_2\cdots m_k)^2=0.$$

Como $m_1n_2\cdots n_k,\ n_1m_2\cdots n_k,\ldots,\ n_1n_2\cdots m_k\in\mathbb{Z}$, se sigue que

$$\begin{aligned} m_1n_2\cdots n_k=0 &\Rightarrow p/m_1n_2\cdots n_k \Rightarrow p/m_1\\ n_1m_2\cdots n_k=0 &\Rightarrow p/n_1m_2\cdots n_k \Rightarrow p/m_2\\ &\ \ \vdots\\ n_1n_2\cdots m_k=0 &\Rightarrow p/n_1n_2\cdots m_k \Rightarrow p/m_k \end{aligned}$$

De esto último se obtiene que $m_i\in<p>$ para cada $i\in\{1,\ 2,\ldots,k\}$. Por lo tanto $\mathbb{Z}_{<p>}$ es un anillo real. □

Se sabe que si A es un dominio entero y $b\in A\setminus\{0\}$, entonces $A[b^{-1}]$ es un anillo ($A[b^{-1}]$ es la intersección de todos los anillos que contienen a A y b^{-1}). Sus elementos son de la forma $g=\sum_{i=1}^{n}a_ib^{-1}$. Si A es real, se tiene el siguiente

EJEMPLO 1.2.10. Si A es un dominio entero real, entonces el anillo $A[b^{-1}]$ con $b\in A\setminus\{0\}$ es real. En efecto, sean $P_1,\ldots,P_m\in A[b^{-1}]$ elementos arbitrarios, entonces $P_j=\sum_{i=0}^{n_j}a_i{}^jb^{-i}$; $j=1,\ldots,m$ puede escribirse como $P_j=\left(\sum_{i=0}^{n_j}a_i{}^jb^{n_j-i}\right)b^{-n_j}$. Si $\sum_{j=1}^{m}P_j{}^2=0$, entonces $\sum_{j=1}^{m}\left[\left(\sum_{i=0}^{n_j}a_i{}^jb^{n_j-i}\right)b^{-n_j}\right]^2=\sum_{j=1}^{m}\left(\sum_{i=0}^{n_j}a_i{}^jb^{n_j-i}\right)^2b^{-2n_j}=0$. De esto se sigue que

$$\sum_{j=1}^{m}\left(\sum_{i=0}^{n_j}a_i{}^jb^{n_j-i}\right)^2\prod_{k\neq j}^{m}b^{2n_k}\Big/\prod_{l=1}^{m}b^{2n_l}=0 \text{ y } \sum_{j=1}^{m}\left(\sum_{i=0}^{n_j}a_i{}^jb^{n_j-i}\right)^2\prod_{k\neq j}^{m}b^{2n_k}=0.$$

Como $\sum_{j=1}^{m}\left(\sum_{i=0}^{n_j} a_i{}^j b^{n_j-i}\right)^2 \prod_{k\neq j}^{m} b^{2n_k} \in$A y A es real, se obtiene que $\sum_{i=0}^{n_j} a_i{}^j b^{n_j-i} \prod_{k\neq j}^{m} b^{n_k} = 0$ para cada j=1,…, m. Dado que $\prod_{k\neq j}^{m} b^{n_k} \neq 0$ para cada j, k=1,…, m y A es un dominio entero se sigue que $\sum_{i=0}^{n_j} a_i{}^j b^{n_j-i} = 0$ para cada j=1 ,…, m. Por tanto, A[b^{-1}] es un anillo real. □

El anillo $\mathbb{Z}_p$ con $p\in\mathbb{Z}$ un número primo no es un anillo real ya que $0=1^2+\cdots+1^2$ (p sumandos). En forma similar (como se ha definido el concepto de ideal semireal) se puede introducir el concepto de ideal real para ideales de anillos, es decir;

DEFINICIÓN 1.2.11. Sea A un anillo e I un ideal de A. Se dice que I es un **ideal real** si A/I es un anillo real.

OBSERVACIÓN 1.2.12. Si A es un anillo real, entonces A es semireal.

DEMOSTRACIÓN

Supóngase que A es un anillo que no es semireal, entonces $-1=\sum_{i=1}^{n} a_i{}^2$ con $a_i\in$A, $i\in\{1, 2,\ldots, n\}$; luego $\sum_{i=1}^{n} a_i{}^2 +1^2=0$. Como A es real, se obtiene que $1=0$, lo cual es una contradicción. □

El recíproco de la observación 1.2.12. no es valido en general. Un ejemplo de un anillo que es semireal pero no es real viene dado por

$$A=\mathbb{R}[x_1,\ldots,x_n]/\langle x_1{}^2+\cdots+x_n{}^2\rangle$$

En efecto, del ejemplo 1.1.13., se sigue que A es un anillo semireal pero A no es real porque $x_1{}^2+\cdots+x_n{}^2=0$ y sin embargo $x_i\neq 0$ para toda $i\in\{1, 2,\ldots, n\}$.

OBSERVACIÓN 1.2.13. Si A es un campo, entonces los conceptos de realidad y semirealidad son equivalentes.

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que existe $\sum_{i=1}^{n} a_i{}^2 =0$ con $a_i\in$A, $i\in\{1, 2,\ldots, n\}$ no todos cero, por ejemplo $a_1\neq 0$. Entonces $-a_1{}^2=\sum_{i=2}^{n} a_i{}^2$. Como A es un campo, se sigue que $-1=\sum_{i=2}^{n} (a_i/a_1)^2$ pero esto último es una contradicción al hecho de que A es un campo semireal.

($\Leftarrow$)

La condición suficiente es un caso particular de la observación 1.2.12. □

Es interesante subrayar que según la observación 1.2.13., resultados tales como; teorema 1.1.19., proposición 1.1.28., corolario 1.1.29., etc. pueden rescribirse en términos del concepto de realidad. Por ejemplo el teorema 1.1.19., se escribe como:

TEOREMA 1.2.14. Sea A un anillo. Entonces A es semireal si y sólo si existe un ideal primo *P* de A tal que F=*qf*(A/*P*) es un campo real.

En el caso de ideales de anillos, se tienen los siguientes tres resultados.

OBSERVACIÓN 1.2.15. Sea A un anillo y *m* un ideal maximal de A, entonces los conceptos de ideal real e ideal semireal son equivalentes.

DEMOSTRACIÓN

La equivalencia se sigue directamente de la observación 1.2.13. □

OBSERVACIÓN 1.2.16. Sea A un anillo e *I* un ideal de A. Si *I* es real, entonces *I* es semireal.

DEMOSTRACIÓN

Se sigue directamente de la observación 1.2.12. □

OBSERVACIÓN 1.2.17. Sean A, B anillos y φ:A$\rightarrow$B un homomorfismo inyectivo de anillos. Si B es un anillo real, entonces A es un anillo real.

DEMOSTRACIÓN

Supóngase que A no es un anillo real, esto significa que existe $\sum_{i=1}^{n} a_i^2 = 0$ con $a_i \in$A, $i \in \{1, 2, \ldots, n\}$ donde al menos una de las a_i es diferente de cero; por ejemplo $a_1 \neq 0$. Entonces $\sum_{i=1}^{n} \varphi(a_i)^2 = 0$ y $\varphi(a_1) \neq 0$; esto último contradice el hecho de que B sea un anillo real. □

OBSERVACIÓN 1.2.18. Sea A un anillo, S un sistema multiplicativo en A y S^{-1}A el anillo de cocientes de A con respecto a S. Si A es un anillo real, entonces S^{-1}A es un anillo real.

DEMOSTRACIÓN

Supóngase que

$$\overline{(a_1, s_1)^2} + \overline{(a_2, s_2)^2} + \cdots + \overline{(a_n, s_n)^2} = \overline{(0,1)}$$

es una suma de cuadrados en S^{-1}A, con $a_i \in$A, $s_i \in$S, $i \in \{1, 2, \ldots, n\}$. Entonces

$$\overline{(a_1^2, s_1^2)} + \overline{(a_2^2, s_2^2)} + \cdots + \overline{(a_n^2, s_n^2)} = \overline{(0,1)}$$

de esto se sigue

$$\overline{(a_1^2 s_2^2 \cdots s_n^2 + s_1^2 a_2^2 \cdots s_n^2 + \cdots + s_1^2 s_2^2 \cdots a_n^2, s_1^2 s_2^2 \cdots s_n^2)} = \overline{(0,1)}$$

$$\overline{(b_1^2 + b_2^2 + \cdots + b_n^2, s^2)} = \overline{(0,1)}$$

con $b_i = s_1 s_2 \cdots a_i \cdots s_n$ y $s^2 = \prod_{i=1}^{n} s_i^2$. Esto último significa que existe un elemento t en S tal que $t^2(b_1^2 + b_2^2 + \cdots + b_n^2) = 0$ y $(tb_1)^2 + \cdots + (tb_n)^2 = 0$. Como A es un anillo real, $tb_i = 0$ para toda $i \in \{1,2,\ldots,n\}$, esto significa que $tb_i = 0$ si y sólo si $ts_1 s_2 \cdots a_i \cdots s_n = 0$ si y sólo si $\overline{(a_i, s_i)} = \overline{(0,1)}$. □

Para anillos semireales e ideales de estos anillos, se tienen las siguientes propiedades.

TEOREMA 1.2.19. Sea A un anillo, entonces las siguientes afirmaciones son equivalentes.

1° A es un anillo semireal.
2° A tiene un ideal semireal.
3° A tiene un ideal real.
4° A tiene un ideal primo semireal.
5° A tiene un ideal primo real.
6° A tiene un ideal primo P tal que la localización A_P es un anillo semireal.
7° A tiene un ideal maximal m tal que la localización A_m es un anillo semireal.
8° Existe un anillo de cocientes de A que es semireal.
9° Existe un homomorfismo $\varphi: A \to F$ con F un campo real.

DEMOSTRACIÓN

(1°) $\Rightarrow$ (2°)

El ideal cero {0} es el ideal semireal de A ($A \cong A/\{0\}$, $\varphi: A \to A/\{0\}$, $\varphi(a) = a + \{0\}$ es un isomorfismo).

(2°) $\Rightarrow$ (1°)

Si A tiene un ideal I semireal, entonces A/I es un anillo semireal. Sea $\varphi: A \to A/I$, $\varphi(a) = \overline{a}$, con $a \in A$ y φ el homomorfismo natural. Por la observación 1.2.3., se concluye que A es un anillo semireal.

(1°) $\Rightarrow$ (5°)

Que A sea un anillo semireal, por el teorema 1.1.19., será equivalente a: existe un ideal primo P de A tal que el campo de cocientes $qf(A/P)$ es real. Sea $\psi: A/P \to qf(A/P)$; $\psi(\overline{a}) = \overline{(a, 1)}$; ψ está bien definido y es un homomorfismo inyectivo. Por la observación 1.2.17., se sigue que A/P es un anillo real y por definición P es un ideal real.

$(5°) \Rightarrow (3°)$

Si A tiene un ideal primo real P, entonces A tiene un ideal propio real P.

$(3°) \Rightarrow (2°)$

Si A tiene un ideal propio I que es real, entonces I es un ideal semireal.

$(1°) \Rightarrow (8°)$

Sea S={1}; es claro que S es un sistema multiplicativo en A. Ahora, sea $S^{-1}A = \{\overline{(a,1)} \mid a \in A\}$. $S^{-1}A \cong A$ con $\varphi: A \to S^{-1}A$; $\varphi(a)=\overline{(a,1)}$ el homomorfismo natural; claramente φ es una biyección. Como A es un anillo semireal, se concluye que $S^{-1}A$ es un anillo semireal.

$(8°) \Rightarrow (1°)$

Es la demostración de la observación 1.2.4.

$(5°) \Rightarrow (4°)$

Se sigue de la definición.

$(4°) \Rightarrow (2°)$

Sea P en A un ideal primo semireal, entonces A tiene un ideal semireal.

$(7°) \Rightarrow (6°)$

Como m es un ideal maximal de A esto significa que A tiene un ideal primo m tal que la localización A_m es semireal.

$(6°) \Rightarrow (1°)$

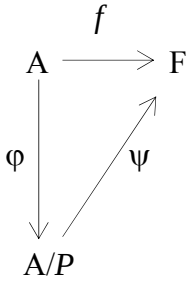
Sea $\varphi: A \to A_P$, $\varphi(a)=\overline{(a,1)}$ el homomorfismo natural. Por la observación 1.2.4., se sigue el resultado, es decir, A es un anillo semireal.

$(5°) \Rightarrow (7°)$

Se sabe que si A tiene un ideal primo real, entonces A es un anillo semireal (ya que $(5°) \Rightarrow (1°)$). Por el criterio Global-Local se sigue que A_m es semireal.

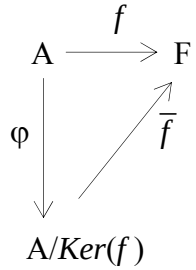
$(5°) \Rightarrow (9°)$

Sea P un ideal primo de A y F=qf(A/P) el campo de cocientes del dominio entero A/P. Sea $\psi: A/P \to qf(A/P)$; $\psi(\overline{a})=\overline{(\overline{a},\overline{1})}$. La aplicación ψ está bien definida y es un homomorfismo de anillos. Sea; $\varphi: A \to A/P$; $\varphi(a)=a+P$ el homomorfismo canónico, entonces $f: A \to F$; $f(a)=\overline{(\overline{a},\overline{1})}$ está bien definida, y es un homomorfismo ya que φ y ψ lo son. Como P es un ideal real, esto es equivalente a A/P es un anillo real, por la observación 1.2.18., se sigue que F es real.



(9°)⇒(5°)

Sea f:A→F, con F un campo real. Por el primer teorema del homomorfismo existe un homomorfismo inyectivo $\overline{f}$:A/*Ker*(f)→F; $\overline{f}$ (a+*Ker*(f))=f(a) y *Ker*(f) es primo para cada a∈A. Entonces por la observación 1.2.17, A/*Ker*(f) es un anillo real. Esto último significa que *Ker*(f) es un ideal primo real. □



Si A es un anillo y m es un ideal maximal de A, entonces m es un ideal primo de A; luego se tiene la siguiente

OBSERVACIÓN 1.2.20. Si un anillo A tiene un ideal maximal real, entonces A tiene un ideal primo real. □

Se observa que, si A tiene un ideal primo real, en general A no necesariamente tiene un ideal maximal real. Por ejemplo, ℤ tiene un ideal primo real, el ideal 0ℤ. Pero todos sus ideales maximales no son reales[†)], 2ℤ es un ideal maximal de ℤ que no es real (ℤ/2ℤ≅ℤ2={ $\overline{0}$, $\overline{1}$ } no es real).

A continuación se dan dos resultados que se desprenden del teorema 1.2.19.

COROLARIO 1.2.21. Sea A un dominio Prüfer con campo de cocientes F. Entonces las afirmaciones (1°) a (9°) del teorema 1.2.19. son equivalentes a

10° A es un anillo real.

11° F es un campo real.

DEMOSTRACIÓN (1°) ⇒ (11°)

La demostración se sigue directamente del corolario 1.1.29. y de la observación 1.2.13..

(11°) ⇒ (10°)

Sea φ:A→F; φ(a)=$\overline{(a,1)}$ el homomorfismo natural inyecto. Por la observación 1.2.17., se sigue que A es un anillo real.

(10°) ⇒ (1°)

Esta es la demostración de la observación 1.2.12.. □

COROLARIO 1.2.22. Sea A un dominio regular con campo de cocientes F. Entonces las afirmaciones (1°) a (9°) del teorema 1.2.19. son equivalentes a

10°′ A es un anillo real.

11°′ F es un campo real

DEMOSTRACIÓN (1°) ⇒ (11°′)

La demostración se sigue directamente del teorema 1.1.32. y de la observación

[†)] Los ideales maximales de ℤ son de la forma pℤ con p primo (p≥2).

1.2.13.. Las demostraciones de $(11°')\Rightarrow(10°')$ y $(10°')\Rightarrow(1°)$ son similares a las demostraciones de $(11°)\Rightarrow(10°)$ y $(10°)\Rightarrow(1°)$ del corolario anterior. □

Se recuerda que si A es un anillo e I un ideal de A, el **radical** de I escrito $rad_A(I)$ es el conjunto $rad_A(I):=\{a\in A \mid \text{existe } n(a)\in\mathbb{N} \text{ con } a^{n(a)}\in I\}$. El conjunto $rad_A(I)$ es un ideal de A que contiene a I. De hecho el radical de I es la intersección de todos los ideales primos que contienen a I, esto es;

OBSERVACIÓN 1.2.23. Sea A un anillo e I un ideal de A. Entonces el radical de I, escrito $rad_A(I)$ es la intersección de todos los ideales primos de A que contienen a I.

DEMOSTRACIÓN

Sea $a\in rad_A(I)$ y P un ideal primo de A que contiene a I. Entonces existe $n(a)\in\mathbb{N}$ tal que $a^{n(a)}\in I\subseteq P$. Como P es un ideal primo y $a\in P$; se tiene que $rad_A(I)\subseteq\cap P$, donde $I\subseteq P$. Ahora, sea $b\in\cap P$ (con $I\subseteq P$) y supóngase que $b\notin rad_A(I)$. Sea $S=\{b^m \mid m\in\mathbb{N}\cup\{0\}\}$. Claramente S es un conjunto multiplicativamente cerrado en A e $I\cap S=\varnothing$. Por la proposición 1.1.18., existe un ideal primo P' de A tal que $I\subseteq P'$ y $P'\cap S=\varnothing$. Entonces $b\in P'\cap S=\varnothing$ pero esto no es posible. Luego, $\cap P\subseteq rad_A(I)$ donde $I\subseteq P$. □

En el caso particular en que I es el ideal cero de A, se tiene que

$$rad_A(0)=\{a\in A \mid \text{existe } n(a)\in\mathbb{N} \text{ con } a^{n(a)}=0\}.$$

$rad_A(0)$ se denomina **nilradical** de A, (escrito $nil(A)$). El conjunto $nil(A)$ es un ideal de A y es la intersección de todos los ideales primos de A. Cuando $nil(A)=0$ se dice que A es un **anillo reducido**. Sea A un anillo y considérese el conjunto $\wp$ de todos los ideales primos de A que contienen a un ideal I. Por el corolario 1.1.17., se sigue que $\wp\neq\varnothing$. Ordenando parcialmente a $\wp$ por la inclusión inversa [es decir, si $P_1, P_2\in\wp$, entonces $P_1\leq P_2$ si y sólo si $P_1\supseteq P_2$] y utilizando lema de Zorn, se tiene un elemento maximal de $(\wp, \supseteq)$ que es justamente un elemento minimal de $(\wp, \subseteq)$. Tal elemento se denomina **ideal primo minimal de *I***. Los ideales primos minimales del ideal cero son llamados **ideales primos minimales de A**.

PROPOSICIÓN 1.2.24. Sea A un anillo e I un ideal de A. Entonces existe al menos un ideal primo minimal de I.

DEMOSTRACIÓN

Sea $\mathcal{A}$ un subconjunto no vacío totalmente ordenado de $\mathcal{P}$ con respecto al anterior orden parcial. Sea $\mathsf{A}:=\bigcap_{P\in\mathcal{A}} P$, A es un ideal propio de A ya que $\mathcal{A}\neq\varnothing$; se tiene que probar que A es un ideal primo de A. En efecto, sean $a\notin\mathsf{A}$ y $b\in A$ tal que $ab\in\mathsf{A}$; por demostrar que $b\in\mathsf{A}$. Sean $P, P'\in\mathcal{A}$ con $a\notin P'$. Como $\mathcal{A}$ está totalmente ordenado, se tiene que $P'\subseteq P$ o $P\subseteq P'$. Si $P'\subseteq P$, se sigue que $ab\in P'$ y $a\notin P'$ lo que significa que $b\in P'\subseteq P$. Si $P\subseteq P'$, entonces

$a \notin P$ y $ab \in P$, así $b \in P$. En ambos casos, como P es un elemento arbitrario de $\mathcal{A}$, se sigue que $b \in \mathsf{A}$. Por lo tanto A es un ideal primo de A; luego $\mathsf{A} \in \mathcal{P}$ y es una cota superior de $\mathcal{A}$ en $(\mathcal{P}, \supseteq)$. Por el lema de Zorn, el conjunto $(\mathcal{P}, \supseteq)$ tiene al menos un elemento maximal y el conjunto $(\mathcal{P}, \subseteq)$ tiene al menos un elemento minimal. Por lo tanto, existe al menos un ideal primo minimal de I. □

De este resultado se obtiene que si I y P con $P \supseteq I$ son ideales de un anillo A con P ideal primo, entonces existe un ideal primo minimal P' de I tal que $I \subseteq P' \subsetneq P$.

OBSERVACIÓN.1.2.25. Sea A un anillo e I un ideal de A, entonces $rad_{\mathrm{A}}(I)$ es la intersección de todos los ideales primos minimales de I.

DEMOSTRACIÓN

Por 1.2.23., bastará probar que $\cap_{P \in \wp(I)} P = \cap_{P \in \mathcal{M}(I)} P$ donde $\wp(I) = \{P \mid P \supseteq I$ ideal primo de A$\}$ y $\mathcal{M}(I) = \{P \mid P$ ideal primo minimal de $I\}$. Como $\mathcal{M}(I) \subseteq \wp(I)$, se sigue que $\cap_{P \in \wp(I)} P \subseteq \cap_{P \in \mathcal{M}(I)} P$. Recíprocamente, sea $x \in \cap_{P \in \mathcal{M}(I)} P$ tal que $x \notin P$, P ideal primo de A que contiene a I. Entonces por 1.2.24., existe un ideal primo minimal P' de I con $I \subseteq P' \subsetneq P$, luego $x \notin P'$ pero esto último es una contradicción. □

OBSERVACIÓN.1.2.26. Sean I y P con $P \supseteq I$ ideales de un anillo A donde P es un ideal primo. Si P' es un ideal primo minimal de I con $P' \subsetneq P$ y P es semireal, entonces P' es semireal.

DEMOSTRACIÓN

Como $P' \subsetneq P$, existe un homomorfismo $\varphi: \mathrm{A}/P' \to \mathrm{A}/P$; $\varphi(a+P') = a+P$. El resultado se sigue de la observación 1.1.8.. □

LEMA 1.2.27. Un anillo A es real si y sólo si $nil(\mathrm{A}) = 0$ y todo ideal primo minimal de A es real.

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que $nil(\mathrm{A}) \neq 0$, entonces existe al menos un elemento $a \in \mathrm{A} \setminus \{0\}$ con $a^{n(a)} = 0$. Como A es real, se tiene que $a = 0$; pero esto no puede ser posible. Por lo tanto $nil(\mathrm{A}) = 0$. Sea P un ideal primo minimal de A y A_P la localización de A en P. Considérese el homomorfismo natural $\varphi: \mathrm{A} \to \mathrm{A}_P$; $\varphi(a) = \overline{(a,1)}$. Si A es un anillo real, se sigue que A_P es un anillo real (ver la observación 1.2.18.). Como $P\mathrm{A}_P$ es el único ideal maximal de A_P, con la inclusión inversa, se tiene que $P\mathrm{A}_P$ es el único ideal primo minimal de A_P, esto es, $nil(\mathrm{A}_P) = \cap P = P\mathrm{A}_P$ con P ideal primo de A. Dado que $nil(\mathrm{A}_P) = 0$ se sigue que $P\mathrm{A}_P = 0$ y $\mathrm{A}_P / P\mathrm{A}_P = \mathrm{A}_P$. Dado que $\mathrm{A}_P / P\mathrm{A}_P \cong qf(\mathrm{A}/P)$, se sigue que $qf(\mathrm{A}/P) \cong \mathrm{A}_P$. Así $qf(\mathrm{A}/P)$ es un campo real y A/P es un anillo real. Por lo tanto P es un ideal primo real.

($\Leftarrow$)

Sea P un ideal primo minimal de A y $a_i \in A$, $i=1,\ldots,n$ tal que $\sum_{i=1}^{n} a_i^2 = 0$, entonces $\sum_{i=1}^{n} a_i^2 \in P$. Ya que P es real, se sigue que $a_i \in P$ para cada $i \in \{1,2,\ldots,n\}$, entonces $a_i \in \cap P$ con P ideal primo minimal de A. Como $nil(A)=0$ y $nil(A)=\cap P=0$, P ideal primo minimal de A (ver observación 1.2.25.), se sigue que $a_i=0$ para toda $i \in \{1,2,\ldots,n\}$. Por lo tanto A es un anillo real. □

El producto directo de anillos $\prod_{i\in I} A_i$ con las operaciones de suma y multiplicación por componentes es un anillo; y si los A_i son anillos reales, entonces el producto directo $\prod_{i\in I} A_i$ es un anillo real. Sin embargo, en general el producto directo de campos $\prod_{i\in I} F_i$ no es un campo (existen elementos no cero que no son unidades en $\prod_{i\in I} F_i$). Sea A un anillo real y $(P_i)_{i\in I}$ la familia de ideales primos minimales de A. Si $(F_i)_{i\in I}$ con $F_i = qf(A/P_i)$ es una familia de campos, entonces se tiene

TEOREMA 1.2.28. Un anillo A es real si y sólo si A puede ser encajado en un producto directo de campos reales.

DEMOSTRACIÓN ($\Rightarrow$)

Por el lema 1.2.27., los ideales primos minimales P_i de A para cada $i \in I$ son ideales reales y los campos de cocientes $F_i = qf(A/P_i)$ para toda $i \in I$ son reales. Sea $\varphi: A \to \prod_{i\in I} F_i$; $a \mapsto (\overline{(a_i, 1)})_{i\in I}$ el homomorfismo obvio. Es claro que $Ker(\varphi) = \cap_{i\in I} P_i$, P_i ideal primo minimal de A, como A es un anillo real, $nil(A)=0$ y $Ker(\varphi)=0$. Luego φ es inyectivo y encaja el anillo A en el producto directo $\prod_{i\in I} F_i$ de campos reales.

($\Leftarrow$)

Como cada F_i, $i \in I$ es un campo real, se tiene que $\prod_{i\in I} F_i$ es un anillo real; por la observación 1.2.17., se sigue que A es real. □

Si un anillo A es real, entonces A es un anillo semireal. Pareciera que el lema 1.2.27. es valido si en vez de la palabra real se escribiera la palabra semireal. Pero se puede ver que la afirmación:

Un anillo A es semireal si y sólo si nil(A)=0 y todo ideal primo minimal es semireal

es falsa en general. Por ejemplo el anillo $\mathbb{R}[x]/\langle x^2\rangle$ es semireal (ver ejemplo 1.1.13.) pero $nil(\mathbb{R}[x]/\langle x^2\rangle) \neq 0$. Sin embargo se puede enunciar un resultado acerca de anillos semireales e ideales primos minimales semireales.

PROPOSICIÓN 1.2.29. Un anillo A es semireal si y sólo si uno de sus ideales primos minimales es semireal.

DEMOSTRACIÓN

Si A es un anillo semireal esto será equivalente a: A tiene un ideal primo P

semireal (ver teorema 1.2.19.). Por la proposición 1.2.24., P tiene un ideal primo minimal P_0, y por la observación 1.2.26., se sigue que P_0 es un ideal semireal. □

Sea (A , m) un anillo local y F=A/m su campo residual. En general F no es un campo real. Aquellos anillos locales (A , m) cuyo campo residual es un campo real serán de importancia aquí, es decir,

DEFINICIÓN 1.2.30. Se dice que un anillo local (A , m) es un anillo **local real** si el ideal maximal m es real o equivalentemente si el campo residual es real.

Si un anillo local (A , m) es semireal o real, entonces no necesariamente es un anillo local real. Por ejemplo, la localización $\mathbb{Z}_{<p>}=\{\overline{(m,n)} \mid m\in\mathbb{Z}, n\in\mathbb{Z}\setminus<p> \text{ y } (p\ ,\ n)=1\}$ (ver ejemplo 1.2.9.) es un anillo real y por consiguiente semireal, pero $\mathbb{Z}_{<p>}$ no es un anillo local real ya que el ideal $<p>$ no es maximal para todo entero primo p. También, no todo anillo local real (A , m) es un anillo real. Un ejemplo de esto es la localización $A_{<\overline{x}_1,\ldots,\overline{x}_n>}$ que es un anillo local real ya que el ideal maximal $<\overline{x}_1,\ldots,\overline{x}_n>$ es real; donde $A=\mathbb{R}[x_1,\ldots,x_n]/<x_1^2+\cdots+x_n^2>$, Este anillo no es real ya que si $\overline{x}_1^2+\cdots+\overline{x}_n^2=\overline{0}$ se tendrá que $\overline{x}_i\neq 0$ para toda $i\in\{1,\ldots,n\}$.

OBSERVACIÓN 1.2.31. Si (A , m) es un anillo local real, entonces (A , m) es un anillo semireal.

DEMOSTRACIÓN

Sea φ:A$\rightarrow$A/m el homomorfismo natural con m el ideal maximal de (A , m). Como A/m es un campo real, se sigue que también es semireal. Luego (A , m) es un anillo semireal. □

Si (A , m) es un anillo local real, ¿bajo qué condiciones (A , m) es un anillo real? Esto lo contesta las siguientes

OBSERVACIÓN 1.2.32. Si (A , m) es un anillo de valoración local real con campo de cocientes F, entonces (A , m) es real.

DEMOSTRACIÓN

Como (A , m) es un anillo local real, se sigue que (A , m) es semireal y como es de valoración, se tiene de 1.1.28., que F es real (A semireal $\Leftrightarrow$ F real). Sea φ:A$\rightarrow$F el homomorfismo inyectivo. Por 1.2.17., se sigue que (A , m) es real. □

OBSERVACIÓN 1.2.33. Si (A , m) es un anillo local regular que es local real con campo de cocientes F, entonces (A , m) es real.

DEMOSTRACIÓN

De 1.1.31., se tiene que s(A/m)$\leq s$(F). Como (A , m) es un anillo local real, se sigue

que A/m es semireal y F es semireal; así, F es un campo real. Sea φ:A$\rightarrow$F el homomorfismo inyectivo. Por 1.2.17., se sigue que (A , m) es real. □

OBSERVACIÓN 1.2.34. Si (A , m) es un anillo Prüfer local real con campo de cocientes F, entonces (A , m) es real.

DEMOSTRACIÓN

Que (A , m) sea un anillo local real, significa que (A , m) es semireal. Por el teorema 1.1.32., se sigue que (A , m) es real. □

Para terminar este capítulo se tiene el siguiente

LEMA 1.2.35. Sea (A , m) un anillo de valoración local real con campo de cocientes F y $a_1,\ldots,a_n\in$F. Si $\sum_{i=1}^{n} a_i^{\,2} \in$(A , m), entonces $a_i\in$(A , m) para cada $i\in\{1,\ldots,n\}$.

DEMOSTRACIÓN

Del lema 1.1.27., se puede suponer sin perdida de generalidad que $a_i/a_1\in$A para cada $i\in\{1,2,\ldots,n\}$, entonces $\sum_{i=1}^{n}(a_i/a_1)^2\in$A. Por otro lado, como $\sum_{i=1}^{n} a_i^{\,2} \in$A, se sigue que $a_1^{\,2}\sum_{i=1}^{n}(a_i/a_1)^2\in$A. Como A es un anillo real (ver proposición 1.2.32.), se tiene que $\sum_{i=1}^{n}(a_i/a_1)^2\neq 0$ pues si $\sum_{i=1}^{n}(a_i/a_1)^2=0$, se tendría que $1+\sum_{i=2}^{n}(a_i/a_1)^2=0$ y $1=0$ lo cual no puede ser posible. Se afirma que $\sum_{i=1}^{n}(a_i/a_1)^2$ es una unidad en A. En efecto, si $\sum_{i=1}^{n}(a_i/a_1)^2$ no fuera una unidad en A, se tendría que $\sum_{i=1}^{n}(a_i/a_1)^2\in m$, es decir, $1+(a_2/a_1)^2+\cdots+(a_n/a_1)^2\in m$ pero esto significa que $-1=(a_2/a_1)^2+\cdots+(a_n/a_1)^2$ lo cual no es posible ya que F es un campo real; así, $\sum_{i=1}^{n}(a_i/a_1)^2$ es una unidad en A. Sea $a_1^{\,2}=[a_1^{\,2}\sum_{i=1}^{n}(a_i/a_1)^2][(\sum_{i=1}^{n}(a_i/a_1)^2)^{-1}]\in$A, entonces $a_1^{\,2}\in$A. Si $a_1\in$A perfecto, si no, $a_1^{-1}\in$A y $a_1^{\,2}a_1^{-1}=a_1\in$A. Ahora, supóngase que $a_i/a_2\in$A para toda $i\in\{1,2,\ldots,n\}$. Repitiendo la demostración, se obtiene que $a_2\in$A. Siguiendo con este proceso, es decir, tomando $a_i/a_j\in$A para $j\in\{1,2,\ldots,n\}$, se tiene que $a_i\in$A para toda $i\in\{1,2,\ldots,n\}$. □

2. LA TEORÍA DE ARTIN-SCHREIER.

INTRODUCCIÓN.

En este capítulo se exponen algunos resultados de la teoría de Artin-Schreier para campos. (La teoría de campos ordenados tiene su origen en los trabajos de Artin y Schreier desarrollada en la primera mitad del siglo pasado, ellos descubrieron la conexión entre las nociones de campo ordenado y campo real; *un campo es ordenado si y sólo si es real*). Se introducen los conceptos de clase pre-positiva (preorden) y clase positiva (orden) para un campo dado, y se proporcionan algunas de sus propiedades: por ejemplo el teorema clásico de Artin y Schreier. A continuación, se establece la teoría de Artin-Schreier para anillos; esta teoría fue desarrollada a partir de los años 70. Ella es, "similar" a la teoría de Artin-Schreier para campos. Se establecen las nociones de clase pre-positiva y clase positiva para anillos, y entre sus propiedades se da la generalización del teorema clásico de Artin y Schreier. Finalmente se introduce la noción de espectro real (espacio de órdenes) para anillos a partir de la dada para campos. En esta sección, un orden ya no es considerado como un subconjunto de un campo o de un anillo si no más bien como un elemento de un cierto espacio topológico (espacio de Harrison) y los elementos del campo o del anillo como las funciones sobre este espacio. Aquí, al igual que en el capítulo 1, la palabra anillo significa anillo conmutativo con unitario y homomorfismo significa homomorfismo de anillos que lleva 1 a 1.

2.1. CAMPOS ORDENADOS.

DEFINICIÓN 2.1.1. Sea K un campo. Una relación binaria $\leq$ en K es una **relación de orden** de K si $\leq$ satisface que para x, y y z elementos arbitrarios en K.

i) $x \leq x$.
ii) si $x \leq y$ y $y \leq x$, entonces $x = y$.
iii) si $x \leq y$ y $y \leq z$, entonces $x \leq z$.
iv) $x \leq y$ o $y \leq x$.
v) si $x \leq y$, entonces $x+z \leq y+z$.
vi) si $0 \leq x$ y $0 \leq y$, entonces $0 \leq xy$.

El par $(K, \leq)$ se denomina **campo ordenado**.

EJEMPLO 2.1.2. $\mathbb{Q}$ y $\mathbb{R}$ con sus relaciones de órdenes usuales son campos ordenados.

Se recuerda que si K es un campo, la función $\varphi:\mathbb{Z} \to K$, $n \mapsto n\cdot 1$ ($n\cdot 1 = 1+1+\cdots+1$, (n veces)) es un homomorfismo cuya imagen se denomina **subcampo primo** de K; su núcleo es un ideal $m\mathbb{Z}$ para un único $m \geq 0$ llamado **característica** de K y denotado por *car*(K). La característica de un campo es cero o un número primo. En el caso de campos ordenados se tiene la siguiente

OBSERVACIÓN 2.1.3. Todo campo ordenado es de característica cero.

DEMOSTRACIÓN

Supóngase que K es un campo ordenado de característica $p\neq 0$. Si $x\in K$ con $x\geq 0$ y $x\neq 0$, entonces $0=px=x+\cdots+x>0$ lo cual no es posible. □

DEFINICIÓN 2.1.4. Sea K un campo. Un subconjunto T en K es una **clase pre-positiva** de la relación de orden ≤ en K si

1°) $T+T\subseteq T$.
2°) $T\cdot T\subseteq T$.
3°) $K^2\subseteq T$.
4°) $-1\notin T$.

Donde $T+T=\{t+s \mid t, s\in T\}$, $T\cdot T=\{t\cdot s \mid t, s\in T\}$ y $K^2=\{x^2 \mid x\in K\}$.

El conjunto $\sum K^2:=\{\sum_{i=1}^{n} x_i^2 \mid x_i\in K\}$ de sumas finitas de cuadrados en un campo K

satisface 1º), 2º) y 3º) de la definición 2.1.4., pero en general no satisface 4º), esto es, $\sum K^2$ no es una clase pre-positiva en K; por ejemplo si K es igual a ℂ. De 1º) y 3º) de la definición 2.1.4., se sigue que $\sum K^2$ está contenido en toda clase pre-positiva de K. En el caso en que K es un campo real, $\sum K^2$ es siempre una clase pre-positiva de K.

EJEMPLO 2.1.5. El conjunto $T=\{x\in\mathbb{R} \mid 0\leq x\}$ es una clase pre-positiva en ℝ.

Se observa que T en el ejemplo anterior, satisface $T\cup -T=\mathbb{R}$ con $-T=\{-x\in\mathbb{R} \mid x\in T\}$. Aquellas clases pre-positivas en K que satisfagan $T\cup -T=K$ serán de importancia aquí, es decir,

DEFINICIÓN 2.1.6. Sea K un campo. Una clase pre-positiva T en K es una **clase positiva** de la relación de orden ≤ en K si

5°) $T\cup -T=K$.

EJEMPLO 2.1.7. Sea K un campo ordenado, entonces el conjunto $T=\{x\in K \mid 0\leq x\}$ es una clase positiva de la relación de orden ≤ en K.

EJEMPLO 2.1.8. Considérese el campo cuadrático $\mathbb{Q}(\sqrt{2})$ cuyos elementos son de la forma $a+b\sqrt{2}$ con $a, b\in\mathbb{Q}$, entonces los conjuntos:

$$T=\{r+s\sqrt{2} \mid r\geq 0 \text{ y } r^2\geq 2s^2 \text{ o } s\geq 0 \text{ y } 2s^2\geq r^2\} \text{ y } T'=\{r+s\sqrt{2} \mid r\geq 0 \text{ y } r^2\geq 2s^2 \text{ o } s\leq 0 \text{ y } 2s^2\geq r^2\}$$

son clases positivas de la relación de orden ≤ en $\mathbb{Q}(\sqrt{2})$.

Como existen únicamente dos formas de encajar $\mathbb{Q}(\sqrt{2})$ en $\mathbb{R}$, (se consideran los homomorfismos de $\mathbb{Q}$-álgebras $\varphi : \mathbb{Q}(\sqrt{2})\to\mathbb{R}$; $a+b\sqrt{2}\mapsto a+b\sqrt{2}$ y $\psi : \mathbb{Q}(\sqrt{2})\to\mathbb{R}$; $a+b\sqrt{2}\mapsto a-b\sqrt{2}$) existen entonces dos formas de ordenar a $\mathbb{Q}(\sqrt{2})$. Luego se tiene que T y T′ del ejemplo anterior, son las únicas clases positivas de la relación de orden $\leq$ en $\mathbb{Q}(\sqrt{2})$.

De las definiciones 2.1.4. y 2.1.6., se sigue directamente que toda clase positiva T de una relación de orden $\leq$ en un campo K es una clase pre-positiva de $\leq$ en K. El recíproco de esta observación es falso en general; un ejemplo de una clase pre-positiva que no es una clase positiva, viene dado como: Considérese el campo $\mathbb{Q}(\sqrt{2})$ del ejemplo 2.1.8.. Se sabe que $\mathbb{Q}$ es un campo real y es fácil verificar que $\mathbb{Q}(\sqrt{2})$ también es un campo real [†)], entonces $\sum\mathbb{Q}(\sqrt{2})^2$ es una clase pre-positiva en $\mathbb{Q}(\sqrt{2})$. Como $\mathbb{Q}(\sqrt{2})$ tiene únicamente dos clases positivas T y T′ (ver ejemplo 2.1.8.) y ninguna de ellas es $\sum\mathbb{Q}(\sqrt{2})^2$, se sigue que $\sum\mathbb{Q}(\sqrt{2})^2$ no es una clase positiva de la relación de orden $\leq$ en $\mathbb{Q}(\sqrt{2})$.[‡)]

OBSERVACIÓN 2.1.9. Sea K un campo, entonces T es una clase positiva de una relación de orden $\leq$ en K si

1°) $T+T\subseteq T$.
2°) $T\cdot T\subseteq T$.
3°)′ $T\cap -T=\{0\}$.
5°) $T\cup -T=K$.

DEMOSTRACIÓN

Supóngase que $T\cap -T\neq\{0\}$, entonces existen elementos t_1, $t_2\in T$ tal que $t_1=-t_2$ con $t_2\neq 0$. Como $1/t_2\in K$ y $(1/t_2)^2\in T$, se sigue que $-1=t_1/t_2=t_1t_2(1/t_2)^2\in T$; pero esto último contradice 4º) de la definición 2.1.4.. Recíprocamente, supóngase que $-1\in T$. Como $1\in T$, entonces $-1\in -T$, esto significa que $-1\in T\cap -T=\{0\}$ lo cual no es posible; así, $-1\notin T$. Por otro lado, si, $x\in K$ entonces $x\in T$ o $-x\in T$, luego $x^2=x\cdot x=(-x)(-x)\in T$ y $K^2\subseteq T$. □

Sea K un campo ordenado. Si T es una clase positiva en K, T tiene asociada una relación de orden $\leq_T$ en K definida como:

$$x\leq_T y \Leftrightarrow y-x\in T, \text{ para x, } y\in K.$$

Dada una relación de orden $\leq_T$ en K asociada a la clase positiva T en K, se tienen las siguientes equivalencias

1) $0\leq_T x \Leftrightarrow x\in T$.
2) $x\leq_T 0 \Leftrightarrow x\in -T$.
3) $0<_T x \Leftrightarrow 0\leq_T x$ y $x\neq_T 0 \Leftrightarrow x\notin -T$.
4) $x<_T 0 \Leftrightarrow x\leq_T 0$ y $x\neq_T 0 \Leftrightarrow x\notin T$.

[†)] Aplicando la observación 1.2.17. al homomorfismo inyectivo $\varphi:\mathbb{Q}(\sqrt{2})\to\mathbb{R}$ $a+b\sqrt{2}\mapsto a+b\sqrt{2}$ se obtiene el resultado.

[‡)] $\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ pero $\sqrt{2}\notin \sum\mathbb{Q}(\sqrt{2})^2\cup -\sum\mathbb{Q}(\sqrt{2})^2$, luego $\sum\mathbb{Q}(\sqrt{2})^2\cup -\sum\mathbb{Q}(\sqrt{2})^2\subsetneq\mathbb{Q}(\sqrt{2})$.

5) $x=0 \Leftrightarrow 0\leq_T x$ y $x\leq_T 0 \Leftrightarrow x\in T$ y $x\in -T \Leftrightarrow x\in T\cap -T$.

Así, para todo elemento $x\in K$, una y sólo una de las siguientes relaciones se cumple

$$i)\ x\notin T \text{ o } ii)\ x\in T\cap -T \text{ o } iii)\ x\notin -T$$

De lo anterior, se observa que existe una relación estrecha entre ambos conceptos, esto significa que, se puede trabajar con clases positivas sin hacer mención explícita de la relación de orden asociada y viceversa. De esto y abusando del lenguaje, de aquí en adelante, en vez de llamar al conjunto T una clase positiva de la relación de orden $\leq_T$ en K, simplemente se dirá que T es un **orden** en K y se omitirá mencionar a la relación de orden $\leq_T$. En el caso de clases pre-positivas, ellas serán denominadas **preórdenes**.

Algunas veces será más conveniente excluir el cero de un orden T; el conjunto así obtenido se denomina **orden reducido** y se escribe $\dot{T}=T\setminus\{0\}$. Es fácil verificar que

$$\dot{T}+\dot{T}\subseteq \dot{T}$$
$$\dot{T}\cdot\dot{T}\subseteq \dot{T}$$
$$\dot{T}\cap -\dot{T}=\varnothing$$
$$\dot{T}\cup -\dot{T}=\dot{K}$$

o equivalentemente

$$\dot{T}+\dot{T}\subseteq \dot{T}$$
$$\dot{T}\cdot\dot{T}\subseteq \dot{T}$$
$$\dot{K}^2\subseteq \dot{T}$$
$$-1\notin \dot{T}$$
$$\dot{T}\cup -\dot{T}=\dot{K}$$

donde

$$\dot{K}=K\setminus\{0\}.$$

Recíprocamente, si $S\subsetneq \dot{K}$ satisface

$$S+S\subseteq S.$$
$$S\cdot S\subseteq S.$$
$$S\cap -S=\varnothing.$$
$$S\cup -S=\dot{K}.$$

o equivalentemente

$$S+S\subseteq S.$$
$$S\cdot S\subseteq S.$$
$$\dot{K}^2\subseteq S.$$
$$-1\notin S$$
$$S\cup -S=\dot{K}$$

entonces $S\cup\{0\}$ define un orden T en K con $\dot{T}=S$.

OBSERVACIÓN 2.1.10. Sea K un campo y T un preorden en K, entonces *i*) $0\in T$, *ii*) $1\in T$, *iii*) $a^{-1}\in T$ para cada $a\in\dot{T}$.

DEMOSTRACIÓN

Únicamente se probará la afirmación. *iii*) Sea $a\in\dot{T}$, $a^{-1}\in K$, entonces $(a^{-1})^2\in K^2\subseteq T$. Luego $a^{-1}=a(a^{-1})^2\in T$. □

Sea T_0 un preorden en un campo K y considérese la familia $\mathcal{F}$ de todos los preórdenes T en K que contienen a T_0, como $T_0\in\mathcal{F}$, $\mathcal{F}\neq\emptyset$. Ordenando a $\mathcal{F}$ con la inclusión $\subseteq$, se observa que $(\mathcal{F}, \subseteq)$ es un conjunto parcialmente ordenado. Sea $\mathcal{F}$ un conjunto no vacío totalmente ordenado de $\mathcal{F}$ y $\mathsf{T}=\cup T$ con $T\in\mathcal{F}$. Claramente T es un preorden en K que contiene a T_0.[†)] T También es una cota superior de $\mathcal{F}$ en $\mathcal{F}$. Por el lema de Zorn, el conjunto parcialmente ordenado $(\mathcal{F}, \subseteq)$ tiene al menos un elemento maximal. Tales elementos maximales se denominan **preórdenes maximales** en K. De manera similar se define orden maximal. Para preórdenes maximales se tiene la siguiente

PROPOSICIÓN 2.1.11. Sea K un campo y T un preorden en K. Entonces T es un orden en K si y sólo si T es un preorden maximal en K.

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que T es un preorden en K que no es maximal, esto significa que existe un preorden T' en K, tal que $T\subsetneq T'\subsetneq K$. Sea $x\in T'$ con $x\notin T$, entonces $-x\in T$ y $-x\in T'$ con $-x\neq 0$. Luego $-x^{-1}\in T'$ y $-1=x(-x^{-1})\in T'$ lo cual es una contradicción.

($\Leftarrow$)

De acuerdo a 2.1.6., bastará probar que $T\cup -T=K$. Supóngase que $T\cup -T\subsetneq K$ y sea $x_0\in K$ tal que $x_0\notin T\cup -T$. Defínase $T'=T+Tx_0$ con $Tx_0=\{tx_0 \mid t\in T\}$; como T' no es un orden en K, entonces para $x_0\in K$, existen $s, t\in T$ tal que $-1=t+sx_0$ y $-sx_0=1+t$. De esto, se sigue que $-sx_0\in T$; pero $s(-x_0)\in T$ significa que $-x_0\in T$, es decir, $x_0\in -T$ lo cual es una contradicción. □

De 2.1.11., se obtiene que los preórdenes maximales y los órdenes en un campo K son el mismo objeto. Sin embargo, como no todo preorden en un campo K es un orden en K; se tiene la siguiente

PROPOSICIÓN 2.1.12. Sea K un campo, entonces todo preorden en K está contenido en un orden en K.

[†)] Sean $x, y\in\mathsf{T}$, entonces existen al menos dos preórdenes T_1, T_2 en $\mathcal{F}$ tal que $x\in T_1$ y $y\in T_2$ Dado que $T_1\subsetneq T_2$ o $T_2\subsetneq T_1$ se tiene que $x, y\in T_1$ o $x, y\in T_2$. Como T_1 y T_2 son preórdenes en K, entonces $x+y\in T_1$ o $x+y\in T_2$, también $xy\in T_1$ o $xy\in T_2$; así, $x+y\in\mathsf{T}$ y $xy\in\mathsf{T}$. Ahora, sea $x\in K$, entonces existe $T\in\mathsf{T}$ tal que $x^2\in T$. Finalmente, $-1\notin\mathsf{T}$ porque de lo contrario existiría un preorden $T\in\mathcal{F}$ tal que $-1\in T$. Luego T es un preorden en K que contiene a T.

DEMOSTRACIÓN

Sea T un preorden en K y considérese la familia $\mathcal{F}$ de todos los preórdenes T′en K que contienen a T (ver lo escrito después de la observación 2.1.10.). Por el lema de Zorn, el conjunto parcialmente ordenado por inclusión $(\mathcal{F}, \subseteq)$ tiene al menos un elemento maximal, es decir, $(\mathcal{F}, \subseteq)$ tiene al menos un preorden maximal. Sea T′ un preorden maximal en *K* que contiene a T, entonces por 2.1.11., T′ es un orden en K que contiene a T. □

Como una consecuencia de la proposición anterior se tiene

COROLARIO 2.1.13. Sea K un campo, entonces todo preorden T en K es igual a la intersección de todos los órdenes en K que contienen a T.

DEMOSTRACIÓN

Como $T\subseteq\cap T'$, para todo orden T′ que contiene a T, restará probar que $\cap T'\subseteq T$. Sea $x_0\notin T$, entonces $Tx_0\cap(1+T)=\varnothing$ (ya que si $sx_0=1+t$ con t, $s\in T$, se seguiría que $x_0=(1+t)s(1/s)^2\in T$ lo cual no es posible). Sea $T''=T-Tx_0$. T″ es un preorden en K que contiene a T y a $-x_0$.[†)] Por la proposición 2.1.12., el preorden T″ está contenido en un orden S en K; luego $-x_0\in S$ y $x_0\notin S$. Así, $x_0\notin\cap T'$; por lo tanto $\cap T'\subseteq T$ para todo orden T′ que contiene a T. □

Sean T un preorden en un campo K y $x_0\in K\setminus\{0\}$. Si existen $n\in\mathbb{N}\cup\{0\}$ y $t\in T$ con $x_0^{2n+1}+x_0\,t\in T$, entonces $x_0\in T$. En efecto, como $x_0^{2n}+t\in T\setminus\{0\}$, se tiene que $(x_0^{2n}+t)^{-1}\in T$ y $x_0\in(x_0^{2n}+t)^{-1}T\subseteq T$.

Considérese el conjunto $X=\{x\in K \mid \text{existen } n\in\mathbb{N}\cup\{0\} \text{ y } t\in T \text{ tal que } x^{2n+1}+xt\in T\}$. Dado que, para $n=0$ y $t=0$, se tiene que $x\in T$, el preorden T está contenido en X, es decir, $T=\{x\in K \mid \text{existen } n\in\mathbb{N}\cup\{0\} \text{ y } t\in T \text{ tal que } x^{2n+1}+xt\in T\}$ para todo preorden T en K. Del corolario 2.1.13., se sigue que X, para un preorden T en K, es igual a la intersección de todos los órdenes en K que contienen a T. De la similitud que existe entre X y el radical de un ideal en un anillo, se conviene en llamar al conjunto X para un preorden T en K, el **radical del preorden T**, esto es, $rad(T):=\{x\in K \mid \text{existen } n\in\mathbb{N}\cup\{0\} \text{ y } t\in T \text{ tal que } x^{2n+1}+xt\in T\}$. Luego siguiendo esta similitud, se dirá que un preorden T en un campo K es un **preorden radical** si $T=rad(T)$. Se observa que todo preorden en un campo K es un preorden radical. De lo anterior, el corolario 2.1.13., se puede escribir como: *El radical de todo preorden T en un campo K es igual a la intersección de todos los órdenes en K que contienen a T.*

A continuación se enuncia el resultado principal en esta sección

TEOREMA 2.1.14. (*Clásico de Artin y Schreier*) Un campo K es ordenado si y sólo si K es un campo real.

[†)] Es fácil verificar que $T''+T''\subseteq T$, $T''\cdot T''\subseteq T''$, $K^2\subseteq T''$ y $-1\notin T''$.

DEMOSTRACIÓN ($\Rightarrow$)

Sea T un orden en K, entonces $\sum K^2 \subseteq T$. Como $-1 \notin T$, se sigue que $-1 \notin \sum K^2$. Luego K es un campo real.

($\Leftarrow$)

Si K es un campo real, entonces $-1 \notin \sum K^2$, esto es, $\sum K^2$ es un preorden en K. Por 2.1.12., $\sum K^2$ está contenido en un orden en K. Por tanto K es ordenado. □

Como una aplicación del teorema clásico de Artin y Schreier se tiene el siguiente

COROLARIO 2.1.15. Sea K un campo ordenado, entonces $\sum K^2$ es la intersección de todos los órdenes en K.

DEMOSTRACIÓN

Como K es ordenado, esto significa que K es real, entonces $-1 \notin \sum K^2$ y $\sum K^2$ es un preorden en K. Por 2.1.13., y por el hecho de que $\sum K^2$ está contenido en todo orden de K, se sigue que $\sum K^2 = \cap T$ para todo orden T en K. □

El corolario 2.1.15., afirma que los elementos en K, que se pueden escribir como una suma finita de cuadrados en K son precisamente aquellos elementos que están en todo orden de K y recíprocamente. Esto motiva la siguiente

DEFINICIÓN 2.1.16. Sea K un campo ordenado. Se dice que un elemento $a \in K$ es **totalmente positivo** si $a \in T$ para todo orden T en K.

Otra consecuencia del teorema clásico de Artin y Schreier que se sigue directamente de 2.1.3., es la siguiente

OBSERVACIÓN 2.1.17. Todo campo real es de característica cero. □

De la proposición 2.1.11., se deduce el siguiente

LEMA 2.1.18. Sea K un campo ordenado, T_1 y T_2 órdenes en K. Si $T_1 \subseteq T_2$, entonces $T_1 = T_2$.

DEMOSTRACIÓN

Supóngase que $T_1 \subsetneq T_2$ y considérese un elemento $x \in T_2$ tal que $x \notin T_1$, entonces $-x \in T_1$ y $-x \in T_2$; pero esto último, no puede ser posible. □

El lema 2.1.18., asegura que, no es posible construir cadenas de contenciones de órdenes en un campo K, es decir, todos los órdenes en K son maximales. Resumiendo 2.1.18. y 2.1.11., se tiene que: *los preórdenes maximales, los órdenes y los órdenes maximales en un campo K son el mismo objeto.*

PROPOSICIÓN 2.1.19. Sea K un campo ordenado. Entonces K tiene un único orden si y sólo si $\sum K^2$ es un orden en K.

DEMOSTRACIÓN ($\Rightarrow$)

Como $\sum K^2 = \cap T$ para todo orden T en K (ver 2.1.15.) y dado que $T = \cap T$ para todo orden T en K, el resultado se sigue.

($\Leftarrow$)

Como $\sum K^2$ es un orden en K, entonces $\sum K^2 \subseteq T$ para todo orden T en K. Por el lema 2.1.18., se sigue que $\sum K^2 = T$ para todo orden T en K. Luego $\sum K^2$ es el único orden en K. □

EJEMPLO 2.1.20. Los campos $\mathbb{Q}$ y $\mathbb{R}$ tienen un único orden, ya que $\sum \mathbb{Q}^2$ y $\sum \mathbb{R}^2$ son órdenes en $\mathbb{Q}$ y $\mathbb{R}$ respectivamente.

EJEMPLO 2.1.21. El campo cuadrático $\mathbb{Q}(\sqrt{2})$ es el ejemplo más sencillo de un campo ordenado que tiene mas de un orden (ver ejemplo 2.1.8.).

2.2. ANILLOS ORDENADOS.

Como se comentó en la introducción de este capítulo, en esta sección se desarrollará la teoría de Artin-Schreier para anillos en forma paralela a la desarrollada en la sección anterior para campos. Se empieza dando la siguiente

DEFINICIÓN 2.2.1. Sea A un anillo. Una relación binaria $\leq$ en A es una **relación de orden** de A si $\leq$ satisface que para a, b y c elementos arbitrarios en A

i) $a \leq a$.
ii) si $a \leq b$ y $b \leq a$, entonces $a = b$.
iii) si $a \leq b$ y $b \leq c$, entonces $a \leq c$.
iv) $a \leq b$ o $b \leq a$.
v) si $a \leq b$, entonces $a + c \leq b + c$.
vi) si $0 \leq a$ y $0 \leq b$, entonces $0 \leq ab$.

El par $(A, \leq)$ se denomina **anillo ordenado**.

EJEMPLO 2.2.2. $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ con sus relaciones de órdenes usuales son anillos ordenados.

EJEMPLO 2.2.3. El anillo $\mathbb{Z}[\sqrt{2}]$ con la relación de orden: Si $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ con $\alpha = m_1 + n_1\sqrt{2}$ y $\beta = m_2 + n_2\sqrt{2}$, entonces

$$\alpha \leq \beta \text{ si } [m_2 - m_1 \geq 0 \text{ y } (m_2 - m_1)^2 \geq 2(n_2 - n_1)^2] \text{ o } [n_2 - n_1 \geq 0 \text{ y } 2(n_2 - n_1)^2 \geq (m_2 - m_1)^2]$$

es un anillo ordenado.

Como en el caso de campos, si A es un anillo, la función $\varphi: \mathbb{Z} \to A$; con regla de correspondencia $\varphi(n) = n \cdot 1$ ($n \cdot 1 = 1 + 1 + \cdots + 1$, ($n$ veces)) es un homomorfismo de anillos cuya imagen se denomina **subanillo primo** de A. Su núcleo $Ker(\varphi) = m\mathbb{Z}$, para un único $m \geq 0$ es

llamado **característica** de A. En el caso de anillos se tiene el siguiente resultado que es paralelo a 2.1.3..

OBSERVACIÓN 2.2.4. Todo anillo ordenado A es de característica cero.

DEMOSTRACIÓN

La demostración de que $car(A)=0$ es similar a la demostración de 2.1.3.. □

A continuación se introduce el concepto de preorden en un anillo en una forma similar que para campos, es decir,

DEFINICIÓN 2.2.5. Sea A un anillo. Un subconjunto T en A es un **preorden** en A si

i) $T+T\subseteq T$.
ii) $T\cdot T\subseteq T$.
iii) $A^2\subseteq T$.
iv) $-1\notin T$.

Como en el caso de campos, se tiene el siguiente (ver 2.1.5.)

EJEMPLO 2.2.6. Sea A un anillo, entonces el conjunto $T=\{a\in A|0\leq a\}$ es un preorden en A.

EJEMPLO 2.2.7. Sea $\mathbb{R}[x]$ el anillo de polinomios en la indeterminada x con coeficientes en $\mathbb{R}$. El conjunto $T(a)=\{a_0+a_1(x-a)+\cdots+a_n(x-a)^n|\, a_0\geq 0\}$ para cada $a\in\mathbb{R}$ fija, es un preorden en $\mathbb{R}[x]$. En efecto, sean $f, g\in T(a)$;

$$f=a_0+a_1(x-a)+\cdots+a_n(x-a)^n \text{ y } g=b_0+b_1(x-a)+\cdots+b_m(x-a)^m$$

con $a_0\geq 0$ y $b_0\geq 0$. Supóngase que $m\leq n$, entonces

$$f+g=(a_0+b_0)+(a_1+b_1)(x-a)+\cdots+(a_m+b_m)(x-a)^m+\cdots+a_n(x-a)^n.$$

Como $a_0+b_0\geq 0$, se sigue que $f+g\in T(a)$ y $T(a)+T(a)\subseteq T(a)$. Sea ahora;

$$fg=a_0b_0+\cdots+a_0b_m(x-a)^m+\cdots+a_nb_0(x-a)^n+\cdots+a_nb_m(x-a)^{n+m},$$

luego $fg\in T(a)$ ya que $a_0b_0\geq 0$; así, $T(a)T(a)\subseteq T(a)$. Si $f\in\mathbb{R}[x]$, $f=a_0+a_1(x-a)+\cdots+a_n(x-a)^n$, entonces

$$f^2=a_0^2+\cdots+a_n^2(x-a)^{2n}$$

con $a_0^2\geq 0$ y se sigue que $f^2\in T(a)$ y $\mathbb{R}[x]^2\subseteq T(a)$. Finalmente $-1\notin T(a)$ ya que $a_0\geq 0$ para todo $f\in T(a)$. De 2.2.5., se sigue que $T(a)$ para toda $a\in\mathbb{R}$ fija, es un preorden en $\mathbb{R}[x]$.

EJEMPLO 2.2.8. Los conjuntos

$$T(a_+)=\{0\}\cup\{a_m(x-a)^m+a_{m+1}(x-a)^{m+1}+\cdots+a_n(x-a)^n \mid 0\le m\le n,\ a_m>0\}\ \text{y}$$

$$T(a_-)=\{0\}\cup\left\{ a_m(x-a)^m+a_{m+1}(x-a)^{m+1}+\cdots+a_n(x-a)^n \mid 0\le m\le n,\ \begin{cases} a_m>0 & \text{si } m \text{ es par} \\ a_m<0 & \text{si } m \text{ es impar} \end{cases} \right\}$$

para toda $a\in\mathbb{R}$ fija, son preórdenes en $\mathbb{R}[x]$. En efecto, sean $f, g\in T(a_+)$ con

$$f=a_m(x-a)^m+a_{m+1}(x-a)^{m+1}+\cdots+a_n(x-a)^n,\ g=b_t(x-a)^t+b_{t+1}(x-a)^{t+1}+\cdots+b_s(x-a)^s$$

donde $0\le m\le n$, $a_m>0$; $0\le t\le s$, $b_t>0$. Si $m\le t$ y $s\le n$, entonces

$$f+g=a_m(x-a)^m+\cdots+(a_t+b_t)(x-a)^t+\cdots+(a_s+b_s)(x-a)^s+\cdots+a_n(x-a)^n$$

donde $0\le m\le n$, $a_m>0$ luego $f+g\in T(a_+)$ y $T(a_+)+T(a_+)\subseteq T(a_+)$ (para los casos $m\le t$ y $n\le s$, $t\le m$ y $n\le s$, $t\le m$ y $s\le n$ también se cumple que $f+g\in T(a_+)$). Ahora, considérese el producto de f y g, con $0\le m\le n$, $a_m>0$; $0\le t\le s$, $b_t>0$ y $m\le t$ y $s\le n$. Entonces

$$fg=a_mb_t(x-a)^{m+t}+\cdots+a_nb_s(x-a)^{n+s}$$

$$=c_{m+t}(x-a)^{m+t}+\cdots+c_{n+s}(x-a)^{n+s},$$

Dado que $0\le m+t\le n+s$ y $c_{m+t}=a_mb_t>0$; se sigue que $fg\in T(a_+)$ y $T(a_+)\cdot T(a_+)\subseteq T(a_+)$. Si $f\in\mathbb{R}[x]$ con

$$f=a_0+a_1(x-a)+\cdots+a_n(x-a)^n,$$

entonces

$$f^2=a_0^2+\cdots+a_n^2(x-a)^{2n}.$$

Si $f\equiv 0$, $f^2\in T(a_+)$: Si f no es el polinomio cero, entonces haciendo $a_j=min\{a_i \mid a_i\neq 0\}$, se tiene que $a_j^2>0$ y $f^2\in T(a_+)$; de esta forma $\mathbb{R}[x]^2\subseteq T(a_+)$. Si $f\in T(a_+)$, entonces se sabe que el término constante en f es cero o mayor que cero; luego $-1\notin T(a_+)$. Por lo tanto $T(a_+)$ es un preorden en $\mathbb{R}[x]$. En forma similar se prueba que $T(a_-)$ es un preorden en $\mathbb{R}[x]$.

De los dos ejemplos anteriores es fácil ver que

$$T(a_-)\subsetneq T(a),\ T(a_+)\subsetneq T(a),\ T(a_-)\not\subseteq T(a_+) \text{ y } T(a_+)\not\subseteq T(a_-)$$

para cada $a\in\mathbb{R}$ fija. También se observa que $T(a)=T(a_+)+\langle x-a\rangle$ para toda $a\in\mathbb{R}$.

EJEMPLO 2.2.9. El conjunto $T(a)^{(r)}=T(a_+)+\langle(x-a)^r\rangle$ con $r\in\mathbb{N}$ y $a\in\mathbb{R}$ fija donde $T(a_+)$ es el preorden del ejemplo 2.2.8., y $\langle(x-a)^r\rangle=\{(x-a)^rq \mid q\in\mathbb{R}[x]\}$ es un preorden en $\mathbb{R}[x]$.

En efecto, sea $T(a_+)$ como en el ejemplo anterior, $T(a)^{(r)}=\{p+(x-a)^rq \mid p\in T(a_+), q\in\mathbb{R}[x]\}$ y considérese $f_1, f_2\in T(a)^{(r)}$ con $f_1=p_1+(x-a)^rq_1$ y $f_2=p_2+(x-a)^rq_2$, entonces

$$f_1+f_2=(p_1+p_2)+(x-a)^r(q_1+q_2).$$

Dado que $p_1+p_2\in T(a_+)$ y $q_1+q_2\in\mathbb{R}[x]$, entonces $f_1+f_2\in T(a)^{(r)}$ y $T(a)^{(r)}+T(a)^{(r)}\subseteq T(a)^{(r)}$. Como

$$f_1f_2=p_1p_2+(x-a)^r[p_1q_2+p_2q_1+(x-a)^rq_1q_2]$$

con $p_1p_2\in T(a_+)$ y $(p_1q_2+p_2q_1+(x-a)^rq_1q_2)\in\mathbb{R}[x]$; se tiene que $f_1f_2\in T(a)^{(r)}$ y $T(a)^{(r)}\cdot T(a)^{(r)}\subseteq T(a)^{(r)}$. Sea $f\in\mathbb{R}[x]$, el polinomio $f=a_0+a_1(x-a)+\cdots+a_n(x-a)^n$ y

$$f^2=a_0^2+a_1'(x-a)+\cdots+a_r'(x-a)^r+\cdots+a_n'(x-a)^n+a'_{n+1}(x-a)^{n+1}+\cdots+a_n^2(x-a)^{2n};$$

$$f^2=a_0^2+a_1'(x-a)+\cdots+a'_{r-1}(x-a)^{r-1}+(x-a)^r(a_r'+a'_{r+1}(x-a)+\cdots+a_n^2(x-a)^{2n-r}),$$

con $a_0^2+a'_1(x-a)+\cdots+a'_{r-1}(x-a)^{r-1}\in T(a_+)$ y $(a'_r+a'_{r+1}(x-a)+\cdots+a_n^2(x-a)^{2n-r})\in\mathbb{R}[x]$; luego, $f^2\in T(a)^{(r)}$ y $\mathbb{R}[x]^2\subseteq T(a)^{(r)}$. Dado que $-1=[-1+(x+a)]+(x+a)(-1)$ donde $-1\in\mathbb{R}[x]$ y $r=1$, se tiene que $-1+(x+a)\notin T(a_+)$; entonces $-1\notin T(a)^{(r)}$. Por lo tanto $T(a)^{(r)}$es un preorden en $\mathbb{R}[x]$ para todo $r\in\mathbb{N}$ y $a\in\mathbb{R}$.

Los conjuntos

$$T(+\infty)=\{0\}\cup\{a_0+a_1x+\cdots+a_nx^n \mid a_n>0\} \text{ y}$$

$$T(-\infty)=\{0\}\cup\{a_0+a_1x+\cdots+a_nx^n \mid a_n>0 \text{ si } n \text{ es par y } a_n<0 \text{ si } n \text{ es impar}\}$$

son preordenes en el anillo $\mathbb{R}[x]$. En efecto, es sencillo verificar que se satisface la definición 2.2.5.. Por otro lado, si K es un campo y T es un preorden en K, entonces se tiene que $T\cap -T=\{0\}$. En el caso en que A es un anillo y T es un preorden en A, en general se tendrá que $T\cap -T\neq\{0\}$. Como un ejemplo de esto, se tiene el preorden $T(a)$ del ejemplo 2.2.7., que cumple $T(a)\cap -T(a)=<x-a>\neq\{0\}$ para toda $a\in\mathbb{R}$ fija.

DEFINICIÓN 2.2.10. Sea A un anillo y T un preorden en A. El conjunto $\mathcal{C}(T)=T\cap -T$ se denomina **centro** de T.

En el caso particular en que A es un campo, se tiene que $\mathcal{C}(T)=\{0\}$ que es un ideal primo. De hecho es un ideal maximal.

Acerca de las estructuras que pueden ser definidas en el centro de un preorden en un anillo A, se tienen los siguientes

PROPOSICIÓN 2.2.11. Sea A un anillo y T un preorden en A, entonces el centro de T, $\mathcal{C}(T)$ es un subgrupo de A bajo la suma.

DEMOSTRACIÓN

1°) $\mathcal{C}(T)\neq\varnothing$ pues $0\in\mathcal{C}(T)$. 2°) Sean $a, b\in\mathcal{C}(T)$, entonces $a, b\in T$ y $a, b\in -T$. Luego

$a+b\in$T y $a+b\in$-T; de esta forma, $a+b\in\mathcal{C}$(T). 3°) Sea $a\in\mathcal{C}$(T), entonces $a\in$T y $a\in$-T, luego $-a\in$T, $-a\in$-T y $\mathcal{C}$(T) es un subgrupo aditivo de A. □

OBSERVACIÓN 2.2.12. Sea A un anillo y T un preorden en A. Si T$\cup$-T=A, entonces el centro $\mathcal{C}$(T) de T es un ideal de A.

DEMOSTRACIÓN

Sea $a\in\mathcal{C}$(T), entonces $a\in$T y $-a\in$T. Sea $b\in$A, como T$\cup$-T=A, se sigue que $b\in$T o $b\in$-T. Si $b\in$T, se tiene que $ab\in$T y $ab\in$-T, esto significa que $ab\in\mathcal{C}$(T) y $\mathcal{C}$(T) es un ideal en A. El otro caso es similar. □

En el caso del preorden T(a) para cada $a\in\mathbb{R}$ fija del ejemplo 2.2.7., su centro $\mathcal{C}$(T(a))=<x-a> es un ideal primo de $\mathbb{R}[x]$ (de hecho <x-a> es un ideal maximal de $\mathbb{R}[x]$). En este caso particular, T(a) no satisface 3°)′ de la observación 2.1.9., esto indica que es necesario generalizar la definición de orden en el caso de anillos. Esto último y 2.2.12., proporcionan información acerca de cuando un preorden T en un anillo A es un orden en A, es decir,

DEFINICIÓN 2.2.13. Sea A un anillo y T un preorden en A. T es un **orden** en A si

v) $\mathcal{C}$(T)=T$\cap$-T es un ideal primo de A.

vi) T$\cup$-T=A.

Se observa que si al menos uno de los órdenes en un anillo A tiene como centro el ideal cero, entonces A es un dominio entero. Este resultado es falso para cualquier anillo ordenado, esto es, *no todo anillo ordenado es un dominio entero*; como un ejemplo se tiene el anillo $\mathcal{E}(n)$ de gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$ (ver capítulo 4). Se sabe que $\mathcal{E}(n)$ es un anillo ordenado[†)]; un orden T en $\mathcal{E}(n)$ viene dado como T=$\{f\in\mathcal{E}(n) \mid f(0)\geq 0\}$ con centro el ideal $m(n)$ ($\neq(0)$) cuyos elementos son los gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$ que se anulan en cero. El anillo $\mathcal{E}(n)$ no es un dominio entero.

EJEMPLO 2.2.14. El preorden T(a) del ejemplo 2.2.7., es un orden en $\mathbb{R}[x]$ para toda $a\in\mathbb{R}$ fija.

En efecto, *v*) sea T(a)=$\{a_0+a_1(x-a)+\cdots+a_n(x-a)^n \mid a_0\geq 0\}$, claramente T($a$)$\cap$-T($a$)= <$x$-$a$> con <$x$-$a$> un ideal maximal en $\mathbb{R}[x]$. *vi*) Sea $f\in\mathbb{R}[x]$, $f=a_0+a_1(x-a)+\cdots+a_n(x-a)^n$. Como $a_0\in\mathbb{R}$, se sigue que $a_0<0$ o $a_0=0$ o $a_0>0$. Así, T(a)$\cup$-T(a)=$\mathbb{R}[x]$.

En el ejemplo anterior se observa que el centro del orden T(a), para toda $a\in\mathbb{R}$, $\mathcal{C}$(T(a))=<x-a> es un ideal real de $\mathbb{R}[x]$ ya que $\mathbb{R}[x]/\langle x-a\rangle\cong\mathbb{R}$.

EJEMPLO 2.2.15. Los preórdenes T(a_+) y T(a_-), del ejemplo 2.2.8., son órdenes en $\mathbb{R}[x]$ para cada $a\in\mathbb{R}$ fija.

[†)] De hecho $\mathcal{E}(n)$ es un anillo real.

En efecto, *v*) claramente $T(a_+)\cap\text{-}T(a_+)=\{0\}$ el cual es un ideal primo en $\mathbb{R}[x]$. *vi*) Sea $f\in\mathbb{R}[x]$, $f=a_0+a_1(x-a)+\cdots+a_n(x-a)^n$. Como $a_0\in\mathbb{R}$, se tiene que $a_0<0$ o $a_0=0$ o $a_0>0$, esto es, $f\notin T(a_+)$ o $f\notin T(a_+)\cap\text{-}T(a_+)$ o $f\notin\text{-}T(a_+)$; en cualesquiera de los casos, $f\in T(a_+)\cup\text{-}T(a_+)$. En forma similar se prueba que $T(a_-)$ es un orden en $\mathbb{R}[x]$.

Es fácil ver que los preórdenes $T(+\infty)$ y $T(-\infty)$ en $\mathbb{R}[x]$ son órdenes en $\mathbb{R}[x]$ con centros $\mathcal{C}(T(+\infty))=\{0\}$ y $\mathcal{C}(T(-\infty))=\{0\}$. Por otro lado, se observa que:

$T(+\infty)\not\subseteq T(-\infty)$ y $T(-\infty)\not\subseteq T(+\infty)$, $T(+\infty)\not\subseteq T(a)$ y $T(a)\not\subseteq T(+\infty)$, $T(-\infty)\not\subseteq T(a)$ y $T(a)\not\subseteq T(-\infty)$, $T(+\infty)\not\subseteq T(a_+)$ y $T(a_+)\not\subseteq T(+\infty)$, $T(-\infty)\not\subseteq T(a_+)$ y $T(a_+)\not\subseteq T(-\infty)$, $T(+\infty)\not\subseteq T(a_-)$ y $T(a_-)\not\subseteq T(+\infty)$, $T(-\infty)\not\subseteq T(a_-)$ y $T(a_-)\not\subseteq T(\infty)$

para toda $a\in\mathbb{R}$ fija. Se observa también que existe una biyección entre el conjunto de cortaduras de los números reales $C(-\infty)=(\varnothing\,,\mathbb{R})$, $C(a_-)=((-\infty\,,a)\,,[a\,,+\infty))$, $C(a_+)=((-\infty\,,a],(a\,,+\infty))$ y $C(+\infty)=(\mathbb{R}\,,\varnothing)$ para cada $a\in\mathbb{R}$ y el conjunto de los órdenes $T(-\infty)$, $T(a_-)$, $T(a_+)$ y $T(+\infty)$ para toda $a\in\mathbb{R}$ fija. La biyección viene dada como: A $C(-\infty)$ se le asigna $T(-\infty)$, a $C(a_-)$ se le asigna $T(a_-)$, a $C(a_+)$ se le asigna $T(a_+)$ y a $C(+\infty)$ se le asigna $T(+\infty)$ para cada $a\in\mathbb{R}$

OBSERVACIÓN 2.2.16. Si $\varphi:A\to B$ es un homomorfismo de anillos semireales y T_B es un orden en B, entonces $\varphi^{-1}(T_B)$ es un orden de A con centro $\varphi^{-1}(\mathcal{C}(T_B))$.

DEMOSTRACIÓN.

Sean $a,\ b\in\varphi^{-1}(T_B)$, entonces $\varphi(a),\ \varphi(b)\in T_B$ lo cual significa que $\varphi(a+b)\in T_B$ y $\varphi(ab)\in T_B$, luego $a+b\in\varphi^{-1}(T_B)$ y $ab\in\varphi^{-1}(T_B)$. De esta forma, $\varphi^{-1}(T_B)+\varphi^{-1}(T_B)\subseteq\varphi^{-1}(T_B)$ y $\varphi^{-1}(T_B)\varphi^{-1}(T_B)\subseteq\varphi^{-1}(T_B)$. Si $a\in A$, entonces $\varphi(a^2)=\varphi(a)^2\in B^2\subseteq T_B$ y $a^2\in\varphi^{-1}(T_B)$, esto es, $A^2\subseteq\varphi^{-1}(T_B)$. Si $-1\in\varphi^{-1}(T_B)$, se tendrá que $\varphi(-1)=-\varphi(1)=-1\in T_B$ lo cual no es posible; luego $-1\notin\varphi^{-1}(T_B)$. Sea $\mathcal{C}(T_B)$ el centro de T_B, $\varphi^{-1}(\mathcal{C}(T_B))=\varphi^{-1}(T_B\cap\text{-}T_B)=\varphi^{-1}(T_B)\cap\text{-}\varphi^{-1}(T_B)$.[†] Dado que $\mathcal{C}(T_B)$ es un ideal primo en B, se sigue que $\varphi^{-1}(\mathcal{C}(T_B))$ es un ideal primo en A. Finalmente, se tiene que $\varphi^{-1}(B)=\varphi^{-1}(T_B\cup\text{-}T_B)=\varphi^{-1}(T_B)\cup\text{-}\varphi^{-1}(T_B)=A$.[‡] Por lo tanto se sigue que $\varphi^{-1}(T_B)$ es un orden en el anillo A con centro $\varphi^{-1}(\mathcal{C}(T_B))$. □

PROPOSICIÓN 2.2.17. Un subconjunto T en un anillo A es un orden de A si y sólo si existe un campo ordenado (K , P) y un homomorfismo $\varphi:A\to K$ tal que $T=\{a\in A\mid\varphi(a)\in P\}$.

DEMOSTRACIÓN ($\Rightarrow$)

Sea T un orden de un anillo A con centro $\mathcal{C}(T)$ y considérese el dominio entero $A/\mathcal{C}(T)$. Se afirma que $P=\{\overline{(a,b)}\mid ab\in T\}$ es un orden del campo de cocientes $K=qf(A/\mathcal{C}(T))$ y $\varphi^{-1}(P)=T$ donde $\varphi:A\to K$ es el homomorfismo natural. En efecto, sean $\overline{(a,b)},\ \overline{(c,d)}\in P$, luego se tiene que $ab\in T$, $cd\in T$ y $(ab)(cd)\in T$. Dado que $b^2,\ d^2\in T$ y $abd^2+cb^2d\in T$, se sigue

---

[†] Sea $a\in\varphi^{-1}(\text{-}T_B)$, entonces $\varphi(a)\in\text{-}T_B$, esto es, $-\varphi(a)\in T_B$ y $\varphi(-a)\in T_B$, luego $-a\in\varphi^{-1}(T_B)$ y $a\in\text{-}\varphi^{-1}(T_B)$. El recíproco es similar.

[‡] Si $\varphi(A)\subseteq B$, entonces $A\subseteq\varphi^{-1}(\varphi(A))\subseteq\varphi^{-1}(B)\subseteq A$.

que $(ad+bc)bd \in T$, $\overline{(ad+bc,bd)} \in P$ y $\overline{(ac,bd)} \in P$. De esta forma, $P+P \subseteq P$ y $PP \subseteq P$. Si $\overline{(a,b)^2} \in K^2$, como $\overline{(a,b)^2} = \overline{(a^2,b^2)}$, se tiene que a^2, $b^2 \in A^2 \subseteq T$ y $a^2b^2 \in T$, entonces se obtiene que $\overline{(a,b)^2} \in P$ y $K^2 \subseteq P$. Si $\overline{(-1,1)} \in P$, se sigue que $(-1)(1)=-1 \in T$ lo cual es una contradicción; de esta forma se tiene que $\overline{(-1,1)} \notin P$. Finalmente, sea $\overline{(a,b)} \in K$ con $a, b \in A$ y $b \notin \mathcal{C}(T)$ ($b \notin T$ o $b \notin -T$). Dado que $A=T \cup -T$, se sigue que $a \in T$ o $a \in -T$. Si $b \in T \setminus \mathcal{C}(T)$, resulta que $ab \in T$ o $ab \in -T$; lo cual significa que $ab \in T \cup -T$, luego $\overline{(a,b)} \in P$ o $\overline{(a,b)} \in -P$; así, $\overline{(a,b)} \in P \cup -P$ y $P \cup -P = K$. Por lo tanto, P es un orden en K. Falta probar que $\varphi^{-1}(P)=T$. Sea $a \in \varphi^{-1}(P)$, entonces $\varphi(a)=\overline{(b,c)} \in P$ con $c \notin \mathcal{C}(T)$ y $bc \in T$. Si $c \in T$, entonces $b \in T$ ya que $c \notin -T$. Haciendo $ac=b+d$ para algún $d \in \mathcal{C}(T)$, se tiene que $ac \in T$. Dado que $c \notin -T$ y $a \in T$, entonces $\varphi^{-1}(P) \subseteq T$ y recíprocamente.

($\Leftarrow$)

Sea (K , P) un campo ordenado y $\varphi: A \to K$ un homomorfismo. Claramente el conjunto de elementos en A cuya imagen bajo φ están en P, esto es, $\{a \in A \mid \varphi(a) \in P\}$ es un orden en A. □

COROLARIO 2.2.18. Todos los centros de órdenes en A son precisamente ideales primos reales en A.

DEMOSTRACIÓN

Como $F=qf(A/\mathcal{C}(T))$ es un campo ordenado, por el teorema clásico de Artin y Schreier, $F=qf(A/\mathcal{C}(T))$ es un campo real. Por 1.2.17., $A/\mathcal{C}(T)$ es un dominio entero real y $\mathcal{C}(T)$ es un ideal primo real. □

Para los órdenes $T(a)$, $T(a_+)$ y $T(a_-)$ de los ejemplos 2.2.14. y 2.2.15., que satisfacen $T(a_+) \subsetneq T(a)$ y $T(a_-) \subsetneq T(a)$ sus centros $\mathcal{C}(T(a))=\langle x-a \rangle$, $\mathcal{C}(T(a_+))=\{0\}$ y $\mathcal{C}(T(a_-))=\{0\}$ satisfacen $\{0\} \subsetneq \langle x-a \rangle$ para cada $a \in \mathbb{R}$. En el caso general, se tiene la siguiente

OBSERVACIÓN 2.2.19. Sea A un anillo, T y T′ órdenes en A con centros $\mathcal{C}(T)$ y $\mathcal{C}(T')$ respectivamente. Si $T \subsetneq T'$, entonces $\mathcal{C}(T) \subsetneq \mathcal{C}(T')$.

DEMOSTRACIÓN

Supóngase que $\mathcal{C}(T)=\mathcal{C}(T')$ y sea $a \in T'$ con $a \notin T$, entonces $a \in -T \subsetneq -T'$. Como $a \in T'$, se tiene que $a \in T' \cap -T' = \mathcal{C}(T')$. Dado que $\mathcal{C}(T)=\mathcal{C}(T')$ y $a \in \mathcal{C}(T)$, se sigue que $a \in T$ lo cual es una contradicción. □

El concepto de preorden maximal (orden maximal) en un anillo, se define en forma similar que para campos utilizando el lema de Zorn (ver lo escrito después de 2.1.10.). Se observa que $T(+\infty)$ y $T(-\infty)$ son órdenes maximales en $\mathbb{R}[x]$. En efecto, supóngase que $T(+\infty)$ no es un orden maximal en $\mathbb{R}[x]$, entonces existe un orden T en $\mathbb{R}[x]$ tal que $T(+\infty) \subsetneq T$. Como el centro de $T(+\infty)$ es $\{0\}$ y los únicos ideales primos reales en $\mathbb{R}[x]$ son

$\{0\}$ y $\langle x\text{-}a\rangle$ para toda $a\in\mathbb{R}$ fija, se sigue de la observación 2.2.19., que el centro del orden T es $\langle x\text{-}a\rangle$ para $a\in\mathbb{R}$ fija. Se afirma que $T=T(a)$ con $a\in\mathbb{R}$ fija. En efecto, sea $f\in T$; como $\langle x\text{-}a\rangle = T\cap -T\subseteq T$, se sigue que $(x-a),(x-a)^2\in T$ y en general $(x-a)^n\in T$ para $n\in\mathbb{N}$, luego $(x-a)+(x-a)^2+\cdots+(x-a)^n\in T$. Entonces se tiene que

$$a_0 = f-[a_1(x-a)+a_2(x-a)^2+\cdots+a_n(x-a)^n]\in T$$

con $a_0\geq 0$, por consiguiente $T\subseteq T(a)$. La otra contención se prueba de manera similar; de lo anterior se tiene que $T(+\infty)\subsetneq T(a)$. Ahora, considérese el polinomio $f=x-(a+1)$, se observa que f está en $T(+\infty)$ y f no está en $T(a)$ pero esto último no puede ser posible. Por lo tanto $T(+\infty)$ es un orden maximal en $\mathbb{R}[x]$. De manera similar se prueba que $T(-\infty)$ es un orden maximal.

Se sabe que todo orden T en un campo K es un orden maximal en K (ver 2.1.18.); en el caso de anillos, no todo orden en A es un orden maximal en A. Pero si el centro de T es un ideal maximal, entonces la situación cambia, es decir,

OBSERVACIÓN 2.2.20. Sea A un anillo y T un orden en A. Si $\mathcal{C}(T)$, el centro de T es un ideal maximal, entonces T es un orden maximal en A.

DEMOSTRACIÓN

Supóngase que T no es un orden maximal en A, es decir, existe un orden T' en A tal que $T\subsetneq T'\subsetneq A$. Sea $\mathcal{C}(T')$ el centro de T', como $T\subsetneq T'$, se sigue que $\mathcal{C}(T)\subsetneq\mathcal{C}(T')$ (ver 2.2.19.). Pero esto último no puede ser posible ya que $\mathcal{C}(T)$ es un ideal maximal. □

$T(+\infty)$ y $T(-\infty)$ son ejemplos de órdenes que muestran que el recíproco de la observación 2.2.20., es falso en general.

El siguiente criterio establece cuando un preorden en un anillo A es un orden en A.

TEOREMA 2.2.21. Sea A un anillo y T un preorden en A. Entonces T es un orden en A si y sólo si para cada $ab\in -T$ implica que al menos $a\in T$ o $b\in T$.

DEMOSTRACIÓN ($\Rightarrow$)

Sea T un orden en A con centro $\mathcal{C}(T)$ y supóngase que $ab\in -T$ pero $a\notin T$ y $b\notin T$. Entonces $a\in -T$ y $b\in -T$; luego $ab\in T$ y $ab\in\mathcal{C}(T)$. Como $\mathcal{C}(T)$ es un ideal primo de A, se sigue que $a\in\mathcal{C}(T)$ o $b\in\mathcal{C}(T)$ lo cual es una contradicción.

($\Leftarrow$)

Por la definición 2.2.13., se tendrá que probar que $\mathcal{C}(T)$ el centro de T es un ideal primo de A y $T\cup -T=A$. En efecto, sea $ab\in\mathcal{C}(T)$ con $a\notin\mathcal{C}(T)$ para $a, b\in A$; como $ab\in -T$ implica $a\in T$ o $b\in T$, se sigue que *i*) $ab\in -T$ implica $b\in T$ y *ii*) $a(-b)\in -T$ implica $-b\in T$. Luego $b\in\mathcal{C}(T)$ y es un ideal primo de A. Por otro lado, sean $a, b\in A$ con $b=-a$, dado que $ab\in -T$, entonces $a\in T$

o $b\in T$, luego $ab=a(-a)=-a^2\in -T$ implica que $a\in T$ o $-a\in T$, es decir, $a\in T$ o $a\in -T$. Lo anterior significa que $A\subseteq T\cup -T$; así, $T\cup -T=A$. Por lo tanto T es un orden en A. □

Para generalizar el teorema clásico de Artin y Schreier, se necesita generalizar resultados tales como 2.1.11. y 2.1.12.. Para ello se empieza demostrando algunos resultados sobre existencia de órdenes.

LEMA 2.2.22. Sea A un anillo, T un preorden en A y a, $b\in A$ con $ab\in -T$. Entonces al menos uno de los siguientes subconjuntos de A, $T_1=T+Ta$ o $T_2=T+Tb$ es un preorden en A.

DEMOSTRACIÓN

Supóngase que ninguno de los subconjuntos T_1 y T_2 es un preorden en A. Claramente T_1 y T_2 satisfacen *i*), *ii*) y *iii*) de la definición 2.2.5., y por tanto se tiene que $-1\in T_1$ y $-1\in T_2$. Es decir, existen elementos t_1, t_2, s_1, $s_2\in T$ tal que $-1=t_1+s_1a$, $-1=t_2+s_2b$ y $(-s_1a)(-s_2b)=(s_1s_2)(ab)=1+t\in T$ con $t\in T$. Por lo tanto $-1=t-(s_1s_2)(ab)\in T$, lo cual es una contradicción. □

Como un caso particular del lema anterior se tiene el siguiente

COROLARIO 2.2.23. Sea A un anillo y T un preorden en A. Entonces para cada $a\in A$, $T+Ta$ o $T-Ta$ es un preorden en A.

DEMOSTRACIÓN

Sean a, $b\in A$ con $b=-a$, entonces $ab=a(-a)=-a^2\in -T$. Por 2.2.22., se sigue que, uno de los siguientes conjuntos $T+Ta$ o $T-Ta$ es un preorden en A. □

Para anillos, se cumple que todo orden es un preorden. 2.2.9. da un ejemplo de un preorden que no es un orden. En efecto, se puede probar que $T(a)^{(r)}\cap -T(a)^{(r)}=\langle (x-a)^r\rangle$ (para toda $r\in\mathbb{N}$ y toda $a\in\mathbb{R}$ fija) y $\langle (x-a)^r\rangle$ es un ideal primo si y sólo si $r=1$ (recuérdese que $T(a)^{(r)}=T(a_+)+\langle (x-a)^r\rangle$). Para $r\geq 2$, $T(a)^{(r)}$ es un preorden que no es un orden. De 2.2.20., se sigue que $T(a)$ es un orden maximal en $\mathbb{R}[x]$ y $T(a_+)$, $T(a_-)$ no lo son. De esto se observa que 2.1.11. no es valido en general para anillos, esto es, existen órdenes que no son preórdenes maximales. Por ejemplo los órdenes $T(a_+)$ y $T(a_-)$ para cada $a\in\mathbb{R}$ del ejemplo 2.2.15., no son preórdenes maximales.[†)] Sin embargo el recíproco es cierto para anillos, es decir,

OBSERVACIÓN 2.2.24. Sea A un anillo y T un preorden maximal en A, entonces T es un orden en A.

DEMOSTRACIÓN

Supóngase que $ab\in -T$ para a, $b\in A$. Por el lema 2.2.22., uno de los siguientes conjuntos $T+Ta$ o $T+Tb$ es un preorden en A. Como T es un preorden maximal, $T+Ta=T$ o $T+Tb=T$. Esto significa que $a\in T$ o $b\in T$. Luego por el teorema 2.2.21., T es un orden en A.□

[†)] Como se recordará $T(a_-)\subsetneq T(a)$ y $T(a_+)\subsetneq T(a)$ con $T(a)=T(a_+)+\langle x-a\rangle$.

El siguiente resultado que es una consecuencia del teorema anterior generaliza la proposición 2.1.12..

COROLARIO 2.2.25. Sea A un anillo, entonces todo preorden T en A está contenido en un orden en A.

DEMOSTRACIÓN

Como en campos, una vez que se ha aplica el lema de Zorn a la familia de preordenes T′ en A que contienen a un preorden fijo T, se obtiene al menos un elemento maximal de esta familia, esto es, A tiene al menos un preorden maximal. El resultado se sigue de la observación 2.2.24.. □

Los órdenes del ejemplo 2.2.14., $T(a)$ para cada $a\in\mathbb{R}$ fija son órdenes maximales ya que sus centros $\mathcal{C}(T(a))=\langle x-a\rangle$ son ideales maximales en $\mathbb{R}[x]$. Sin embargo, los órdenes del ejemplo 2.2.15., $T(a_+)$ y $T(a_-)$ para toda $a\in\mathbb{R}$ fija no lo son ya que sus centros son $\mathcal{C}(T(a_+))=\{0\}$ y $\mathcal{C}(T(a_-))=\{0\}$ respectivamente. A continuación, como otra consecuencia de 2.2.25., se establece la generalización de la proposición 2.1.11.. Ella afirma que los órdenes maximales y los preórdenes maximales son el mismo objeto.

COROLARIO 2.2.26. Sea A un anillo y T un orden en A. Entonces T es un orden maximal si y sólo si T es un preorden maximal.

DEMOSTRACIÓN ($\Rightarrow$)

Sea T un orden maximal en A, entonces T es un preorden en A; luego existe un preorden maximal T′ en A con $T\subseteq T'$. Por 2.2.24., T′ es un orden en A y por la maximalidad de T como orden, se tiene que $T=T'$.

($\Leftarrow$)

Sea T un preorden maximal en A, por 2.2.24., T es un orden en A; entonces existe un orden maximal T′ en A tal que $T\subseteq T'$. Como T′ es un preorden en A, por la maximalidad de T como preorden, se sigue que $T=T'$. □

A continuación se enuncia la generalización del teorema clásico de Artin y Schreier.

TEOREMA 2.2.27 (*Artin-Schreier*) Un anillo A es semireal si y sólo si A es ordenado.

DEMOSTRACIÓN ($\Rightarrow$)

Como A es un anillo semireal, se sigue que $-1\notin\sum\mathbf{A}^2$, esto significa que $\sum\mathbf{A}^2$ es un preorden en A. Por 2.2.25., $\sum\mathbf{A}^2$ está contenido en un orden T en A. Luego A es ordenado.

($\Leftarrow$)

Supóngase que A no es semireal, es decir, $-1\in\sum\mathbf{A}^2$. Como A es ordenado, existe al menos un orden T tal que $\sum\mathbf{A}^2\subsetneq T$, luego $-1\in T$; pero esto último no es posible. □

Se observa que todo anillo real es ordenado pero no todo anillo ordenado es real. Un ejemplo de un anillo ordenado que no es real es el anillo $\mathbb{R}[x, y]/\langle x^2+y^2\rangle$.

Como en campos, aquí se introduce el concepto de radical de un preorden en un anillo en la misma forma, esto es,

DEFINICIÓN 2.2.28. Sea A un anillo y T un preorden en A. El **radical** de T escrito *rad*(T) es el conjunto

$$rad(T)=\{a\in A \mid \text{existe } t(a)\in T \text{ y } n(a)\in\mathbb{N}\cup\{0\} \text{ tal que } a^{2n(a)+1}+at(a)\in T\}.$$

DEFINICIÓN 2.2.29. Sea A un anillo y T un preorden en A. T es un **preorden radical** en A si T=*rad*(T).

Para anillos también se cumple que $T\subseteq rad(T)$ pero ya no es cierto (como en el caso de campos) que todo preorden en un anillo A es un preorden radical en A Por ejemplo el preorden $T(0)^{(2)}=T(0_+)+\langle x^2\rangle$ del ejemplo 2.2.9., satisface que $T(0)^{(2)}\subsetneq rad(T(0)^{(2)})=T(0)$.

LEMA 2.2.30. Sea A un anillo y T un orden en A, entonces *rad*(T)=T.

DEMOSTRACIÓN

Sea $a\in rad(T)$, entonces existen t, $t'\in T$ y $n\in\mathbb{N}\cup\{0\}$ tal que $t'=a^{2n+1}+at\in T$. Supóngase que $a\notin T$, entonces $-a\in T$ y $a^{2n+1}=t'+(-a)t\in T+(-a)T\subseteq T$. También se cumple que $(-a)^{2n+1}\in T$. Luego $a^{2n+1}\in T\cap -T=\mathcal{C}(T)$. Como $\mathcal{C}(T)$ es un ideal primo de A, $a\in\mathcal{C}(T)$ y $a\in T$ lo cual es una contradicción. □

Como una consecuencia directa de 2.2.30., se tiene

COROLARIO 2.2.31. Sea A un anillo y T un preorden en A, entonces la intersección de cualquier familia de órdenes que contienen a T es un preorden radical.

DEMOSTRACIÓN

Sea $T=\cap P$, con $P\supsetneq T$ orden en A y $a\in rad(T)$, entonces existen $t\in T$ y $n\in\mathbb{N}\cup\{0\}$ tal que $a^{2n+1}+at\in T$. Luego $a^{2n+1}+at\in P$ para todo orden P en A que contiene a T. Por el lema 2.2.30., se sigue que $a\in P$ para todo orden P en A que contiene a T. □

El siguiente resultado generaliza el corolario 2.1.13..

TEOREMA 2.2.32. Sea A un anillo y T un preorden en A. Entonces el radical de T es igual a la intersección de todos los órdenes P en A que contienen a T.

DEMOSTRACIÓN

Si $a\in rad(T)$, existen $n\in\mathbb{N}\cup\{0\}$ y $t\in T$ tal que $a^{2n+1}+at\in T\subsetneq P$. Del corolario 2.2.31., se sigue que $a\in P$, luego $rad(T)\subseteq\cap P$ con P orden en A que contiene a T. Recíprocamente, supóngase que $a\notin rad(T)$; se afirma que existe un orden $P\supsetneq T$ en A tal que $a\notin P$. En efecto,

sea $S=\{1, a^1, a^2, \ldots, a^n, \ldots\}$ un sistema multiplicativo en A y considérese el anillo de cocientes $S^{-1}A=\{\overline{(b, a^n)} \mid b\in A, a^n\in S\}$. Sea $T''=T'-aT'$ con $T'=\{\overline{(t, a^n)} \mid t\in T, n\in\mathbb{N}\cup\{0\}\}$; T'' es un preorden en $S^{-1}A$.†) Por el corolario 2.2.25., el preorden T'' está contenido en un orden P'' en el anillo $S^{-1}A$. Sea $P=\varphi^{-1}(P'')$ ($\varphi: A\to S^{-1}A$ el homomorfismo canónico), $P=\{p\in A \mid \overline{(p, 1)}\in P''\}$ un orden en A que contiene a T.‡) Si $T\not\subseteq P$, entonces existe un $p\in P$ tal que $p\notin T$. Esto significa que $\overline{(p, a^{2n})}\notin T\subseteq T''$; luego $\overline{(p, 1)}\notin P''$ lo cual es una contradicción. Si $a\in P$, entonces $\overline{(a, 1)}\in P''$ y $\overline{(-a, 1)}\in P''$, luego $\overline{(-a^2, 1)}\in P''$. De esta forma,

$$\begin{aligned}\overline{(-1\ ,\ 1)}&=\overline{(-a\ ,\ 1)}\overline{(1\ ,\ a)}\\&=\overline{(-a\ ,\ 1)}\overline{(a\ ,\ 1)}\overline{(1\ ,\ a)}^2\\&=\overline{(-a\ ,\ 1)}\overline{(a\ ,\ 1)}\overline{(1\ ,\ a^2)}\in P''\end{aligned}$$

lo cual es una contradicción. Por lo tanto, $a\notin P$ y $rad(T)\subseteq P$ con P orden de A que contiene a T. □

Finalmente para terminar esta sección se enuncia el siguiente resultado que es una consecuencia del teorema anterior

COROLARIO 2.2.33. Sea A un anillo. Un elemento $a\in A$ es totalmente positivo (está en todo orden T de A) si y sólo si a satisface $a^{2n+1}+a(b_1{}^2+\cdots+b_s{}^2)=c_1{}^2+\cdots+c_r{}^2$ donde $b_1, \ldots, b_s, c_1, \ldots, c_r\in A$.

---

†) $T''=T'-aT'$ es un preorden en $S^{-1}A$. En efecto, sean $\overline{(t-at'\ ,\ a^{2n})}$, $\overline{(s-as'\ ,\ a^{2m})}\in T''$ con $t, t', s, s'\in T$, entonces

$$\begin{aligned}\overline{(t-at'\ ,\ a^{2n})}+\overline{(s-as'\ ,\ a^{2m})}&=\overline{((t-at')a^{2m}+(s-as')a^{2n}\ ,\ a^{2n}a^{2m})}\\&=\overline{(ta^{2m}-at'a^{2m}+sa^{2n}-as'a^{2n}\ ,\ a^{2(n+m)})}\\&=\overline{((ta^{2m}+sa^{2n})-(t'a^{2m}+s'a^{2n})a\ ,\ a^{2(n+m)})}\in T''.\end{aligned}$$

Así, $T''+T''\subseteq T''$.

Sea ahora

$$\begin{aligned}\overline{(t-at'\ ,\ a^{2n})}\overline{(s-as'\ ,\ a^{2m})}&=\overline{((t-at')\cdot(s-as')\ ,\ a^{2n}a^{2m})}\\&=\overline{((ts+a^2t's')-(ts'-t's)a\ ,\ a^{2(n+m)})}\in T''.\end{aligned}$$

Así, $T''\cdot T''\subseteq T''$.

Por otro lado, si $\overline{(b\ ,\ a^n)}^2\in(S^{-1}A)^2$, entonces $\overline{(b\ ,\ a^n)}^2=\overline{(b^2\ ,\ a^{2n})}=\overline{(b^2-a(0)\ ,\ a^{2n})}\in T''$ pues $b\in A$ y $0\in T$; así, $(S^{-1}A)^2\subseteq T''$. Finalmente si $\overline{(-1\ ,\ a^{2n})}\in T''$, entonces para un entero no negativo m, se tiene que $\overline{(-1\ ,\ a^{2n})}=\overline{(t-at'\ ,\ a^{2m})}\in S^{-1}A$. Luego existe $\tilde{n}\in\mathbb{N}\cup\{0\}$ tal que

$$\begin{aligned}a^{2\tilde{n}+1}(-1a^{2m}-(t-at')a^{2n})&=0\\-a^{2\tilde{n}+1}a^{2m}&=(t-at')a^{2n}\in A.\\-a^{2(\tilde{n}+m)+1}&=a^{2n}t-a^{2n+1}t'\\a^{2(\tilde{n}+m)+1}&=-a^{2n}t+a^{2n+1}t'\\a^{2(\tilde{n}+m)+1}+a^{2n}t&=a^{2n+1}t'\\a^{2(\tilde{n}+m)+1}+a(a^{2n}t)&=a(a^n)^2t'\in T\end{aligned}$$

Esto último indica que $a\in rad(T)$ lo cual no puede ser posible. Por lo tanto T'' es un preorden en $S^{-1}A$.

‡) $P=\{p\in A \mid \overline{(p\ ,\ 1)}\in P''\}$ es un orden de A que contiene a T. Si $p, q\in P$, entonces $\overline{(p,\ 1)}$, $\overline{(q\ ,\ 1)}\in P''$ y $\overline{(p\ ,\ 1)}+\overline{(q\ ,\ 1)}=\overline{(p+q\ ,\ 1)}\in P''$ luego $p+q\in P$ y $P+P\subseteq P$. También, $\overline{(p\ ,\ 1)}\overline{(q\ ,\ 1)}=\overline{(pq\ ,\ 1)}\in P''$, entonces $pq\in P$ y $P\cdot P\subseteq P$. Sea $a^2\in A^2$, entonces $\overline{(a\ ,\ 1)}^2=\overline{(a^2\ ,\ 1)}\in P''$ y $a^2\in P$, lo cual significa que $A^2\subseteq P$. Si $-1\in P$, entonces $\overline{(-1,\ 1)}\in P''$ no puede ser posible; así, $-1\notin P$. Ahora, sean $p, q\in P$ tal que $pq\in -P$, entonces se tiene que $\overline{(p\ ,\ 1)}\overline{(q\ ,\ 1)}\in P''$. Dado que P'' es un orden en $S^{-1}A$, se sigue que $\overline{(p\ ,\ 1)}\overline{(q\ ,\ 1)}\in -P''$ implica que $\overline{(p\ ,\ 1)}\in P''$ o $\overline{(q\ ,\ 1)}\in P''$, esto es, $p\in P$ o $q\in P$. Por lo tanto P es un orden en A que contiene a T.

DEMOSTRACIÓN ($\Rightarrow$)

Si $a\in\cap$T con T cualquier orden que contiene a $\sum\mathbf{A^2}$, por 2.2.32., se sigue que $\cap$T=$rad(\sum\mathbf{A^2})$ con $\sum\mathbf{A^2}\subsetneq$T, entonces $a\in rad(\sum\mathbf{A^2})$, es decir, $a^{2n+1}+a\sum_{i=1}^{s}b_i^2\in\sum\mathbf{A^2}$

($\Leftarrow$)

Si $a\in$A satisface que $a^{2n+1}+a\sum b_i^2=\sum c_j^2$ con b_i, $c_j\in$A, i=1,…, s, j=1,…,r, entonces $a^{2n+1}+a\sum b_i^2\in\sum\mathbf{A^2}$, es decir, $a\in rad(\sum\mathbf{A^2})$. Como $rad(\sum\mathbf{A^2})=\cap$T con $\sum\mathbf{A^2}\subsetneq$T sigue que $a\in\cap$T. □

2.3. EL ESPECTRO REAL.

Sea K un campo y considérese el conjunto X_K de todos los órdenes en K. De 2.1.14., se sigue que $X_K\neq\emptyset$ si y sólo si K es un campo real. A continuación se dotará el conjunto X_K de una estructura topológica adecuada. Por definición, los conjuntos $H(x):=\{T\in X_K \mid x\in T\setminus\{0\}\}$ que serán llamados **conjuntos de Harrison** forman una subbase de conjuntos abiertos para esta topología. Se observa que $H(x)\cup H(-x)=X_K$, $H(x)\cap H(-x)=\emptyset$, es decir, $H(-x)=X_K\setminus H(x)$, (esto significa que $H(x)$ y $H(-x)$ son abiertos y cerrados en X_K) $H(1)=X_K$ y $H(-1)=H(0)=\emptyset$. Para $x_1,\ldots,x_n\in$K, los conjuntos

$$H(x_1,\ldots,x_n)=H(x_1)\cap\cdots\cap H(x_n)$$

$$=\{T\in X_K \mid x_i\in T\setminus\{0\},\ 1\leq i\leq n\}$$

constituyen una base de conjuntos abiertos para la topología

DEFINICIÓN 2.3.1. Sea K un campo real. El espacio X_K se denomina **espectro real** de K y la topología definida por X_K escrita τ_H, **topología de Harrison**.

Para establecer las propiedades topológicas del espectro real X_K, será necesario introducir una segunda topología en X_K. Considérese el conjunto $\{0, 1\}$ con la topología discreta, y para cada $x\in$K la familia de copias $\{0, 1\}_x$ del conjunto $\{0, 1\}$. El producto cartesiano de esta familia es el conjunto $X:=\{0, 1\}^K$ de todas las funciones φ:K $\rightarrow \{0, 1\}$. X puede ser dotado con la topología producto, es decir, los conjuntos

$$\mathsf{U}_1(x_0)=\{\varphi\in X \mid \varphi(x_0)=1\} \text{ y}$$

$$\mathsf{U}_0(x_0)=\{\varphi\in X \mid \varphi(x_0)=0\}$$

(con $x_0\in K\setminus\{0\}$) son por definición los **subbásicos** de X. Un conjunto abierto de X está generado por elementos de la subbase $\{\mathsf{U}_i(x_0) \mid x_0\in K\setminus\{0\},\ i\in\{0, 1\}\}$, esto es, es unión de intersecciones finitas de conjuntos $\mathsf{U}_0(x_0)$ y $\mathsf{U}_1(x_0)$ con $x_0\in K\setminus\{0\}$. Para $x_1,\ldots,x_n\in K\setminus\{0\}$ y $\delta_1,\ldots,\delta_n\in\{0, 1\}$, los conjuntos

$$\mathsf{U}_{\delta_1,\ldots,\delta_n}(x_1,\ldots,x_n)=\mathsf{U}_{\delta_1}(x_1)\cap\cdots\cap\mathsf{U}_{\delta_n}(x_n)$$
$$=\{\varphi\in X \mid \varphi(x_i)=\delta_i,\ i\in\{1,2,\ldots,n\}\}$$

forman una base de conjuntos abiertos para la topología producto de X.

Dado que {0, 1} es un conjunto finito, se sigue que {0, 1} es compacto. Por un teorema de Tychonoff, el espacio producto X es un espacio topológico compacto[†]. Por otro lado, como todo espacio discreto es un espacio de Hausdörff, y el espacio producto de una familia de espacios de Hausdörff es Hausdörff, se sigue que X es Hausdörff. Se observa que $\mathsf{U}_1(x_0)\cup\mathsf{U}_0(x_0)=X$ y $\mathsf{U}_1(x_0)\cap\mathsf{U}_0(x_0)=\varnothing$, es decir, $\mathsf{U}_0(x_0)$ es el complemento de $\mathsf{U}_1(x_0)$ para $x_0\in K\setminus\{0\}$. De esto se sigue que $\mathsf{U}_1(x_0)$ y $\mathsf{U}_0(x_0)$ son abiertos y cerrados en X. Se afirma que X es un espacio totalmente disconexo.[‡] En efecto, sea $\varphi\in X$; para cada $\psi\in X\setminus\{\varphi\}$, existe un subbásico $\mathsf{U}_i(x_0)$ con $i=0$ o $i=1$ tal que $\varphi\in\mathsf{U}_i(x_0)$ y $\psi\notin\mathsf{U}_i(x_0)$. Luego ψ no pertenece a la componente conexa de X que contiene a φ. De esta forma se ha demostrado la siguiente

PROPOSICIÓN 2.3.2. El espacio producto X es un espacio topológico compacto, Hausdörff y totalmente disconexo. □

Sea $F:X_K\to X;\ T\mapsto\varphi_T$ la función definida del espectro real de un campo K al espacio producto X, donde $\varphi_T:K\to\{0,1\}$ tiene regla de correspondencia

$$\varphi_T(x)=\begin{cases}1 & \text{si } x\in T\setminus\{0\}\\ 0 & \text{si } x\in -T\end{cases}$$

con T orden de K. Si $F(T)=F(T')$ para cualesquiera órdenes T y T′ en X_K, entonces $\varphi_T(x)=\varphi_{T'}(x)$ para todo $x\in K$, lo cual significa que $x\in -T\Leftrightarrow x\in -T'$ o equivalentemente $T=T'$, es decir, F es una función inyectiva. F también es suprayectiva a su imagen $F(X_K)$. Dando a $F(X_K)\subsetneq X$ la topología relativa; a X_K se le da la topología inducida que hace a F un homeomorfismo, es decir, U es abierto en X_K si y sólo si F(U) es abierto en $F(X_K)$. También, V es un subbásico (básico) de $F(X_K)$ si y sólo si $F^{-1}(V)$ es un subbásico (básico) de X_K.

DEFINICIÓN 2.3.3. Sea K un campo real. La topología inducida en X_K que hace a F un homeomorfismo se denomina **topología construible**, escrita τ_C y a X_K con esta topología, **espacio construible**.

Los subbásicos de esta topología son conjuntos de la forma

$$\bar{\mathsf{U}}_1(x_0)=F^{-1}(\mathsf{U}_1(x_0)\cap F(X_K))$$
$$=F^{-1}(\{\varphi \mid \varphi(x_0)=1,\ \varphi^{-1}(\{1\}) \text{ orden de } K\})$$

[†] **TEOREMA** (*de Tychonoff*) Si $(X_i : i\in I)$ es una familia de espacios topológicos compactos, entonces el producto $X=\Pi(X_i : i\in I)$ es compacto con la topología producto.

[‡] Un espacio topológico X es **totalmente disconexo** si las componentes conexas de X son los singuletes.

$$\begin{aligned}\bar{U}_0(x_0)&=F^{-1}(U_0(x_0)\cap F(X_K))\\&=F^{-1}(\{\varphi \mid \varphi(x_0)=0,\ \varphi^{-1}(\{0\}) \text{ orden de K}\})\end{aligned}$$

para $x_0\in K\setminus\{0\}$. Como cada orden T en X_K define una función $\varphi_T:K\to\{0,1\}$

$$\varphi_T(x)=\begin{cases}1 & \text{si } x\in T\setminus\{0\}\\ 0 & \text{si } x\in -T\end{cases}$$

y recíprocamente, a cada función φ_T le corresponde un orden T en X_K; se sigue que los subconjuntos $\bar{U}_1(x_0)$ y $\bar{U}_0(x_0)$ con $x_0\in K\setminus\{0\}$ son subbásicos de Harrison, es decir,

$$\bar{U}_i(x_0)=\begin{cases}H(x_0) & \text{si } i=1,\ x_0\neq 0\\ H(-x_0) & \text{si } i=0,\ x_0\neq 0\\ X_K & \text{si } i=0,\ x_0=0\\ \varnothing & \text{si } i=1,\ x_0=0\end{cases}$$

y recíprocamente. En este caso, las topologías de Harrison y construible en X_K coinciden. Un resultado similar a 2.3.2., para el espectro real X_K es la siguiente

PROPOSICIÓN 2.3.4. Sea K un campo real, entonces el espectro real X_K es un espacio compacto, Hausdörff y totalmente disconexo.

DEMOSTRACIÓN

Para probar la compacidad de X_K bastará probar que $F(X_K)$ es cerrado en X.[†)] Sea $f\in X\setminus F(X_K)$ y considérese el conjunto $S=-f^{-1}(\{0\})=\{x\in K\mid f(-x)=0\}$ de K. S por construcción no es un orden en K, es decir, al menos una de las propiedades de 2.1.6., no se cumple. En efecto,

1°) Sean $x, y\in S$ elementos tal que $x+y\notin S$, entonces $f(-x)=0$, $f(-y)=0$ y $f(-(x+y))=1$. Entonces, $f\in U_{0,0,1}(-x,-y,-(x+y))=U_0(-x)\cap U_0(-y)\cap U_1(-(x+y))$ y $U_{0,0,1}(-x,-y,-(x+y))\cap F(X_K)=\varnothing$.

2°) Si $x, y\in S$ con $xy\notin S$, entonces se tiene que $f(-x)=0$, $f(-y)=0$ y $f(-(xy))=1$, esto significa que $f\in U_{0,0,1}(-x,-y,-(xy))=U_0(-x)\cap U_0(-y)\cap U_1(-(xy))$ y $U_{0,0,1}(-x,-y,-(xy))\cap F(X_K)=\varnothing$.

3°) Si se supone que $K^2\not\subseteq S$, entonces existe al menos un elemento $x\in K$ tal que $x^2\notin S$; luego $f(-x^2)=1$ y $U_1(-x^2)\cap F(X_K)=\varnothing$.

4°) Supóngase que $-1\in S$, entonces $f(1)=0$, esto es, $f\in U_0(1)=X\setminus F(X_K)$. Así, $U_0(1)\cap F(X_K)=\varnothing$.

[†)] Todo cerrado en un compacto es compacto.

5°) Finalmente, si $S\cup\text{-}S\subsetneq K$, entonces existe $x\in K$ tal que $x\notin S\cup\text{-}S$. De esto se obtiene que $f(-x)=1$ o $f(x)=1$, es decir, $f\in U_1(-x)\cap U_1(x)=U_{1,1}(-x\,,\,x)$ y $U_{1,1}(-x\,,\,x)\cap F(X_K)=\varnothing$.

En todos los casos se ha obtenido una vecindad abierta de f, ajena de $F(X_K)$ lo que significa que $X\setminus F(X_K)$ es abierto en la topología dada; así, $F(X_K)$ es cerrado en X y por lo tanto compacto. De esta forma X_K es compacto. Por otro lado, como todo subespacio de un espacio de Hausdörff es Hausdörff, se concluye por 2.3.2., que $F(X_K)$ es Hausdörff y por lo tanto X_K es un espacio de Hausdörff. Finalmente se observa que la componente conexa de un orden T en X_K se reduce a $\{T\}$; pues si existiera $T'\in X_K$ con $T'\neq T$ en la misma componente, entonces habría un elemento $x\in K$ tal que $x\in T$ y $-x\in T'$, luego $T\in H(x)$ y $T'\in H(-x)$ lo que proporciona una disconexión de la componente conexa. ¡Contradicción!. □

A continuación se establecen algunos aspectos de la estructura algebraica de la subbase de Harrison $\mathcal{H}=\{H(x)\mid x\in K\setminus\{0\}\}$. Dado que

$$\begin{aligned}H(x)\cap H(y)&=\{T\in X_K\mid x\in T\setminus\{0\}\}\cap\{T\in X_K\mid y\in T\setminus\{0\}\}\\&=\{T\in X_K\mid x,y\in T\setminus\{0\}\}.\\&=H(x,y)\notin\mathcal{H}\end{aligned}$$

se observa que $\mathcal{H}$ no es cerrado bajo intersecciones pero si lo es bajo diferencias simétricas.[†)] Para subconjuntos A y B de un conjunto X, la diferencia simétrica define una estructura de grupo en el conjunto potencia $\mathcal{P}(X)$ de X, con $\varnothing$ (el conjunto vacío) como elemento cero, es decir,

PROPOSICIÓN 2.3.5. Sea X un conjunto no vacío, entonces $(\mathcal{P}(X)\,,\,\Delta)$ es un grupo y cada elemento es de orden 2.

DEMOSTRACIÓN

1°) Es claro que, para A, B y $C\in\mathcal{P}(X)$, se tiene que $A\Delta(B\Delta C)=(A\Delta B)\Delta C$. 2°) Existe $\varnothing\in\mathcal{P}(X)$ tal que $A\Delta\varnothing=\varnothing\Delta A=A$ para cada $A\in\mathcal{P}(X)$. 3°) Para toda $A\in\mathcal{P}(X)$, existe $B\in\mathcal{P}(X)$ tal que $A\Delta B=B\Delta A=\varnothing$; así, $B=A$. De esta forma se ha probado que $(\mathcal{P}(X)\,,\,\Delta)$ es un grupo.

Además

4°) Como $A\Delta B=B\Delta A$ para cada $A, B\in\mathcal{P}(X)$, se tiene adicionalmente que $(\mathcal{P}(X)\,,\,\Delta)$ es un grupo abeliano. □

PROPOSICIÓN 2.3.6. Sea K un campo real, X_K el espectro real de K y $\mathcal{P}(X_K)$ el conjunto potencia de X_K, entonces $(\mathcal{H}\,,\,\Delta)$ es un subgrupo de $(\mathcal{P}(X_K)\,,\,\Delta)$.

[†)] La diferencia simétrica de dos conjuntos A y B escrita $A\Delta B$, se define como el conjunto $(A\setminus B)\cup(B\setminus A)$.

DEMOSTRACIÓN

i) Claramente $\mathcal{H}\neq\emptyset$ pues $X_K=H(1)\in\mathcal{H}$. *ii*) Sean $H(-x), H(-y)\in\mathcal{H}$ con $x, y\in K\backslash\{0\}$; se afirma que $H(-xy)=H(-x)\Delta H(-y)$. En efecto, si $T\in X_K$, entonces se tiene que $-xy\in T$ si y sólo si ($x\in T$ y $-y\in T$) o ($-x\in T$ y $y\in T$), lo que significa que $T\in H(-x)\Delta H(-y)$. □

Aquí, se observa que, como todo subgrupo de un grupo abeliano es un subgrupo normal, se sigue que $(\mathcal{H}, \Delta)$ es un subgrupo normal de $(\mathcal{P}(X_K), \Delta)$. Por otro lado, se tiene

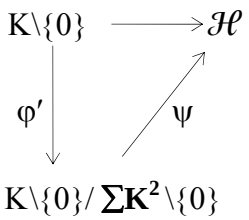
LEMA 2.3.7. $(\sum\mathbf{K^2}\backslash\{0\}, \cdot)$ es un subgrupo multiplicativo del grupo $(K\backslash\{0\}, \cdot)$.

DEMOSTRACIÓN

i) Es claro que $1\in\sum\mathbf{K^2}\backslash\{0\}$. *ii*) Por otro lado sean $x, y\in\sum\mathbf{K^2}\backslash\{0\}$ con $x=\sum_{i=1}^{n} x_i^2$, $y=\sum_{j=1}^{m} y_j^2$, luego $xy=\sum_{i=1}^{n}\sum_{j=1}^{m}(x_i y_j)^2\in\sum\mathbf{K^2}\backslash\{0\}$ *iii*) Finalmente, si $x\in\sum\mathbf{K^2}\backslash\{0\}$, $x=\sum_{i=1}^{n} x_i^2$, entonces $x^{-1}=(\sum_{i=1}^{n} x_i^2)^{-1}=\sum_{i=1}^{n} x_i^2/(\sum_{i=1}^{n} x_i^2)^2=\sum_{i=1}^{n} x_i^2\,(1/\sum_{i=1}^{n} x_i^2)^2\in\sum\mathbf{K^2}\backslash\{0\}$. □

A continuación se enuncia el resultado principal acerca de la estructura algebraica de $\mathcal{H}$.

TEOREMA 2.3.8. $(\mathcal{H}, \Delta)$ es isomorfo al grupo $(K\backslash\{0\}/\sum\mathbf{K^2}\backslash\{0\}, \cdot)$.



DEMOSTRACIÓN

Considérese la función $\varphi: K\backslash\{0\}\to\mathcal{H}$; $\varphi(x)=H(-x)$. Como para todo elemento $H(-x)\in\mathcal{H}$ siempre existe un elemento $x\in K\backslash\{0\}$ tal que; $\varphi(x)=H(-x)$, se sigue que φ es suprayectiva. Por otro lado, como $\varphi(xy)=H(-xy)=H(-x)\Delta H(-y)=\varphi(x)\varphi(y)$, φ es un homomorfismo. Su núcleo, *Ker*(φ) es tal que $H(-x)=\emptyset$. Esto es equivalente a $H(x)=X_K$, es decir, el elemento x está en todo orden de K. Por el corolario 2.1.15. y la definición 2.1.16., se sigue que x se puede escribir como una suma finita de cuadrados en K; así, $Ker(\varphi)=\sum\mathbf{K^2}\backslash\{0\}$. Por el primer teorema del isomorfismo, existe un único isomorfismo $\psi: K\backslash\{0\}/\sum\mathbf{K^2}\backslash\{0\}\to\mathcal{H}$; definido como $\psi(x\sum\mathbf{K^2}\backslash\{0\})=H(-x)$. Por lo tanto $(\mathcal{H}, \Delta)\cong(K\backslash\{0\}/\sum\mathbf{K^2}\backslash\{0\}, \cdot)$. □

Como una consecuencia del teorema anterior, se tiene

COROLARIO 2.3.9. Para $x, y\in K\backslash\{0\}$, $H(-x)=H(-y)$ si y sólo si $x\equiv y\ mod(\sum\mathbf{K^2}\backslash\{0\})$. □

En forma similar que para campos se trata ahora el caso para anillos. Sea A un anillo y considérese el conjunto X_A de todos los órdenes en A. De 2.2.27., se sigue que

$X_A \neq \emptyset$ si y sólo si A es un anillo semireal. Para anillos se puede introducir la topología de Harrison en una forma similar que para campos, esto es, los conjuntos

$$H(a)=\{T\in X_A \mid a\in T\setminus \mathcal{C}(T)\}$$

con $\mathcal{C}(T)$ el centro de un orden T forman una subbase de conjuntos abiertos para esta topología. Aquí como en campos se tiene que $H(1)=X_A$ y $H(-1)=H(0)=\emptyset$. De hecho, $H(a)=\emptyset$ para cada $a\in\mathcal{C}(T)$. Sin embargo, aunque todavía se sigue cumpliendo que $H(a)\cap H(-a)=\emptyset$, resulta que $H(a)\cup H(-a)\subseteq X_A$ en general. Por ejemplo, para el anillo $\mathbb{R}[x]$, se tiene que $H(x)\cup H(-x)=\{T(0)\}\subsetneq X_{\mathbb{R}[x]}$. $X_A\setminus H(a)\cup H(-a)$ es el conjunto de todos los ordenes cuyos centros contienen al elemento a.

Para $a_1,\ldots,a_n\in A$, los conjuntos

$$H(a_1,\ldots,a_n)=H(a_1)\cap\cdots\cap H(a_n)$$

$$=\{T\in X_A \mid a_i\in T\setminus\mathcal{C}(T),\ 1\leq i\leq n\}$$

forman una base de conjuntos abiertos para esta topología.

DEFINICIÓN 2.3.10. Sea A un anillo semireal. El espacio X_A se denomina **espectro real** de A y la topología definida en X_A, escrita τ_H **topología de Harrison**.

EJEMPLO 2.3.11. Considérese el anillo $\mathbb{R}[x]$. Los elementos del espectro real $X_{\mathbb{R}[x]}$ son los órdenes $T(a)$, $T(a_-)$, $T(a_+)$, $T(+\infty)$ y $T(-\infty)$ para toda $a\in\mathbb{R}$ fija. La topología de Harrison τ_H en $X_{\mathbb{R}[x]}$ tiene una base de conjuntos abiertos

$$\{T(c) \mid a<c<b\}\cup\{T(c_-) \mid a<c\leq b\}\cup\{T(c_+) \mid a\leq c<b\}$$

para cada a, b, $c\in\mathbb{R}$ con a, b fijas y $a<b$.

$$\{T(c) \mid a<c\}\cup\{T(c_-) \mid a<c\}\cup\{T(c_+) \mid a\leq c\}\cup\{T(+\infty)\}$$

para cada a, $c\in\mathbb{R}$ con a, fija.

$$\{T(c) \mid c<b\}\cup\{T(c_-) \mid c\leq a\}\cup\{T(c_+) \mid c<b\}\cup\{T(-\infty)\}$$

para cada b, $c\in\mathbb{R}$ con b, fija.

En forma similar que para campos; para establecer las propiedades del espectro real X_A se introduce una segunda topología en X_A (la topología construible en X_A), es decir, se considera el espacio producto $X=\{0,1\}^A$ donde los subbásicos son los conjuntos

$$U_1(a)=\{\varphi\in X \mid \varphi(a)=1\}$$

$$\mathsf{U}_0(a)=\{\varphi\in X \mid \varphi(a)=0\}$$

con $a\in A\backslash \mathcal{C}(T)$ y los básicos vienen dados como

$$\mathsf{U}_{\delta_1,\ldots,\delta_n}(a_1,\ldots,a_n)=\mathsf{U}_{\delta_1}(a_1)\cap\cdots\cap\mathsf{U}_{\delta_n}(a_n)$$

$$=\{\varphi\in X_A \mid \varphi(a_i)=\delta_i,\ i\in\{1,2,\ldots,n\}\}$$

con $a_1,\ldots,a_n\in A\backslash \mathcal{C}(T)$ y $\delta_1,\ldots,\delta_n\in\{0, 1\}$. También se define una función $F:X_A\to X$; $T\mapsto\varphi_T$ donde $\varphi_T:A\to\{0, 1\}$ tiene regla de correspondencia

$$\varphi_T(x)=\begin{cases}1 & \text{si } x\in T\backslash \mathcal{C}(T)\\ 0 & \text{si } x\in -T\end{cases}$$

con T orden de A. Como en campos, F es inyectiva y suprayectiva a su imagen $F(X_A)$. Aquí también, dando a $F(X_A)\subsetneq X=\{0 , 1\}^A$ la topología relativa, se puede dotar a X_A con la topología inducida en X_A que hace que F sea un homeomorfismo. Así, se tiene

DEFINICIÓN 2.3.12. Sea A un anillo semireal. La topología inducida en X_A que hace a F un homeomorfismo se denomina **topología construible** escrita τ_C y a X_A con esta topología, **espacio construible.**

Los subbásicos de esta topología son conjuntos de la forma

$$\overline{\mathsf{U}}_1(a_0)=F^{-1}(\mathsf{U}_1(a_0)\cap F(X_A))$$
$$=F^{-1}(\{\varphi \mid \varphi(a_0)=1,\ \varphi^{-1}(\{1\}) \text{ orden de } A\})$$

$$\overline{\mathsf{U}}_0(a_0)=F^{-1}(\mathsf{U}_0(a_0)\cap F(X_A))$$
$$=F^{-1}(\{\varphi \mid \varphi(a_0)=0,\ \varphi^{-1}(\{0\}) \text{ orden de } A\})$$

para $a_0\in A\backslash \mathcal{C}(T)$. Mientras que para campos, las topologías de Harrison y construibles coinciden, para anillos se tiene que

$$\overline{\mathsf{U}}_1(a_0)=F^{-1}(\mathsf{U}_1(a_0)\cap F(X_A))$$
$$=F^{-1}(\{\varphi \mid \varphi(a_0)=1,\ \varphi^{-1}(\{1\}) \text{ orden de } A\})$$
$$=\{T\in X_A \mid a_0\in T\backslash \mathcal{C}(T)\}=H(a_0)$$

$$\overline{\mathsf{U}}_0(a_0)=F^{-1}(\mathsf{U}_0(a_0)\cap F(X_A))$$
$$=F^{-1}(\{\varphi \mid \varphi(a_0)=0,\ \varphi^{-1}(\{0\}) \text{ orden de } A\})$$
$$=\{T\in X_A \mid a_0\in -T\}=H(-a_0)$$

Si $a_0\in \mathcal{C}(T)=T\cap -T$, entonces

$$\begin{aligned}\bar{U}_0(a_0)&=F^{-1}(U_0(a_0)\cap F(X_A))\\&=F^{-1}(\{\varphi \mid \varphi(a_0)=0,\ \varphi^{-1}(\{0\}) \text{ orden de A}\})\\&=\{T\in X_A \mid a_0\in \mathcal{C}(T)\}=X_A\backslash H(a_0)\cup H(-a_0)\end{aligned}$$

y $\bar{U}_0(0)=X_A$. Así, se observa que para el subbásico $\bar{U}_0(a_0)$ de la topología construible en X_A con $a_0\in\mathcal{C}(T)$, no existe ningún subbásico de la topología de Harrison en X_A. Por lo tanto, τ_C es más fuerte o menos débil o más fina que la topología de Harrison en X_A.

Si $G:(X_A , \tau_H)\to(X_A , \tau_C)$ es un mapeo entre los espacios (X_A , τ_H) y (X_A , τ_C), entonces se observa que G no es continua ya que $G^{-1}(X_A)=X_A\backslash H(a)\cup H(-a)$ no es abierto en la topología τ_H; pero G es una función inyectiva y abierta. La proposición 2.3.2., también es valida en el caso de anillos, esto es,

PROPOSICIÓN 2.3.13. Sea A un anillo semireal, entonces el espacio producto $X=\{0, 1\}^A$ es un espacio topológico compacto, Hausdörff y totalmente disconexo.

DEMOSTRACIÓN

Similar a la demostración de 2.3.2.. □

LEMA 2.3.14. Sea $f:(X , \tau_X)\to(Y , \tau_Y)$, una función entre dos espacios topológicos que satisface

1) f es inyectiva.
2) f es abierta
3) $f(K)$ es compacto en Y para $K\subseteq X$.

Entonces K es compacto en X.

DEMOSTRACIÓN

Sea $\{U_i\}_{i\in I}$ una cubierta abierta de K. Como f es una función abierta, $f(\{U_i\}_{i\in I})$ es una cubierta abierta de la imagen $f(K)$. Dado que $f(K)$ es compacto en Y, de la cubierta abierta $f(\{U_i\}_{i\in I})$ se puede extraer una cubierta finita, esto es, $f(K)\subseteq f(U_1)\cup\cdots\cup f(U_m)$. Ahora, considérese las imágenes inversas. Dado que f es inyectiva, $K=f^{-1}(f(K))$ y

$$\begin{aligned}K=f^{-1}(f(K))&\subseteq f^{-1}(f(U_1)\cup\cdots\cup f(U_m))\\&\subseteq f^{-1}(f(U_1)\cup\cdots\cup f(U_m))\\&\subseteq f^{-1}(f(U_1))\cup\cdots\cup f^{-1}(f(U_m));\end{aligned}$$

así, $K\subseteq U_1\cup\cdots\cup U_m$. Luego K es compacto en X. □

Un resultado paralelo a 2.3.4., es la siguiente

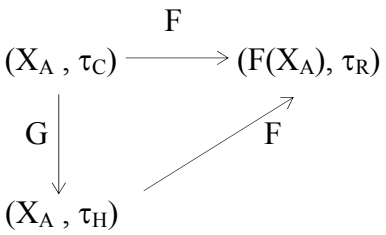
PROPOSICIÓN 2.3.15. Sea A un anillo semireal, entonces el espectro real X_A con la topología de Harrison es un espacio topológico compacto.

DEMOSTRACIÓN

Se probará que la imagen $F(X_A)$ es un conjunto cerrado en X. Sea $f\in X\backslash F(X_A)$ y

considérese el subconjunto $S=-f^{-1}(\{0\})=\{a \mid f(-a)=0\}$ de A. Por construcción, S no es un orden en A. La prueba de que S no satisface alguno de los incisos *i*) a *iv*) de la definición 2.2.5., es exactamente la misma que para campos (ver 1°), 2°), 3°) y 4°) de 2.3.4.). Falta verificar que S no satisface 2.2.21.. Supóngase que $ab\in -S$, y que $a\notin S$ y $b\notin S$, esto significa que $f(-a)=1$, $f(-b)=1$ y $f(-ab)=1$, es decir, $f\in H_1(-a)\cap H_1(-b)\cap H_1(-ab)=H_{1,1,1}(-a, -b, -ab)$ y $H_{1,1,1}(-a, -b, -ab)\cap X_A=\varnothing$. De esto se sigue que $F(X_A)$ es cerrado en X. Como G es abierta, inyectiva y $F(X_A)$ es compacto, del lema anterior se tiene que X_A es compacto. □

Dado que $T(a_+)\subsetneq T(a)$ y $T(a_-)\subsetneq T(a)$ para toda $a\in\mathbb{R}$. Del ejemplo 2.3.11., se observa que todo básico que contiene a $T(a_-)$ contiene a $T(a)$ y también todo básico que contiene $T(a_+)$ contiene a $T(a)$ para cada $a\in\mathbb{R}$, luego $T(a)\in\{\overline{T(a_-)}\}$ y $T(a)\in\{\overline{T(a_+)}\}$. Esto muestra que $X_{\mathbb{R}[x]}$ no es un espacio de Hausdörff.



Se sabe que todos los órdenes en un campo son maximales, esto es, si T y T′ son órdenes en un campo K con $T\subseteq T'$, entonces $T=T'$ (ver 2.1.18.). Esto también puede escribirse como $T\subseteq T'$ si y sólo si $\{T'\}=\overline{\{T\}}$. En el caso de anillos, 2.1.18., ya no es válido en general, es decir, pueden existir órdenes T y T′ en un anillo A tal que $T\subsetneq T'$. Un ejemplo de esto son los ordenes $T(a_+)$, $T(a_-)$ y $T(a)$ del anillo $\mathbb{R}[x]$ (ver ejemplos 2.2.14. y 2.2.15.).

PROPOSICIÓN 2.3.16. Sea A un anillo semireal y $T, T'\in X_A$. Entonces $T\subseteq T'$ si y sólo si T′ es un punto de adherencia de $\{T\}$; es decir, $T'\in\overline{\{T\}}$.

DEMOSTRACIÓN ($\Rightarrow$)

Se tiene que probar que toda vecindad de T′ contiene a T. Bastará considerar como vecindades de T′ a los básicos $H(a_1,\ldots,a_n)$. Que $T'\in H(a_1,\ldots,a_n)$, significa que $a_i\in T'\setminus\mathcal{C}(T')$, $i=1,\ldots,n$; esto es equivalente a que $-a_i\notin T'$, $i=1,\ldots,n$. Dado que $T\subseteq T'$, se tiene que $-a_i\notin T$ para $i=1,\ldots,n$, lo cual significa $a_i\in T\setminus\mathcal{C}(T)$, $i=1,\ldots,n$. Luego $T\in H(a_1,\ldots,a_n)$ y $T'\in\overline{\{T\}}$.

($\Leftarrow$)

Suponiendo que $T\nsubseteq T'$, se puede elegir un elemento $a\in A$ tal que $a\in T$ y $a\notin T'$, entonces $T\in H(a)$ y $T'\in H(-a)$. Como $H(a)\cap H(-a)=\varnothing$, se sigue que $H(-a)$ es una vecindad de T′ que no contiene a T. Esto último es una contradicción ya que $T'\in\overline{\{T\}}$. □

Se dice que un orden T en un anillo A es un **punto cerrado** en X_A si $\{T\}=\overline{\{T\}}$. El conjunto de puntos cerrados en X_A que es un subespacio de X_A será denotado por X_A^m.

COROLARIO 2.3.17. Los órdenes maximales en un anillo semireal A son los puntos cerrados en X_A.

DEMOSTRACIÓN

Sea $T \in X_A^{m}$ un punto cerrado en X_A. Si T' es un orden en A tal que $T \subseteq T'$, entonces por 2.3.16., $T' \in \overline{\{T\}} = \{T\}$, luego $T=T'$ y T es un orden maximal en A. Recíprocamente, sea T un orden maximal en A, si $T' \in \overline{\{T\}}$, por 2.3.16., $T \subseteq T'$. Como T es maximal, $T=T'$ y se obtiene $\{T\}=\overline{\{T\}}$. □

En el caso de campos se observa que, como todo orden es maximal, todo orden es un punto cerrado en el espectro real.

LEMA 2.3.18. Sea A un anillo semireal. Entonces para T_1, $T_2 \in X_A$, las siguientes afirmaciones son equivalentes.

1) $T_1 \not\subseteq T_2$ y $T_2 \not\subseteq T_1$
2) Existe $a \in A$ tal que $T_1 \in H(a)$ y $T_2 \in H(-a)$.
3) Existen vecindades ajenas V_1 y V_2 en X_A tal que $T_1 \in V_1$ y $T_2 \in V_2$.

DEMOSTRACIÓN (1) $\Rightarrow$ (2)

Sean $b \in T_1$ y $c \in T_2$ con $b \notin T_2$ y $c \notin T_1$. Considérese $a=b-c$, entonces $a \in T_1$ y $-a \in T_2$. Si $-a \in T_1$ y $a \in T_2$, se tendrá que $c=-a+b \in T_1$ y $a+c=b \in T_2$ lo cual contradice que $b \notin T_2$ y $c \notin T_1$.

(2) $\Rightarrow$ (3)

Para algún $a \in A$, existen vecindades $V_1=H(a)$ y $V_2=H(-a)$ tal que $T_1 \in V_1$ y $T_2 \in V_2$. Entonces $V_1 \cap V_2 = \varnothing$ ya que $H(a) \cap H(-a) = \varnothing$.

(3) $\Rightarrow$ (1)

Por hipótesis, existen vecindades ajenas V_1 y V_2 con $T_1 \in V_1$ y $T_2 \in V_2$, luego $T_1 \notin V_2$ y $T_2 \notin V_1$. Entonces $T_1 \notin \overline{\{T_2\}}$ y $T_2 \notin \overline{\{T_1\}}$. Por 2.3.16., se sigue que $T_1 \not\subseteq T_2$ y $T_2 \not\subseteq T_1$. □

PROPOSICIÓN 2.3.19. Sea A un anillo semireal y T un orden en A, entonces el conjunto de órdenes que contienen a T forma una cadena bajo la inclusión.

DEMOSTRACIÓN

Supóngase que existen al menos dos órdenes T_1 y T_2 en X_A tal que $T \subseteq T_1$ y $T \subseteq T_2$ pero $T_1 \not\subseteq T_2$ y $T_2 \not\subseteq T_1$. Por 2.3.18., existen vecindades ajenas V_1, V_2 tal que $T_1 \in V_1$ y $T_2 \in V_2$. Por 2.3.16., $T_1 \in \overline{\{T\}}$, $T_2 \in \overline{\{T\}}$, luego $T \in V_1 \cap V_2$ lo cual es una contradicción ya que $V_1 \cap V_2 = \varnothing$. □

Como un caso particular de la proposición anterior se tiene el

COROLARIO 2.3.20. Sea A un anillo semireal y T un orden de A, entonces existe un único orden maximal T' en A, tal que $T \subseteq T'$.

DEMOSTRACIÓN

Supóngase que existen T_1 y T_2 órdenes maximales en A que contienen a T. Por la

proposición anterior, $T\subseteq T_1\subseteq T_2$ y $T\subseteq T_2\subseteq T_1$. Luego $T_1=T_2=T'$ y T' es el único orden maximal que contiene a T. □

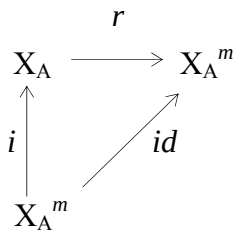
Se sabe que para un anillo semireal A, su espectro real X_A es un espacio compacto que no necesariamente es Hausdörff y $X_A{}^m$ es un subespacio de X_A; de hecho, $X_A{}^m$ es un espacio compacto y Hausdörff, esto es,

PROPOSICIÓN 2.3.21. Sea A un anillo semireal. Entonces $X_A{}^m$ es un espacio topológico compacto y Hausdörff.

DEMOSTRACIÓN

Sea $\mathcal{F}$ una cubierta de $X_A{}^m$ de conjuntos abiertos V de X_A. Considérese un orden $T\in X_A$, entonces por el corolario 2.3.20., existe un orden maximal T' en $X_A{}^m$ tal que $T\subseteq T'$; luego $T\in V$ para algún V en $\mathcal{F}$. Por 2.3.16., se sigue que $T'\in\overline{\{T\}}$, es decir, $V\cap\{T\}\neq\varnothing$ y $T\in V$; de esta forma, $T\in\cup V$ para todo T en X_A. Así, $X_A\subseteq\cup V$ con $V\in\mathcal{F}$ y $\mathcal{F}$ es una cubierta abierta de X_A. Como X_A es compacto, de $\mathcal{F}$ se puede extraer una cubierta finita $\mathcal{F}_m=\{V_j\}$, j=1, 2…, m tal que $X_A\subseteq\cup V_j$. Luego $X_A{}^m\subseteq\cup V_j$, esto es, $X_A{}^m$ es compacto. Por otro lado, sean T_1, $T_2\in X_A{}^m$ con $T_1\neq T_2$, entonces $T_1\not\subseteq T_2$ y $T_2\not\subseteq T_1$. Por 2.3.18., existen abiertos ajenos V_1 y V_2 en X_A con $T_1\in V_1$, $T_2\in V_2$ y por tanto, $X_A{}^m$ es Hausdörff. □

Considérese la función $r:X_A\to X_A{}^m$; $S\mapsto T$, con T el único orden maximal que contiene a S y la función inclusión $i:X_A{}^m\to X_A$. Entonces la función composición $r\circ i:X_A{}^m\to X_A{}^m$, $r\circ i(T)=r(i(T))=r(T)=T$ es la función identidad en $X_A{}^m$. r es llamada una **retracción** de X_A sobre $X_A{}^m$.



LEMA 2.3.22. Sea A un anillo semireal, T un orden maximal en A y C un conjunto cerrado en X_A tal que $T\notin C$. Entonces existen vecindades ajenas V_1 y V_2 en X_A tal que $T\in V_1$ y $C\subsetneq V_2$.

DEMOSTRACIÓN.

Se afirma que para cada $T'\in C$, se cumple $T'\not\subseteq T$ y $T\not\subseteq T'$. En efecto, si $T'\in C$, entonces como $T\notin C$ y C es cerrado, se sigue que $T\notin\overline{\{T'\}}$; por 2.3.16., $T'\not\subseteq T$. Por otro lado, que $T\subseteq T'$ es equivalente a que $T'\in\overline{\{T\}}$. Como T es un orden maximal en A, $\{T\}=\overline{\{T\}}$, esto es, $T=T'$ lo cual es una contradicción; por lo tanto $T\not\subseteq T'$. De 2.3.18., existe un elemento $a(T')$ en A tal que $T\in H(a(T'))$ y $T'\in H(-a(T'))$. Sea $\mathfrak{C}$ la familia de todos los abiertos $H(-a(T'))$ que contienen a T' con $T'\in C$; claramente $\mathfrak{C}$ es una cubierta abierta de C. Como $C\subsetneq X_A$ es un conjunto cerrado, se sigue que C es compacto. Luego de la cubierta abierta $\mathfrak{C}$ se puede extraer una cubierta finita $\{H(-a_j)\}$, $j=1,2,\ldots,n$; $C\subsetneq H(-a_1)\cup\cdots\cup H(-a_m)$,

$T\in(a_1)\cap\cdots\cap H(a_m)=H(a_1,\ldots,a_m)$. Así, $V_1=H(a_1,\ldots,a_m)$ y $V_2=H(-a_1)\cup\cdots\cup H(-a_m)$ son las vecindades. □

PROPOSICIÓN 2.3.23. Sea A un anillo semireal, entonces la función $r:X_A\to X_A{}^m$ es continua.

DEMOSTRACIÓN

Sea $S\in X_A$ un orden tal que $r(S)=T$, T el orden maximal que contiene a S. Sea U un conjunto abierto no vacío en X_A que contiene a T, y sea $C=X_A\backslash U$. Por el lema 2.3.22., existen vecindades ajenas V_1, V_2 en X_A tal que $T\in V_1$ y $C\subsetneq V_2$. Que $S\subseteq T$, por 2.3.18., es equivalente a $T\in\overline{\{S\}}$ lo que implica que $S\in V_1$. Entonces $r(V_1)\subsetneq U\cap X_A{}^m$. Si $S'\in V_1$ con $r(S')=T'\notin U$, entonces $T'\in C\subsetneq V_2$. Como $S'\subseteq T'$, se tiene que $T'\in\overline{\{S'\}}$, y $S'\in V_2$ lo cual es una contradicción ya que $V_1\cap V_2=\varnothing$. □

LEMA 2.3.24. Sea $f:(X\ ,\ \tau_X)\to(Y\ ,\ \tau_Y)$ una función continua y suprayectiva con X compacto y Y Hausdörff. Entonces *f* es cerrada.

DEMOSTRACIÓN

Sea C en Y un conjunto tal que $f^{-1}(C)$ es cerrado en X. Como X es compacto, *f* continua y suprayectiva y Y es Hausdörff, se sigue que $f^{-1}(C)$ y $f(f^{-1}(C))=C$ son compactos y C es cerrado. □

Si X y Y son espacios topológicos, una función $f:(X\ ,\ \tau_X)\to(Y\ ,\ \tau_Y)$ es una **identificación** si *f* es una función continua y suprayectiva que satisface: $U\subseteq Y$ es abierto en Y si y sólo si $f^{-1}(U)$ es abierto en X o equivalentemente $C\subseteq Y$ es cerrado si y sólo si $f^{-1}(C)$ es cerrado en X. Como *r* es continua y suprayectiva, del lema anterior se tiene que *r* es una identificación, es decir, la topología relativa en $X_A{}^m$ es precisamente la topología cociente en el espectro real X_A con respecto a *r*. Para probar esto, se necesitarán algunos resultados de topología.

Se recuerda que si X es un espacio topológico, Y un conjunto y $f:(X\ ,\ \tau_X)\to Y$ una función suprayectiva, entonces la función *f* induce una topología en Y, es decir, un conjunto $V\subseteq Y$ es abierto en Y si y sólo si $f^{-1}(V)$ es abierto en X. Esta topología (denominada topología de identificación de Y con respecto a *f*) hace que *f* sea una identificación. Como una consecuencia inmediata de 2.3.23. y del hecho de que *r* es una identificación, se tiene

COROLARIO 2.3.25. Sea A un anillo semireal, entonces $X_A{}^m$ tiene la topología de identificación. □

PROPOSICIÓN 2.3.26. Sean X y Y espacios topológicos. Si $f:(X\ ,\ \tau_X)\to(Y\ ,\ \tau_Y)$ es una función continua, suprayectiva y abierta (cerrada), entonces *f* es una identificación.

DEMOSTRACIÓN

Sea $U\subseteq Y$ un conjunto tal que $f^{-1}(U)$ es abierto en X. Como *f* es abierta y suprayec-

tiva, se tiene que $f(f^{-1}(U))=U$ es abierto en Y. Luego $U\subseteq Y$ es abierto en Y si y sólo si $f^{-1}(U)$ es abierto en X. □

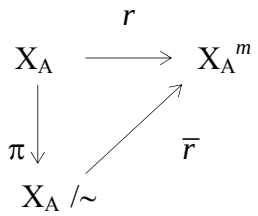
Dado que homeomorfismo, función abierta y función cerrada son conceptos equivalentes para una función $f:(X , \tau_X)\to(Y , \tau_Y)$ que es continua y biyectiva, se tiene

COROLARIO 2.3.27. Sean X y Y espacios topológicos. $f:(X , \tau_X)\to(Y , \tau_Y)$ es continua y biyectiva si y sólo si f es una identificación inyectiva. □

Si A es un anillo semireal y X_A es el espectro real de A, entonces para $r:X_A\to\to{X_A}^m$ se puede definir una relación "$\sim$" en X_A como sigue: Para cualesquiera órdenes S y T en A, $T\sim S$ si y sólo si $r(S)=r(T)$. Claramente $\sim$ es una relación de equivalencia en X_A que define un espacio cociente $Q:=X_A/\sim$ con la topología de identificación. Así, se tiene la

PROPOSICIÓN 2.3.28. Sea A un anillo semireal, entonces la topología relativa en ${X_A}^m$ es precisamente la topología cociente de X_A con respecto a r.

DEMOSTRACIÓN



Sea $r:X_A\to{X_A}^m$ y $\pi:X_A\to X_A/\sim$; $T\mapsto[T]$ la proyección natural. Sea U un conjunto abierto en ${X_A}^m$ y considérese $\bar{r}^{-1}(U)$. Sí $\pi^{-1}(\bar{r}^{-1}(U))=V$, entonces $r^{-1}(U)=V$. Como r es continua, V es un conjunto abierto en X_A. Dado que π es abierta y suprayectiva, $\pi(V)=\pi(\pi^{-1}(\bar{r}^{-1}(U)))=\bar{r}^{-1}(U)$ es abierto en $X_A/\sim$, luego $\bar{r}$ es continua. Se sigue de la suprayectividad de r que $\bar{r}$ es suprayectiva. Sea C en ${X_A}^m$ un conjunto que satisface que $\bar{r}^{-1}(C)$ es cerrado en $X_A/\sim$. Como π es continua, $\pi^{-1}(\bar{r}^{-1}(C))=r^{-1}(C)$ es cerrado en X_A, lo cual es equivalente a que C sea cerrado en ${X_A}^m$. Luego r es una identificación. Claramente r es inyectiva y por 2.3.27., es una función continua y biyectiva. □

Finalmente, para terminar este capítulo se dirá que, aunque no se ha mencionado explícitamente, las ideas que motivaron el desarrollo de la teoría de Artin-Schreier para campos y posteriormente para anillos tiene como base al celebre problema 17 de Hilbert presentado por él al Congreso Internacional de Matemáticas celebrado en París en 1900. Hilbert en las últimas décadas del siglo antepasado estudió el problema de si un polinomio semidefinido positivo[†)] en el dominio entero $\mathbb{R}[x_1,\ldots,x_n]$ podría ser una suma de cuadrados de otros polinomios también en $\mathbb{R}[x_1,\ldots,x_n]$. El resultado fue negativo excepto para $n=1$. La prueba aportada por él fue geométrica y no explícita, es decir, el método de Hilbert era complicado y no se prestaba a una construcción realmente práctica. Los primeros ejemplos explícitos de polinomios semidefinidos positivos que no se podían escribir como suma de cuadrados de polinomios, aparecen hasta 1967. Ellos son los así denominados **polinomios**

[†)] Se recuerda que si k es un campo, el espacio afín k^n es el conjunto $k^n=\{(a_{1,\ldots,}a_n)|\ a_i\in k,\ 1\le i\le n\}$. Dado un polinomio $f\in k[x_{1,\ldots,}x_n]$, $f(x)=\sum a_I x^I$ se define la **función polinomial** asociada a f como $f:k^n\to k$, $f(a)=\sum a_I a^I$. Un polinomio $f\in k[x_{1,\ldots,}x_n]$ es **semidefinido positivo** o también que la función polinomial es **no negativa** si $f(x_1,\ldots,x_n)\ge 0$ para toda $(x_1,\ldots,x_n)\in k^n$.

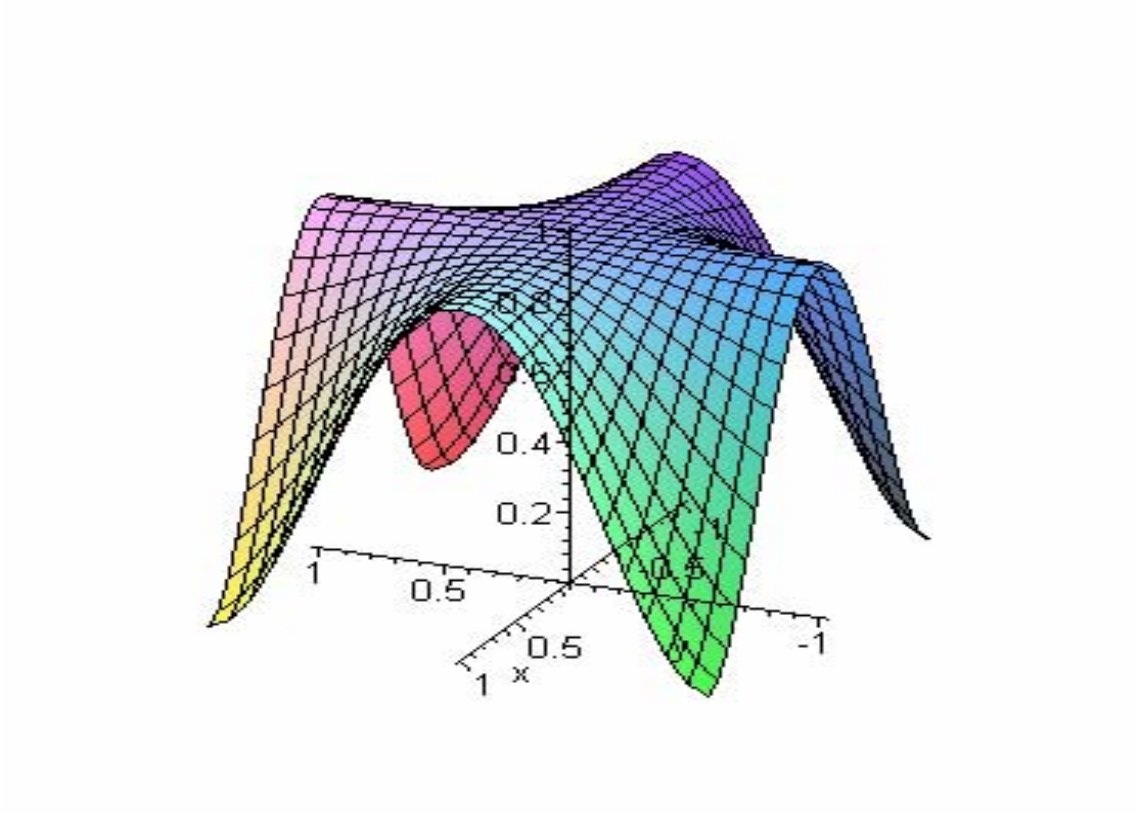
Motzkin. Uno de los ejemplos más sencillos es el siguiente polinomio Motzkin en el anillo $\mathbb{R}[x, y]$;

$$x^4y^2+x^2y^4-3x^2y^2+1$$

cuya función polinomial asociada es

$$f: \mathbb{R}^2\to\mathbb{R},\ f(x, y)=x^2y^4+x^2y^2(x^2-3)+1$$

y tiene como puntos críticos a los puntos de la forma $(x , 0)$, $(0 , y)$ con $x, y\in\mathbb{R}$, esto es, los ejes X, Y. En estos puntos $f(x, y)=1$. También, los puntos $(1 , 1)$, $(1 , -1)$, $(-1 , 1)$ y $(-1 , -1)$ son puntos críticos que son mínimos; $f(1 , 1)=f(1 , -1)=f(-1 , 1)=f(-1 , -1)=0$. Esto muestra que f es semidefinido positivo, es decir, la función polinomial $f(x, y)=x^2y^4+x^2y^2(x^2-3)+1$ es no negativa en $\mathbb{R}^2$. f no se puede escribir como suma de cuadrados de polinomios en $\mathbb{R}[x, y]$ ya que si esto fuera posible, es decir, si $x^4y^2+x^2y^4-3x^2y^2+1=f_1^2+\cdots+f_m^2$, entonces se tendría lo siguiente: x no aparecería en las f_i ya que su cuadrado aparece con coeficiente positivo y la suma es positiva, y en el término de la izquierda no aparecen x^2 ni y^2; lo mismo sucede con y. En forma análoga para las f_i^s con x^2, y^2 ya que ellas no aparecen con x^4 o y^4 en el término de la derecha con coeficiente positivo. En el término de la derecha aparece x^2y^2 con coeficiente positivo pero en el término de la izquierda aparece con el coeficiente -3.



El problema 17 de Hilbert se enuncia como sigue: Sea $f(x_1,\ldots,x_n)\in\mathbb{Q}(x_1,\ldots,x_n)$ una función racional semidefinida positiva, entonces ¿es $f(x_1,\ldots,x_n)$ una suma de cuadrados en

el campo $\mathbb{Q}(x_1,\ldots,x_n)$? La respuesta para los casos n=1 y n=2 era ya conocida afirmativamente en el último decenio del siglo antepasado. Artin, en la década de los 20 del siglo pasado, prueba un resultado más general el cual puede enunciarse como sigue.

TEOREMA 2.3.30. Sea k un campo cerrado real. Si $f \in k[x_1,\ldots,x_n]$ es un polinomio semidefinido positivo, entonces f es suma de cuadrados de polinomios en el campo $k(x_1,\ldots,x_n)$.

La definición de campo cerrado real así como la demostración de este teorema, se darán en el siguiente capítulo.

3. LA TEORÍA DE ARTIN-LANG Y EL NULLSTELLENSATZ REAL.

INTRODUCCIÓN

En la primera parte del capítulo se desarrolla la teoría de Artin-Lang para álgebras afines y sus campos de funciones. Se trabaja siempre con campos cerrados reales y sus cerraduras reales; se exponen resultados importantes tales como el teorema de lugares racionales de Lang y los teoremas del homomorfismo y del encaje. En la segunda parte se introducen los conceptos y resultados necesarios para establecer la generalización del teorema clásico de los ceros de Hilbert (Nullstellensatz clásico) al caso real o teorema de Dubois-Risler (Nullstellensatz real).

3.1. EXTENSIONES DE CAMPOS.

Se recuerda que un anillo A[†)] es un **campo** si todo elemento distinto de cero de A es una unidad; y un subconjunto F de un campo K es un **subcampo** de K si F es un campo con respecto a las operaciones en K. Se dice que un campo K es un **campo de extensión** de un campo F, lo cual se escribe $K:F$ o que $K:F$ es una **extensión de campos** si existe un homomorfismo inyectivo $\varphi:F\to K$. Sea $K:F$ una extensión de campos, $\alpha\in K$ es un **elemento algebraico** sobre F si $f(\alpha)=0$ para algún polinomio $f\in F[x]$ distinto de cero. Un elemento $\alpha\in K$ es **trascendente** sobre F si $f(\alpha)\neq 0$ para todo polinomio $f\in F[x]$ no constante. Un campo de extensión K de un campo F es una **extensión algebraica** sobre F si todo elemento en K es algebraico sobre F. Se dice que un campo K es **algebraicamente cerrado** si K no tiene extensiones algebraicas propias o equivalentemente si toda extensión algebraica L de K satisface que L=K. Una extensión $K:F$ es **finita de grado *n*** sobre F si K como espacio vectorial sobre F es de dimensión finita *n*. Se denota esta dimensión con el símbolo $[K:F]$ y se denomina **grado** de K sobre F.

Se observa que toda extensión finita $K:F$ de campos es algebraica. En efecto, si $\alpha\in K\setminus F$ es arbitrario y $[K:F]=n$ con $n\in\mathbb{N}$, entonces $1,\alpha,\alpha^2,\ldots,\alpha^n$ no son elementos linealmente independientes; de modo que existen elementos $a_0,a_1,\ldots,a_n\in F$ no todos cero tal que $a_0+a_1\alpha+\cdots+a_n\alpha^n=0$. Entonces $f=a_0+a_1x+\cdots+a_nx^n$ es un polinomio distinto de cero en $F[x]$ y $f(\alpha)=0$; luego, α es algebraico sobre F.

F es un **campo intermedio** entre los campos K y *k* si $K:F$ y $F:k$ son extensiones de campos. Si K es un campo y Γ un subconjunto de K, entonces el subcampo de K generado por Γ es la intersección de todos los subcampos de K que contienen a Γ. Sea $K:F$ una extensión de campos y Γ un subconjunto de K. Se denota por $F(\Gamma)$ el subcampo de K generado por $F\cup\Gamma$. $F(\Gamma)$ es el subcampo más pequeño de K que contiene a F y Γ. $F(\Gamma)$ es la intersección de todos los subcampos de K que contienen a F y Γ. $F(\Gamma)$ es un campo intermedio entre K y F, es decir, es un campo de extensión del campo F. Si $\Gamma=\{t_1,\ldots,t_n\}$,

[†)] Como en los capítulos anteriores, aquí anillo significa anillo conmutativo con unitario.

se escribe $F(t_1,\ldots,t_n)$ y es el campo generado sobre F por $t_1,\ldots,t_n$, o el campo obtenido por adjunción de $t_1,\ldots,t_n$ a F. También se dice que $F(t_1,\ldots,t_n)$ es el **campo de cocientes** del dominio entero $F[t_1,\ldots,t_n]$ o **campo de funciones racionales**. En el caso particular en que $\Gamma=\{\alpha\}$, se dice que $K:F$ es una **extensión simple** de campos si $K=F(\alpha)$, es decir, K se obtiene adjuntando uno de sus elementos a F. La extensión $K:F$ es **finitamente generada** si $K=F(t_1,\ldots,t_n)$ para algunos elementos $t_1,\ldots,t_n\in K$. Una extensión finitamente generada no necesariamente es finita. Cuando se habla de una extensión de campos $K:F$, es usual utilizar el siguiente diagrama en el que la letra F se coloca en un nivel más bajo que la letra K para indicar que F está contenido en K.

K
|
F

Una cadena de campos $F\subseteq F_1\subseteq F_2\subseteq\cdots\subseteq F_{n-1}\subseteq F_n\subseteq F_{n+1}\subseteq\cdots\subseteq K$ se denomina **torre** y cada subextensión $F_n:F_{n-1}$ un **piso** de la torre. De particular interés son las torres con un número finito de pisos.

PROPOSICIÓN 3.1.1. Sea $k\subseteq F\subseteq K$ una torre de campos. Si A y B son bases para las extensiones $K:F$ y $F:k$ respectivamente, entonces $AB=\{ab|\ a\in A,\ b\in B\}$ es una base para la extensión $K:k$ y $[K:k]=[F:k][K:F]$. En consecuencia, $K:k$ es finita si y sólo si $K:F$ y $F:k$ son finitas.

DEMOSTRACIÓN

Sea $x\in K$, entonces $x=\sum a_i y_i$ para un número finito de índices i, con $y_i\in F$ y $a_i\in A$. También se tiene que $y_i=\sum z_{ij} b_j$, donde $z_{ij}\in k$ y $b_j\in B$. Luego $x=\sum\sum z_{ij} a_i b_j$ lo cual muestra que K es generado sobre k por AB. Ahora supóngase que $\sum\sum z_{ij} a_i b_j=0$ con $z_{ij}\in k$, $a_i\in A$ y $b_j\in B$. Si $\sum z_{ij} b_j=c_i$, entonces $\sum c_i a_i=0$, con $c_i\in F$. Como los b_j son linealmente independientes sobre k, se sigue que $c_i=0$ para toda i luego $z_{ij}=0$ ya que las a_i son linealmente independientes en F.□

Como una consecuencia de esta proposición, se tiene

COROLARIO 3.1.2. Si $F_1\subseteq F_2\subseteq\cdots\subseteq F_n$ es una torre de campos y $F_{i+1}:F_i$ es una extensión (finita) para cada $i=1, 2,\ldots, n$, entonces $F_n:F_1$ es una extensión (finita) y

$$[F_n:F_1]=[F_n:F_{n-1}][F_{n-1}:F_{n-2}]\cdots[F_2:F_1].$$

DEMOSTRACIÓN

Se obtiene directamente de 3.1.1., por inducción. □

Un polinomio no constante $f\in F[x]$ es **irreducible** sobre F si f no puede expresarse como producto de dos polinomios en $F[x]$ de grado menor que el grado de f. Esto es, para

cualquier factorización $f=gh$ en F[x], g o h es una unidad en F[x] [†)]. Se recuerda que un ideal I de un anillo A es un **ideal principal** de A si I es generado por un elemento en A, es decir, $I=<a>$ para alguna $a\in$A, y A es un **dominio de ideales principales** si todo ideal de A es principal.

PROPOSICIÓN 3.1.3. Si F es un campo, entonces F[x] es un dominio de ideales principales.

DEMOSTRACIÓN

Sea I un ideal de F[x]. Si $I=\{0\}$, entonces $I=<0>$. Supóngase que $I\neq\{0\}$ y sea $g\in I$ un elemento distinto de cero de grado mínimo. Si g tiene grado cero, se sigue que $g\in$F y es una unidad; luego, $I=<1>=$F[x] e I es un ideal principal. Si g tiene grado ≥ 1, entonces tomando un elemento arbitrario $f\in I$, por el algoritmo de la división, existen polinomios q, r en F[x] tal que $f=qg+r$, donde $grad(r)<grad(g)$. Como f, $g\in I$, se tiene que $f-qg=r\in I$ y dado que g es un polinomio no cero de grado mínimo en I, se sigue que $r=0$, luego $f=qg$, esto es, $I=<g>$. □

Los polinomios irreducibles en el anillo de polinomios F[x] están estrechamente relacionados con los ideales maximales en F[x], es decir,

PROPOSICIÓN 3.1.4. Sea F[x] el anillo de polinomios en la indeterminada x con coeficientes en un campo F. Entonces un ideal $<f>\neq\{0\}$ con $f\in$F[x] es maximal si y sólo si f es irreducible sobre F.

DEMOSTRACIÓN ($\Rightarrow$)

Sea $<f>$ un ideal maximal de F[x] que no es el ideal cero, entonces $<f>\neq$F[x] y $f\notin$F. Sea $f=gh$ una factorización de f en F[x], entonces $gh\in<f>$ implica que $g\in<f>$ o $h\in<f>$, esto es, g o h tienen a f como un factor común. Es decir, los grados de los polinomios g y h no pueden ser menores que el grado de f. Por lo tanto, f es irreducible sobre F.

($\Leftarrow$)

Sea $f\in$F[x] un polinomio irreducible sobre F y supóngase que I es un ideal en F[x] tal que $<f>\subseteq I\subseteq$F[x]. Por la proposición 3.1.3., existe un polinomio $g\in$F[x] tal que $I=<g>$, luego $f\in<g>$ lo que significa que $f=gh$ para algún polinomio $h\in$F[x]. Como f es irreducible, se tiene que g o h es de grado cero. Si g es una constante en F[x] distinta de cero, entonces g es una unidad en F[x] y $<f>=I=$F[x]. Si h es de grado cero, entonces $h(x)=\alpha$ con $\alpha\in$F y $g=\alpha^{-1}f$ está en $<f>$; así, $I=<f>$. Por lo tanto, $<g>\subsetneq I\subsetneq$F[$x$] lo cual no puede ser posible. Luego $<f>$ es maximal. □

Un resultado más general establece que si un anillo A es un dominio de ideales principales, entonces todo ideal primo es maximal y recíprocamente.

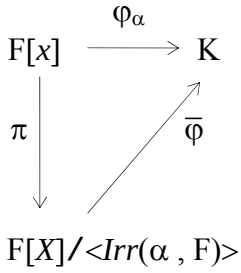
[†)] Las unidades en F[x] son los elementos distintos de cero de F.

Sea $K:F$ una extensión de campos, $\alpha\in K$ un elemento arbitrario y $\varphi_\alpha:F[x]\to K$; $a_0+a_1x+\cdots+a_nx^n\mapsto a_0+a_1\alpha+\cdots+a_n\alpha^n$ con $\varphi_\alpha(x)=\alpha$ y $\varphi_\alpha(a)=a$ para cada $a\in F$ (φ_α transforma isomorficamente a F vía la función identidad) el homomorfismo de evaluación en α, entonces se tiene el siguiente

TEOREMA 3.1.5. Sea $K:F$ una extensión de campos y $\alpha\in K$ un elemento algebraico sobre F. Entonces existe un polinomio irreducible $f\in F[x]$ con $f(\alpha)=0$. f está determinado de forma única salvo un factor constante en F, y es un polinomio de grado mínimo ≥ 1 en $F[x]$. Además, si $g(\alpha)=0$ para algún polinomio $g\in F[x]$ con $g\neq 0$, entonces f divide a g.

DEMOSTRACIÓN

Sea $\varphi_\alpha:F[x]\to K$ el homomorfismo de evaluación; su núcleo $Ker(\varphi_\alpha)=\langle f\rangle$ para algún polinomio $f\in F[x]$. Si $g\in Ker(\varphi_\alpha)$ con $g\neq 0$, entonces $g\in\langle f\rangle$ y f divide a g (ya que por el algoritmo de la división, $g=qf+r$ con q, $r\in F[x]$ donde ya sea $r=0$ o $grad(r)<grad(f)$. Como $r(\alpha)=0$, se sigue que $r=0$). Si h es otro polinomio del mismo grado que f, entonces $h=cf$ para algún $c\in F$; luego f es un polinomio de grado mínimo que tiene a α como un cero. Supóngase que $f=gh$, entonces $g(\alpha)=0$ o $h(\alpha)=0$. Si $g(\alpha)=0$, como $grad(g)\leq grad(f)$, se tiene que $grad(g)=grad(f)$ lo cual implica que h es una constante. Luego f es irreducible en $F[x]$.□



Si $K:F$ es una extensión de campos y $\alpha\in K$ es un elemento algebraico sobre F, entonces por 3.1.5., el único polinomio mónico f en $F[x]$ que anula a α (porque puede haber otros polinomios mónicos) es el polinomio irreducible para α sobre F que se denota por $Irr(\alpha, F)$. El grado de este polinomio es el grado de α sobre F que se escribe como $grad(\alpha, F)$. El núcleo del homomorfismo de evaluación φ_α es $\langle Irr(\alpha, F)\rangle$ que es un ideal maximal de $F[x]$ (ver 3.1.4.). Luego, $F[x]/\langle Irr(\alpha, F)\rangle$ es un campo isomorfo a $\varphi_\alpha(F[x])$ en K y es el menor subcampo de K que contiene a F y α. Como antes, este campo se denota como $F(\alpha)$. Si α es trascendente sobre F, ello es equivalente a $f(\alpha)\neq 0$ para cada polinomio $f\in F[x]$ no constante lo cual a su vez es equivalente a que $\varphi_\alpha(f)\neq 0$ para todo polinomio $f\in F[x]$ no constante con φ_α el homomorfismo de evaluación. Esto último equivale a que $Ker(\varphi_\alpha)=\{0\}$, esto es, $F[x]$ es encajado en K via el homomorfismo de evaluación. Luego la imagen, $\varphi_\alpha(F[x])$ es un dominio entero que no es un campo. K contiene al campo de cocientes $qf(F[x])=F(\alpha)$ y es el menor subcampo en K que contiene a F y α.

PROPOSICIÓN 3.1.6. Sea $K:F$ una extensión de campos y $\alpha\in K$ un elemento algebraico sobre F, entonces $F[\alpha]=F(\alpha)$ y $F(\alpha):F$ es una extensión finita de grado $[F(\alpha):F]$ igual al grado de $Irr(\alpha, F)$.

DEMOSTRACIÓN

Considérese el homomorfismo $\varphi: F[x]\to F[\alpha]$; $g\mapsto g(\alpha)$. Por la proposición 3.1.3.,

$Ker(\varphi)=<f>$ para algún $f\in F[x]$ con $f(\alpha)=0$. Como α es algebraico, $Ker(\varphi)\neq\{0\}$ y también $Ker(\varphi)\neq F[x]$ ya que $\varphi\neq 0$. Luego $f\neq 0$ y $grad(f)\geq 1$. Si f no es un polinomio mónico, bastará dividir éste por su coeficiente principal para obtener un polinomio mónico. Supóngase que f es un polinomio mónico; por el primer teorema del isomorfismo, se tiene que $F[x]/<f>=F[x]/Ker(\varphi)\cong Im(\varphi)=F[\alpha]$. Como $F[\alpha]$ es un dominio entero, el ideal $<f>$ es primo en $F[x]$; esto significa que f es irreducible en F. Por 3.1.4., se sigue que $<f>$ es maximal; de esta forma $F[x]/<f>$ es un campo. Como $F(\alpha)$ es el campo más pequeño que contiene a F y α, y dado que $F[x]/<f>=F[\alpha]\subseteq F(\alpha)$, se sigue que $F[\alpha]=F(\alpha)$. Por otro lado, si $g(\alpha)\in F[\alpha]$ para algún polinomio $g\in F[x]$, por el algoritmo de la división, se tiene que $g(x)=q(x)f(x)+r(x)$ donde los polinomios q, r están en $F[x]$ y $grad(r)<grad(f)$. Luego $g(\alpha)=q(\alpha)f(\alpha)+r(\alpha)=0+r(\alpha)$, con $r(\alpha)=b_0+b_1\alpha+\cdots+b_n\alpha^n$ y $n=grad(f)$. De esta forma, el conjunto $\{1_F, \alpha,\ldots,\alpha^{n-1}\}$ genera el espacio F-vectorial $F(\alpha)$. Se afirma que $\{1_F, \alpha,\ldots,\alpha^{n-1}\}$ es una base de $F(\alpha)$; en efecto, si $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=0$ con $a_i\in F$, $i=1,\ldots,n-1$, entonces $g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}\in F[x]$ tiene a α como una raíz y es de grado $\leq n-1$. Dado que $f \mid g$ (ver teorema 3.1.5.) y $grad(f)=n$, se sigue que $g=0$, esto es, $a_i=0$ para cada $i=1,\ldots,n-1$; luego $\{1_F, \alpha,\ldots,\alpha^{n-1}\}$ es linealmente independiente y en consecuencia es una base de $F(\alpha)$. Por lo tanto, $[F(\alpha):F]=n$. □

Más generalmente

COROLARIO 3.1.7. Sea $K:F$ una extensión de campos y $\alpha_1,\ldots,\alpha_n\in K$ elementos algebraicos sobre F. Entonces $F(\alpha_1,\ldots,\alpha_n):F$ es una extensión finita y por lo tanto algebraica.

DEMOSTRACIÓN (se hace por inducción sobre n.)

Para $n=1$, el resultado se sigue de 3.1.6.. Supóngase que $n>1$ y que el corolario es cierto para $n-1$, es decir, $F(\alpha_1,\ldots,\alpha_{n-1}):F$ es finita. Como α_n es algebraico sobre F y $F[x]\subseteq F(\alpha_1,\ldots,\alpha_{n-1})[x]$, se sigue que α_n es algebraico sobre $F(\alpha_1,\ldots,\alpha_{n-1})$. Por la proposición 3.1.6., $F(\alpha_1,\ldots,\alpha_{n-1},\alpha_n):F(\alpha_1,\ldots,\alpha_{n-1})$ es finita. Por 3.1.1., se tiene que $[F(\alpha_1,\ldots,\alpha_n):F]=[F(\alpha_1,\ldots,\alpha_{n-1},\alpha_n):F(\alpha_1,\ldots,\alpha_{n-1})][F(\alpha_1,\ldots,\alpha_{n-1}):F]$ es finito. □

PROPOSICIÓN 3.1.8. Sea $k\subseteq F\subseteq K$ una torre de campos. Entonces $K:k$ es algebraica si y sólo si $K:F$ y $F:k$ son algebraicas.

DEMOSTRACIÓN ($\Rightarrow$)

Primero se probará que $K:F$ es algebraica. Sea $\alpha\in K$, como $K:k$ es algebraica, existe f en $k[x]$ tal que $f(\alpha)=0$. Dado que $k\subseteq F$ y $k[x]\subseteq F[x]$, entonces $f(\alpha)=0$ en $F[x]$; así, α es algebraico sobre F y $K:F$ es algebraica. Ahora se prueba que $F:k$ es algebraica; sea $\alpha\in F$, como $F\subseteq K$, $\alpha\in K$ y dado que $K:k$ es algebraica, existe $f\in k[x]$ tal que $f(\alpha)=0$. Luego α es algebraico sobre k y $F:k$ es algebraica.

($\Leftarrow$)

Sea $\alpha\in K$ y $f=Irr(\alpha, F)$. Si $a_0,\ldots,a_n\in F$ son los coeficientes de f algebraicos sobre k,

entonces α es algebraico sobre $k(a_0,\ldots,a_n)$. Por el corolario 3.1.7., $k(a_0,\ldots,a_n):k$ es una extensión finita y $k(\alpha):k$ también es finita. Luego α es algebraico sobre k. □

Para extensiones algebraicas se tiene la siguiente

PROPOSICIÓN 3.1.9. $K:F$ es una extensión finita si y sólo si $K:F$ es algebraica y finitamente generada

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que $K:F$ es una extensión finita. Si $[K:F]=1$, $K=F(1)=F$. Si $F\subsetneq K$, entonces existe un elemento $\alpha_1\in K$ con $\alpha_1\notin F$ y $[F(\alpha_1):F]>1$. Si $K=F(\alpha_1)$ la demostración concluye. Si $F(\alpha_1)\subsetneq K$, entonces existe un $\alpha_2\in K$ con $\alpha_2\notin F(\alpha_1)$ y $[F(\alpha_1,\alpha_2):F(\alpha_1)]>1$. Ya que el proceso se detiene, $K=F(\alpha_1,\ldots,\alpha_n)$.

($\Leftarrow$)

Dado que $K:F$ es una extensión finitamente generada, existen elementos $\alpha_1,\ldots,\alpha_n\in K$ tal que $K=F(\alpha_1,\ldots,\alpha_n)$. Como $K:F$ es una extensión algebraica, $\alpha_1,\ldots,\alpha_n$ son elementos algebraicos sobre F. También las subextensiones

$$F(\alpha_1):F,\ F(\alpha_1,\alpha_2):F(\alpha_1),\ldots,F(\alpha_1,\ldots,\alpha_n):F(\alpha_1,\ldots,\alpha_{n-1})$$

son extensiones algebraicas. Dado que $F\subseteq F(\alpha_1)\subseteq F(\alpha_1,\alpha_2)\subseteq\cdots\subseteq F(\alpha_1,\ldots,\alpha_n)=K$ es una torre finita de campos con $F(\alpha_1,\ldots,\alpha_j):F(\alpha_1,\ldots,\alpha_{j-1})$ una extensión finita para $j=2,3,\ldots,n$, entonces por 3.1.2., se sigue que $K:F$ es finita. □

Un ejemplo de una extensión algebraica que no es finita es la extensión $\overline{\mathbb{Q}}:\mathbb{Q}$, donde $\overline{\mathbb{Q}}$ es el campo de los números complejos que son algebraicos sobre $\mathbb{Q}$

COROLARIO 3.1.10. Si $K:F$ es una extensión de campos y $\alpha_1,\ \alpha_2\in K$ son elementos algebraicos sobre F, entonces $\alpha_1+\alpha_2$, $\alpha_1-\alpha_2$, $\alpha_1\alpha_2$ y α_1/α_2 con $\alpha_2\neq 0$ son algebraicos sobre F.

DEMOSTRACIÓN

Dado que $F(\alpha_1,\alpha_2):F$ es una extensión algebraica y $\alpha_1+\alpha_2$, $\alpha_1-\alpha_2$, $\alpha_1\alpha_2$ y α_1/α_2 con $\alpha_2\neq 0$ son elementos de $F(\alpha_1,\alpha_2)$; el resultado se sigue. □

COROLARIO 3.1.11. Sea $K:F$ una extensión de campos, entonces el conjunto $\overline{F}^{K}=\{x\in K \mid x \text{ es algebraico sobre } F\}$ es un subcampo de K.

DEMOSTRACIÓN

Sean $\alpha_1,\ \alpha_2\in \overline{F}^{K}$. Como $F(\alpha_1,\alpha_2)\subseteq \overline{F}^{K}$, por el corolario anterior se sigue que $\alpha_1+\alpha_2$, $\alpha_1-\alpha_2$, $\alpha_1\alpha_2$ y α_1/α_2 con $\alpha_2\neq 0$ están en $\overline{F}^{K}$. Así, $\overline{F}^{K}$ es un subcampo de K. □

El campo $\overline{F}^{K}$ introducido en 3.1.11., se denomina **cerradura algebraica** de F en K y es algebaicamente cerrado en K. Este concepto puede generalizarse de la siguiente forma.

DEFINICIÓN 3.1.12. Sea K un campo. Un campo $\overline{K}$ es la **cerradura algebraica** de K si

i) $\overline{K}:K$ es una extensión algebraica.

ii) $\overline{K}$ es algebraicamente cerrado.

TEOREMA 3.1.13. Todo campo F tiene una cerradura algebraica $\overline{F}$.

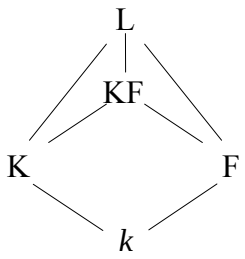
DEMOSTRACIÓN

Considérese la familia $\mathcal{F}=\{K_i|\ i\in I\}$ de todos los campos de extensión K_i de un campo F tal que la extensión $K_i:F$ es algebraica; $\mathcal{F}\neq\varnothing$ ya que $F\in\mathcal{F}$. Ordenando parcialmente por inclusión, $(\mathcal{F}, \subseteq)$ es un conjunto parcialmente ordenado. Sea L un subconjunto de $\mathcal{F}$ totalmente ordenado y considérese a $E=\cup K_i$ con K_i en L. Se afirma que E es un campo y $E:F$ es algebraica. En efecto, sean a, $b\in E$, entonces existen campos K_{i_1}, K_{i_2} en L con $a\in K_{i_1}$, $b\in K_{i_2}$. Como L es totalmente ordenado, K_{i_1} es un subcampo de K_{i_2} o K_{i_2} es un subcampo de K_{i_1}. Supóngase que $K_{i_1}\subseteq K_{i_2}$; entonces a, $b\in K_{i_2}$. Se usan las operaciones de suma y multiplicación en K_{i_2} para definir las operaciones de suma y multiplicación en E. Es rutinario probar que E es un campo con neutro multiplicativo, el $1\in F$. Así, E es un campo y $K_i\subseteq E$ para cada $i\in I$. A continuación se probará que $E:F$ es algebraica. Sea $\alpha\in E$, entonces $\alpha\in K_{i_0}$ para algún $i_0\in I$ con K_{i_0} en L. Luego α es algebraica sobre F y $E:F$ es una extensión algebraica y una cota superior para L. Por el lema de Zorn, existe al menos un elemento maximal $\overline{F}$ de $\mathcal{F}$. Se afirma que $\overline{F}$ es algebraicamente cerrado. En efecto, sea $f\in\overline{F}[x]$, donde $f\notin\overline{F}$. Si f no tiene ceros en $\overline{F}$, se puede tomar un elemento $w\notin\overline{F}$ y formar un campo $\overline{F}(w)$ con w cero de f. Sea $\beta\in\overline{F}(w)$, entonces β es un cero del polinomio $g=\alpha_0+\alpha_1x+\cdots+\alpha_nx^n$ en $\overline{F}[x]$ con $\alpha_i\in\overline{F}$ y por tanto α_i es algebraico sobre F. Luego $F(\alpha_0,\ldots,\alpha_n):F$ es finita y dado que β es algebraico sobre $F(\alpha_0,\ldots,\alpha_n)$, $\overline{F}(\alpha_0,\ldots,\alpha_n,\beta):F(\alpha_0,\ldots,\alpha_n)$ es una extensión finita; luego $F(\alpha_0,\ldots,\alpha_n,\beta):F$ es una extensión finita. De esta forma β es algebraico sobre F. Entonces $\overline{F}(w)\in\mathcal{F}$ y $\overline{F}\subseteq\overline{F}(w)$ lo cual contradice la elección de $\overline{F}$ como un elemento maximal de $\mathcal{F}$. Por tanto f tiene un cero en F y $\overline{F}$ es algebraicamente cerrado. □

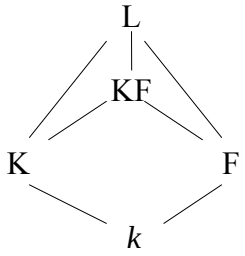
Sean $K:k$ y $F:k$ dos extensiones de campos. Si K y F están contenidos en un campo L, se define el **campo producto** KF como el subcampo de L generado por el conjunto $K\cup F$, esto es, $KF=K(F)=F(K)=FK$. Se observa que si k es un subcampo de $K\cap F$ tal que $K=k(\Gamma)$ y $\Gamma\subseteq K$, entonces $KF=F(\Gamma)$. Si $K:k$ y $F:k$ son extensiones finitas, entonces el campo producto KF es el conjunto de los elementos de la forma $\sum_i x_iy_j$, $x_i\in K$ y y_iF. En el caso general, el campo producto KF es el campo de cocientes del dominio entero $k[K\cap F]$,

esto es, KF= $qf\left(k[\mathrm{K}\cap\mathrm{F}]\right)$ cuyos elementos son de la forma $(\sum_i x_i y_j)(\sum_j x_i' y_j')^{-1}$, x_i, $x_j' \in$K y y_i, $y_j' \in$F. El conjunto KF es el mínimo subcampo de L que contiene a K y F. También se dice que KF es la intersección de todos los subcampos de L que contienen a K y F.

El siguiente diagrama proporciona una descripción gráfica.



PROPOSICIÓN 3.1.14. Dadas las extensiones de campos



la extensión KF : k es algebraica si y sólo si K : k y F : k son algebraicas.

DEMOSTRACIÓN ($\Rightarrow$)

Por hipótesis KF : k es algebraica. Por 3.1.8., se sigue que KF : K, KF : F, K : k y F : k son algebraicas.

($\Leftarrow$)

Sea Γ=K$\cup$F, entonces KF=$k(\Gamma)$ y cada elemento de Γ es algebraico sobre k. Por 3.1.7., la extensión $k(\Gamma)$: k es algebraica, esto es, KF : k es algebraica. □

Sea K : F una extensión de campos. Si al menos un elemento $x \in$K no es algebraico sobre F, se dirá que la extensión es **trascendente**. Si $\Gamma=\{\alpha_1,\ldots,\alpha_n\}$ es un conjunto finito de elementos de K, se dice que Γ es **algebraicamente independiente** sobre F o que los elementos $\alpha_1,\ldots,\alpha_n$ son algebraicamente independientes sobre F si el único polinomio en $\mathrm{F}[x_1,\ldots,x_n]$ que se anula en $\alpha_1,\ldots,\alpha_n$ es el polinomio cero de $\mathrm{F}[x_1,\ldots,x_n]$.

Sea K : F una extensión de campos y $\{\alpha_1,\ldots,\alpha_n\}$ en K un conjunto algebraicamente independiente sobre F. Si se supone que $\{\alpha_1,\ldots,\alpha_r\}$ con $r<n$ es un subconjunto de $\{\alpha_1,\ldots,\alpha_n\}$ que no es algebraicamente independiente sobre F, entonces existe un polinomio no cero $f \in \mathrm{F}[x_1,\ldots,x_r]$ tal que $f(\alpha_1,\ldots,\alpha_r)=0$. Pero f en el anillo $\mathrm{F}[x_1,\ldots,x_r,x_{r+1},\ldots x_n]$ satisface que $f(\alpha_1,\ldots,\alpha_r,\alpha_{r+1},\ldots\alpha_n)=0$ lo cual contradice el hecho de que $\{\alpha_1,\ldots,\alpha_n\}$ sea algebraicamente independiente sobre F. De esta forma se tiene que

todo subconjunto de un conjunto algebraicamente independiente es algebraicamente independiente; luego si $K:F$ es una extensión algebraica, entonces el único subconjunto algebraicamente independiente de K es el conjunto vacío. También, todo elemento de un conjunto algebraicamente independiente de K es necesariamente trascendente sobre F. En efecto, si $\{\alpha_1,\ldots,\alpha_n\}$ en K es un conjunto algebraicamente independiente sobre F y si se supone que existe un elemento α_{i_0} en $\{\alpha_1,\ldots,\alpha_n\}$ que no es trascendente sobre F, entonces existe un polinomio $f \in F[x_{i_0}]$ no cero tal que $f(\alpha_{i_0}) = 0$. Pero f en $F[x_1,\ldots,x_{i_0},x_{i_0+1},\ldots x_n]$ satisface que $f(\alpha_1,\ldots,\alpha_{i_0},\alpha_{i_0+1},\ldots\alpha_n) = 0$ lo cual contradice el hecho de que $\{\alpha_1,\ldots,\alpha_n\}$ sea algebraicamente independiente sobre F. Si $\alpha_1,\ldots,\alpha_n \in K$ son algebraicamente independientes sobre F, entonces $F[\alpha_1,\ldots,\alpha_n]$ es un anillo de polinomios.

Cuando n=1, $\Gamma=\{\alpha\}$ es algebraicamente independiente si y sólo si α es trascendente sobre F. Si Γ es infinito, Γ es algebraicamente independiente si todo subconjunto finito de Γ es algebraicamente independiente. El concepto de independencia algebraica generaliza el concepto de independencia lineal en el sentido de que si S en K es un conjunto linealmente dependiente sobre F, entonces existe un polinomio no cero f de grado mayor o igual a uno en el anillo $F[x_1,\ldots,x_n]$ tal que $f(s_1,\ldots,s_n)=0$ para elementos distintos de cero $s_1,\ldots,s_n \in S$. Esto es, todo conjunto algebraicamente independiente es también linealmente independiente, pero no recíprocamente.

Se dice que $K:F$ es una extensión **trascendente pura** si existe un subconjunto Γ del campo K algebraicamente independiente tal que $K=F(\Gamma)$.

PROPOSICIÓN 3.1.15. Toda extensión de campos $K:F$ contiene un conjunto Γ que es algebraicamente independiente maximal. $K:F(\Gamma)$ es algebraica y $F(\Gamma):F$ es trascendente pura.

DEMOSTRACIÓN

La existencia de Γ es una consecuencia del lema de Zorn. En efecto, sea $\mathfrak{A}$ la familia de todos los subconjuntos algebraicamente independientes de K. Si $\mathfrak{A}=\varnothing$ no hay nada que hacer; si $\mathfrak{A}\neq\varnothing$, $(\mathfrak{A}, \subseteq)$ es un conjunto parcialmente ordenado. Sea $\mathcal{A}$ un subconjunto no vacío totalmente ordenado de $\mathfrak{A}$ y $\Lambda=\cup\Gamma'$ con $\Gamma'\in\mathcal{A}$. Claramente Λ es un subconjunto algebraicamente independiente de K y una cota superior de $\mathcal{A}$. Por el lema de Zorn, el conjunto parcialmente ordenado $(\mathfrak{A}, \subseteq)$ tiene al menos un elemento maximal Γ. Por otro lado, supóngase que $K:F(\Gamma)$ no es una extensión algebraica, es decir, existe un elemento $\alpha\in K$ trascendente sobre $F(\Gamma)$ y en particular sobre F. Entonces $\Gamma\cup\{\alpha\}$ es un conjunto algebraicamente independiente; esto último contradice la maximalidad de Γ. Finalmente, como Γ es un conjunto algebraicamente independiente, se tiene que $F(\Gamma):F$ es trascendente pura. □

Todo subconjunto B de K que satisface las propiedades de Γ en la proposición anterior, esto es, que B es algebraicamente independiente maximal, se denomina **base de trascendencia** de K sobre F. Se observa que un subconjunto B de K es una base de trascendencia de K sobre F si *i*) B es algebraicamente independiente sobre F y *ii*) $K:F(B)$ es algebraica. Todo subconjunto Γ de K que satisface *ii*) anterior, se denomina **conjunto**

generador de K sobre F o se dice que K es generado por un subconjunto Γ sobre F. Se observa que una base de trascendencia de una extensión puede ser un conjunto vacío en cuyo caso se dice que la extensión $K:F$ es algebraica. Una base de trascendencia de un campo K sobre un subcampo F es el análogo de una base de un espacio vectorial K sobre F. En general, una base de trascendencia no es una base de un espacio vectorial; por ejemplo, si $f/g \in F(x)$ con $f, g \in \neq 0$, entonces el polinomio no cero $h(y_1, y_2)=g(y_1)y_2-f(y_1)$ que está en el anillo $F[y_1, y_2]$ es tal que $h(x, f/g)=g(x)(f/g)-f(x)=0$. Así, $\{x, f/g\}$ es algebraicamente independiente en $F(x)$. De esto se ve que $\{x\}$ es una base trascendente de $F(x)$ sobre F que no es una base de espacio vectorial ya que $\{1_F, x, x^2, x^3, \ldots\}$ es linealmente independiente en $F(x)$.

LEMA 3.1.16. Sea $K:F$ una extensión de campos, Γ en K un conjunto generador de K sobre F. Si S en K es un conjunto finito de elementos algebraicamente independientes sobre F, entonces $|S| \leq |\Gamma|$.

DEMOSTRACIÓN

Sea $\alpha \in S$; como α es algebraico sobre $F(\Gamma)$, existe un polinomio con coeficientes en $F(\Gamma)$ que tiene a α como una raíz. Dado que solamente un número finito de elementos de Γ son coeficientes de este polinomio, se tiene que para un cierto número $n \in \mathbb{N}$, existen un polinomio $p \in F[x, x_1, \ldots, x_n]$ y elementos $\gamma_1, \ldots, \gamma_n \in \Gamma$ tal que $p(\alpha, \gamma_1, \ldots, \gamma_n)=0$. Como α es algebraicamente independiente sobre F, esto es, trascendente sobre F y considerando a p como un polinomio en el anillo $F[x_1, \ldots, x_n][x]$[†)], existe al menos un coeficiente $q \in F[x_1, \ldots, x_n]$ de p que tiene grado positivo en $x_1, \ldots, x_n$. Si x_i es una indeterminada que aparece en un monomio de q con coeficiente no cero, se tiene que γ_i es algebraico sobre $F(\gamma_1, \ldots, \gamma_{i-1}, \gamma_i, \gamma_{i+1}, \ldots, \gamma_n, \alpha)$. Luego, $(\Gamma \setminus \{\gamma_i\}) \cup \{\alpha\}$ es un subconjunto de K que satisface que $K:(\Gamma \setminus \{\gamma_i\}) \cup \{\alpha\}$ es algebraica. De esta forma $(\Gamma \setminus \{\gamma_i\}) \cup \{\alpha\}$ es un nuevo conjunto generador de $K:F$. Prosiguiendo por inducción, sea $S_1 \subseteq S$ un subconjunto con r elementos para el cual existe un subconjunto $\Gamma_1 \subseteq \Gamma$ también con r elementos tal que $\Gamma' = (\Gamma \setminus \Gamma_1) \cup S_1$ es un subconjunto de K que satisface que $K:\Gamma'$ es algebraica. Si $S_1=S$, la existencia de Γ_1 significa que, $|S| \leq |\Gamma|$. Si existe $\alpha \in S \setminus S_1$; como α es algebraico sobre $F(\Gamma')$, existe un polinomio $p' \in F[x_1, \ldots, x_r, y_1, \ldots, y_{n-r}][x]$ tal que $p'(\alpha_1, \ldots, \alpha_r, \gamma_1, \ldots, \gamma_{n-r})=0$ con $\alpha_i \in S$, $i=1, \ldots, r$, $\gamma_j \in \Gamma \setminus \Gamma_1$, $j=1, \ldots, n-r$, ($\gamma_1, \ldots, \gamma_{n-r}$ son ciertos elementos en $\Gamma \setminus \Gamma_1$). Si p' se considera ahora como un polinomio en $F[y_1, \ldots, y_{n-r}][x_1, \ldots, x_r]$, esto es, un polinomio con coeficientes en $F[y_1, \ldots, y_{n-r}]$, se tiene que, como $\{\alpha_1, \ldots, \alpha_r, \alpha\}$ es algebraicamente independiente sobre F, existe al menos un coeficiente $q' \in F[y_1, \ldots, y_{n-r}]$ de p' que tiene grado positivo en $y_1, \ldots, y_{n-r}$. Siguiendo el razonamiento anterior, existe un elemento $\gamma_i \in \Gamma \setminus \Gamma_1$ algebraico sobre $F(\alpha, \alpha_1, \ldots, \alpha_r, \gamma_1, \ldots, \gamma_{i-1}, \gamma_{i+1}, \ldots, \gamma_{n-r})$. Así, $\Gamma \setminus \Gamma_1$ es no vacío, y si $S' = S_1 \cup \{\alpha\}$ y $\Gamma'' = \Gamma_1 \cup \{\gamma_i\}$; S_1 y Γ'' ambos con $r+1$ elementos, se tiene que $S' \cup (\Gamma \setminus \Gamma'')$ es un nuevo subconjunto de K tal que $K:S \cup (\Gamma \setminus \Gamma'')$ es algebraica. Este proceso de inducción termina cuando se tiene un conjunto $\Gamma^* \subseteq \Gamma$, con el mismo número de elementos que S, tal que $S \cup (\Gamma \setminus \Gamma^*)$ es un subconjunto de K con $K:S \cup (\Gamma \setminus \Gamma^*)$ algebraica. Por lo tanto $|S| \leq |\Gamma|$. □

---

†) p se considera como un polinomio en x con coeficientes en $F[x_1, \ldots, x_n]$.

PROPOSICIÓN 3.1.17. Sea $K:F$ una extensión de campos, B y B' bases de trascendencia de K sobre F. Entonces $|B|=|B'|$.

DEMOSTRACIÓN (Caso finito)

Se sabe que B y B' son conjuntos algebraicamente independientes sobre F y que $K:F(B)$ y $K:F(B')$ son extensiones algebraicas. Si $B\subseteq B'$, por el lema 3.1.16., se tiene que $|B|\leq |B'|$. También, si $B'\subseteq B$, se tendrá que $|B'|\leq |B|$. Por lo tanto se concluye que $|B|=|B'|$.

(Caso infinito)

Se probará que si B y B' son bases de trascendencia de K sobre F y $|B|$ es infinito entonces $|B'|$ es infinito y $|B|=|B'|$. En efecto, dado que B' es una base de trascendencia de K sobre F, se sigue del caso finito que el cardinal de B' es infinito. Sea $\alpha\in B$, entonces α es algebraico sobre $F(B')$ (ver proposición 3.1.15.). Considérese el polinomio irreducible para α sobre $F(B')$; $f=Irr(\alpha, F(B'))$. Los coeficientes de este polinomio están en el campo $F(\Gamma_\alpha)$ con Γ_α un subconjunto finito de B'. De esta forma, $f\in F(\Gamma_\alpha)[x]$ y α es algebraico sobre $F(\Gamma_\alpha)$. Para cada $\alpha\in B'$ se considera el respectivo polinomio irreducible de α sobre $F(B')$ y el respectivo conjunto finito Γ_α de B'. Se afirma que $\cup\Gamma_\alpha=B'$ es una base de trascendencia de K sobre F. En efecto, $\cup\Gamma_\alpha$ como un conjunto de B' es algebraicamente independiente. También se tiene que todo elemento α de B es algebraico sobre $F(\cup_{\alpha\in B}\Gamma_\alpha)$. Luego la extensión $F(\cup_{\alpha\in B}\Gamma_\alpha)(B):F(\cup_{\alpha\in B}\Gamma_\alpha)$ es algebraica. Como $F(B)\subseteq F(\cup_{\alpha\in B}\Gamma_\alpha)(B)$, se sigue que todo elemento de $F(B)$ es algebraico sobre $F(\cup_{\alpha\in B}\Gamma_\alpha)$. Por la proposición 3.1.15., $\cup_{\alpha\in B}\Gamma_\alpha$ es una base de trascendencia de K sobre F, esto es, $\cup_{\alpha\in B}\Gamma_\alpha=B$. A continuación se probará que $|B|\geq|B'|$. Se observa que los conjuntos finitos Γ_α con $\alpha\in B$ no son mutuamente ajenos. Por el principio del buen orden en B, B tiene un primer elemento que se escribe como 1. Sea $\Gamma'_1=\Gamma_1$ y $\Gamma'_\alpha=\Gamma_\alpha\setminus\cup_{i<\alpha}\Gamma_i$ para cada $\alpha\in B$ con $\alpha>1$. Claramente Γ'_α es finito, $\cup_{\alpha\in B}\Gamma_\alpha=\cup_{\alpha\in B}\Gamma'_\alpha$ y los Γ'_α son mutuamente ajenos. Para cada $\alpha\in B$ considérese un orden $\leq$ fijo de $\Gamma'_\alpha=\{\gamma_1,\ldots,\gamma_{k\alpha}\}$; considérese también la función $\varphi:\cup_{\alpha\in B}\Gamma_\alpha\to B\times\mathbb{N}$; $\gamma_i\mapsto(\alpha\ ,\ i)$. φ es inyectiva, esto es, $\cup_{\alpha\in B}\Gamma'_\alpha$ es equipotente con algún subconjunto de $B\times\mathbb{N}$. De esta forma $|B'|=|\cup_{\alpha\in B}\Gamma_\alpha|=|\cup_{\alpha\in B}\Gamma'_\alpha|\leq|B\times\mathbb{N}|=|B||\mathbb{N}|=|B|\aleph_0=|B|$. En forma similar se tiene que $|B|\leq|B'|$. Por lo tanto, $|B|=|B'|$. □

Si $K:F$ es una extensión de campos y B una base de trascendencia de K sobre F, se define el **grado de trascendencia** de K sobre F como el número de elementos de B y se denota $grtr(K:F)$. Por ejemplo, si $F[x_1,\ldots,x_n]$ es el anillo de polinomios en las indeterminadas $x_1,\ldots,x_n$ con coeficientes en el campo F, entonces $grtr(F(x_1,\ldots,x_n):F)=n$. Se observa que $K:F$ es algebraica si y sólo si $grtr(K:F)=0$.

PROPOSICIÓN 3.1.18. Sea $K:F$ una extensión de campos, Γ en K un conjunto generador de K sobre F, entonces existe un subconjunto $B\subseteq\Gamma$ que es base de trascendencia de $K:F$.

DEMOSTRACIÓN

Sea $\mathfrak{A}$ la familia de todos los subconjuntos de Γ que son algebraicamente independientes. $\mathfrak{A}$ puede ordenarse por inclusión; y por el lema de Zorn, existe un elemento maximal de esta familia; digamos que B es este elemento, esto es, B es un subconjunto

algebraicamente independiente de Γ. De esta forma, todo elemento $u\in\Gamma\setminus B$ es algebraico sobre $F(B)$, entonces $F(\Gamma)$ es algebraico sobre $F(B)$. Así, K es algebraico sobre $F(B)$ por 3.1.8., y por 3.1.15., se concluye que B es una base trascendente de K sobre F. □

COROLARIO 3.1.19. Si $K:F$ es una extensión finitamente generada y B es una base de trascendencia de $K:F$, entonces $grtr(K:F)<\infty$ y $K:F(B)$ es una extensión finita y por lo tanto algebraica.

DEMOSTRACIÓN

Por hipótesis $K=F(S)$ para algún subconjunto finito S de K. Por la proposición 3.1.18., existe una base de trascendencia B' de $K:F$. Como B es una base de trascendencia de $K:F$ y $B'\subseteq S$ con $|B|=|B'|<|S|<\infty$, se tiene que $grtr(K:F)<\infty$. Por otro lado, como $K:F(B)$ es algebraica y finitamente generada, se sigue que $K:F(B)$ es una extensión finita (ver proposición 3.1.9.). □

PROPOSICIÓN 3.1.20. Sea $k\subseteq F\subseteq K$ una torre de campos. Si $F:k$ es algebraica y T en K es algebraicamente independiente sobre k, entonces T es algebraicamente independiente sobre F.

DEMOSTRACIÓN

Si T no es algebraicamente independiente sobre F, entonces existe $t\in T$ algebraico sobre $F(T\setminus\{t\})$. Dado que $F:k$ es algebraica, se sigue que $F(T\setminus\{t\}):k(T\setminus\{t\})$ es algebraica. Luego cada piso en la torre

$$k(T\setminus\{t\})\subseteq F(T\setminus\{t\})\subseteq F(T\setminus\{t\})(t)=F(t)$$

es algebraica, entonces $t\in F(t)$ es algebraico sobre $k(T\setminus\{t\})$. Pero esto contradice la independencia algebraica de T sobre k. □

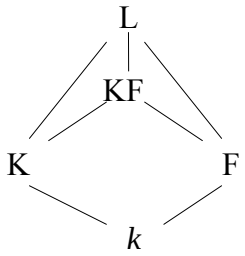
PROPOSICIÓN 3.1.21. Sea $k\subseteq F\subseteq K$ una torre de campos. Entonces $K:k$ es finitamente generada, si y sólo si $K:F$ y $F:k$ son finitamente generadas.

DEMOSTRACIÓN

Si $K=F(S)$ y $F=k(T)$, con S y T finitos, entonces $K=k(S\cup T)$ y $K:k$ es finitamente generada. Claramente si $K:k$ es finitamente generada, entonces $K:F$ es también finitamente generada por el mismo conjunto de generadores. Sea $S=\{s_1,\ldots, s_k\}$ una base de trascendencia de F sobre k, entonces el segundo piso de la torre $k\subseteq k(S)\subseteq F\subseteq K$ es algebraico y K es finitamente generado sobre $k(S)$. Sea $T=\{t_1,\ldots, t_n\}$ una base de trascendencia de K sobre k. Se desea probar que $[F:k]\leq[K:k(T)]$ mostrando que todo subconjunto finito de F que es linealmente independiente sobre k también es linealmente independiente sobre $k(T)$ como un subconjunto de K. Dado que $K:k(T)$ es finita, por el corolario 3.1.19., se sigue el resultado. En primer lugar, se observa que como T es algebraicamente independiente sobre k, por la proposición 3.1.20., T es algebraicamente independiente sobre F. Sea $\Gamma=\{y_1,\ldots,y_m\}$ en F linealmente independiente sobre k y supóngase que $\sum r_i(t_1,\ldots,r_n)y_i=0$, donde $r_i(t_1,\ldots,r_n)\in k(T)$. Supóngase también que cada $r_i(t_1,\ldots,r_n)$ es un polinomio sobre k.

Considerando términos que involucran exponentes similares de los t_i, se obtiene que $\sum(\sum a_{\mu_1\cdots\mu_n})t_1^{\mu_1}\cdots t_n^{\mu_n}=0$, donde $a_{\mu_1\cdots\mu_n}\in k$ es el coeficiente de $t_1^{\mu_1}\cdots t_n^{\mu_n}$ en $r_i(t_1,\ldots,r_n)$. Como T es algebraicamente independiente sobre F se tiene que T también es algebraicamente independiente sobre $k(t_1,\ldots,r_n)\subseteq$F. Así, $\sum a_{\mu_1\cdots\mu_n}y_i=0$ y la dependencia lineal de Γ sobre k implica que $a_{\mu_1\cdots\mu_n}=0$. Luego $r_i(t_1,\ldots,r_n)=0$ para cada i. Esto muestra que Γ es linealmente independiente sobre k(T). □

PROPOSICIÓN 3.1.22. Dadas las extensiones de campos



La extensión KF : k es finitamente generada si y sólo si K : k y F : k son finitamente generadas.

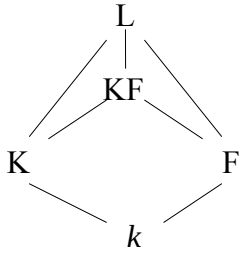
DEMOSTRACIÓN ($\Rightarrow$)

Se sigue de la proposición 3.1.21.

($\Leftarrow$)

Que K : k y F : k sean finitamente generadas, significa que existen $\alpha_1,\ldots,\alpha_n\in$K y $\beta_1,\ldots,\beta_m\in$F tal que K=$k(\alpha_1,\ldots,\alpha_n)$ y F=$k(\beta_1,\ldots,\beta_m)$. Entonces KF=$k(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m)$ y así, KF : k es finitamente generada. □

PROPOSICIÓN 3.1.23. Dadas las extensiones de campos.



La extensión KF : k es finita si y sólo si las extensiones K : k y F : k son finitas. En este caso [KF : k]≤[K : k][F : k].

DEMOSTRACIÓN

Que KF : k sea finita, por la proposición 3.1.9., es equivalente a que KF : k es algebraica y finitamente generada. Por 3.1.14.y 3.1.22., lo anterior es equivalente a que K : k y F : k son algebraicas y finitamente generadas, lo cual nuevamente por 3.1.9 será equivalente a que K : k y F : k sean finitas. □

LEMA 3.1.24. Sea K : F una extensión de campos. Si K=F(*S*) para algún subconjunto *S* de K. Entonces K : F es algebraica si y sólo si cada elemento de *S* es algebraico sobre F.

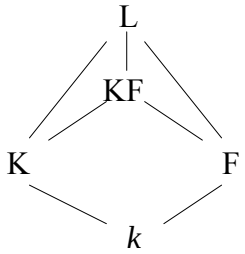
DEMOSTRACIÓN ($\Rightarrow$)

Sea $x \in S$; como $x \in$ K y K : F es algebraica, se sigue que *x* es algebraico sobre F.

($\Leftarrow$)

Por el corolario 3.1.11., se tiene que *S* es un subcampo de K, esto es, $S=\overline{F}^{K}$. Como K=*S*, entonces K : F es algebraica. □

OBSERVACIÓN 3.1.25. Dadas las extensiones de campos



si la extensión K : *k* es algebraica, entonces la extensión KF : F es algebraica.

DEMOSTRACIÓN

Como KF=F(*S*) y cada elemento de K es algebraico sobre *k*, (esto es, existe un polinomio no cero $f \in k[x]$ tal que $f(\alpha)=0$ para toda $\alpha \in$ K y como $f \in$ F[*x*] es tal que $f(\alpha)=0$ para toda $\alpha \in$ K) entonces también cada elemento de K es algebraico sobre F. Luego por el lema 3.1.24., se tiene que la extensión KF : F es algebraica □

El recíproco es falso en general. Por ejemplo si K=$\mathbb{Q}$(*x*), F=$\mathbb{Q}(\sqrt{2},\pi)$ y *k*=$\mathbb{Q}$. Entonces KF : F=$\mathbb{Q}(\sqrt{2},\pi)$. Luego KF : F es algebraica y K : *k* es trascendente.

Para extensiones finitamente generadas se tiene

PROPOSICIÓN 3.1.26. Sea $k \subseteq F \subseteq K$ una torre de campos, B_1 y B_2 bases de trascendencia de F : *k* y K : F respectivamente. Entonces $B_1 \cup B_2$ es una base de trascendencia de K : *k* y *grtr*(K : *k*)=*grtr*(K : F)+*grtr*(F : *k*).

DEMOSTRACIÓN

Sea B_1 una base de trascendencia de F sobre *k* y B_2 una base de trascendencia de K sobre F. Como $B_1 \subseteq$ F, B_1 es algebraicamente dependiente sobre *k*, luego $B_1 \cap B_2 = \varnothing$. Dado que todo elemento de F es algebraico sobre $k(B_1)$, (ver corolario 3.1.19.) se tiene que también es algebraico sobre $k(B_1 \cup B_2)$. De esta forma, $k(B_1 \cup B_2)$(F) : $k(B_1 \cup B_2)$ es algebraica. Como $k(B_1 \cup B_2)=k(B_1)(B_2) \subseteq F(B_2) \subseteq k(B_1 \cup B_2)$(F), F($B_2$) es algebraico sobre $k(B_1 \cup B_2)$. Restará mostrar que $B_1 \cup B_2$ es algebraicamente independiente sobre *k*. En efecto, sea *f* un polinomio sobre *k* en *m*+*n* indeterminadas $x_1, \ldots, x_n, y_1, \ldots, y_m$ tal que

$$f(s_1,\ldots,s_n,\, t_1,\ldots,t_m)=0$$

para algunos elementos distintos $s_1,\ldots,s_n\in B_1$ y $t_1,\ldots,t_m\in B_2$. Sea

$$g(y_1,\ldots,y_m)=f(s_1,\ldots,s_n,\, t_1,\ldots,t_m)\in k(B_1)[y_1,\ldots,y_m]\subseteq \mathrm{F}[y_1,\ldots,y_m].$$

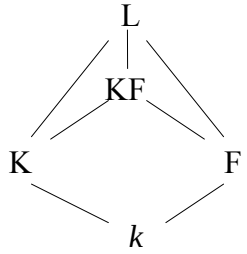
Como $g(t_1,\ldots,t_m)=0$, la independencia algebraica de B_2 sobre F implica que $g=0$, de donde

$$f(x_1,\ldots,x_n,\, y_1,\ldots,y_m)=\sum h_i(x_1,\ldots,x_n)k_i(y_1,\ldots,y_m)$$

con $h_i\in k[x_1,\ldots,x_n]$, $k_i\in k[y_1,\ldots,y_m]$ para cada i. La independencia algebraica de B_1 sobre k implica que $h_i=0$ para toda i, luego $f(x_1,\ldots,x_n,y_1,\ldots,y_m)=0$; por lo tanto $B_1\cup B_2$ es algebraicamente independiente sobre k. Así, $grtr(\mathrm{K}:k)=|B_1\cup B_2|=|B_1|+|B_2|$ y el resultado se sigue. □

Para el campo producto se tiene

PROPOSICIÓN 3.1.27. Dadas las extensiones de campos



$$grtr(\mathrm{KF}:\mathrm{K})\le grtr(\mathrm{F}:k) \text{ y } grtr(\mathrm{KF}:k)\le grtr(\mathrm{K}:k)+grtr(\mathrm{F}:k)$$

DEMOSTRACIÓN

Sea B una base de trascendencia del campo F sobre k. Como KF=K(F) y todo elemento de F es algebraico sobre $k(B)$, se sigue que KF es algebraico sobre K(B). Por la proposición 3.1.19., B contiene una base de trascendencia de KF sobre K. Por lo tanto $grtr(\mathrm{KF}:\mathrm{K})\le grtr(\mathrm{F}:k)$. Por la proposición 3.1.19., se tiene que

$$grtr(\mathrm{KF}:k)\le grtr(\mathrm{KF}:\mathrm{K})+grtr(\mathrm{K}:k).$$

Además, como $grtr(\mathrm{KF}:\mathrm{K})\le grtr(\mathrm{F}:k)$, se sigue que $grtr(\mathrm{KF}:k)\le grtr(\mathrm{K}:k)+grtr(\mathrm{F}:k)$. □

Sea F un campo y F[x] el anillo de polinomios en la indeterminada x con coeficientes en F. Si λ es una raíz de un polinomio $f\in\mathrm{F}[x]$, entonces $f=(x-\lambda)^m g$ para algún polinomio $g\in\mathrm{F}[x]$ con $g(\lambda)\neq 0$. m se denomina **multiplicidad** de λ en F y se dice que λ es una **raíz múltiple** si $m>1$ y **simple** si $m=1$. Un polinomio $f\in\mathrm{F}[x]$ es **separable** sobre F si todos los factores irreducibles de f sobre F tienen únicamente raíces simples. En particular, un polinomio irreducible es separable si sus raíces son simples. Sea K : F una extensión de

campos; un elemento $\alpha \in K$ algebraico sobre F es **separable** sobre F si α es una raíz simple de $Irr(\alpha, F)$. Una extensión $K:F$ es **separable** si ella es algebraica y todo elemento de K es separable sobre F. Sea A un anillo y $f \in A[x]$, $f(x)=a_0+a_1x+\cdots+a_nx^n$ un polinomio sobre A. El polinomio $f'=a_1+2a_2x+\cdots+na_nx^{n-1}$ se denomina **polinomio derivada** de f; su grado siempre es menor que el grado de f y f nunca divide a f'. El polinomio derivada satisface las siguientes propiedades

i) $(f+g)'=f'+g'$, *ii*) $(\alpha f)'=\alpha f'$, *iii*) $(fg)'=fg'+f'g$ y *iv*) $x'=1$, para $f, g \in A[x]$ y $\alpha \in A$.

PROPOSICIÓN 3.1.28. Sea $K:F$ una extensión de campos, $\alpha \in K$ un elemento algebraico sobre F y $f \in F[x]$ un polinomio no cero que tiene a α como una raíz. Entonces α es una raíz simple de f si y sólo si $f'(\alpha) \neq 0$.

DEMOSTRACIÓN ($\Rightarrow$)

Si α es una raíz simple del polinomio f, esto es, si $f=(x-\alpha)g$ con $g \in F[x]$ y $g(\alpha) \neq 0$, entonces se tiene que $f'=(x-\alpha)g'+g$ y $f'(\alpha)=(\alpha-\alpha)g'(\alpha)+g(\alpha)$. Luego $f'(\alpha) \neq 0$.

($\Leftarrow$)

Supóngase que α es una raíz de un polinomio f de multiplicidad $m>1$, $f=(x-\alpha)^m g$ con $g(\alpha) \neq 0$. Luego $f'=m(x-\alpha)^{m-1}g+(x-\alpha)^m g'$. Como $m-1>0$, se tiene que $f'(\alpha)=0$ lo cual es una contradicción. Por lo tanto $m=1$ y α es una raíz simple de f. □

PROPOSICIÓN 3.1.29. Sea F un campo y $f \in F[x]$ un polinomio de grado ≥ 1. Si la característica de F es cero, entonces $f'(x) \neq 0$.

DEMOSTRACIÓN

Sea $f(x)=a_0+a_1x+\cdots+a_nx^n$ con $a_n \neq 0$ y $n \geq 1$. Si $f'(x)=0$, entonces $na_n=0$; pero esto último no es posible ya que F es de característica cero. Por lo tanto $f'(x) \neq 0$. □

COROLARIO 3.1.30. Sea F un campo y $f \in F[x]$ un polinomio irreducible. Si la característica de F es cero, entonces f tiene solamente raíces simples.

DEMOSTRACIÓN

Como la característica del campo F es cero, se sigue de la proposición 3.1.29., que $f'(x) \neq 0$. También de 3.1.28., se obtiene que f tiene tiene todas sus raíces simples. □

Sea $K:F$ una extensión algebraica de campos con característica de F igual a cero, $\alpha \in K$ y $f=Irr(\alpha, F)$. Entonces de la proposición 3.1.29. se tiene que $f'(\alpha) \neq 0$ y del corolario 3.1.30., se sigue que α es una raíz simple de f. Por lo tanto α es separable sobre F. Así, se ha probado la siguiente

PROPOSICIÓN 3.1.31. Sea $K:F$ una extensión algebraica de campos con característica de F igual a cero, entonces $K:F$ es una extensión separable. □

PROPOSICIÓN 3.1.32. Toda extensión finita separable $K:F$ con F un campo infinito es simple.

DEMOSTRACIÓN

Sean β, γ elementos en el campo K, $f=Irr(\beta, F)$ que tiene raíces distintas $\beta=\beta_1, \beta_2, \ldots, \beta_n$ en $\overline{F}$ y $g=Irr(\gamma, F)$ que tiene raíces distintas $\gamma=\gamma_1, \gamma_2, \ldots, \gamma_m$ en $\overline{F}$, la cerradura algebraica de F, donde todas las raíces son simples ya que $K:F$ es una extensión separable. Como F es un campo infinito, se puede encontrar un elemento $a \in F$ con $a \neq (\beta_i-\beta)/(\gamma-\gamma_j)$ para toda $i \neq 1$ y $j \neq 1$; es decir, $a(\gamma-\gamma_j) \neq \beta_i-\beta$ y $\beta+a\gamma \neq \beta_i+a\gamma_j$ para toda $i \neq 1$ y $j \neq 1$. Haciendo $\alpha=\beta+a\gamma$, se tiene que $\alpha \neq \beta_i+a\gamma_j$ y $\alpha-a\gamma_j \neq \beta_i$ para toda $i \neq 1$ y $j \neq 1$. Sea $h(x)=f(\alpha-ax) \in F(\alpha)[x]$; como $h(\gamma)=f(\alpha-a\gamma)=f(\beta)=0$ y por construcción $h(\gamma_j) \neq 0$ para toda $j \neq 1$, se sigue que $h(x)$ y $g(x)$ tienen un factor común en $F(\alpha)[x]$ que es el polinomio $Irr(\gamma, F(\alpha))$. Como γ es la única raíz común de los polinomios $g(x)$ y $h(x)$, el polinomio $Irr(\gamma, F(\alpha))$ debe ser lineal. De esta forma, $\gamma \in F(\alpha)$ y $\beta=(\alpha-a\gamma) \in F(\alpha)$; por lo tanto $F(\beta, \gamma)=F(\alpha)$. Continuando con este proceso inductivamente, se obtiene el resultado. □

Como una consecuencia inmediata de las proposiciones 3.1.31. y 3.1.32., se obtiene el siguiente

COROLARIO 3.1.33. Toda extensión finita de un campo de característica cero es simple.□

Para campos finitos de característica *p*, la proposición 1.2.28. se sigue cumpliendo, esto es, si F es un campo finito, entonces toda extensión finita $K:F$ es separable.

3.2. CAMPOS CERRADOS REALES Y ÁLGEBRAS AFINES.

Se dice que $K:F$ es una **extensión real** si K y F son campos reales. Si K es un campo real y F es un subcampo de K, $K:F$ es una extensión real ya que todo subcampo de un campo real es real. Más generalmente si $K:F$ es una extensión de campos con K un campo real, entonces se sigue de la observación 1.2.17., que $K:F$ es una extensión real. En esta sección se retoma el concepto de extensión algebraica y se centra la atención en extensiones algebraicas de campos reales.

DEFINICIÓN 3.2.1. Un campo K es un **campo cerrado real** si

i) K es un campo real y

ii) ninguna extensión algebraica propia de K es real.

El siguiente resultado afirma que dado un campo real, siempre se puede encontrar un campo cerrado real que lo contiene, es decir,

PROPOSICIÓN 3.2.2. Dado un campo real K existe siempre una extensión algebraica $L:K$ con L un campo cerrado real

DEMOSTRACIÓN

Sea $\overline{K}$ una cerradura algebraica de K y considérese la familia $\Re$ de todos los subcampos reales de $\overline{K}$ que contienen a K. Como $K\in\Re$, $\Re\neq\varnothing$ y $(\Re, \subseteq)$ es un conjunto parcialmente ordenado. Sea $\Re'=\{K_\alpha\}$ un subconjunto no vacío totalmente ordenado de $\Re$. Se afirma que la unión $R=\cup K_\alpha$ con $K_\alpha\in\Re'$ es un campo real contenido en $\overline{K}$ y que contiene a K. Es claro que R es un campo; se probará que R es real. Supóngase que $-1=\sum_{i=1}^{n} a_i^2$ se cumple en R con $a_1,\ldots,a_n\in R$, entonces existen $K_{\alpha_1},\ldots,K_{\alpha_n}\subseteq R$ tal que $a_i\in K_{\alpha_1}$. Claramente uno de los campos en $\{K_{\alpha_1},\ldots,K_{\alpha_n}\}$ digamos K_{α_1} satisface que $a_1,\ldots,a_n\in K_{\alpha_1}$. Como $-1=\sum_{i=1}^{n} a_i^2$ se cumple en R y $K_{\alpha_1}\subseteq R$, entonces $-1=\sum_{i=1}^{n} a_i^2$ se cumple en K_{α_1} lo cual es una contradicción ya que K_{α_1} es un campo real. Así, R es un campo real que es una cota superior de $\Re'$. Por el lema de Zorn existe un elemento maximal L que es un campo real que contiene a K y está contenido en $\overline{K}$. Como ninguna extensión algebraica propia de L es real, se sigue que L es un campo cerrado real. □

Regresando a campos reales, se tiene

PROPOSICIÓN 3.2.3. Sea K un campo real. Entonces $K(\sqrt{a})$ es real si y sólo si $a\in T$ con T un orden en K.

DEMOSTRACIÓN $(\Rightarrow)$

Sea T' un orden en $K(\sqrt{a})$ que contiene a T, luego $a=(\sqrt{a})^2\in T'$ y $a\in T'\cap K=T$.

$(\Leftarrow)$

Supóngase que $K(\sqrt{a})$ no es real, es decir, existen elementos $b_i, c_i\in K$, $i=1, 2,\ldots, n$ no todos cero tal que $b_i+c_i\sqrt{a}\in K(\sqrt{a})$ y $\sum_{i=1}^{n}(b_i+c_i\sqrt{a})^2=0$. Entonces $\sum_{i=1}^{n} b_i^2+2\sum_{i=1}^{n} b_i c_i\sqrt{a}+\sum_{i=1}^{n} c_i^2 a=0$. Como $\sqrt{a}$ es de grado 2 sobre K, se sigue que $\sum_{i=1}^{n} b_i c_i\sqrt{a}=0$ y $\sum_{i=1}^{n} b_i^2+a\sum_{i=1}^{n} c_i^2=0$, esto es, $a=-(\sum_{i=1}^{n} b_i^2/\sum_{i=1}^{n} c_i^2)$. Por lo tanto $a\notin T$ lo cual es una contradicción. □

La proposición anterior también se puede escribir como: Sea K un campo real, entonces para cualquier elemento $a\in K$ se tiene que $K(\sqrt{a})$ es real o $K(\sqrt{-a})$ es real. Obviamente, si a es una suma de cuadrados, $K(\sqrt{a})$ es real.

Se ve que $\sum\mathbb{Q}^2 \neq \mathbb{Q}^2$ con $\mathbb{Q}$ el campo de los números racionales. †) Pero si K es un campo cerrado real, entonces $\sum K^2 = K^2$. En efecto, sea $a \in \sum K^2 \subseteq T$, T orden en K. Por 3.2.3., $K(\sqrt{a})$ es un campo real y como K es cerrado real, se sigue que $K = K(\sqrt{a})$, es decir, $\sqrt{a} \in K$ y $a \in K^2$.

COROLARIO 3.2.4. Sea K un campo cerrado real y $a \in K$, entonces existe $b \in K$ tal que $a = b^2$ o $a = -b^2$

DEMOSTRACIÓN

Para cada elemento $a \in K$, por 3.2.3., se tiene que $K(\sqrt{a})$ es real o $K(\sqrt{-a})$ es real. Dado que K es cerrado real, $K = K(\sqrt{a})$ o $K = K(\sqrt{-a})$ es real, esto es, existe $b \in K$ tal que $a = b^2$ o $a = -b^2$. □

COROLARIO 3.2.5. Si K es un campo cerrado real, entonces K tiene un único orden.

DEMOSTRACIÓN

Como K es un campo real, $T = \sum K^2$ es un preorden en K. Por la observación hecha después de la proposición 3.2.3., se sabe que $\sum K^2 = K^2$ y por el corolario 3.2.4., se tiene que $K^2 \cup -K^2 = K$. Luego $T = K^2$ es un orden en K y el resultado se sigue de 2.1.19.. □

Sea $K : F$ una extensión de campos y T un orden en F. Se dice que un orden T' en K **contiene** o **extiende** T a K o T es la **restricción** de T' a F, si $T' \cap F = T$.

LEMA 3.2.6. Sea $K : F$ una extensión de campos con F un campo real y T un orden de F. Entonces K es un campo real si y sólo si $\sum_{i=1}^{n} a_i x_i^2 = 0$, con $a_1, \ldots, a_n \in T \setminus \{0\}$ y $x_1, \ldots, x_n \in K$, implica $x_i = 0$, $i = 1, \ldots, n$.

DEMOSTRACIÓN ($\Rightarrow$)

Dado que $a_i \in T \setminus \{0\}$, para $i = 1, \ldots, n$, entonces existen elementos $b_i \in K$, $i = 1, \ldots, n$ tal que $a_i = b_i^2$. Luego $\sum_{i=1}^{n} a_i x_i^2 = 0$ es equivalente a $\sum_{i=1}^{n} (b_i x_i)^2 = 0$. Como K es real, $b_i x_i = 0$ para cada $i = 1, \ldots, n$ y dado que $a_i \in T \setminus \{0\}$, se sigue que $x_i = 0$, para toda $i = 1, \ldots, n$.

($\Leftarrow$)

Sea $T_0 = \{ \sum_{i=1}^{n} a_i v_i^2 \mid a_1, \ldots, a_n \in T \setminus \{0\}$ y $v_1, \ldots, v_n \in K \}$. Claramente T_0 es un preorden en K que está contenido en un orden T' en K, es decir, existe un orden T' en K que contiene a T_0. Como $T' \cap F$ es un orden en F y $T \subseteq T' \cap F$, del lema 2.1.18., se sigue que $T' \cap F = T$, esto es, T' contiene a T. Por lo tanto K es un campo real. □

---

†) Se tiene que $\mathbb{Q}^2 \subsetneq \sum\mathbb{Q}^2$; pero la contención recíproca no es cierta en general.

Se dice que un campo K es **cuadráticamente cerrado** si todo elemento en K es un cuadrado o equivalentemente si para cada $a\in$K, $\sqrt{a}$ o $\sqrt{-a}$ está en K.

LEMA 3.2.7. Sea K un campo cerrado real. Entonces K(i) es cuadráticamente cerrado.[†)]

DEMOSTRACIÓN

Sea $x\in$K(i), entonces existen elementos a, $b\in$K tal que $x=a+bi$. Si $b=0$, $x=a$ y por 3.2.4., se tiene que a es un cuadrado o el inverso aditivo de un cuadrado. De esto se sigue que x es un cuadrado en K(i). Si $b\neq 0$, se tendrá que encontrar elementos u, $v\in$K tal que $a+bi=(u+vi)^2$; es decir, $a=u^2-v^2$, $b=2uv$. Sustituyendo v en las igualdades anteriores y haciendo $y=u^2$, se tiene $y^2-ay-(b^2/4)=0$ y $y=(a+\sqrt{a^2+b^2})/2$, con $a^2+b^2>0$ y $\sqrt{a^2+b^2}$ la raíz cuadrada positiva de a^2+b^2 en K. Se afirma que $y\in$T$\setminus\{0\}$, es decir, $a+\sqrt{a^2+b^2}\in$T$\setminus\{0\}$, ya que en caso contrario (esto es, $a+\sqrt{a^2+b^2}\in$-T) se tendría que $a-\sqrt{a^2+b^2}\in$-T (ya que $\sqrt{a^2+b^2}\notin$-T y $a\notin$T), de esta forma $a^2-(a^2+b^2)\in$T, es decir, $-b^2\in$T. Así, $b=0$, esto es, $b\in$T$\cap$-T lo cual contradice la elección de b. De esta forma quedan determinadas u y v. □

PROPOSICIÓN 3.2.8. Sea K un campo cerrado real. Entonces K(i) es algebraicamente cerrado y los polinomios irreducibles en K[x] tienen grado ≤ 2.

DEMOSTRACIÓN

Sea L : K(i) una extensión finita de K(i); se tiene que probar que L=K(i). Sin pérdida de generalidad se puede suponer que L : K es una extensión de Galois con grupo G.[‡)] Sea $[L:K]=2^r m$, con $m\in\mathbb{Z}$ un número impar, entonces por el teorema fundamental de Galois, el subgrupo de Sylow de orden 2^r de G le corresponde un campo de extensión L′ de K de grado un número natural m impar; esto significa que L′ es real y por tanto $m=1$. Así, L : K es una extensión de Galois de grado 2^r y L : K(i) es una extensión de Galois de grado 2^s. Aplicando la correspondencia de Galois a la extensión de campos L : K(i), donde su grupo de Galois es un 2-grupo, se sigue que $s=0$, ya que si $s\geq 1$ y aplicando la correspondencia de Galois a la extensión, existiría una extensión cuadrática de K(i) lo cual contradice el hecho de que K(i) es algebraicamente cerrado; luego L=K(i). Finalmente, como K(i) es algebraicamente cerrado se concluye que los polinomios irreducibles en el campo K tienen grado ≤ 2. □

El hablar de un concepto análogo a la cerradura algebraica en el caso de campos reales conduce a la siguiente

DEFINICIÓN 3.2.9. Sea K un campo real y T un orden en K. Una **cerradura real** de K es un campo $\widetilde{K}$ que satisface:

i) $\widetilde{K}$ es cerrado real.

ii) $\widetilde{K}$: K es algebraica.

[†)] $i=\sqrt{-1}$.

[‡)] Aquí se toma la menor extensión de Galois de K que contiene a L.

iii) el único orden $\widetilde{T}$ de $\widetilde{K}$ es una extensión del orden dado en K, es decir, $T=\widetilde{T}\cap K$.

El siguiente resultado asegura que para cada campo real, siempre existe una cerradura real, es decir,

PROPOSICIÓN 3.2.10. Sea K un campo real. Entonces existe una cerradura real $\widetilde{K}$ de K.

DEMOSTRACIÓN

Considérese la familia $\Re=\{K_\alpha\}$ de campos reales que contiene a K tal que $K_\alpha : K$ es una extensión algebraica para cada índice α. Sea T un orden de K y T_α un orden de K_α que contiene a T. Claramente $\Re\neq\varnothing$ y $(\Re\ ,\subseteq)$ es un conjunto parcialmente ordenado. Sea $\Re'$ un subconjunto no vacío totalmente ordenado de $\Re$. La unión $R=\cup_\alpha K_\alpha$ con $K_\alpha\in\Re'$ es un campo real que contiene a K. Como $T_\alpha\cap K=T$, para toda α, se tiene que $\cup(T_\alpha\cap K)=T$ es equivalente a $(\cup T_\alpha)\cap K=T$. Esto significa que $\cup T_\alpha$ para toda α es un orden de R. En efecto, sean $x, y\in\cup T_\alpha$, entonces existen al menos ordenes T_{α_1} y T_{α_2} donde $T_{\alpha_1}\subsetneq T_{\alpha_2}$ o $T_{\alpha_2}\subsetneq T_{\alpha_1}$ con $x\in T_{\alpha_1}$ y $y\in T_{\alpha_2}$. Como $T_{\alpha_1}\subseteq T_{\alpha_2}$ o $T_{\alpha_2}\subseteq T_{\alpha_1}$, se tiene que $x, y\in T_{\alpha_1}$ o $x, y\in T_{\alpha_2}$ y $x+y\in T_{\alpha_1}$ o $x+y\in T_{\alpha_2}$. También $xy\in T_{\alpha_1}$ o $xy\in T_{\alpha_2}$. Así, $\cup T_\alpha+\cup T_\alpha\subseteq\cup T_\alpha$ y $\cup T_\alpha\cup T_\alpha\subseteq\cup T_\alpha$. Sea $x\in R$, entonces existe al menos un K_{α_j} tal que $x\in K_{\alpha_j}^2\subseteq T_{\alpha_j}\subseteq\cup T_\alpha$. También $-1\notin\cup T_\alpha$ ya que en caso contrario se tendría que $-1\in K_{\alpha_0}$ para alguna α_0 ¡contradicción! Finalmente, si $x\in R$, con $x\in T_{\alpha_0}=T_{\alpha_0}\cup -T_{\alpha_0}$ para alguna α_0; esto último significa que $x\in T_{\alpha_0}$ o $x\in -T_{\alpha_0}$, es decir, $x\in\cup T_\alpha$ o $x\in -\cup T_\alpha$. Luego $(\cup T_\alpha)\cup(-\cup T_\alpha)=R$ y $\cup T_\alpha$ es un orden en R. Sea $x\in R=\cup T_\alpha$ entonces $x\in T_{\alpha_0}$ para al menos un orden T_{α_0}. Como $K_{\alpha_0} : K$ es algebraica, se tiene que el elemento x es algebraico sobre K. Luego $R : K$ es algebraica. R es una cota superior de $\Re'$ y por el lema de Zorn existe al menos un elemento maximal $\widetilde{K}$. El campo $\widetilde{K}$ es un campo real que contiene a K con orden $\widetilde{T}$; $\widetilde{T}\cap K=T$ y $\widetilde{K} : K$ es una extensión algebraica. Por la maximalidad, $\widetilde{K}$ satisface que es un campo real y ninguna extensión algebraica de $\widetilde{K}$ es real, esto es, $\widetilde{K}$ es cerrado real. Por 3.2.5., $\widetilde{K}$ tiene un único orden $\widetilde{T}$ y este orden es una extensión del orden dado en K, esto es, $\widetilde{T}\cap K=T$. □

Dado un campo real K, la cerradura algebraica $\widetilde{K}$ de K es única salvo isomorfismos sobre K. La demostración de esta afirmación se dará en la siguiente sección.[†)]

Sea K un campo. Por una **K-álgebra** B se entiende un espacio vectorial sobre K junto con una operación binaria de multiplicación $\cdot: B\times B\to B$ que satisface:

i) $(au)v=a(uv)=u(av)$, $a\in K$, $u, v\in B$.

ii) $(u+v)w=uw+vw$, $u, v, w\in B$.

iii) $u(v+w)=uv+uw$, $u, v, w\in B$.

[†)] ver corolario 3.3.21.

Una K-álgebra B es asociativa si
iv) $u(vw)=(uv)w$ para cada $u, v, w\in B$.

y conmutativa si
v) $uv=uv$ para toda $u, v\in B$.

Sea B una K-álgebra, $B_1\subseteq B$ es una **K-subálgebra** de B si B_1 es un subespacio vectorial que satisface: si $u, v\in B_1$, entonces $uv\in B_1$. B_1 hereda la estructura de álgebra de B. También, las subálgebras de un álgebra asociativa o un álgebra conmutativa son subálgebras asociativas o conmutativas.

Si B_1 y B_2 son K-álgebras, la función lineal (homomorfismo de espacios vectoriales) $\varphi:B_1 \to B_2$ es un **homomorfismo de K-álgebras** si $\varphi(uv)=\varphi(u)\varphi(v)$.

Si B es una K-álgebra y como espacio vectorial tiene dimensión finita, entonces se dirá que B es una **K-álgebra finita**.

Si Γ es un subconjunto de una K-álgebra B, se define la K-subálgebra A de B generada por Γ como la intersección no vacía de la familia de todas las subálgebras de B que contienen a Γ (la intersección de cualquier familia no vacía de K-subálgebras del álgebra B es una K-subálgebra de B). Esta K-subálgebra es denotada por $K[\Gamma]$ y es la menor K-subálgebra de B que contiene a Γ en el sentido de que $K[\Gamma]$ está contenida en cualquier otra K-subálgebra de B que contiene a Γ. Se dice que una K-subálgebra A de B es **finitamente generada** si existen elementos $b_1,\ldots, b_n\in B$ tal que $A=K[b_1,\ldots,b_n]$. De particular interés se tienen las K-álgebras finitamente generadas que son conmutativas, es decir,

DEFINICIÓN 3.2.11. Sea K un campo. Un **álgebra afín** A es una K-álgebra conmutativa finitamente generada.

El siguiente resultado afirma que las álgebras afines son imágenes homomorfas de anillos de polinomios.

PROPOSICIÓN 3.2.12. Sea K un campo. B es un álgebra afín si y sólo si existe un homomorfismo suprayectivo $\varphi:K[x_1,\ldots,x_n]\to\to B$ para alguna $n\in\mathbb{N}$.

DEMOSTRACIÓN ($\Rightarrow$)

Si B es un álgebra afín, entonces existen n elementos $b_1,\ldots,b_n\in B$ tal que $B=K[b_1,\ldots,b_n]$. La función $x_i \mapsto b_i$ para $i=1,\ldots,n$ se extiende en forma única a un homomorfismo suprayectivo de K-álgebras

$$\varphi:K[x_1,\ldots,x_n] \to K[b_1,\ldots,b_n]$$
$$\sum a_{i_1\ldots i_n} x_1^{i_1}\ldots x_1^{i_n} \mapsto \sum a_{i_1\ldots i_n} b_1^{i_1}\ldots b_n^{i_n}.$$

donde $(i_1,\ldots,i_n)\in(\mathbb{N}\cup\{0\})^n$.

($\Leftarrow$)

Sea $\varphi(K[x_1,\ldots,x_n])$; como φ es suprayectivo, se tiene que $\varphi(K[x_1,\ldots,x_n])=B$ y 0

$$\varphi(K[x_1,\ldots,x_n])=K[\varphi(x_1),\ldots,\varphi(x_n)]=K[b_1,\ldots,b_n]$$

con $b_1,\ldots,b_n\in B$. Así, existen elementos $b_i\in B$ $i=1,\ldots,n$ tal que $B=K[b_1,\ldots,b_n]$, es decir, B es una K-álgebra conmutativa finitamente generada. □

Asociados a las álgebras afines se tienen los campos de funciones que son campos de cocientes de ciertos dominios *k*-afines, es decir,

DEFINICIÓN 3.2.13. Un campo de extensión K de un campo F es un **campo de funciones** en *n* indeterminadas si existen elementos $t_1,\ldots,t_n\in K$ trascendentes sobre F tal que

1°.- $grtr(K:F)=n$.
2°.- $K:F(t_1,\ldots,t_n)$ es una extensión finita.
3°.- K es algebraicamente cerrado sobre F.[†)]

Así, para un dominio entero *k*-afín $A=k[a_1,\ldots,a_n]$ y para ciertos elementos $a_1,\ldots,a_n\in k$, el campo de cocientes $F=qf(A)$ es un campo de funciones sobre un cierto campo base *k*.

Sea *k* un campo y $k[x_1,\ldots,x_n]$ el anillo de polinomios en *n* indeterminadas con coeficientes en *k*. Si $g\in k[x_1,\ldots,x_n]$ es un polinomio irreducible y se considera el dominio entero $k[x_1,\ldots,x_n]/\langle g\rangle$, entonces el campo de funciones es el campo de cocientes del dominio entero $k[x_1,\ldots,x_n]/\langle g\rangle$ que se escribe $k(g)$, es decir,

$$k(g)=qf(k[x_1,\ldots,x_n]/\langle g\rangle).$$

Si $\pi:k[x_1,\ldots,x_n]\to k[x_1,\ldots,x_n]/\langle g\rangle$; $h\mapsto \overline{h}$ es la proyección canónica donde $\pi(x_i)=\overline{x}_i$, entonces $k(g)=k(\overline{x}_1,\ldots,\overline{x}_n)$ o $k(g)=k(\pi(x_1),\ldots,\pi(x_n))$ es el campo de cocientes de $k(g)=k[\overline{x}_1,\ldots,\overline{x}_n]$.

3.3. LA TEORÍA DE ARTIN-LANG.

Se empieza esta sección estableciendo algunos conceptos y resultados necesarios de la teoría de formas cuadráticas que serán utilizados aquí. Se recuerda que una **forma cuadrática** de grado *n* sobre un campo F es un polinomio homogéneo de grado 2 en las indeterminadas $x_1,\ldots,x_n$ con coeficientes en F, es decir, $f(x_1,\ldots,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n}b_{ij}x_ix_j$ con $a_{ij}\in F$, o más simétricamente como $f(x_1,\ldots,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n}b_{ij}x_ix_j$ donde $b_{ij}=(1/2)(a_{ij}+a_{ji})$. Dada una forma cuadrática *f* de grado *n* sobre un campo F o más brevemente una F-forma *f* de

[†)] También se dice que F no tiene extensiones algebraicas propias.

grado n, se puede asociar a f una matriz simétrica escrita como M_f $(=(b_{ij}))$ con entradas en F. Si X es una matriz columna; en notación matricial la F-forma f puede escribirse como $f(\mathrm{X}) = \mathrm{X}^t M_f \mathrm{X}$, donde X^t es la transpuesta de la matriz X. Dos F-formas f y g de grado n son **equivalentes** (escrito $f \sim g$) si existe una matriz invertible A $n \times n$ con entradas en F tal que $g(\mathrm{AX})=f(\mathrm{X})$; esta relación es de equivalencia. Se observa que f es equivalente a g si y sólo si $M_f = \mathrm{A}^t M_g \mathrm{A}$; esto se sigue de

$$g(\mathrm{AX})=(\mathrm{AX})^t M_g(\mathrm{AX})=\mathrm{X}^t(\mathrm{A}^t M_g \mathrm{A})\mathrm{X}=\mathrm{X}^t M_f \mathrm{X}=f(\mathrm{X}).$$

Una F-forma f de grado n es **isótropa** si existe un elemento $(x_1,\ldots,x_n)$ en F^n no cero tal que $f(x_1,\ldots,x_n)=0$.[†)] En otro caso se dice que f es **anisótropa** sobre F.

Sea V un espacio vectorial de dimensión finita sobre un campo F. Una función $B:\mathrm{V}\times\mathrm{V}\to\mathrm{F}$ es **bilineal** si satisface

i) $B(x_1+x_2, y)=B(x_1, y)+B(x_2, y)$ y $B(x, y_1+y_2)=B(x, y_1)+B(x, y_2)$ para cada $x, x_1, x_2, y, y_1, y_2 \in \mathrm{V}$.

ii) $B(ax, y)=B(x, ay)=aB(x, y)$ para toda $a\in\mathrm{F}$, $x, y\in\mathrm{V}$.

Si además

iii). $B(x, y)=B(y, x)$ para toda $x, y\in\mathrm{V}$.

se dice que B es una forma **bilineal simétrica** sobre V.

Toda forma bilineal simétrica B de grado n sobre un espacio vectorial V satisface la igualdad

$$B(x+y, x+y)=B(x, x)+B(y, y)+2B(x, y)$$

para cada $x, y\in\mathrm{V}$. Si F es un campo de característica distinta de 2, se tiene

$$B(x, y)=(1/2)[B(x+y, x+y)-B(x, x)-B(y, y)]$$

para toda $x, y\in\mathrm{V}$. Esta igualdad se denomina **identidad polar**.

Sea V un espacio vectorial de dimensión finita sobre un campo F. Una función $q:\mathrm{V}\to\mathrm{F}$ es una **función cuadrática** si

i) $q(ax)=a^2 q(x)$ para cada $a\in\mathrm{F}$ y $x\in\mathrm{V}$.

ii) la función de $\mathrm{V}\times\mathrm{V}$ a F, $(x, y) \mapsto q(x+y)-q(x)-q(y)$ es bilineal.

Se observa que si la característica del campo F es distinta de 2, toda función cuadrática $q:\mathrm{V}\to\mathrm{F}$ define una forma bilineal simétrica $B:\mathrm{V}\mathrm{x}\mathrm{V}\to\mathrm{F}$ dada como

---

[†)] A tal vector $(x_1,\ldots, x_n)\in\mathrm{F}^n$ se le denomina **vector isótropo**.

$$B(x, y)=(1/2)[q(x+y)-q(x)-q(y)].$$

Dado que $B(x, x)=(1/2)[q(2x)-2q(x)]=(1/2)[4q(x)-2q(x)]=q(x)$, toda función bilineal simétrica B:VxV→F define una función cuadrática q:V→F; $q(x)=B(x , x)$. Así, para un campo de característica distinta de 2, toda forma bilineal simétrica B sobre un espacio vectorial de dimensión finita define en forma única una función cuadrática q:V→F y recíprocamente, toda función cuadrática define una forma bilineal simétrica de manera única. Un **espacio cuadrático** es un espacio vectorial V de dimensión finita sobre un campo F de característica distinta de 2, junto con una función cuadrática q:V→F. Este espacio cuadrático es denotado como (V , q) o (V , B), donde B es la forma bilineal correspondiente a la función cuadrática q. Dada una base $\{e_1,\ldots,e_n\}$ en un espacio cuadrático (V , B), si $B(e_i , e_j)=b_{ij}$ con $b_{ij}\in$F son las entradas de la matriz de B relativa a la base $\{e_1,\ldots, e_n\}$, entonces

$$q(x) = B(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} x_j e_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij} x_i x_j$$

Se observa que la matriz (b_{ij}) define una forma cuadrática $f(x_1,\ldots,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij} x_i x_j$

Sea (V , B) un espacio cuadrático sobre un campo F y x, y elementos en V. Se dice que x es **ortogonal** a y si $B(x , y)=0$. El conjunto $U^{\perp}=\{y\in V \mid B(x , y)=0$ para toda $x\in U\}$ donde U es un subespacio vectorial de V, se denomina **complemente ortogonal** de U. $U^{\perp}$ es un subespacio vectorial de V. El complemento ortogonal de V, $V^{\perp}$, se denomina **radical** de V y se escribe $V^{\perp}=rad(V)$. Un espacio cuadrático (V , B) es **regular** si el vector cero en V es el único vector ortogonal a todo vector en V, es decir, si $rad(V)=\{0\}$.

Se observa que si V se puede escribir como $V=rad(V)\oplus U$, donde (U , B_U) es un subespacio cuadrático con B_U la restricción de B a U, entonces el subespacio U es regular ya que si $x\in U$ satisface que $B_U(x, u)=0$ para todo $u\in U$, se sigue que todo elemento $y\in V$ se puede escribir como $y=u+v$ con $v\in rad(V)$ y $u\in U$. Así, se tiene que

$$B(x, y)=B(x, v+u)=B(x , v)+B(x , u)=B(x , v)+B_U(x , u)=0,$$

luego entonces $x\in rad(V)\cap U=\{0\}$.

PROPOSICIÓN 3.3.1. Todo espacio cuadrático (V , B) admite una base ortogonal.[†)]

DEMOSTRACIÓN

Por la observación anterior será suficiente probar la proposición en el caso en que V es regular ya que una base ortogonal para U se puede completar con una base de $rad(V)$. La demostración se hará por inducción sobre la dimensión del espacio V.

Si $dim(V)=0$, se sigue el resultado. Supóngase que la proposición es cierta para todo espacio regular de dimensión n y sea $dim(V)=n+1$. Si $v\in V$ es tal que $B(v , v)\neq 0$ [‡)], entonces $V=\langle v\rangle\oplus\langle v\rangle^{\perp}$. Aplicando la hipótesis inductiva a $\langle v\rangle^{\perp}$, se tiene una base para este subespacio que completada con v proporciona una base ortogonal para V. Si $w\in\langle v\rangle^{\perp}$ y

[†)] Una base es ortogonal si sus elementos son ortogonales por parejas.

[‡)] Tal vector existe por la regularidad y por la identidad polar.

además $B(w\ ,\ w')=0$ para todo $w'\in\langle v\rangle^{\perp}$, entonces para cada $v\in V$, $B(w\ ,\ v)=0$, y así, $w=0$. De esta forma $\langle v\rangle^{\perp}$ es regular y $\langle v\rangle\cap\langle v\rangle^{\perp}=0$ lo que significa que $\langle v\rangle\oplus\langle v\rangle^{\perp}=V$. □

Se observa que para un espacio cuadrático $(V\ ,\ B)$, la proposición anterior asegura que se puede construir una base ortogonal que incluya a un vector no isótropo de V.

Sea f una forma cuadrática de grado n sobre un campo F y $a_1\in F\setminus\{0\}$ un elemento que satisface $f(x_1,\ldots,x_n)=a_1$ con $x_1,\ldots,x_n\in F$, entonces para cada espacio cuadrático $(V\ ,\ B)$ sobre el campo F correspondiente a la clase de equivalencia $[f\ ]$ de f, existe un vector $v\in V$ con $B(v\ ,\ v)=a_1$. Por la observación anterior, existe una base ortogonal $\{v_1,\ldots,v_n\}$ de V con $v=v_1$ que define la forma f_B con matriz asociada $(B(v_i\ ,\ v_j))_{ij}$ y $f\sim f_B$. De esta forma, f es equivalente a una forma cuadrática cuya matriz diagonal es

$$M_f=\begin{bmatrix} a_1 & & & & & 0 \\ & a_2 & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & a_{n-1} & \\ 0 & & & & & a_n \end{bmatrix}$$

donde $a_2=B(v_2\ ,\ v_2),\ldots,a_n=B(v_n\ ,\ v_n)$. En este caso se escribe $f\sim\langle a_1,\ldots,a_n\rangle$. Se dice que $\langle a_1,\ldots,a_n\rangle$ es la representación diagonal de la forma f. Como polinomio, la representación diagonal $\langle a_1,\ldots,a_n\rangle$ se escribe como $a_1x_1^2+\cdots+a_nx_n^2$.

Sean $(V_1\ ,\ B_1)$ y $(V_2\ ,\ B_2)$ espacios cuadráticos de dimensiones n y m respectivamente sobre un campo F. Se define el espacio cuadrático **suma ortogonal** de los espacios $(V_1\ ,\ B_1)$ y $(V_2\ ,\ B_2)$ escrito $V_1\perp V_2$ como el espacio $(V\ ,\ B)$ que satisface $V=V_1\oplus V_2$ y $B:V\times V\to F$, $B((x_1\ ,\ x_2),\ (y_1\ ,\ y_2))=B_1(x_1\ ,\ y_1)+B_2(x_2\ ,\ y_2)$. B así definida es bilineal y $B\,|\,V_1\times V_1=B_1$, $B\,|\,V_2\times V_2=B_2$.

Se dice que dos espacios cuadráticos $(V_1\ ,\ B_1)$, $(V_2\ ,\ B_2)$ sobre un campo F son **isométricos,** escrito $V_1\approx V_2$ si existe un isomorfismo lineal $\varphi:V_1\to V_2$ tal que $B_2(\varphi(x),\varphi(x))=B_1(x,\ y)$ para cada $x,\ y\in V$. La isometría de espacios cuadráticos es una relación de equivalencia.

Sean f y g formas de grado n sobre un campo F, $(F^n,\ B_f\ )$, $(F^n,\ B_g\ )$ espacios cuadráticos, donde F^n es el espacio vectorial sobre F de las n-adas de elementos de F y

$$B_f:F^n\times F^n\to F,\ B_f(e_i\ ,\ e_j)=b_{ij},$$
$$B_g:F^n\times F^n\to F,\ B_g(e_i\ ,\ e_j)=b_{ij}'.$$

donde $M_f=(b_{ij})$, $M_g=(b_{ij}')$ y $\{e_1,\ldots,e_n\}$ la base canónica de F^n. Si las formas f y g son equivalentes, entonces los espacios cuadráticos $(F^n,\ B_f\ )$ y $(F^n,\ B_g\ )$ son isométricos. En efecto, como f y g son equivalentes existe una matriz invertible A tal que $g(AX)=f(X)$. Sea $\varphi:F^n\to F^n$, $\varphi(X)=AX$, entonces

$$B_g(\varphi(X)\ ,\ \varphi(Y))=B_g(AX\ ,\ AY)=(AY)^tM_g(AX)=Y^t(A^tM_gA)X=Y^tM_fX=B_f(X\ ,\ Y).$$

Si f y g son dos formas de grados n y m respectivamente sobre un campo F, $f \perp g$ denota la forma sobre F correspondiente a la clase de isometría del espacio suma ortogonal de (F^n, B_f) y (F^m, B_g).

PROPOSICIÓN 3.3.2. Sea (V , B) un espacio cuadrático sobre un campo F y U un subespacio regular de V, entonces $V=U\perp U^{\perp}$.

DEMOSTRACIÓN

Como $U\cap U^{\perp}=\{0\}$, es decir, $U\cap U^{\perp}=rad(U)$ bastará probar que $U+U^{\perp}=V$. Sea $\{v_1,\ldots, v_n\}$ una base ortogonal de U. Como U es un subespacio regular, $B(v_i , v_i)\neq 0$. De esta forma, para cualquier $x\in V$, si se escribe $y=x-\sum(B(x , v_i)/B(v_i , v_i))v_i$, se tiene que $B(y , v_j)=0$ para $j=1,\ldots,k$. Entonces $B(y , u)=0$ para todo $u\in U$ y $U+U^{\perp}=V$. □

Como una consecuencia de la proposición anterior se tiene el

COROLARIO 3.3.3. Sea (V , B) un espacio cuadrático sobre un campo F y U un subespacio regular de V. Si $V=U\perp W$, entonces $W=U^{\perp}$.

DEMOSTRACIÓN

De 3.3.2., se sigue que $V=U\perp U^{\perp}$, es decir, $V=U\oplus U^{\perp}$, entonces $dim(V)=dim(U)+dim(U^{\perp})$. Como $V=U\perp W$, se tiene que $W\subseteq U^{\perp}$, luego $W=U^{\perp}$. □

La forma cuadrática <1,-1> que bajo isometría corresponde al polinomio $f(x,y)=x^2-y^2$, es claramente isótropa sobre cualquier campo F. El espacio cuadrático correspondiente a esta forma se denomina **plano hiperbólico** sobre F y es denotado por H. Un **espacio hiperbólico** es un espacio cuadrático que es suma ortogonal de planos hiperbólicos.

Sean f y g F-formas de grados m y n respectivamente y supóngase que $f\sim<a_1,\ldots,a_m>$ y $g\sim<b_1,\ldots,b_n>$. Se define el **producto tensorial** de f y g como la mn-forma diagonal

$$f\otimes g=<a_1b_1,\ldots,a_1b_n, a_2b_1,\ldots,a_2b_n,\ldots,a_mb_1,\ldots,a_mb_n>$$

Se observa que el producto tensorial de F-formas es asociativo, conmutativo y distributivo respecto a la suma ortogonal de formas diagonales. También posee un elemento identidad que es la forma <1>.

Sean (V_1 , B_1), (V_2 , B_2) dos espacios cuadráticos de dimensiones m y n respectivamente. El espacio cuadrático (V , B), donde $V=V_1\otimes V_2$ y $B:V\times V\to F$ es la única forma bilineal simétrica que satisface

$$B(x_1\otimes y_1 , x_2\otimes y_2)=B_1(x_1 , y_1)\cdot B_2(x_2 , y_2)$$

y se denomina producto tensorial de los espacios V_1 y V_2.

Ahora, considérese una extensión de campos $K:F$; se verá a continuación que toda F-forma cuadrática f es una K-forma, pero en general se tendrá que las propiedades de f como una F-forma serán distintas a las propiedades de f como una K-forma.[†)] Por ejemplo las propiedades de anisotropía e isotropía no se preservan.

LEMA 3.3.4. Sea $K:F$ una extensión de campos, (V , B) un F-espacio cuadrático y (V_K , B_K) el espacio donde $V_K=K\otimes_F V$ se considera con su estructura de K-espacio vectorial y $B_K:V_K\times V_K\to K$ se define como $B_K(a\otimes u , b\otimes v)=abB(u , v)$, $a, b\in K$, $u, v\in V$. Entonces (V_K , B_K) es un K-espacio cuadrático. También, si f es una F-forma cuadrática en (V , B), f será una K-forma cuadrática en (V_K , B_K).

DEMOSTRACIÓN

Claramente B_K es una forma bilineal simétrica sobre K. Por otro lado, si $\{v_1,\ldots,v_n\}$ es una base de V sobre F ortogonal relativa a B y $a(b\otimes v)=ab\otimes v$ es la acción de K sobre V_K, entonces $\{1\otimes v_1,\ldots,1\otimes v_n\}$ es una base ortogonal sobre K de V_K. De esta forma, la matriz $(B_K(1\otimes v_i , 1\otimes v_j))_{ij}$ relativa a B_K es precisamente la matriz que define a la forma f como una K-forma. □

Sea $K:F$ una extensión finita de campos, (es decir, K es una F-álgebra de dimensión finita), $x\in K$ un elemento arbitrario y $T_x:K\to K$; $T_x(\alpha)=x\alpha$ para cada $\alpha\in K$ una transformación del espacio vectorial K. Se define la **traza** de la transformación T_x escrita $tr_{K:F}(T_x)$ como la traza de la matriz asociada a T_x en cualquier base de K. Sea $K:F$ una extensión finita de campos; la función $T_{K:F}:K\to F$, $x\mapsto tr_{K:F}(T_x)$ se denomina **función traza** de K. Si $K:F$ es una extensión finita separable, entonces $T_{K:F}(x)=\sigma_1(x)+\cdots+\sigma_n(x)$ para cada $x\in K$, donde $\sigma_1(x),\ldots,\sigma_n(x)$ son los F-homomorfismos de K en su cerradura algebraica $\overline{K}$.

PROPOSICIÓN 3.3.5. Sea $K:F$ una extensión de campos y $\varphi_1,\ldots,\varphi_n$ n monomorfismos diferentes de K en F. Si $a_1\varphi_1(x)+\cdots+a_n\varphi_n(x)=0$ para todo elemento $x\in K$ y $a_i\in F$, entonces $a_1=\cdots=a_n=0$.

DEMOSTRACIÓN (se hace por inducción sobre n).

Si $n=1$, $a_1\varphi_1(x)=0$ para toda $x\in K$, en particular $a_1\varphi_1(1)=0$, luego $a_1=0$. Supóngase que $n>1$ y que la proposición es valida para n-1 monomorfismos y también que $a_1\varphi_1(x)+\cdots+a_n\varphi_n(x)=0$ con todas las $a_i\neq 0$. Luego existe $c\in K$ tal que $\varphi_1(c)\neq\varphi_n(c)$. De $a_1\varphi_1(x)+\cdots+a_n\varphi_n(x)=0$ se tiene que $a_1\varphi_1(cx)+\cdots+a_n\varphi_n(cx)=0$, esto es, $a_1\varphi_1(c)\varphi_1(x)+\cdots+a_n\varphi_n(c)\varphi_n(x)=0$. Multiplicando esta última expresión por $\varphi_n(c^{-1})$ y restándole la expresión $(a_1\varphi_1(x)+\cdots+a_n\varphi_n(x))=0$ se obtiene

$$a_1[(\varphi_n(c^{-1})\varphi_1(c)-1]\varphi_1(x)+\cdots+a_n[(\varphi_n(c^{-1})\varphi_n(c)-1]\varphi_n(x)=0.$$

[†)] Por ejemplo la $\mathbb{Q}$-forma $f(x , y)=x^2-2y^2$ es anisotrópica ya que $\sqrt{2}\notin\mathbb{Q}$; pero vista como una $\mathbb{Q}(\sqrt{2})$-forma es isótropa.

Se observa que el n-ésimo término de la suma se anula y por la hipótesis de inducción se obtiene que $\varphi_i(c)\varphi_n(c^{-1})=1$ para cada $i=1,\ldots,n$; en particular $\varphi_1(c)\varphi_n(c^{-1})=1$, luego $\varphi_1(c)=\varphi_n(c)$ lo cual contradice la elección de c. Por lo tanto, $a_i=0$ para toda $i=1,\ldots,n$. □

COROLARIO 3.3.6. Si $K:F$ es una extensión finita separable de campos. Entonces la función traza $T_{K:F}:K\to F$ es F-lineal no nula.

DEMOSTRACIÓN

Sean $\sigma_1,\ldots,\sigma_n$ los F-homomorfismos inyectivos de K en su cerradura algebraica K, entonces $T_{K:F}(x)=\sigma_1(x)+\cdots+\sigma_n(x)$. Por 3.3.5., $T_{K:F}(x)\neq 0$, $x\in K$ con $x\neq 0$. □

Sea $K:F$ una extensión finita de campos; la función traza puede utilizarse para definir una forma bilineal simétrica sobre F.

$$T:K\times K\to F,\ (x\ ,y)\mapsto T_{K:F}(xy)$$

T se denomina **forma traza** asociada a K.

COROLARIO 3.3.7. Sea $K:F$ una extensión finita separable de campos, $T:K\times K\to F$ la forma traza asociada a K, entonces (K , T) es un espacio cuadrático regular sobre F.

DEMOSTRACIÓN

Por 3.3.6., existe un elemento $x_0\in K$ tal que $T_{K:F}(x_0)\neq 0$. Sea $y\in K$ un elemento tal que $T(x,y)=0$, para cada $x\in K$, si $y\neq 0$, $0=T(x_0/y,\ y)=T_{K:F}(x_0)\neq 0$ lo cual es una contradicción. □

Sea $f=\langle a_1,\ldots,a_n\rangle$ una forma cuadrática diagonal de grado n sobre un campo real F y T un orden en F. Se define la **signatura** de f escrito $sig_T(f)$ como $sig_T(f)=\eta^+-\eta^-$, donde η^+ es el número de $a_i\in T$ y η^- es el número de $a_i\in -T$. Antes de enunciar y probar el primer resultado importante en esta sección se darán algunos conceptos y resultados que son necesarios.

Sea A un anillo I y J ideales de A; se dice que I y J son **comaximales** si $I+J=A$. Si $I_1,\ldots,I_n$ son ideales en A, la familia $\{I_1,\ldots,I_n\}$ es comaximal si I_i, I_j, $i\neq j$ son comaximales, $i, j=1,\ldots,n$. Si $I_1,\ldots,I_n$, P son ideales de un anillo A con P ideal primo, se observa que la afirmación $I_i\subseteq P$ para algún índice $i\in\{1,2,\ldots,n\}$ es equivalente a $\bigcap_{i=1}^{n} I_i\subseteq P$ y también equivalente a $\prod_{i=1}^{n} I_i\subseteq P$. La demostración de las equivalencias anteriores es directa. Por ejemplo para probar que $\prod_{i=1}^{n} I_i\subseteq P\Rightarrow I_i\subseteq P$, se supone que para cada $i\in\{1,2,\ldots,n\}$, se cumple que $I_i\not\subseteq P$. Entonces, para toda i, existe $a_i\in I_i\setminus P$; pero entonces $a_1\cdots a_n\in\prod_{i=1}^{n} I_i\setminus P$ ya

que P es primo. Esto último contradice la tercera equivalencia. Si $I_1,\ldots,I_n$ son ideales en A, entonces $I_1\cdots I_n\subseteq I_1\cap\cdots\cap I_n$

LEMA 3.3.8. Sea $\{I_1,\ldots,I_n\}$ una familia comaximal de ideales en un anillo A. Entonces los ideales $J:=I_1\cap\cdots\cap I_{n-1}$ e I_n son comaximales.

DEMOSTRACIÓN

Supóngase que J e I_n no son ideales comaximales en A; entonces existe un ideal maximal m de A que satisface $J+I_n\subseteq m\subsetneq$A, luego $I_n\subseteq m$ y $J\subseteq m$. Como m es un ideal primo y $\cap I_i\subseteq m$, existe $j_0\in\{1,2,\ldots,n\text{-}1\}$ tal que $I_{j_0}\subseteq m$, entonces $I_{j_0}+I_n\subseteq m\subsetneq$A. Esto último es una contradicción ya que I_{j_0} e I_n son comaximales. Por lo tanto no existe ideal maximal m en A que contenga a $I_{j_0}+I_n$. Así, $I_{j_0}+I_n$=A. □

PROPOSICIÓN 3.3.9. Sea A un anillo e $\{I_1,\ldots,I_n\}$ una familia comaximal de ideales de A. Entonces $I_1\cdot I_2\cdots I_n=I_1\cap I_2\cap\cdots\cap I_n$.

DEMOSTRACIÓN

Se probará por inducción sobre n. Para n=2, se tiene que $I_1\cdot I_2\subseteq I_1\cap I_2$. Como I_1 e I_2 son comaximales, I_1+I_2=A. Así, $I_1\cap I_2=(I_1\cap I_2)A=(I_1\cap I_2)(I_1+I_2)=(I_1\cap I_2)I_1+(I_1\cap I_2)I_2$. Pero $(I_1\cap I_2)I_1\subseteq I_1I_2$ e $(I_1\cap I_2)I_2\subseteq I_1I_2$. De esto se sigue que $I_1\cap I_2\subseteq I_1I_2$. Supóngase que $n\geq 3$ y que el resultado es valido para n-1, es decir, $I_1\cdot I_2\cdots I_{n-1}=I_1\cap I_2\cap\cdots\cap I_{n-1}$. Por el lema 3.3.8., se tiene que $I_1\cap I_2\cap\cdots\cap I_{n-1}$ e I_n son comaximales y por el caso n=2, se sigue que

$$(I_1\cdot I_2\cdots I_{n-1})\cap I_n=(I_1\cap I_2\cap\cdots\cap I_{n-1})I_n.$$

Luego

$$I_1\cap I_2\cap\cdots\cap I_n=(I_1\cap I_2\cap\cdots\cap I_{n-1})\cap I_n=(I_1\cap I_2\cap\cdots\cap I_{n-1})I_n=I_1\cdot I_2\cdots I_n.$$

Por lo tanto $I_1\cdots I_n=I_1\cap\cdots\cap I_n$. □

Se observa de 3.3.8. y 3.3.9., que si $\{I_1,\ldots,I_n\}$ es una familia comaximal de ideales de A, entonces $I_i+\Pi\, I_j$=A con $i\neq j$, i=1,…,n.

A continuación se enuncia el teorema chino del residuo.

TEOREMA 3.3.10. Sea A un anillo e $\{I_1,\ldots,I_n\}$ una familia comaximal de ideales en A. Si $x_1,\ldots,x_n\in$A, entonces existe $x\in$A tal que $x\equiv x_i\ mod(I_i)$, i=1,…,n.

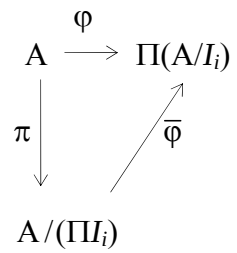
DEMOSTRACIÓN

Se probará por inducción sobre n. Si n=2, como I_1+I_2=A, existen elementos $a_1\in I_1$, $a_2\in I_2$ tal que a_1+a_2=1. Dado que a_1=1-$a_2\in I_1$ y a_2=1-$a_1\in I_2$, se sigue que $a_1\equiv 1\ mod(I_2)$, $a_2\equiv 1 mod(I_1)$ y $a_1x_2\equiv x_2\ mod(I_2)$, $a_2x_1\equiv x_1 mod(I_1)$. Haciendo $x=a_1x_2+a_2x_1$, se tiene el resultado.

Sea $i\geq 3$ y supóngase que el teorema es valido para n-1 ideales comaximales dos a dos. Dado que $\{I_1,\ldots,I_n\}$ es una familia comaximal, por la observación a 3.3.8. y por 3.3.9., se tiene que $I_i+\Pi\, I_j=A$ con $i\neq j$, $i=1,\ldots,n$. Entonces existen elementos $z_i\in I_i$ y $y_i\in\Pi I_j$ con $i\neq j$, $i=1,\ldots,n$ tal que $y_i+z_i=1$, $i=1,\ldots,n$. Haciendo $x=x_1y_1+\cdots+x_ny_n$, se sigue que $x\equiv x_iy_i mod(I_i)$, $i=1,\ldots,n$. De $y_i+z_i=1$, $i=1,\ldots,n$ se obtiene $z_i=1-y_i\in I_i$, $y_i\equiv 1\ mod(I_i)$ y $x_iy_i\equiv x_i mod(I_i)$, $i=1,\ldots,n$. Así, $x\equiv x_i\ mod(I_i)$ para $i=1,\ldots,n$. □

Como una consecuencia del teorema chino del residuo se tiene el siguiente

COROLARIO 3.3.11. Sea A un anillo e $\{I_1,\ldots,I_n\}$ una familia comaximal de ideales en A Entonces $A/(I_1\cdot I_2\cdots I_n)\cong(A/I_1)\times\cdots\times(A/I_n)$.[†)]



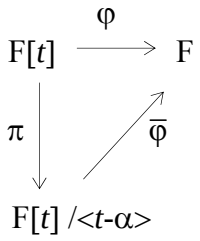
DEMOSTRACIÓN

Sea

$$\varphi:A\to(A/I_1)\times\cdots\times(A/I_n);\ a\mapsto(a+I_1,\ldots,a+I_n).$$

Claramente φ es un homomorfismo de anillos cuyo núcleo es $\cap I_i=\Pi I_i$. Por el teorema chino del residuo se sigue que φ es suprayectivo y por el primer teorema del isomorfismo se obtiene el resultado. □

OBSERVACIÓN 3.3.12. Sea F un campo y F[t] el anillo de polinomios en la indeterminada t con coeficientes en F. Entonces. F[t] /<t-α>≅F



DEMOSTRACIÓN

Sea $\varphi:F[t]\to F;\ f(t)\mapsto f(\alpha)$ con $\alpha\in F$. φ es un homomorfismo suprayectivo. Como F[t] es un D.I.P., su núcleo es un ideal principal, es decir, $Ker(\varphi)=<f>$. Sea $g(t)=t-\alpha$, como $g(\alpha)=0$, se tiene que $<g>\subseteq<f>$. Por el algoritmo de la división, existen polinomios q, $r\in F[t]$ tal que $f=qg+r$ con $r=0$ o $grad(r)<grad(g)$. Como $grad(g)=1$, se sigue que $r=0$, es decir, $f=qg$ y $<f>\subseteq<t-\alpha>$. Así, la función $\bar{\varphi}:F[t]/<t-\alpha>\to F$, $h+<t-\alpha>\mapsto h(\alpha)$ es un F-isomorfismo. □

OBSERVACIÓN 3.3.13. Sea F un campo cerrado real, $\bar{F}=F(\sqrt{-1})$ y F[t] el anillo de polinomios en la indeterminada t con coeficientes en F. Entonces $F[t]/<t^2+at+b>\cong\bar{F}$, donde el discriminante a^2-4b es negativo.

DEMOSTRACIÓN

Como $g(t)=t^2+at+b$ es un polinomio irreducible en el anillo F[t], se tiene que $t^2+at+b=(t-\beta_1)(t-\beta_2)$ en $\bar{F}[t]$ con $\beta_1=(-a+\sqrt{a^2-4b})/2$ y $\beta_2=(-a-\sqrt{a^2-4b})/2$. Dado que para todo campo cerrado real, todo elemento es un cuadrado o el negativo de un cuadrado (ver

[†)] Esto también se puede escribir como: la sucesión $0\to I_1\cdot I_2\cdots I_n\to A\to(A/I_1)\times\cdots\times(A/I_n)\to 0$ es exacta.

corolario 3.2.4.), se sigue que $\sqrt{a^2-4b}$ tiene sentido en F con a^2-4$b\in$-T, T el orden en F. Sea φ:F[t] $\to$ F; $f(t)\mapsto f(\beta_1)$. φ es un homomorfismo suprayectivo cuyo núcleo es un ideal principal $Ker(\varphi)=<f>$. Como $g(\beta_1)=0$, se tiene que $<g>\subseteq< f >$. Por el algoritmo de la división, existen polinomios q, $r\in$F[t] tal que $f=qg+r$ con $r=0$ o $grad(r)<grad(g)$. Así, $grad(r)=0$ o $grad(r)=1$. Si $grad(r)=1$, entonces $r(\beta_1)=0$ y $\beta_1\in$F. □

A continuación se prueba una caracterización de separabilidad vía el producto tensorial.

LEMA 3.3.14. Sea K : F una extensión de campos y $f\in$F[t] un polinomio de grado ≥1. Entonces K$\otimes_F$(F[x] /<f>)≅K[x] /<f> como K-álgebras.

DEMOSTRACIÓN

Sea φ:K[x] $\to$ K$\otimes_F$(F[x] /<f>); $\sum a_i x^i \mapsto \sum a_i\otimes(x^i+<f>)$. φ es un homomorfismo suprayectivo de K-álgebras que mapea f (x) a cero. Como ambas álgebras K⊗F y F[x] /<f> son de la misma dimensión, igual al grado de f, se sigue que K$\otimes_F$(F[x] /<f>)≅K[x] /<f>. □

TEOREMA 3.3.15. Sea F un campo real, T un orden de F y $\tilde{F}$ su cerradura real. Si $f\in$F[t] es un polinomio separable no constante y K=F[t] /<f>, entonces el número de raíces distintas de f en $\tilde{F}$ es la signatura de la forma traza en K con respecto al orden T.

DEMOSTRACIÓN

Sea $f\in$F[t] un polinomio y considérese K=F[t] /<f>; K es una F-álgebra de dimensión ≤ $grad(f)$. Sea T un orden en F y $\tilde{F}$ su cerradura real, es decir, $\tilde{F}$ es un cerrado real que contiene a F y cuyo único orden $\tilde{T}$ induce el orden T sobre el campo F. Como K es un espacio vectorial de dimensión finita sobre el campo F y la función T_f :K×K$\to$F, $T_f(x,y)=T_{K:F}(x\cdot y)$ es la forma traza, entonces por 3.3.7., (K , T_f) es un espacio cuadrático regular sobre F. Por 3.3.4., del espacio cuadrático (K , T_f) se puede construir un espacio cuadrático ($\tilde{F}\otimes_F$K , $(T_f)_F$), donde la conexión que existe entre las formas T_f y $(T_f)_F$ es $(T_f)_F(a\otimes u)=a^2T_f(u)$. También por 3.3.7., se observa que si $\{u_1,\ldots,u_n\}$ es una base de K, entonces la matriz simétrica asociada con la forma T_f en la base anterior, es la misma que la matriz simétrica asociada con la forma $(T_f)_F$ en la base $\{1\otimes u_1,\ldots,1\otimes u_n\}$ en $\tilde{F}\otimes_F$K. Así, la forma traza $(T_f)_F$ asociada a la F-álgebra $\tilde{F}\otimes_F$K es precisamente la forma traza T_f asociada a la F-álgebra K=F[x]/<f>, considerada sobre $\tilde{F}$. Se afirma que la signatura de la forma traza T_f es el número de raíces del polinomo f en $\tilde{F}$, donde f es un polinomio separable no constante. En efecto, como $sig(T_f)=sig(T_f)_F$, la signatura de T_f se calculará sobre $\tilde{F}$. Por la proposición 3.3.9., f puede factorizarse en polinomios irreducibles lineales y cuadráticos, es decir, $f=g_1\cdot g_2\cdots g_r\cdot h_1\cdot h_2\cdots h_s$ donde $grad(g_i)=1$, $grad(h_j)=2$, i=1,…,r; j=1,…,s. Todos los factores son diferentes ya que f tiene todas sus raices simples; por el lema 3.3.14. $\tilde{F}\otimes_F$K≅$\tilde{F}$[t]/<f>, como $\tilde{F}$-álgebras. Por el corolario del teorema chino del residuo y por las observaciones 3.3.12. y 3.3.13., se tiene que $\tilde{F}\otimes_F$K≅$\tilde{F}\times\cdots\times\tilde{F}\times\overline{\tilde{F}}\times\cdots\times\overline{\tilde{F}}$ ($\tilde{F}$ r-vece) y

($\overline{\overline{\tilde{F}}}$ *s*-veces) donde $\overline{\overline{\tilde{F}}}$ es la cerradura algebraica de $\tilde{F}$. Se observa que la forma traza $(T_f)_F$ asociada a la F-álgebra $\tilde{F}\otimes_F K$, restringida a cada factor de la forma $\tilde{F}$ es la $\tilde{F}$-forma <1> y restringida a cada factor de la forma $\overline{\overline{\tilde{F}}}$ tiene por matriz en la base $\{1, \boldsymbol{i}\}$ la matriz

$$\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}^{\dagger)}$$

Luego $\overline{\overline{\tilde{F}}}$ como espacio cuadrático es un plano hiperbólico sobre $\tilde{F}$. Se observa también que los subespacios son mutuamente ortogonales respecto a la forma traza $(T_f)_F$ de $\tilde{F}\otimes_F K$, es decir, los diferentes factores tienen producto igual a cero. Así, con respecto al único orden en $\tilde{F}$, la signatura de la forma traza de $\tilde{F}\otimes_F K$ es igual a *r*, es decir, $sig_T(T_f)_F = r$. □

Como una primera consecuencia del teorema 3.3.15., se tiene el

COROLARIO 3.3.16. Sea $K:F$ una extensión finita de campos con $K=F(\alpha)$. Entonces un orden T sobre F se extiende a K si y sólo si el F-polinomio mínimo f_α de α tiene una raíz en toda cerradura real de F con respecto al orden T.

DEMOSTRACIÓN ($\Rightarrow$)

Si T se extiende a K, se considera una cerradura real $\widetilde{K}$ con orden único $\tilde{T}$ de F con su orden T, tal que $K\subseteq\widetilde{K}$, luego *f* tiene una raíz en $\widetilde{K}$, y como el número de raíces en una cerradura real es independiente de la cerradura elegida, se sigue que *f* tendrá una raíz en cualquier otra cerradura real de F con respecto al orden T.

($\Leftarrow$)

Si el polinomio f_α tiene una raíz β en una cerradura real $\widetilde{K}$ con orden único $\tilde{T}$ en F; F con su orden T, entonces $F(\alpha)$ es F-isomorfo a $F(\beta)$, luego el orden inducido por el único orden $\tilde{T}$ de $\widetilde{K}$ sobre $F(\beta)$ proporciona un orden sobre $F(\alpha)=K$ vía el isomorfismo. □

Para la demostración del primer resultado importante se necesita un lema más.

LEMA 3.3.17. Sea F un campo real y *f* una F-forma cuadrática. Entonces la función signatura $sig(f):X_F \to \mathbb{Z}$; $sig(f)(T)=sig_T(f)$ con X_F el espectro real de F, es continua si $\mathbb{Z}$ está dotado con la topología discreta.

---

†) $T_f : \overline{\overline{\tilde{F}}} \times \overline{\overline{\tilde{F}}} \to \tilde{F}$, $T_f((x_1, x_2), (y_1, y_2)) = T_{\overline{\overline{\tilde{F}}}:\tilde{F}}((x_1, x_2)\cdot(y_1, y_2)) = \mathrm{Id} + \overline{\mathrm{Id}}$, donde Id e $\overline{\mathrm{Id}}$ son los automorfismos identidad y conjugado. Asi en la base $\{1, \boldsymbol{i}\}$ se tiene

$T_f((1,0),(1,0)) = T_{\overline{\overline{\tilde{F}}}:\tilde{F}}(1) = \mathrm{Id}(1) + \overline{\mathrm{Id}}(1) = 1+1 = 2$

$T_f((1,0),(0,1)) = T_{\overline{\overline{\tilde{F}}}:\tilde{F}}(\boldsymbol{i}) = \mathrm{Id}(\boldsymbol{i}) + \overline{\mathrm{Id}}(\boldsymbol{i}) = 1+(-1) = 0$

$T_f((0,1),(1,0)) = T_{\overline{\overline{\tilde{F}}}:\tilde{F}}(\boldsymbol{i}) = \mathrm{Id}(\boldsymbol{i}) + \overline{\mathrm{Id}}(\boldsymbol{i}) = 1+(-1) = 0$

$T_f((0,1),(0,1)) = T_{\overline{\overline{\tilde{F}}}:\tilde{F}}(-1) = \mathrm{Id}(-1) + \overline{\mathrm{Id}}(-1) = -1+(-1) = -2.$

DEMOSTRACIÓN

Sea f una F-forma cuadrática de grado n y $\langle a_1,\ldots,a_n\rangle$ su representación diagonal. Dado que $sig\langle a_1,\ldots,a_n\rangle = sig\langle a_1\rangle+\cdots+sig\langle a_n\rangle$ y suma de funciones continuas es una función continua, será suficiente considerar la forma $f=\langle a\rangle$. Se observa que

$$sig\langle a\rangle^{-1}(1)=\{T\in X_F \mid sig\langle a\rangle=1\}=\{T\in X_F \mid a\in T\}=H(a),$$
$$sig\langle a\rangle^{-1}(-1)=\{T\in X_F \mid sig\langle a\rangle=-1\}=\{T\in X_F \mid -a\in T\}=H(-a) \text{ y}$$
$$sig\langle a\rangle^{-1}(n)=\{T\in X_F \mid sig\langle a\rangle=n\}=\varnothing$$

si $n\in\mathbb{Z}/\{-1\ ,\ 1\}$. □

TEOREMA 3.3.18. Sea $K:F$ una extensión finita de campos reales, X_K, X_F los espectros reales de K y F respectivamente. Sea $\mathcal{E}_{K:F}: X_K \to X_F;\ T' \mapsto T'\cap F=T$ la función definida por la restricción de ordenes de K a F. Entonces $Im(\mathcal{E}_{K:F})$ es un abierto en X_F.

DEMOSTRACIÓN

Como K es un campo real, $car(K)=0$. Por el corolario 3.1.30., K es una extensión simple. Sea f_α el polinomio mínimo de α; por la proposición 3.3.16., se tiene que un orden $T\in X_F$ se extiende a K si y sólo si f_α tiene una raíz en una cerradura real $\tilde{F}$ de F con respecto al orden T. Por el teorema 3.3.15., el número de raíces de f_α en $\tilde{F}$ es la signatura de la forma traza T_f. Así, el orden T se extiende a K si y sólo si $sig_T(T_f)>0$. Se sigue que la imagen de $\mathcal{E}_{K:F}$ es el soporte de la forma traza T_f, el cual por 3.3.17., es un conjunto abierto y cerrado en X_F. □

PROPOSICIÓN 3.3.19. Sea $K:F$ una extensión finita de campos reales, T un orden de F, T' con $T'\cap F=T$ un orden en K y $\varphi: F \to L$ un homomorfismo inyectivo (encaje) de F en un campo cerrado real L que preserva el orden.[†)] Entonces existe una extensión φ' de φ a K que preserva el orden.

DEMOSTRACIÓN

Como K es un campo real, $car(K)=0$. Por el corolario 3.1.30., K es una extensión simple, $K=F(\alpha)$ con $\alpha\in K$. Sea f_α el F-polinomio mínimo de α y considérese una cerradura real $\tilde{K}$ de K. Por la afirmación al teorema 3.3.15., como f_α tiene una raíz en $\tilde{K}$, entonces el polinomio $f_\alpha^{\varphi}(x)$, (con f_α^{φ} el F-polinomio mínimo f_α de α) que se obtiene aplicando φ a los coeficientes de f_α tendrá una raíz en L, donde φ identifica a F como un subcampo de L. Entonces como $K:F$ es una extensión finita, $\alpha\in K$ es algebraico sobre F y $\varphi: F\to L$ es un homomorfismo inyectivo, entonces φ puede extenderse a $F(\alpha)=K$ si el polinomio $f_\alpha^{\varphi}(x)$ tiene una raíz en L, es decir, existe una extensión φ' de φ a K. Supóngase a continuación que ninguna extensión de φ a K preserva el orden. Sean $\varphi_1,\ldots,\varphi_n$ las posibles extensiones de φ a K, entonces existen $\alpha_1,\ldots,\alpha_n\in K$ tal que $\alpha_i\in T'$, pero $\varphi_i(\alpha_i)\notin L^2$ donde L^2 es el único orden de L (ver 3.2.5.). Por el corolario 3.2.7., se puede extender el orden T' a

---

[†)] Se dice que un homomorfismo inyectivo (o un isomorfismo) $\psi: F_1\to F_2$ de campos reales F_1 y F_2 preserva el orden si $a<_T b$ si y sólo si $\psi(a)<_S \psi(b)$ con T en F_1, S en F_2 órdenes.

$K(\sqrt{\alpha_1},...,\sqrt{\alpha_n})$. Sea ψ una extensión de φ_j a $K(\sqrt{\alpha_1},...,\sqrt{\alpha_n})$, entonces se tiene que $\varphi_j(\alpha_j)=\psi(\alpha_j)=\psi((\sqrt{\alpha_j})^2)=(\psi(\sqrt{\alpha_j}))^2$, luego $\varphi_j(\alpha_j)\in L^2$, que contradice la elección de α_j. □

PROPOSICIÓN 3.3.20. Sea F un campo real, $\tilde{F}$ una cerradura real de F y L un campo cerrado real. Si $\varphi:F\to L$ es un homomorfismo inyectivo que preserva el orden, entonces φ se extiende en forma única a $\tilde{F}$.

DEMOSTRACIÓN

Por la proposición 3.3.19., y por el lema de Zorn, φ puede extenderse a $\tilde{F}$. Para la unicidad sean ψ_1 y ψ_2 extensiones de φ a $\tilde{F}$. Tomando $\alpha\in\tilde{F}$ y considerando a $\alpha_1,\alpha_2,\ldots,\alpha_r$ con $\alpha_1<\alpha_2<\cdots<\alpha_r$ todas las raíces del F-polinomio mínimo f_α de α que están en $\tilde{F}$, entonces por la afirmación al teorema 3.3.15., $\psi_1(\alpha_1),\ldots,\psi_1(\alpha_r)$ con $\psi_1(\alpha_1)<\cdots<\psi_1(\alpha_r)$ y $\psi_2(\alpha_1),\ldots,\psi_2(\alpha_r)$ con $\psi_2(\alpha_1)<\cdots<\psi_2(\alpha_r)$ son todas las raíces de f_α^{φ}. Luego $\psi_1(\alpha_i)=\psi_2(\alpha_i)$, $i=1,\ldots,r$ y $\psi_1(\alpha)=\psi_2(\alpha)$. Por lo tanto $\psi_1=\psi_2$. □

Como una consecuencia del resultado anterior se prueba la unicidad de cerraduras reales.

COROLARIO 3.3.21. Sea F un campo real y $\tilde{F}_1$, $\tilde{F}_2$ cerraduras reales de F con respecto a un orden T en F, entonces existe un F-isomorfismo $\psi:\tilde{F}_1\to\tilde{F}_2$ que preserva el orden.

DEMOSTRACIÓN

Sean $\boldsymbol{i}:F\to\tilde{F}_1$ y $\boldsymbol{j}:F\to\tilde{F}_2$ los homomorfismos inyectivos canónicos. Por la proposición 3.3.20., se tiene una extensión de $\boldsymbol{i}$; $\psi':\tilde{F}_2\to\tilde{F}_1$ y una extensión de $\boldsymbol{j}$; $\psi'':\tilde{F}_1\to\tilde{F}_2$. Entonces por la unicidad en 3.3.20., $\psi'\circ\psi'':\tilde{F}_1\to\tilde{F}_1$ es la identidad sobre $\tilde{F}_1$ y $\psi''\circ\psi':\tilde{F}_2\to\tilde{F}_2$ es la identidad sobre $\tilde{F}_2$. De esto se obtiene que ψ' y ψ'' son isomorfismos inversos sobre F que preservan el orden. □

Este corolario junto con la proposición 3.2.10., aseguran que para cada campo real, siempre existe una cerradura real que es única salvo isomorfismos.

Se recuerda (ver cap 1, pag 11) que si K es un campo, un subanillo A de K es un anillo de valoración si para cada elemento $x\in K\setminus A$, se tiene que $x^{-1}\in A$. Esto significa que K es el campo de cocientes de A, es decir, $K=qf(A)$. También, de los lemas 1.1.25. y 1.1.26., se obtiene que si A es un anillo de valoración en un campo K y si m es el conjunto de no-unidades en A, entonces m es el único ideal maximal de A. El campo $K'=A/m$ se denomina campo residual de A.

Sea $K:k$ una extensión de campos reales, donde k es un campo cerrado real y T un orden de K. Se definen los conjuntos

$$A(k,T):=\{x\in K \mid |x|_T <_T a \text{ para algún } a\in k\}.$$

$$m(k\,,\,\mathrm{T}):=\{x\in \mathrm{K} \mid |x|_{\mathrm{T}} <_{\mathrm{T}} b \text{ para toda } b\in k \text{ positiva}\}.^{\dagger)}$$

A continuación se prueba que $A(k\,,\,\mathrm{T})$ es un anillo de valoración y $m(k\,,\,\mathrm{T})$ es su ideal maximal

OBSERVACIÓN 3.3.22. Sea $\mathrm{K}:k$ una extensión de campos reales, k un campo cerrado real y T un orden en K. Entonces el conjunto $A(k\,,\,\mathrm{T})$ es un anillo de valoración local real, $m(k\,,\,\mathrm{T})$ su ideal maximal y la imagen de $\mathrm{T}\cap A(k\,,\,\mathrm{T})$ en el campo residual K' de $A(k\,,\,\mathrm{T})$ es un orden en K'.

DEMOSTRACIÓN

Primero se prueba que $A(k\,,\,\mathrm{T})$ es un subanillo de K. 1°) Es claro que $1_{\mathrm{K}}\in A(k\,,\,\mathrm{T})$ pues $|1_{\mathrm{K}}|_{\mathrm{T}} <_{\mathrm{T}} a$, para alguna $a\in k$. 2°) y 3°) Si x, $y\in A(k\,,\,\mathrm{T})$, entonces $|x|_{\mathrm{T}} <_{\mathrm{T}} a_1$ y $|y|_{\mathrm{T}} <_{\mathrm{T}} a_2$ para algunos elementos a_1, $a_2\in k$, luego $|x+y|_{\mathrm{T}} \leq_{\mathrm{T}} |x|_{\mathrm{T}} + |y|_{\mathrm{T}} <_{\mathrm{T}} a_1 + a_2 = a$ para algún elemento $a\in k$ y $|xy|_{\mathrm{T}} =_{\mathrm{T}} |x|_{\mathrm{T}}|y|_{\mathrm{T}} <_{\mathrm{T}} a_1a_2 = a$ para alguna $a\in k$. Así, $x+y\in A(k, \mathrm{T})$ y $xy\in A(k, \mathrm{T})$. 4°) Como $|-x|_{\mathrm{T}} =_{\mathrm{T}} |x|_{\mathrm{T}}$ para toda $x\in A(k\,,\,\mathrm{T})$, entonces $-x\in A(k\,,\,\mathrm{T})$. De esta forma, $A(k\,,\,\mathrm{T})$ es un subanillo de K, esto es, $A(k\,,\,\mathrm{T})$ es un dominio entero. Por otro lado, 1°) Como $0\in m(k\,,\,\mathrm{T})$ ya que $|0|_{\mathrm{T}} <_{\mathrm{T}} a$, para toda $a\in k$ positiva, se sigue que $m(k\,,\,\mathrm{T})\neq\emptyset$. 2°) Sean x, $y\in m(k\,,\,\mathrm{T})$, entonces $|x|_{\mathrm{T}} <_{\mathrm{T}} a_1$, y $|y|_{\mathrm{T}} <_{\mathrm{T}} a_2$, para todas a_1 y $a_2\in k$; así, $x+y\in m(k\,,\,\mathrm{T})$. 3°) Si, $x\in m(k\,,\,\mathrm{T})$ y $y\in\mathrm{K}$, entonces $|x|_{\mathrm{T}} <_{\mathrm{T}} a_1$, para toda $a\in k$ positiva y $|xy|_{\mathrm{T}} =_{\mathrm{T}} |x|_{\mathrm{T}}|y|_{\mathrm{T}} <_{\mathrm{T}} a|y|_{\mathrm{T}}$ para toda $a\in k$ positiva; luego $|xy|_{\mathrm{T}} <_{\mathrm{T}} a$ para cada $a\in k$ positiva. De esta forma $xy\in m(k\,,\,\mathrm{T})$; así, $m(k\,,\,\mathrm{T})$ es un ideal de $A(k\,,\,\mathrm{T})$.

A continuación se probará que $A(k\,,\,\mathrm{T})$ es un anillo de valoración. En efecto, sea $x\in\mathrm{K}\setminus\{0\}$ un elemento tal que $x\notin A(k\,,\,\mathrm{T})$, entonces *i*) en el caso $x>0$, $x>a$ para toda $a\in k$, se tiene que $x^{-1}<b$ para cada $b\in k$ positiva, luego $x^{-1}\in m(k\,,\,\mathrm{T})\subseteq A(k\,,\,\mathrm{T})$. *ii*) Si $x<0$, $-a<x$ para toda $a\in k$, entonces $-x>0$ y $-x>a$ para cada $a\in k$ positiva, luego $-x^{-1}<b$ para toda $b\in k$ positiva. Así, $A(k\,,\,\mathrm{T})$ es un anillo de valoración de K, y por el lema 1.1.26., $A(k\,,\,\mathrm{T})$ es un anillo local y $m(k\,,\,\mathrm{T})$ su ideal maximal. Finalmente, para ver que $A(k\,,\,\mathrm{T})$ es un anillo local real se considera el homomorfismo natural

$$\varphi: A(k\,,\,\mathrm{T})\twoheadrightarrow \mathrm{K}';\ x\mapsto x+m(k\,,\,\mathrm{T}).$$

donde $\mathrm{K}'=A(k\,,\,\mathrm{T})/m(k\,,\,\mathrm{T})$ es el campo residual de $A(k\,,\,\mathrm{T})$. Sea $\mathrm{T}'=\{\varphi(x) \mid x\in\mathrm{T}\cap A(k, \mathrm{T})\}$; T' es un orden en K'. En efecto, 1°) y 2°). Sean $\overline{x}$, $\overline{y}\in\mathrm{T}'$ con $\overline{x}=\varphi(x)$, $\overline{y}=\varphi(y)$, entonces $\overline{x}+\overline{y}=\varphi(x)+\varphi(y)=\varphi(x+y)$ y $\overline{x}\cdot\overline{y}=\varphi(x)\varphi(y)=\varphi(xy)$. Como x, $y\in\mathrm{T}\cap A(k\,,\,\mathrm{T})$, se sigue que $x+y$, $xy\in\mathrm{T}\cap A(k\,,\,\mathrm{T})$ y $\varphi(x+y)$, $\varphi(xy)\in\mathrm{T}'$. 3°) Si $-\overline{1}\in\mathrm{T}'$, entonces $-\overline{1}=\overline{x}_1^{\,2}+\cdots+\overline{x}_n^{\,2}$, con $x_i\in A(\mathrm{F}\,,\,\mathrm{T})$, $i=1,\ldots,n$. Luego $x_1^{\,2}+\cdots+x_n^{\,2}+1\in m(k\,,\,\mathrm{T})$, entonces $|x_1^{\,2}+\cdots+x_n^{\,2}+1|_{\mathrm{T}}<_{\mathrm{T}}a$ para

---

$^{\dagger)}$ El valor absoluto de x con respecto al orden T se define como en el caso del campo $\mathbb{R}$, es decir,

$$|x|_{\mathrm{T}}=\begin{cases} x \text{ si } x\in\mathrm{T} \\ -x \text{ si } x\notin\mathrm{T}\end{cases}$$

toda $a \in k$ positiva, lo cual es un absurdo ya que $x_1^2+\cdots+x_n^2+1 \in T$. 4°) Considérese $\overline{x} \in K'$, con $\overline{x}=\varphi(x)$ donde $x \in T \cap A(k, T)$, entonces $x^2 \in T \cap A(k, T)$ porque tanto x como x^2 están en $A(k, T)$; luego $\varphi(x^2)=\varphi(x)^2 \in T'$ y $x^2 \in T'$. 5°) Si $\overline{x} \in T' \cup -T'$, se tiene que $\overline{x} \in T'$ o $\overline{x} \in -T'$, es decir, $x \in T \cap A(k, T)$ o $x \in -T \cap A(k, T)$. En ambas situaciones, $x \in A(k, T)$ y $\overline{x} \in K'$. Ahora, sea $x \in K'$, entonces $x \in A(k, T)$, $\overline{x}=\varphi(x)$. De esta forma $x \in T \cap A(k, T)$ o $x \in -T \cap A(k, T)$, esto es, $\overline{x} \in T$ o $\overline{x} \in -T'$. □

TEOREMA 3.3.23. Sea $K : k$ una extensión de campos reales, donde k es un campo cerrado real y K es un campo de funciones de grado trascendente 1. Si $x \in K$ es un elemento trascendente sobre el campo base k, entonces existe un orden T en K y un elemento $\delta \in k$ tal que $(x-\delta)^{-1} \notin A(k, T)$.

DEMOSTRACIÓN

Como K es un campo real, existe al menos un orden T_0 en K. Sea S_0 la restricción a $k(x)$ del orden T_0; $S_0=T_0 \cap k(x)$. Por el teorema 3.3.18., existe una vecindad abierta $H(f_1,..., f_n)$ de S_0 que está contenida en la imagen de X_K bajo el mapeo $\mathcal{E}_{K;k(x)}$, es decir, $H(f_1,..., f_n) \subseteq \mathcal{E}_{K;k(x)}(X_K)$ donde $H(f_1,\ldots,f_n)=\{T' \mid f_i(x) \notin -T',\ i=1,\ldots,n\}$. Si $f_i \neq 0$ para cada $i=1,\ldots,n$; por 3.2.8., se tiene que

$$f_i(x)=(x-\alpha_{i1})\cdots(x-\alpha_{ir})(x^2+p_{i1}x+q_{i1})\cdots(x^2+p_{is}x+q_{is})$$
$$=(x-\alpha_{i1})\cdots(x-\alpha_{ir})[(x+\frac{p_{i1}}{2})^2+\frac{4q_{i1}-p_{i1}^{\ 2}}{4}]\cdots[(x+\frac{p_{is}}{2})^2+\frac{4q_{i1}-p_{i1}^{\ 2}}{4}]$$

para $\alpha_{11},\ldots,\alpha_{nr}$, $p_{11},\ldots,p_{ns}$, $q_{11},\ldots,q_{ns} \in k$, e $i=1,\ldots,n$. Como $\frac{4q_{ij}-p_{ij}^{\ 2}}{4}=d_{ij}^2$ $i=1,\ldots,n$, $j=1,\ldots,s$ es un cuadrado,

$$H(f_i)=H((x-\alpha_{i1})\cdots(x-\alpha_{ir})[(x+\frac{p_{i1}}{2})^2+d_{i1}^2]\cdots[(x+\frac{p_{is}}{2})^2+d_{is}^2])$$

se puede escribir como $H(f_i)=H((x-\alpha_{i1})\cdots(x-\alpha_{ir}))$ ya que la suma de cuadrados está en el orden.

Para cada orden S en $k(x)$, se definen los conjuntos

$$X_i(S)=\{a \in k \mid f_i(a)=0;\ a <_S x\}$$
$$=\{a \in k \mid f_i(a)=0;\ x-a \in S\}$$

$$Y_i(S)=\{b \in k \mid f_i(b)=0;\ x <_S b\}$$
$$=\{b \in k \mid f_i(b)=0;\ b-x \in S\}$$

$i=1,\ldots,n$. Los conjuntos $X_i(S)$ y $Y_i(S)$, $i=1,\ldots,n$ determinan el signo de f_i con respecto al orden S, $i=1,\ldots,n$. Si un orden S en $k(x)$ satisface $X_i(S)=X_i(S_0)$ para cada $i=1,\ldots,n$, se sigue que $f_i \in S_0$ implica $f_i \in S$; de esta forma $S \in H(f_1,\ldots,f_n)$. En efecto, sea $f_i(x) \in S_0$, con

$f_i=(x-\alpha_{i1})\cdots(x-\alpha_{ir})$, donde $\alpha_{i1},\ldots,\alpha_{ir}$ son raíces de f_i, $i=1,\ldots,n$, entonces como $X_i(S)=X_i(S_0)$, se sigue que $f_i(x)=(x-\alpha_{i1})\cdots(x-\alpha_{ir})\in S$. Dado que $S\in H(f_1,\ldots,f_n)$, S es imagen de un orden T en K, es decir, $(S=T\cap k(x))$ S puede ser extendido a un orden en K. Sean $X(S_0)=X_1(S_0)\cup\cdots\cup X_n(S_0)$ y $Y(S_0)=Y_1(S_0)\cup\cdots\cup Y_n(S_0)$. Considérese

$$\alpha=max\{a|\ a\in X(S_0)\}\ \text{y}\ \beta=min\{b|\ b\in Y(S_0)\}$$

con respecto al (único) orden en k. Si $X(S_0)=\varnothing$, se toma $\alpha=-\infty$, y si $Y(S_0)=\varnothing$ se toma $\beta=+\infty$. Dado que $\alpha<x<\beta$ en S_0, $\alpha\in X(S_0)$ y $\beta\in Y(S_0)$, entonces $\alpha<\beta$ en el orden de k. Sea $\delta\in k$ con $\delta=(\alpha+\beta)/2$; luego $\alpha<\delta<\beta$. Sea S un orden en el campo $k(x)$ tal que $|x-\delta|_S <_S \varepsilon$ para todo $\varepsilon\in k$ positivo. Se afirma que $X_i(S)=X_i(S_0)$, $i=1,\ldots,n$, donde como antes

$$X_i(S)=\{a\in k\mid f_i(a)=0;\ x-a\in S\}$$
$$X_i(S_0)=\{a\in k\mid f_i(a)=0;\ x-a\in S_0\}.$$

Supóngase que $x-a\in S$ y $x-a\notin S_0$, entonces $a\in Y_i(S)$ y $\beta\leq_S a$. Que el elemento $x-a\in S$, significa que $(x-\delta)+(\delta-a)\in S$ lo que equivale a $(x-\delta)\geq_S(a-\delta)\geq_S\beta-(\alpha+\beta)/2=_S(\alpha-\beta)/2>_S 0$ lo cual es una contradicción; así, $X_i(S)\subseteq X_i(S_0)$. En forma simétrica, si $x-a\in S_0$ y $x-a\notin S$, se obtiene que $X_i(S_0)\subseteq X_i(S)$ para cada $i=1,\ldots,n$. Como $X_i(S)=X_i(S_0)$ para cada $i=1,\ldots,n$, se sigue que $S\in H(f_1,\ldots,f_n)$, es decir, el orden S puede ser extendido a un orden T en K que satisfaga $|x-\delta|_T <_T \varepsilon$ para todo $\varepsilon\in k$ positivo, luego $x-\delta\in m$. Así, se concluye que $x-\delta\in A(k, T)$. □

Como consecuencia del teorema anterior, se tiene el

COROLARIO 3.3.24. Sea $K:k$ una extensión de campos reales, donde k es un campo cerrado real y K un campo de funciones de grado trascendente 1. Si $x\in K$ es un elemento trascendente sobre k entonces

i) $x\in A(k, T)$.

ii) $F=k$, F el campo residual de $A(k, T)$.

DEMOSTRACIÓN

i) Del teorema 3.3.23., se sigue que existe un orden T en K y un elemento $\delta\in k$ tal que $(x-\delta)^{-1}\notin A(k, T)$; lo anterior significa que el elemento $x-\delta$ es una no-unidad en $A(k, T)$, es decir, $x-\delta\in m(k, T)$, de esta forma se tiene que $|x-\delta|_T <_T a$ para todo $a\in k$ positivo. Como $|x|_T - |\delta|_T \leq_T |x-\delta|_T <_T a$, se sigue que $|x|_T <_T |\delta|_T + a$ para todo $a\in k$ positivo. Por lo tanto $x\in A(k, T)$.

ii) Como k es un campo cerrado real, para probar que $F=k$ bastará probar que la extensión $F:k$ es una extensión algebraica. Supóngase que $F:k$ no es una extensión algebraica. Sea $y\in A(k, T)$ tal que $\overline{y}\in F$ sea trascendente en F sobre k. Como $x-\delta\in m(k, T)$, se sigue que $\overline{x}=\overline{\delta}\in k$. Supóngase que $\alpha x+\beta y=0$ en K con $\alpha, \beta\in k$, entonces $\alpha\overline{x}+\beta\overline{y}=0$ en F y $\alpha\overline{\delta}+\beta\overline{y}=0$ en F. Si $\beta\neq 0$, $\overline{y}=(-\alpha/\beta)\overline{\delta}$ es algebraico sobre k lo cual contradice la

elección de $\overline{y}$; así, $\beta=0$ y $\alpha\overline{x}=0$, luego $\alpha=0$. De esta forma, x y y son algebraicamente independientes sobre k, esto es, $dim_k K\geq 2$ ¡contradicción! Por lo tanto $F=k$. □

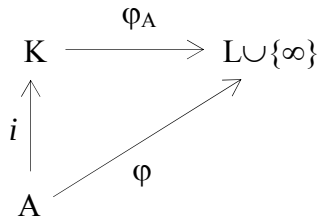
Si A es un anillo de valoración en un campo K, se tiene un homomorfismo natural $\varphi:A\to L$ $(=A/m)$, donde m es su ideal maximal. Extendiendo la función φ a todo K se obtiene la función

$$\varphi_A:K\to L\cup\{\infty\}$$

$$\varphi_A(x)=\begin{cases} x+m & \text{si } x\in A \\ \infty & \text{si } x\in K\setminus A. \end{cases}$$

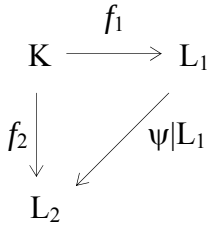
donde ∞ es un elemento adicional que no está en L y satisface

1°) Si $\alpha\in L\setminus\{0\}$, entonces $\alpha\cdot\infty=\infty\cdot\alpha=\infty\cdot\infty=\infty$.
2°) Si $\beta\in L$, entonces $\beta+\infty=\infty+\beta=\infty$.
3°) $1/\infty=0$.
4°) $\infty+\infty$, $0\cdot\infty$, $0/0$ y ∞/∞ no están definidas.



Además, $\varphi_A^{-1}(L)=A$ es un subanillo de K con $\varphi_A:A\to L$ un homomorfismo tal que $\varphi_A(x)=\infty$ si $\varphi_A(1/x)=0$. Así, un **lugar** de un campo K en un campo L es una función $f:K\to L\cup\{\infty\}$ tal que $f^{-1}(L)=A$ es un subanillo de K con $f: A\to L$ un homomorfismo en A tal que $f(x)=\infty$ si $f(1/x)=0$.

Los elementos de K que no se aplican en ∞ se llaman **finitos** por el lugar y los restantes se denominan **infinitos**. Como ya se menciono, el conjunto $A=\{x\in K \mid f(x)<\infty\}\subseteq K$ de los elementos $x\in K$ que son finitos por el lugar es un anillo de valoración de K; su ideal maximal consta de aquellos elementos $x\in A$ tal que $f(x)=0$. Dos lugares $f_1:K\to L_1\cup\{\infty\}$ y $f_2:K\to L_2\cup\{\infty\}$ son equivalentes si dada una biyección $\psi:L_1\cup\{\infty\}\to L_2\cup\{\infty\}$, la función $\psi\mid L_1:L_1\to L_2$ es un isomorfismo tal que $f_2=(\psi\mid L_1)\circ f_1$. Se observa que la equivalencia de lugares es una relación de equivalencia y que dos lugares son equivalentes si y sólo si tienen el mismo anillo de valoración. Para esto último, si $f_1:K\to L_1\cup\{\infty\}$ y $f_2:K\to L_2\cup\{\infty\}$ son lugares equivalentes con anillos de valoración A_1 y A_2 respectivamente, entonces existe un isomorfismo $\psi:L_1\to L_2$. Como $L_1=A_1/m_1$ y $L_2=A_2/m_2$, se sigue que $A_1/m_1\cong A_2/m_2$ y $m_1\cong m_2$. Recíprocamente, si $f_1:K\to L_1\cup\{\infty\}$ y $f_2:K\to L_2\cup\{\infty\}$ son dos lugares con anillos de valoración A_1 y A_2 respectivamente y si $A_1=A_2$, entonces $m_1=m_2$ y $A_1/m_1\cong A_2/m_2$, es decir, $L_1\cong L_2$ y f_1, f_2 son equivalentes. Se tiene también que la composición de dos lugares es un lugar. Sea $K:F$ una extención de campos; f es un lugar de K sobre F si f es un isomorfismo en F. En este caso $f(F)$ se identifica con F. Si f toma sus valores en $f(F)$, se dice que f es un **lugar racional** sobre F.



PROPOSICIÓN 3.3.25. Existe una correspondencia biyectiva entre la familia de clases de equivalencia de lugares de un campo K y la familia de anillos de valoración de K.

DEMOSTRACIÓN

Sea $F:£\to\Re$; $F([f])=A_f$ donde $£=\{[f] \mid f:K\to L\cup\{\infty\}$ es un lugar de K en L$\}$ y $\Re=\{A\subseteq K|$ A es un anillo de valoración de K$\}$. Si $F([f_1])=F([f_2])$, entonces $A_{f_1}=A_{f_2}$ si y sólo si f_1 es equivalente a f_2 si y sólo si $[f_1]=[f_2]$. Por otro lado, si A es un anillo de valoración en K, entonces la función

$$\varphi_A:K\to L\cup\{\infty\}$$

$$\varphi_A(x)=\begin{cases} x+m \text{ si } x\in A \\ \infty \quad \text{si } x\in K\setminus A. \end{cases}$$

con m el ideal maximal de A es obviamente un lugar. □

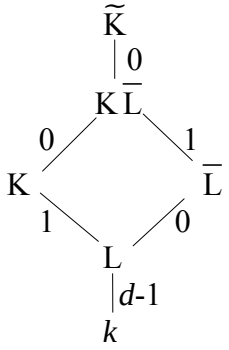
TEOREMA 3.3.26. (*de Lang de existencia de lugares racionales*) Sea $K:k$ una extensión de campos reales donde k es un campo cerrado real y K un campo de funciones de grado trascendente d. Sean $a_1,...,a_n\in K$, entonces existe un k-lugar $\varphi:K\to k\cup\{\infty\}$ tal que $\varphi(a_i)$ es finito para cada $i=1,\ldots,n$.

DEMOSTRACIÓN

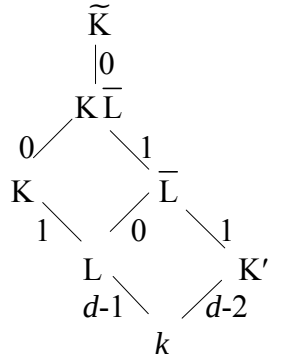
Sea d el grado de trascendencia de $K:k$. Si $d=0$, la extensión $K:k$ es algebraica finita. Como K es real y k es cerrado real, se sigue que $K=k$. Luego $id:k\to k\cup\{\infty\}$ es obviamente un k-lugar sobre k que satisface $id(a_i)<\infty$ para cada $i=1,\ldots,n$.

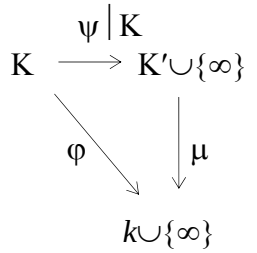
Para $d\geq 1$ la demostración se efectúa por inducción. Si $d=1$, sea $x\in K$ un elemento que se puede escribir como una suma finita de cuadrados de los a_i, $i=1,\ldots,n$; esto es, $x=\sum_{i=1}^{n} a_i^2$. El elemento x es algebraico o trascendente sobre k. Supóngase primero que x es trascendente sobre k y considérese el orden T en K construido en la demostración del teorema 3.3.23.. Sea $\varphi:K\to K'\cup\{\infty\}$ el lugar asociado con el anillo de valoración $A(k, T)$, donde $K'\cong A(k, T)/m(k, T)$ es el campo residual de $A(k, T)$; $\varphi(x)<\infty$ para todo elemento $x\in A(k, T)$ y $\varphi(x)=0$ para cada $x\in m(k, T)$. Por el corolario 3.3.24., se tiene que $\varphi:K\to k\cup\{\infty\}$ ya que $K'=k$ y $\varphi(x)<\infty$ para cada $x\in A(k, T)$. Como $x=\sum_{i=1}^{n} a_i^2\in A(k, T)$, con $a_1,\ldots,a_n\in K$, del lema 1.2.35., se sigue que $a_1,\ldots,a_n\in A(k, T)$, es decir, $\varphi(a_i)<\infty$ para cada $i=1,\ldots,n$; luego φ es el lugar. Si x es algebraico sobre k, entonces la extensión de campos $k(x):k$ es algebraica (ver proposición 3.1.6.). Como $k(x)$ es un campo real, se sigue que $k(x)=k$; de esta forma, $x\in k$. Se puede dar un k-lugar $\varphi:K\to k\cup\{\infty\}$ considerando algún elemento trascendente $x'\in K$. Como $k\subseteq A(k, T)$, entonces $\varphi(x)<\infty$ y por 1.2.35., se tiene que $\varphi(a_i)<\infty$ para cada $i=1,\ldots,n$. Considérese ahora que $d>1$. Sea T un orden de K. Por 3.2.10.,

existe una cerradura real $\widetilde{K}$ de K con respecto al orden T de K. Sea $\{t_1,\ldots,t_d\}$ una base trascendente de $K:k$, $L\subseteq K$ con $L=k(t_1,\ldots,t_{d-1})$ un campo de funciones de grado trascendente 1 y $\overline{L}$ la cerradura algebraica de L en K. Como $L\subseteq K$, $\overline{L}\subseteq\widetilde{K}$ y K, $\widetilde{K}$ son campos reales, se sigue que L y $\overline{L}$ son campos reales. Por otro lado, que L sea un campo real y no tenga extensiones algebraicas propias reales, significa que $\overline{L}$ es un campo cerrado real; así, $\overline{L}$ es una cerradura real de L en $\widetilde{K}$. Entonces la extensión $K:K\cap\overline{L}$ tiene grado de trascendencia 1 y K es un campo de funciones en una variable sobre el campo $K\cap\overline{L}$. También, la extensión $K\overline{L}:\overline{L}$ tiene grado de trascendencia 1 y él campo producto $K\overline{L}$ es un campo de funciones en una variable sobre el campo $\overline{L}$



De la proposición 3.1.26., se sigue que $grtr(K\overline{L}:\overline{L})\leq grtr(K:L)=1$ y $grtr(K\overline{L}:\overline{L})=1$ ya que si fuera cero, se tendría que $K\overline{L}:\overline{L}$ sería algebraica lo cual no puede ser posible. Como K es un campo de funciones de grado trascendente 1 sobre el campo L, $K\overline{L}$ es también un campo de funciones de grado trascendente 1 sobre $\overline{L}$. Que $grtr(K\overline{L}:\overline{L})=1$ (se satisfacen las hipótesis del teorema para el caso $d=1$) significa que existe un $\overline{L}$-lugar $\psi:K\overline{L}\to\overline{L}\cup\{\infty\}$ tal que $\psi(a_i)<\infty$ para cada $i=1,\ldots,n$. Como $\overline{L}:L$ es una extensión algebraica, $\overline{L}$ no es un campo de funciones sobre L, luego se necesita encontrar un subcampo de $\overline{L}$ que sea un campo de funciones, es decir, que satisfaga las hipótesis del teorema. Sea A el anillo de valoración asociado al lugar $\psi\,|\,K:K\to K'\cup\{\infty\}$, donde $K'=A/m$ es el campo residual de A. Como $K'\subseteq\overline{L}$, K′ es un campo real; que $A\subseteq K$ sea un dominio k-afín y K un campo de funciones ($K=qf(k[x_1,\ldots,x_d])$), significa que existen $x_1,\ldots,x_r$ con $r<d$ tal que $A=k[x_1,\ldots,x_r]$ y $K'\cong qf(k[x_1,\ldots,x_r])$. Del diagrama se observa que $r=d-2$, esto es, $grtr(K':k)=d-2$ sobre k.





Por la hipótesis de inducción, K′ tiene un k-lugar $\mu:K'\to k\cup\{\infty\}$ tal que $\mu(\psi\,|\,K(a_i))<\infty$ para cada $i=1,\ldots,n$. Como la composición de los lugares $\psi\,|\,K$ y μ es un lugar, se sigue que $\varphi:K\to k\cup\{\infty\}$, $\varphi=\mu_o(\psi\,|\,K)$ es el lugar requerido. □

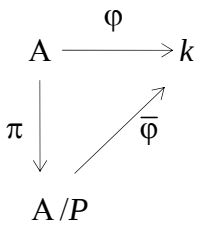
Si A es un dominio entero k-afín real, esto es, $A=k[a_1,\ldots,a_n]$ para ciertos elementos $a_1,\ldots,a_n\in A$, se sigue del teorema 1.2.18., que el campo de cocientes $K=qf(A)$ es un campo de funciones real. Si k es un campo cerrado real, entonces se satisfacen las hipótesis del teorema de existencia de lugares es racionales de Lang, es decir, existe un k-lugar $\varphi:K\to k\cup\{\infty\}$ tal que $\varphi(a_i)<\infty$ para cada $i=1,\ldots,n$. De esta forma el homomorfismo φ restringido al dominio A, $\varphi\,|\,A:A\to k$ es un homomorfismo de k-álgebras. Así, se ha demostrado el teorema del homomorfismo de Lang. □

TEOREMA 3.2.27. Si A es un dominio k-afín real con k un campo cerrado real, entonces existe un homomorfismo de k-álgebras $\varphi:A\to k$.

Como una consecuencia del teorema del homomorfismo de Lang se tienen los siguientes tres corolarios.

COROLARIO 3.3.28. Sea A un álgebra k-afín semireal con k un campo cerrado real, entonces existe un homomorfismo de k-álgebras $\varphi:A\to k$.

DEMOSTRACIÓN



Como A es semireal, A tiene un ideal primo real P (ver teorema 1.2.19.). Entonces A/P es un dominio entero real que es k-afín.[†)] Por el teorema del homomorfismo de Lang, existe un homomorfismo de k-álgebras $\bar{\varphi}:A/P\to k$. Sea $\pi:A\to A/P$ el homomorfismo canónico, entonces $\varphi:A\to k$; $\varphi=\bar{\varphi}\,o\pi$ es el homomorfismo buscado. □

COROLARIO 3.2.29. Sea A un dominio k-afín real con k un campo cerrado real y $f_1,\ldots,f_n\in A\setminus\{0\}$, entonces existe un homomorfismo de k-álgebras $\varphi:A\to k$ tal que $\varphi(f_i)\neq 0$ para toda $i=1,\ldots,n$.

DEMOSTRACIÓN

Considérese $A[\frac{1}{f_1\cdots f_n}]$. Como A es un anillo, $A[\frac{1}{f_1\cdots f_n}]$ también es un anillo ($A[\frac{1}{f_1\cdots f_n}]$ es la intersección de todos los anillos que contienen a A y $\frac{1}{f_1\cdots f_n}$). $A[\frac{1}{f_1\cdots f_n}]$ es un dominio entero ya que si $p, q\in A[\frac{1}{f_1\cdots f_n}]\setminus\{0\}$ con

$$p=a_0+a_1(\tfrac{1}{f_1\cdots f_n})+\cdots+a_r(\tfrac{1}{f_1\cdots f_n})^r \text{ y } q=b_0+b_1(\tfrac{1}{f_1\cdots f_n})+\cdots+b_s(\tfrac{1}{f_1\cdots f_n})^s,$$

[†)] Si A es afín, de $A\to A/P\to 0$, se sigue que A/P es también afín, es decir, $(A/P)[a_1,\ldots,a_n]$ con $\pi(a_i)=a_i$, $a_i\in A$; $i=1,\ldots,n$.

entonces el coeficiente $a_r\, b_s$ de $(\frac{1}{f_1\cdots f_n})^{r+s}$ en el producto pq es distinto de cero. De esta forma, $pq\neq 0$ y $A[\frac{1}{f_1\cdots f_n}]$ no tiene divisores de cero. Por otro lado, como A es un dominio k-afín, existen elementos $a_1,\ldots,a_n$ en el anillo A tal que $A=k[a_1,\ldots,a_n]$. Dado que $k[a_1,\ldots,a_n][\frac{1}{f_1\cdots f_n}]=k[a_1,\ldots,a_n,\frac{1}{f_1\cdots f_n}]$, se sigue que $A[\frac{1}{f_1\cdots f_n}]=k[a_1,\ldots,a_n,\frac{1}{f_1\cdots f_n}]$, es decir, $A[\frac{1}{f_1\cdots f_n}]$ es un dominio k-afín. Del ejemplo 1.2.10., se tiene que $A[\frac{1}{f_1\cdots f_n}]$ es un anillo real y por el teorema del homomorfismo de Lang, existe un homomorfismo $\psi:A[\frac{1}{f_1\cdots f_n}]\rightarrow k$. Considérese el homomorfismo $\varphi=\psi\,|\,A:A\rightarrow k$ $(A\subseteq A[\frac{1}{f_1\cdots f_n}])$; φ satisface que $\varphi(f_i)\neq 0$ para $i=1,\ldots,n$; si esto no fuera cierto, se tendría que

$$1=\varphi(1)=\varphi(\frac{f_1\cdots f_n}{f_1\cdots f_n})=\varphi(\frac{f_1}{f_1\cdots f_n})\cdots\varphi(\frac{f_n}{f_1\cdots f_n})=0$$

lo cual no puede ser posible. □

COROLARIO 3.3.30. Sea A un álgebra k-áfín real con k un campo cerrado real y $f_1,\ldots,f_n$ elementos en A. Si T es un orden en A tal que $f_i>_T 0$ para cada $i=1,\ldots,n$, entonces existe un homomorfismo de k-álgebras $\varphi:A\rightarrow k$ tal que $\varphi(f_i)>0$ $i=1,\ldots,n$, con respecto al único orden de k.

DEMOSTRACIÓN

Sea $\mathcal{C}(T)=T\cap -T$ el centro de T y considérese el dominio entero $\overline{A}=A/\mathcal{C}(T)$. El orden T induce un orden $\overline{T}=\{a+\mathcal{C}(T)\,|\,a\in T\}$ que satisface $\overline{T}\cap -\overline{T}=\{\overline{0}\}$. Como $\mathcal{C}(T)$ es un ideal primo real, $\overline{A}$ es un dominio k-afín real; así, $\overline{T}$ es un orden en $\overline{A}$ que se puede extender a un único orden $\overline{P}=\{\overline{(a,b)}\,(a,b)\in qf(\overline{A})\,|\,ab\in\overline{T}\}$ en K $(=qf(\overline{A}))$. Ahora, como $f_i>_T 0$, $i=1,\ldots,n$, se tiene que $f_i\notin\mathcal{C}(T)$, $i=1,\ldots,n$. Luego $f_i\neq 0$; de hecho, $f_i\in T\setminus\{0\}$, $i=1,\ldots,n$. Sea $\widetilde{K}$ la cerradura real de K con respecto al orden $\overline{P}$ y considérese $\overline{A}[\sqrt{f_1},\ldots,\sqrt{f_n},\frac{1}{f_1\cdots f_n}]$; se sabe que $\overline{A}[\frac{1}{f_1\cdots f_n}]$ es un dominio entero k-afín real (ver ejemplo 1.2.10.) y por lo tanto

$$A[\sqrt{f_1},\ldots,\sqrt{f_n},\ \frac{1}{f_1\cdots f_n}]=A[\frac{1}{f_1\cdots f_n}][\sqrt{f_1},\ldots,\sqrt{f_n}]$$

es un dominio entero k-afín real. Por el teorema del homomorfismo de Lang, existe un homomorfismo

$$\psi:A[\sqrt{f_1},\ldots,\sqrt{f_n},\ \frac{1}{f_1\cdots f_n}]\rightarrow k.$$

Considérese el homomorfismo restricción $\psi|\overline{A}:\overline{A}\to k$ y la función proyección $\pi:A\to\overline{A}$, entonces la función $\varphi:A\to k$ definida como $\varphi=(\psi|\overline{A})\circ\pi$ es el homomorfismo buscado, donde $\varphi(f_i)=(\psi|\overline{A}\circ\pi)(\overline{f_i})=\psi|\overline{A}(\overline{f_i})=\psi|\overline{A}(\sqrt{f_i})\psi|\overline{A}(\sqrt{f_i})\in\overline{P}\cap k$. Luego, $\varphi(f_i)>0$ en el único orden de k. □

Sea k un campo cerrado real y $k[x_1,\ldots,x_n]$ el anillo de polinomios en n indeterminadas con coeficientes en k. Dado un polinomio $f\in k[x_1,\ldots,x_n]$, $f(x)=\sum a_I x^I$ se define la **función polinomial** asociada al polinomio f, como la función $f:k^n\to k$, $f(b)=\sum a_I b^I$, donde $k^n=\{(a_1,\ldots,a_n)|\ a_i\in k,\ 1\le i\le n\}$ es el espacio afín. Un polinomio $f\in k[x_1,\ldots,x_n]$ es **semidefinido positivo** (o la función polinomial es no negativa) si $f(x_1,\ldots,x_n)\ge 0$ para toda $(a_1,\ldots,a_n)\in k^n$. También se dice que un polinomio $f\in k[x_1,\ldots,x_n]$ es **indefinido,** (o la función polinomial cambia de signo) si existen elementos $(a_1,\ldots,a_n)$, $(b_1,\ldots,b_n)\in k^n$ tal que $f(a_1,\ldots,a_n)<0<f(b_1,\ldots,b_n)$ donde la relación de orden $<$ está referida al único orden de k, es decir, f es indefinido si no es semidefinido positivo ni semidefinido negativo.

A continuación se prueba el resultado de Artin acerca del problema 17 de Hilbert, enunciado al final del capítulo 2, como una consecuencia del corolario 3.3.30..

TEOREMA 3.3.31. Sea k un campo cerrado real y $f\in k[x_1,\ldots,x_n]$ un polinomio semidefinido positivo, entonces f es una suma finita de cuadrádos en el campo $k(x_1,\ldots,x_n)$.

DEMOSTRACIÓN

Supóngase que $f\notin\sum k(x_1,\ldots,x_n)^2$. Por el corolario 3.3.30., existe un homomorfismo de k-álgebras $\varphi:k[x_1,\ldots,x_n]\to k$ tal que $\varphi(-f)>0$. Sea $\varphi(x_i)=a_i$, $a_i\in k$; para cada $i=1,\ldots,n$, entonces

$$\begin{aligned} f(a_1,\ldots,a_n)&=f(\varphi(x_1),\ldots,\varphi(x_n))\\ &=\sum a_I\varphi(x)^I\\ &=\sum a_I\varphi(x^I)\\ &=\sum\varphi(a_I x^I)\\ &=\varphi(\sum a_I x^I)\\ &=\varphi(f(x_1,\ldots,x_n))<0 \end{aligned}$$

Esto último contradice el hecho de que f es semidefinido positivo. □

Sea k un campo cerrado real y $f\in k[x_1,\ldots,x_n]\setminus\{0\}$ un polinomio semidefinido positivo; por 3.3.31.,

$$f=(p_1/q_1)^2+\cdots+(p_m/q_m)^2,$$

con $p_i/q_i\in k(x_1,\ldots,x_n)$, $i=1,\ldots,m$. Si $f_1=p_1q_2\cdots q_m,\ldots,f_m=p_mq_1\cdots q_{m-1}$ y $h=q_1\ldots q_m$, entonces $h^2f=f_1^2+\cdots+f_m^2$. Luego si h tiene grado mínimo, se tiene la siguiente

OBSERVACIÓN 3.3.32. Sean f, $h\in k[x_1,\ldots,x_n]\setminus\{0\}$ con f un polinomio semidefinido positivo, irreducible y h un polinomio de grado mínimo que satisfacen $h^2f=f_1^2+\cdots+f_m^2$. Entonces los polinomios f_i no son todos divisibles por f, $i=1,\ldots,m$.

DEMOSTRACIÓN

Supóngase que existen m polinomios $g_1,\ldots,g_m\in k[x_1,\ldots,x_n]$ con $f_i=fg_i$, $i=1,\ldots,m$. Dado que $h^2f=f_1^2+\cdots+f_m^2$, se sigue que $h^2f=f^2g_1^2+\cdots+f^2g_m^2$; esto es, $h^2f=f^2(g_1^2+\cdots+g_m^2)$ y $h^2=f(g_1^2+\cdots+g_m^2)$, luego $f\mid h^2$. Dado que f es irreducible, se tiene que $f\mid h$, esto es, existe $h_0\in k[x_1,\ldots,x_n]$ tal que $h=h_0f$; luego $h_0^2f^2=f(g_1^2+\cdots+g_m^2)$ y $h_0^2f=g_1^2+\cdots+g_m^2$. Esto último contradice la elección del grado mínimo de h. □

LEMA 3.3.33. Sea k un campo cerrado real y $f\in k[x_1,\ldots,x_n]\setminus\{0\}$ un polinomio irreducible. Si $\langle f\rangle$ es un ideal real, entonces f es indefinido.

DEMOSTRACIÓN

Supóngase que f no es un polinomio indefinido; entonces f es semidefinido positivo o semidefinido negativo. Si f es semidefinido positivo[†)]; por 3.3.32., existen polinomios $f_1,\ldots,f_m\in k[x_1,\ldots,x_n]$ tal que no todos son divisibles por f. Entonces si $f_1^2+\cdots+f_m^2=0$ en $k[x_1,\ldots,x_n]/\langle f\rangle$, $k[x_1,\ldots,x_n]/\langle f\rangle$ no es real porque no todos los f_i son cero, lo cual contradice el hecho de que $\langle f\rangle$ sea un ideal real. □

Sea F un campo ordenado y T un orden en F, se puede definir una topología en F, denominada **topología intervalo**, denotada τ_F donde la noción de intervalo en F se introduce en forma similar que en $\mathbb{R}$; es decir, si a, $b\in$F con $a<_T b$, entonces

$(a\ ,\ b):=\{x\in\text{F}\mid a<_T x<_T b\}$
$[a\ ,\ b):=\{x\in\text{F}\mid a\le_T x<_T b\}$
$(a\ ,\ b]:=\{x\in\text{F}\mid a<_T x\le_T b\}$
$[a\ ,\ b]:=\{x\in\text{F}\mid a\le_T x\le_T b\}$
$(a\ ,\ +\infty):=\{x\in\text{F}\mid x>_T a\}$
$[a\ ,\ +\infty):=\{x\in\text{F}\mid x\ge_T a\ \}$
$(-\infty\ ,\ b):=\{x\in\text{F}\mid x<_T b\}$
$(-\infty\ ,\ b]:=\{x\in\text{F}\mid x\le_T b\}$ etc.

Si $B_x=\{(a\ ,\ b)\mid a<_T x<_T b\}$; una base para esta topología viene dada por la familia $\mathcal{B}_x=\cup\{B_x\mid x\in\text{F}\}$. Algunos de los resultados de $\mathbb{R}$ con su topología usual que también se cumplen en el espacio $(\text{F}\ ,\ \tau_F)$ y que serán de utilidad aquí son los siguientes.

PROPOSICIÓN 3.3.34. Sea F un campo ordenado y T un orden de F. Entonces el espacio $(\text{F}\ ,\ \tau_F)$ es Hausdörff.

DEMOSTRACIÓN

Sean x, y dos elementos en F y supóngase que $x<_T y$. Si existe un punto z en F tal

[†)] Si f es semidefinido negativo, se elige $-f$ que es semidefinido positivo.

que $x<_T z<_T y$, entonces los básicos $U=\{w\in F \mid w<_T z\}$ y $V=\{w\in F \mid w>_T z\}$ también satisfacen que $U\cap V=\emptyset$ y $x\in U$, $y\in V$. Así, F con la topología intervalo es un espacio topológico de Hausdörff. □

LEMA 3.3.35. Sea F un campo ordenado y F(t) el campo de funciones racionales. Entonces F(t)\F es denso con respecto a la topología intervalo en F(t).

DEMOSTRACIÓN

Considérese un intervalo abierto $(f, f')_T$ en la topología intervalo de F(t), con respecto a un orden T en F(t), donde $f<_T f'$, $f, f'\in F$. Por demostrar que $(f, f')_T\cap(F(t)\backslash F)\neq\emptyset$. Si $(f+f')/2\in F(t)\backslash F$ la demostración termina. Si $(f+f')/2\in F$, es decir, si $(f+f')/2=c_0$, entonces por una traslación se puede suponer que $c_0=0$. Considérese intervalos abiertos de la forma $(-g, g)_T$ con $g\in T$. Si $g\in F(t)\backslash F$, entonces bastará tomar $h=g/2$, $h\in(-g, g)_T\cap(F(t)\backslash F)$ y $(-g, g)_T\cap(F(t)\backslash F)\neq\emptyset$. Si $g\in F$, se puede suponer sin perdida de generalidad que $t\in T$. De esta forma $g^{-1}+t\in T$ y $g^{-1}<_T g^{-1}+t$. Luego $0<_T(g^{-1}+t)^{-1}<_T g$, esto es, $g^{-1}+t\in(-g, g)_T$ y se puede tomar $h=(g^{-1}+t)^{-1}\notin F$. □

Para terminar esta sección se demuestra el teorema del encaje de Lang.

TEOREMA 3.3.36. Sea K : k una extensión de campos reales con k un campo cerrado real y K un campo de funciones de grado trascendente d. Sea F un campo cerrado real de grado trascendente $\geq d$ que contiene a k, entonces existe un k-encaje $\varphi: K\to F$.

DEMOSTRACIÓN

Sea $\{x_1,\ldots,x_d\}$ una base trascendente de K sobre k. Escribiendo $K=k(x_1,\ldots,x_d, \alpha)$, donde $\alpha\in K$ es un elemento algebraico sobre $F':=k(x_1,\ldots,x_d)$, entonces existe un polinomio irreducible $f(z)\in F'[z]$ único salvo un factor constante en F′ tal que $f(\alpha)=0$ y es de grado mínimo mayor o igual que 1 en F′[z], esto es, $f(z)$ es el polinomio minimal de α sobre F′; así, $K = qf(k[x_1,...,x_n,z]/<f>)$. Como K es un campo real, por el lema 3.3.33., f es un polinomio indefinido sobre k, entonces existen puntos $(a_1,\ldots,a_d, b_1)$, $(a_1,\ldots,a_d, b_2)\in k^{d+1}$ tal que $f(a_1,\ldots,a_d, b_1)<0<f(a_1,\ldots,a_d, b_2)$. Sea $t_1\in F$ un elemento trascendente sobre k y considérese a $k(t_1)$ con orden $T_1=T\cap k(t_1)$ (la restricción de T a $k(t_1)$). Como $k(t_1)\backslash k$ es denso en $k(t_1)$ con respecto a la topología intervalo de T_1 (véase lema 3.3.35.) y por la continuidad de f sobre $k(t_1)$ con respecto a la topología intervalo de T_1, se sigue que existe $y_1\in k(t_1)\backslash k$ tal que

$$f(y_1, a_2,\ldots,a_d, b_1)<0<f(y_1, a_2,\ldots,a_d, b_2).$$

Sea ahora L_1 la cerradura algebraica de $k(y_1)$ en F y sea $t_2\in F$ un elemento trascendente sobre L_1. Considérese a $L_1(t_2)$ con orden $T_2=T_1\cap L_1(t_2)$ la restricción de T_1 a $L_1(t_2)$. Como $L_1(t_2)\setminus L_1$ es denso en $L_1(t_2)$ (con la topología intervalo de T_2) y por la continuidad de f sobre $L_1(t_2)$ con respecto a la topología intervalo de T_2, se sigue que existe $y_2\in L_1(t_2)\backslash L_1$ tal que

$$f(y_1, y_2, a_3,\ldots,a_d, b_1)<0<f(y_1, y_2, a_3,\ldots,a_d, b_2).$$

Continuando con este proceso se puede construir $y=(y_1, y_2,\ldots,y_d)\in F^d$ (como $grtr(F)\geq d$, la construcción está garantizada hasta llegar a y_d) tal que

$$f(y_1, y_2,\ldots,y_d, b_1)<0<f(y_1, y_2,\ldots,y_d, b_2) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(*)$$

con $y_1, y_2,\ldots,y_d$ algebraicamente independientes sobre el campo base k. Como F es un campo cerrado real, de (*) se sigue que $f(y_1, y_2,\ldots,y_d, \beta)=0$ para algún $\beta\in F$. Así, se tiene un k-isomorfismo $\varphi: K \to F$; $x \mapsto y_i$ y $\alpha \mapsto \beta$. □

3.4. EL TEOREMA DE LOS CEROS DE HILBERT REAL.

Si k es un campo, el **espacio afín** k^n es el conjunto $k^n=\{(a_1,\ldots,a_n) \mid a_i\in k,\ 1\leq i\leq n\}$ de todas las n-adas de elementos de k. Sean $f_1,\ldots,f_s$ polinomios en el anillo $k[x_1,\ldots,x_n]$; como se recordará, el conjunto en el espacio afín k^n; $\mathbb{V}(f_1,\ldots,f_s)=\{(a_1,\ldots,a_n)\in k^n \mid f_i(a_1,\ldots,a_n)=0;\ i=1,2,\ldots,s\}$ es la **variedad afín** definida por los polinomios $f_1,\ldots,f_s$. Si V_1 y V_2 en k^n son variedades afines, entonces la unión $V_1\cup V_2$ e intersección $V_1\cap V_2$ también son variedades afines.

Sea I un ideal en $k[x_1,\ldots,x_n]$, se define la **variedad afín del ideal** I escrito $\mathbb{V}(I)$ como el subconjunto en k^n, $\mathbb{V}(I)=\{(a_1,\ldots,a_n)\in k^n \mid f(a_1,\ldots,a_n)=0$ para cada $f\in I\}$. Un subconjunto X en k^n es un **conjunto algebraico** si $X=\mathbb{V}(I)$ para algún ideal I en el anillo $k[x_1,\ldots,x_n]$. Claramente $\mathbb{V}(0)=k^n$ y $\mathbb{V}\big(k[x_1,\ldots,x_n]\big)=\varnothing$.

OBSERVACIÓN 3.4.1. Sean I y J ideales en el anillo $k[x_1,\ldots,x_n]$, entonces

i) Si $I\subseteq J$, $\mathbb{V}(J)\subseteq\mathbb{V}(I)$.
ii) $\mathbb{V}(IJ)=\mathbb{V}(I)\cup\mathbb{V}(J)$.
iii) $\mathbb{V}(I\cap J)=\mathbb{V}(I)\cup\mathbb{V}(J)$.
iv) $\mathbb{V}(\sum I_\lambda)=\cap\mathbb{V}(I_\lambda)$ con $\lambda\in\Lambda$.

DEMOSTRACIÓN.

i) Sea $p\in\mathbb{V}(J)$, entonces $f(p)=0$ para cada $f\in J$, luego $f(p)=0$ para toda $f\in I$. Así, $p\in\mathbb{V}(I)$. *ii*) Sea $p\in\mathbb{V}(IJ)$, entonces $f(p)g(p)=0$ para cada $f\in I$ y $g\in J$. Si $f(p)=0$ para toda $f\in I$, se sigue que $p\in\mathbb{V}(I)$. Si $f(p)\neq 0$ para alguna $f\in I$, se tendrá que $g(p)=0$ para cada $g\in J$ y $p\in\mathbb{V}(J)$. En cualesquiera de las dos situaciones, se tiene que $p\in\mathbb{V}(I)\cup\mathbb{V}(J)$. Recíprocamente, dado que $IJ\subseteq I$ e $IJ\subseteq J$, se sigue que $\mathbb{V}(I)\subseteq\mathbb{V}(IJ)$ y $\mathbb{V}(J)\subseteq\mathbb{V}(IJ)$. Luego $\mathbb{V}(I)\cup\mathbb{V}(J)\subseteq\mathbb{V}(IJ)$. *iii*) Sea $p\in\mathbb{V}(I)\cup\mathbb{V}(J)$, entonces $p\in\mathbb{V}(I)$ o $p\in\mathbb{V}(J)$. Esto significa que $f(p)=0$ para cada $f\in I$ o $f(p)=0$ para todo $f\in J$; luego $f(p)=0$ para todo $f\in I\cap J$. Así, $p\in\mathbb{V}(I\cap J)$ y $\mathbb{V}(I)\cup\mathbb{V}(J)\subseteq\mathbb{V}(I\cap J)$. Recíprocamente, dado que $IJ\subseteq I\cap J$, se tiene que $\mathbb{V}(I\cap J)\subseteq\mathbb{V}(IJ)=\mathbb{V}(I)\cup\mathbb{V}(J)$. *iv*) Si $p\in\mathbb{V}(\sum I_\lambda)$, entonces $p\in\mathbb{V}(I_\lambda)$ para toda $\lambda\in\Lambda$ ya que $I_\lambda\subseteq\sum I_\lambda$ para cada $\lambda\in\Lambda$; luego $p\in\cap\mathbb{V}(I_\lambda)$. Ahora, considérese $p\in\cap\mathbb{V}(I_\lambda)$ con $\lambda\in\Lambda$ y sea h un polinomio en $\sum I_\lambda$, entonces existen polinomios $f_\lambda\in I_\lambda$ tal que $h=\sum f_\lambda$. Como $p\in\mathbb{V}(I_\lambda)$ con $\lambda\in\Lambda$, se sigue que $f_\lambda(p)=0$. Como h es arbitraria, se tiene que $p\in\mathbb{V}(\sum I_\lambda)$. □

De lo anterior, se obtiene que los subconjuntos algebraicos de k^n, constituyen los conjuntos cerrados de una topología en k^n denominada **topología de Zariski**.

Sea X un subconjunto en el espacio afín k^n; se define el ideal de X, escrito $\mathbb{I}(X)$ como el conjunto $\mathbb{I}(X)=\{f\in k[x_1,\ldots,x_n] \mid f(a_1,\ldots,a_n)=0$, para cada $(a_1,\ldots,a_n)\in X\}$. Claramente $\mathbb{I}(X)$ es un ideal en el anillo de polinomios $k[x_1,\ldots,x_n]$.

OBSERVACIÓN 3.4.2. Sean X, Y subconjuntos de k^n e I un ideal en $k[x_1,\ldots,x_n]$

i) Si $X\subseteq Y$, entonces $\mathbb{I}(Y)\subseteq\mathbb{I}(X)$

ii) $X\subseteq\mathbb{V}(\mathbb{I}(X))$

iii) $X=\mathbb{V}(\mathbb{I}(X)) \Leftrightarrow$ X es un conjunto algebraico

iv) $I\subseteq\mathbb{I}(\mathbb{V}(I))$

DEMOSTRACIÓN.

i) Sea $f\in\mathbb{I}(Y)$, entonces $f(p)=0$ para todo $p\in Y$. Como $X\subseteq Y$, se sigue que $f(p)=0$ para cada $p\in X$; luego $f\in\mathbb{I}(X)$. *ii*) Sea $p\in X$, entonces $f(p)=0$ para cada $f\in\mathbb{I}(X)$, esto significa que $p\in\mathbb{V}(\mathbb{I}(X))$. *iii*) Si $X=\mathbb{V}(\mathbb{I}(X))$, como $\mathbb{I}(X)$ es un ideal en $k[x_1,\ldots,x_n]$, se sigue directamente que X es un conjunto algebraico en k^n. Recíprocamente, si $X=\mathbb{V}(I)$ es un conjunto algebraico, entonces $\mathbb{I}(X)$ es un ideal en $k[x_1,\ldots,x_n]$ que contiene a I, luego $\mathbb{V}(\mathbb{I}(X))\subseteq\mathbb{V}(I)=X$. *iv*) Si $f\in I$, entonces $f(p)=0$ para cada $p\in\mathbb{V}(I)$, es decir, $f\in\mathbb{I}(\mathbb{V}(I))$. □

Se observa que la igualdad en la observación 3.4.2. *iv*) ($I\subseteq\mathbb{I}(\mathbb{V}(I))$) no se cumple en general. En efecto, considérese el ideal $I=\langle x^2, y^2\rangle\subsetneq\mathbb{R}[x, y]$. Claramente se observa que $\langle x^2, y^2\rangle\subsetneq\mathbb{I}(\mathbb{V}(\langle x^2, y^2\rangle))$ (ver 3.4.2*iii*)). Primero se verá quien es el ideal $\mathbb{I}(\mathbb{V}(\langle x^2, y^2\rangle))$. Para $x^2=0$ y $y^2=0$, se tiene que $\mathbb{V}(\langle x^2, y^2\rangle)=\{(0, 0)\}$ es la variedad que consiste del origen de coordenadas en $\mathbb{R}^2$. El ideal $\mathbb{I}(\{(0, 0)\})$ consiste de todos los polinomios que se anulan en el origen de $\mathbb{R}^2$. Se afirma que $\mathbb{I}(\mathbb{V}(\langle x^2, y^2\rangle))=\langle x, y\rangle$. En efecto, si $f\in\langle x, y\rangle$ y h_1, h_2 están en el anillo $\mathbb{R}[x, y]$, entonces $f(x, y)=h_1(x, y)x+h_2(x, y)y$. Obviamente $f(x, y)$ se anula en (0 , 0); entonces se tiene $f(x, y)\in\mathbb{I}(\mathbb{V}(\langle x^2, y^2\rangle))$. Si $f(x, y)\in\mathbb{I}(\{(0, 0)\})$, luego $f(x,y)=\sum_{ij} a_{ij}x^i y^j$ se anula en el origen de $\mathbb{R}^2$. Esto significa que $a_{00}=f(0, 0)=0$ y se sigue que

$$f(x, y)=a_{00}+\sum_{i,j\neq 0} a_{ij}x^i y^j = 0 + (\sum_{i>0,\, j} a_{ij}x^{i-1}y^j)x + (\sum_{i,\, j>0} a_{ij}x^i y^{j-1})y\in\langle x,y\rangle;$$

entonces se obtiene $\mathbb{I}(\mathbb{V}(\langle x^2, y^2\rangle))=\langle x, y\rangle$. Además se tiene $\langle x^2, y^2\rangle\subsetneq\langle x, y\rangle$ ya que $p\notin\langle x^2, y^2\rangle$ pues en todo polinomio de la forma $f(x, y)=h_1(x, y)x+h_2(x, y)y$, cada monomio tiene al menos grado igual a dos. Mas adelante, cuando se enuncie el teorema fuerte de los ceros de Hilbert, quedará claro que la igualdad se da si el ideal I es un ideal radical. Si en 3.4.2.*i*), X y Y son conjuntos algebraicos, se tiene

PROPOSICIÓN 3.4.3. Si X y Y son conjuntos algebraicos en k^n. Entonces $X\subseteq Y$, si y sólo si $\mathbb{I}(Y)\subseteq\mathbb{I}(X)$.

DEMOSTRACIÓN ($\Rightarrow$)

Ver 3.4.2.*i*).

($\Leftarrow$)

Por la observación 3.4.2.*ii*), se tiene que $X=\mathbb{V}(\mathbb{I}(X))$ y $Y=\mathbb{V}(\mathbb{I}(Y))$. Si $p\in\mathbb{V}(\mathbb{I}(X))$, se sigue que $f(p)=0$ para cada $f\in\mathbb{I}(X)$. Como $\mathbb{I}(Y)\subseteq\mathbb{I}(X)$, se tiene que $f\in\mathbb{I}(Y)$; luego $X=\mathbb{V}(\mathbb{I}(X))\subseteq\mathbb{V}(\mathbb{I}(Y))=Y$. □

Un conjunto algebraico X en k^n es **irreducible** si siempre que $X=X_1\cup X_2$, con X_1, X_2 subconjuntos algebraicos propios de X en k^n, entonces $X_1=X$ o $X_2=X$; es decir, no existe una descomposición de X como una unión de dos subconjuntos algebraicos propios.

OBSERVACIÓN 3.4.4. Sea X en k^n un conjunto algebraico, entonces las siguientes afirmaciones son equivalentes.

i) X es irreducible

ii) Cualesquier dos conjuntos abiertos U_1, U_2 no vacíos en X satisfacen que $U_1\cap U_2\neq\emptyset$

iii) Todo subconjunto abierto no vacío U en X es denso en X

DEMOSTRACIÓN

i) $\Rightarrow$ *ii*) Dado que $X=(X\backslash U_1)\cup(X\backslash U_2)$ si y sólo si $U_1\cap U_2=\emptyset$, el resultado se sigue. *ii*) $\Rightarrow$ *iii*) Ya que un subconjunto de un espacio topológico es denso si y sólo si él intersecta a todo abierto en el espacio, se sigue que $U\cap U'\neq\emptyset$ para todo abierto U' en X. *iii*) $\Rightarrow$ *i*) Se sigue directamente de la definición de densidad. □

OBSERVACIÓN 3.4.5. Sea X en k^n un conjunto algebraico e $\mathbb{I}(X)$ el ideal de X. Entonces X es irreducible si y sólo si $\mathbb{I}(X)$ es primo.

DEMOSTRACIÓN ($\Rightarrow$)

Sea $fg\in\mathbb{I}(X)$, si $X_1=X\cap\mathbb{V}(f)$ y $X_2=X\cap\mathbb{V}(g)$; X_1 y X_2 son variedades afines ya que la intersección de variedades afines es una variedad afín. Dado que $fg\in\mathbb{I}(X)$, se sigue que $X=X_1\cup X_2$. Como X es irreducible, se tiene que $X=X_1$ o $X=X_2$. Si $X=X\cap\mathbb{V}(f)$, se sigue que $f(x)=0$ para cada $x\in X$; luego $f\in\mathbb{I}(X)$ e $\mathbb{I}(X)$ es un ideal primo.

($\Leftarrow$)

Sea $X=X_1\cup X_2$ y supóngase que $X\neq X_1$. Como $X_2\subseteq X$, se sigue que $\mathbb{I}(X)\subseteq\mathbb{I}(X_2)$. Ahora, dado que $X_1\subsetneq X$, se tiene que $\mathbb{I}(X)\subsetneq\mathbb{I}(X_1)$. Tomando $f\in\mathbb{I}(X_1)\backslash\mathbb{I}(X)$ y $g\in\mathbb{I}(X_2)$, entonces $fg\in\mathbb{I}(X)$. Como $\mathbb{I}(X)$ es un ideal primo y $f\notin\mathbb{I}(X)$ se sigue que $g\in\mathbb{I}(X)$; luego $\mathbb{I}(X_2)\subseteq\mathbb{I}(X)$. Así, $\mathbb{I}(X)=\mathbb{I}(X_2)$ y $X=X_2$. Por lo tanto X es irreducible. □

Sea $K:k$ una extensión de campos e I un ideal en $k[x_1,\ldots,x_n]$; se denota por $I\mathrm{K}[x_1,\ldots,x_n]$ el ideal generado por I en el anillo $\mathrm{K}[x_1,\ldots,x_n]$. En el caso en que el ideal I es primo, se tiene la siguiente

OBSERVACIÓN 3.4.6. Sea $\bar{k}$: k una extensión de campos con $\bar{k}$ $(=k(\sqrt{-1}))$ la cerradura algebraica de k. Si P es un ideal primo real en $k[x_1,\ldots,x_n]$, entonces $P\bar{k}[x_1,\ldots,x_n]$ es un ideal primo en $\bar{k}[x_1,\ldots,x_n]$ y $\mathbb{V}(P\bar{k}[x_1,\ldots,x_n])$ es un conjunto algebraico irreducible sobre $\bar{k}$.

DEMOSTRACIÓN

Primero se probará que $P\bar{k}[x_1,\ldots,x_n]$ es un ideal primo. Sean f, $g\in\bar{k}[x_1,\ldots,x_n]$; $f=f_1+\sqrt{-1}f_2$ y $g=g_1+\sqrt{-1}g_2$ con f_1, f_2, g_1 y $g_2\in k[x_1,\ldots,x_n]$ tal que $fg\in P\bar{k}[x_1,\ldots,x_n]$. Como $(f_1g_1-f_2g_2)+\sqrt{-1}(f_1g_2+f_2g_1)\in P\bar{k}[x_1,\ldots,x_n]$, donde $(f_1g_1-f_2g_2)\in P$, y $(f_1g_2+f_2g_1)\in P$; se tiene que $g_1(f_1g_1-f_2g_2)+g_2(f_1g_2+f_2g_1)\in P$ y $g_1(f_1g_2+f_2g_1)-g_2(f_1g_1-f_2g_2)\in P$; luego $f_1(g_1^2+g_2^2)\in P$ y $f_2(g_1^2+g_2^2)\in P$. Supóngase que $f\notin\in P\bar{k}[x_1,\ldots,x_n]$, entonces $f_1\notin$P o $f_2\notin P$. En cualesquiera de las dos situaciones, $g_1^2+g_2^2\in$P. Como P es un ideal real, se sigue que g_1, $g_2\in P$ y $g\in P\bar{k}[x_1,\ldots,x_n]$. Similarmente, si se supone que $g\notin P\bar{k}[x_1,\ldots,x_n]$, se obtiene que $f\in P\bar{k}[x_1,\ldots,x_n]$. Por lo tanto $P\bar{k}[x_1,\ldots,x_n]$ es un ideal primo en $\bar{k}[x_1,\ldots,x_n]$. La segunda parte se sigue de 3.4.5.. □

Antes de pasar a establecer los teoremas (clásicos) de los ceros de Hilbert, se darán algunos resultados necesarios para su demostración.

PROPOSICIÓN 3.4.7. Sean A y B anillos con A⊆B. Si B es finitamente generado como un A-módulo y x es un elemento en B, entonces x satisface que $a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n=0$ con $a_i\in$A, $i=1,2,\ldots,n$-1.

DEMOSTRACIÓN

Como B es finitamente generado como un A-módulo, existen elementos $b_1,\ldots,b_n$ en B tal que $B=b_1A+\cdots+b_nA$. Para cada $i=1,\ldots,n$; $b_ix\in$B, luego existen elementos $a_{ij}\in$A, $i,j=1,2,\ldots,n$ tal que $b_ix=\sum_{j=1}^{n}a_{ij}b_j$. Esto puede escribirse como $\sum_{i=1}^{n}\sum_{j=1}^{n}(\delta_{ij}x-a_{ij})b_j=0$, donde δ_{ij} es igual a 1 si $i=j$ y cero si $i\neq j$; $i,j=1,2,\ldots,n$ (es decir, δ_{ij} son las entradas de la matriz identidad). Sea $\mathbb{M}$ la matriz con entradas $\mathbb{M}_{ij}=\delta_{ij}x-a_{ij}$; $\mathbb{b}$ la matriz columna con entradas b_i y $Adj(\mathbb{M})$ o $\mathbb{M}^{Adj}$ la matriz adjunta de $\mathbb{M}$. Dado que $\mathbb{M}\mathbb{b}=0$ y $\mathbb{M}^{Adj}\mathbb{M}\mathbb{b}=det(\mathbb{M})\mathbb{I}\mathbb{b}$, se sigue que $det(\mathbb{M})\mathbb{b}=0$ para cada $i=1,2,\ldots,n$. Como $1\in$B es una combinación lineal de los b_i, $i=1,\ldots,n$, se tiene que $det\mathbb{M}=det\mathbb{M}1=0$. Así, se sigue que $det(\delta_{ij}x-a_{ij})=0$. □

LEMA 3.4.8. Si A es un subanillo de un campo K y K es finitamente generado como un A-módulo, entonces A es un campo.

DEMOSTRACIÓN

Para cada $a\in$A con $a\neq0$, el inverso $a^{-1}\in$K existe. Por la proposición 3.4.7., a^{-1} satisface $a_0+a_1a^{-1}+\cdots+a_{n-1}a^{-(n-1)}+a^{-n}=0$ con $a_i\in$A, $i=1,2,\ldots,n$. Multiplicando esta igualdad

por a^{n-1}, se tiene que $a_0a^{n-1}+a_1a^{n-2}+\cdots+a_{n-1}+a^{-1}=0$, luego $a^{-1}=-(a_0a^{n-1}+a_1a^{n-2}+\cdots+a_{n-1})\in$A. Por lo tanto A es un campo. □

PROPOSICIÓN 3.4.9. Sea k un campo infinito y A=$k[a_1,\ldots,a_n]$ una k-álgebra afín. Si A es un campo, entonces A$:k$ es una extensión algebraica.

DEMOSTRACIÓN

Supóngase que $y_1,\ldots,y_m$ son algebraicamente independientes y sea B=$k[y_1,\ldots,y_m]$. Entonces A es finitamente generado como un B-módulo. Como A es un campo, del lema 3.4.8., se sigue que B es un campo; luego m=0 y A es una k-álgebra afín, es decir, A$:k$ es una extensión finita y por lo tanto algebraica. □

PROPOSICIÓN 3.4.10. Sea k un campo algebraicamente cerrado y A=$k[x_1,\ldots,x_n]$ una álgebra k-afín. Entonces un ideal m en A es maximal si y sólo si existen elementos $a_1,...,a_n\in k$ tal que m=$<x_1-a_1,\ldots,x_n-a_n>$.

DEMOSTRACIÓN ($\Rightarrow$)

Sea m un ideal maximal de la k-álgebra afín A, $f:k\to$ A el homomorfismo de inclusión y π:A$\to$A/m el homomorfismo natural. Entonces el homomorfismo composición $\varphi:k\to$ A/m es un homomorfismo de campos[†)] ya que A es una k-álgebra afín, A/m es un campo, y es finitamente generado como k-álgebra; sus generadores son las imágenes de los x_i, i=1, 2,…, n. Por la proposición 3.4.9., A/m es una extensión algebraica sobre k. Como k es algebraicamente cerrado, A/m=k; luego φ es un isomorfismo. Ahora, para cada $i=1,2,...,n$, $x_i\in$A le corresponde un elemento $b_i\in$A/m. Tomando $a_i=\varphi^{-1}(b_i)$, se tiene que $x_i-a_i\in Ker(\varphi)=m$. De esto se sigue que existen elementos $a_1,...,a_n\in k$ tal que $<x_1-a_1,...,x_n-a_n>\subseteq m$.

($\Leftarrow$)

Considérese el epimorfismo φ: $k[x_1,\ldots,x_n]\to k$; $f\mapsto f(a_1,\ldots,a_n)$ para elementos $a_1,\ldots,a_n$ en k. Como $Ker(\varphi)$=$<x_1-a_1,\ldots,x_n-a_n>$; por el primer teorema del isomorfismo, se sigue que

$$k[x_1,\ldots,x_n]/<x_1-a_1,\ldots,x_n-a_n>\cong k,$$

luego m=$<x_1-a_1,\ldots,x_n-a_n>$ es maximal. □

Se observa que si k no fuera algebraicamente cerrado, esta condición suficiente sería falsa. Por ejemplo el ideal $<1+x^2>$ en $\mathbb{R}[x]$ es tal que el maximal no corresponde a un punto en $\mathbb{R}$. También, si $f\in k[x]$ es un polinomio no constante que no tiene raíces en k, entonces el ideal propio generado por f, I=$<f>\subseteq k[x]$ satisface que $\mathbb{V}(I)=\{p\in k\mid f(p)=0\}=\varnothing$. Por ejemplo, los polinomios 1, $1+x^2$, $1+x^2+x^4$, $1+x^2+x^4+x^6$ etc en el anillo $\mathbb{R}[x]$ no tienen raíces reales y las variedades $\mathbb{V}(<1>)$, $\mathbb{V}(<1+x^2>)$, $\mathbb{V}(<1+x^2+x^4>)$ etc, son conjuntos vacíos. Los

[†)] φ es inyectivo

polinomios $1+x^2+y^2$, $1+x^2+y^4$, $1+x^2+y^6$ etc, en el anillo $\mathbb{R}[x\ ,\ y]$ dan ideales diferentes los cuales corresponden a conjuntos algebraicos que son vacíos. Si el campo k es algebraicamente cerrado, todo polinomio no constante en $k[x]$ tiene una raíz en k. En este caso, $\mathbb{V}(<f>)=\varnothing$ si y sólo si $<f>=<1>$. En el caso general, la cerradura algebraica de k, $\overline{k}$ es suficiente para garantizar que el único ideal I en $k[x_1,\ldots,x_n]$ que satisface $\mathbb{R}(I)=\varnothing$ es el ideal $I=k[x_1,\ldots,x_n]$, es decir,

TEOREMA 3.4.11. (*débil de los ceros de Hilbert*). Sea k un campo algebraicamente cerrado. Si I es un ideal propio del anillo $k[x_1,\ldots,x_n]$, entonces $\mathbb{V}(I)\neq\varnothing$.

DEMOSTRACIÓN

Si I es un ideal propio de $k[x_1,\ldots,x_n]$, por el corolario 1.1.17., existe un ideal maximal m de $k[x_1,\ldots,x_n]$ tal que $I\subseteq m$. Por la proposición anterior, $m=<x_1-a_1,\ldots,x_n-a_n>$ con $a_1,\ldots,a_n\in k$. Dado que $I\subseteq m$, se tiene que $f(a_1,\ldots,a_n)=0$ para cada $f\in I$, luego $(a_1,\ldots,a_n)\in\mathbb{V}(I)$ y $\mathbb{V}(I)\neq\varnothing$. □

En el caso particular en que $k=\mathbb{C}$, el teorema débil de los ceros de Hilbert puede pensarse como la generalización del teorema fundamental del álgebra al caso de polinomios en $\mathbb{C}[x_1,\ldots,x_n]$, es decir, todo sistema de polinomios en $\mathbb{C}[x_1,\ldots,x_n]$, que generan un ideal propio de $\mathbb{C}[x_1,\ldots,x_n]$ tienen al menos un cero común en $\mathbb{C}^n$.

TEOREMA 3.4.12. (*de los ceros de Hilbert*). Sea k un campo algebraicamente cerrado y f, $f_1,\ldots,f_s$ polinomios en $k[x_1,\ldots,x_n]$ que satisfacen $f\in\mathbb{I}(\mathbb{V}(f_1,\ldots,f_s))$, entonces existe $r\in\mathbb{N}$ tal que $f^r\in<f_1,\ldots,f_s>$.

DEMOSTRACIÓN

Se tendrá que probar que existen $r\in\mathbb{N}$ y $g_1,\ldots,g_s\in k[x_1,\ldots,x_n]$ tal que $f^r=\sum_{i=1}^{s} g_i f_i$ con f un polinomio que se anula en todos los ceros comunes de $f_1,\ldots, f_s$. Considérese el ideal $I=<f_1,\ldots,f_s,1-yf>\subseteq k[x_1,\ldots,x_n,y]$ generado por $f_1,\ldots, f_s$ y el polinomio $1-yf$, donde y es la nueva indeterminada. El conjunto algebraico $\mathbb{V}(I)$ consiste de los elementos $p\in\mathbb{V}(f_1,\ldots,f_s)$ tal que $f(p)=0$, es decir, un punto $q\in\mathbb{V}(I)$ es una $(n+1)$-ada, $q=(a_1,\ldots,a_n,a_{n+1})$ con $g(a_1,\ldots,a_n)=0$ para toda $g\in<f_1,\ldots,f_s>$, esto es, $(a_1,\ldots,a_n)\in\mathbb{V}(f_1,\ldots,f_s)$ y $f(a_1,\ldots,a_n)=1/a_{n+1}$, es decir, $g(a_1,\ldots,a_n,a_{n+1})\neq 0$ y $a_{n+1}=f^{-1}(a_1,\ldots,a_n)$. Se afirma que $\mathbb{V}(I)=\varnothing$; en efecto, sea $(a_1,\ldots,a_n,a_{n+1})\in k^{n+1}$, entonces existen dos posibilidades: o $(a_1,\ldots,a_n)$ es un cero común de $f_1,\ldots,f_s$ o $(a_1,\ldots,a_n)$ no lo es. Si $(a_1,\ldots,a_n)$ es un cero común de $f_1,\ldots,f_s$, se tiene que $f(a_1,\ldots,a_n)=0$ (ya que f se anula en todo cero común de $<f_1,\ldots,f_s>$. Entonces la función polinomial asociada al polinomio $1-yf$, evaluada en el punto $(a_1,\ldots,a_n,a_{n+1})\in k^{n+1}$ con a_{n+1} arbitraria, toma el valor $1-a_{n+1}f(a_1,\ldots,a_n)=1\neq 0$. Luego $(a_1,\ldots,a_n,a_{n+1})\notin\mathbb{V}(I)$. Si $(a_1,\ldots,a_n)$ no es un cero común de $f_1,\ldots,f_s$, entonces para un

índice $j_0 \in \{1,\ldots, s\}$, se tiene que $f_{j_0}(a_1,\ldots,a_n) \neq 0$. Considerando a f_{j_0} como un polinomio en $n+1$ indeterminadas y a su función polinomial asociada como una función que no depende explícitamente de la última variable, se tiene que $f_{j_0}(a_1,\ldots,a_n, a_{n+1}) \neq 0$. En esta situación, se sigue que $(a_1,\ldots,a_n, a_{n+1}) \notin \mathbb{V}(I)$. Como $(a_1,\ldots,a_n, a_{n+1}) \in k^{n+1}$ es arbitrario, se tiene que $\mathbb{V}(I)=\varnothing$ lo cual prueba la afirmación. Ahora, por el teorema débil de los ceros de Hilbert, se tiene que $1 \in I$, es decir, existe una expresión

$$1=\sum_{i=1}^{s} p_i(x_1,\ldots, x_n, y) f_i + q(x_1,\ldots, x_n, y)(1-yf)$$

para algunos polinomios $p_1,\ldots, p_s, q \in k[x_1,\ldots, x_n, y]$. Haciendo $y=\dfrac{1}{f(x_1,\ldots,x_n)}$, la expresión anterior implica

$$1=\sum p_i\left(x,\ldots, x_n, \frac{1}{f(x_1,\ldots,x_n)}\right) f_i.$$

Multiplicando esto por f^{r} †) con $r \in \mathbb{N}$, esto conduce a $f^{r}=\sum_{i=1}^{s} g_i f_i$ para algunos polinomios $g_1,\ldots, g_s \in k[x_1,\ldots, x_n]$. □

TEOREMA 3.4.13. (*fuerte de los ceros de Hilbert*). Sea k un campo algebraicamente cerrado e I un ideal en el anillo $k[x_1,\ldots, x_n]$, entonces $\mathbb{I}\big(\mathbb{V}(I)\big)=rad(I)$.

DEMOSTRACIÓN ($\subseteq$)

Supóngase que $f \in \mathbb{I}\big(\mathbb{V}(I)\big)$, entonces f se anula en todo elemento de $\mathbb{V}(I)$. Por el teorema de los ceros de Hilbert, existe $r \in \mathbb{N}$ tal que $f^{r} \in I$; luego $f \in rad(I)$. Como f es arbitrario, $\mathbb{I}(\mathbb{V}(I)) \subseteq rad(I)$.

($\supseteq$)

Que $f \in rad(I)$, significa que $f^{m} \in I$ para algún número natural m. Luego f^{m} se anula en $\mathbb{V}(I)$, lo cual significa que f se anula en $\mathbb{V}(I)$. Así, $f \in \mathbb{I}\big(\mathbb{V}(I)\big)$ y $rad(I) \subseteq \mathbb{I}\big(\mathbb{V}(I)\big)$. □

Se observa que los teoremas de Hilbert son falsos si el campo k no es algebraicamente cerrado. El teorema débil de los ceros de Hilbert asegura que si un ideal J de $k[x_1,\ldots, x_n]$ es propio entonces existen ceros en el espacio afín k^n, esto es, existen variedades no triviales. Como una consecuencia del teorema fuerte, se tiene que si I es un ideal radical en $k[x_1,\ldots, x_n]$, entonces $\mathbb{I}\big(\mathbb{V}(I)\big)=I$. Lo que resta del capítulo se dedica a desarrollar los conceptos y resultados necesarios para establecer los teoremas de los ceros de Hilbert en el caso real y algunas consecuencias de estos.

Una **variedad afín** en k^n o simplemente una **variedad** se define como un conjunto algebraico irreducible X en k^n y se denota con la letra **V** en vez de X. Sea **V** en k^n una

†) r se escoge de tal forma que sea la mayor potencia de y tal que y^{r} aparezca en q y p_i para toda $i=1,\ldots, s$.

variedad; de 3.4.5., se tiene que $\mathbb{I}(\mathbf{V})$ es un ideal primo, luego $A=k[x_1,\ldots,x_n]/\mathbb{I}(\mathbf{V})$ es un dominio entero denominado **anillo de coordenadas** de la variedad $\mathbf{V}$.[‡)]

Sea I un ideal de polinomios en el anillo $k[x_1,\ldots,x_n]$ e $I\overline{k}[x_1,\ldots,x_n]$ el ideal generado por I en $\overline{k}[x_1,\ldots,x_n]$ con $\overline{k}$ la cerradura algebraica de k. Sea $\mathbf{V}\left(I\overline{k}[x_1,\ldots,x_n]\right)$ el conjunto algebraico definido por el ideal $I\overline{k}[x_1,\ldots,x_n]$ sobre la cerradura algebraica $\overline{k}$; $\mathbf{V}_k(I)=\mathbf{V}\left(I\overline{k}[x_1,\ldots,x_n]\right)\cap k^n$ el conjunto de **puntos reales** o ***k*-puntos** en $\mathbf{V}\left(I\overline{k}[x_1,\ldots,x_n]\right)$ y la k-álgebra afín $A=k[x_1,\ldots,x_n]/I$ el anillo de coordenadas de $\mathbf{V}_k(I)$. Si P es un ideal primo real en $k[x_1,\ldots,x_n]$, entonces por la observación 3.4.6., $P\overline{k}[x_1,\ldots,x_n]$ es un ideal primo en $\overline{k}[x_1,\ldots,x_n]$ y $\mathbf{V}_k(P)$ es una variedad afín irreducible. A los conjuntos de la forma $\mathbf{V}_k(P)$ se les denomina **variedades algebraicas reales.** El siguiente resultado es la versión al caso real del teorema débil de los ceros de Hilbert.

TEOREMA 3.4.14. (*débil de los ceros de Hilbert real*). Sea k un campo cerrado real, I un ideal en $k[x_1,\ldots,x_n]$ y $A=k[x_1,\ldots,x_n]/I$ el anillo de coordenadas de $\mathbf{V}_k(I)$. Entonces A es semireal si y sólo si $\mathbf{V}_k(I)\neq\varnothing$.

DEMOSTRACIÓN ($\Rightarrow$)

Si A es un anillo semireal, por el primer corolario al teorema del homomorfismo de Lang, (corolario 3.3.28.), existe un homomorfismo de k - álgebras $\varphi:A\to k$. Sea

$$\psi:k[x_1,\ldots,x_n]\to k;\ \psi(f(x_1,\ldots,x_n))=f(a_1,\ldots,a_n)$$

el homomorfismo canónico con $(a_1,\ldots,a_n)\in k^n$. Si $f\in I$, entonces

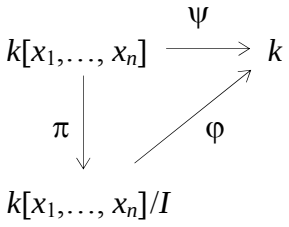
$$\psi(f(x_1,\ldots,x_n))=(\varphi\circ\pi)(f(x_1,\ldots,x_n))=0.$$

Pero $\psi(f(x_1,\ldots,x_n))=\varphi(\pi(f(x_1,\ldots,x_n)))=\varphi(\overline{f(x_1,\ldots,x_n)})=f(a_1,\ldots,a_n)=0$. Por lo tanto, $(a_1,\ldots,a_n)\in\mathbf{V}_k(I)$ y $\mathbf{V}_k(I)\neq\varnothing$.

($\Leftarrow$)

Sea $a=(a_1,\ldots,a_n)\in k^n$ un k-punto y considérese el homomorfismo de evaluación $\varphi:A\to k$; $\varphi(\overline{x}_i)=a_i$, $i=1,\ldots,n$ en $a=(a_1,\ldots,a_n)$. Como k es semireal, de la observación 1.1.8., se sigue que A es semireal. □

El teorema débil de los ceros de Hilbert real es un criterio que da información acerca de cuando una álgebra afín es semireal. A continuación se enuncia el teorema de los ceros de Hilbert para el caso de ideales primos



[‡)] De hecho $k[x_1,\ldots,x_n]/\mathbb{I}(V)$ es una álgebra k-afín.

TEOREMA 3.4.15. (*de los ceros de Hilbert real*). Sea k un campo cerrado real y P un ideal primo en el anillo $k[x_1,\ldots,x_n]$. Entonces $\mathbb{I}(\mathbf{V}_k(P))=P$ si y sólo si P es real.

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que P no es un ideal real, entonces existe $f_1^2+\cdots+f_m^2\in P$ con al menos un $f_i\notin P$; por ejemplo $f_1\notin P$. Como $\mathbb{I}(\mathbf{V}_k(P))=P$, se tiene que $f_1^2+\cdots+f_m^2\in\mathbb{I}(\mathbf{V}_k(P))$; esto es, $f_1^2(x)+\cdots+f_m^2(x)=0\in k$ para todo $x\in\mathbf{V}_k(P)$. Dado que k es un campo real, se sigue que $f_i(x)=0$ para todo $i=1,2,\ldots,m$. Entonces $f_i\in\mathbb{I}(\mathbf{V}_k(P))$ para $i=1,2,\ldots,m$. Luego $P\subsetneq\mathbb{I}(\mathbf{V}_k(P))$ lo cual es una contradicción.

($\Leftarrow$)

De 3.4.2 *iii*), se tiene que $P\subseteq\mathbb{I}(\mathbf{V}_k(P))$; restará probar que $\mathbb{I}(\mathbf{V}_k(P))\subseteq P$. Supóngase que $f\notin P$ y considérese la k-álgebra afín $A=k[x_1,\ldots,x_n]/P$. Como A es un dominio entero real, se tiene que $\overline{f}\neq\overline{0}$. Por el segundo corolario del teorema del homomorfismo de Lang (corolario 3.3.29.), existe un homomorfismo de k-álgebras $\varphi:A\to k$; tal que $\varphi(\overline{f})\neq 0$. Sea $\varphi(\overline{x}_i)=a_i$, $i=1,\ldots,n$, entonces $a=(a_1,\ldots,a_n)\in k^n$ con $(a_1,\ldots,a_n)\in\mathbf{V}_k(P)$; dado que $f\notin P$, se tiene que $f(a_1,\ldots,a_n)\neq 0$. Así, $f\notin\mathbb{I}(\mathbf{V}_k(P))$ e $\mathbb{I}(\mathbf{V}_k(P))\subseteq P$. □

El objetivo a continuación es dar la versión del teorema fuerte de los ceros de Hilbert al caso real. Pareciera ser que este resultado puede establecerse directamente como en el caso de los teoremas 3.4.14. y 3.4.15., pero la situación no es tan sencilla como parece. El problema aquí es que el radical de un ideal no es en general un ideal real o la intersección de todos los ideales primos reales que contienen a ese ideal; por ejemplo, considérese el anillo de polinomios en las indeterminadas x e y con coeficientes en los reales, $\mathbb{R}[x,y]$. Se sabe que $\langle x^2+y^2\rangle$ es un ideal primo semireal que no es real (si $x^2+y^2=0$ se sigue que $x\neq 0$ y $y\neq 0$) y que $\langle x,y\rangle$ es un ideal real ($\mathbb{R}[x,y]/\langle x,y\rangle\cong\mathbb{R}$). Como $rad(\langle x^2+y^2\rangle)=\langle x^2+y^2\rangle\subsetneq\langle x,y\rangle$ y $\langle x,y\rangle$ es el menor ideal primo real que contiene al ideal $\langle x^2+y^2\rangle$, entonces $rad(\langle x^2+y^2\rangle)$ no es la intersección de todos los ideales primos reales que contienen a $\langle x^2+y^2\rangle$. Lo que si se cumple es que todo ideal real I de un anillo A es radical; esto es, si I es un ideal real, entonces $rad(I)=I$. En efecto, si $a^n\in I$, $n>1$, entonces $a^{\frac{n}{2}}\in I$ si n es par y $a^{\frac{n+1}{2}}\in I$ si n es impar. En ambos casos el exponente ha decrecido y por iteración de este proceso, se obtiene que $a\in I$. De esta forma, para establecer el teorema fuerte de los ceros de Hilbert en el caso real, se necesita introducir el concepto de radical en el contexto de ideales reales.

Sea I un ideal de un anillo A y $a\in rad(I)$, entonces existe un número natural m tal que $a^m\in I$. Si I es un ideal real, entonces $rad(I)=I$, luego se tendrá que existen elementos $b_1,\ldots,b_n$ en I tal que $a^{2m}+b_1^2+\cdots+b_n^2\in I$. Teniendo como modelo la definición de radical de un preorden (ver 2.2.28.), se define

DEFINICIÓN 3.4.16. Sea I un ideal en un anillo A. El **radical real** de I, escrito ***r-rad***(I) es el conjunto

$$\boldsymbol{r\text{-}rad}(I)=\{a\in \mathrm{A} \mid \text{existe } m\geq 0 \text{ y } \sigma\in\sum\mathbf{A}^{\mathbf{2}} \text{ tal que } a^{2m}+\sigma\in I\ \}.$$

Se sigue de la definición de radical real de un ideal I que $I\subseteq \boldsymbol{r\text{-}rad}(I)$ y que $\boldsymbol{r\text{-}rad}(I)$ es un ideal.

OBSERVACIÓN 3.4.17. Si I es un ideal real en un anillo A, entonces $\boldsymbol{r\text{-}rad}(I)=I$. En este caso se dice que I es un **ideal radical real**.

DEMOSTRACIÓN

Como $I\subseteq \boldsymbol{r\text{-}rad}(I)$, restará verificar que $\boldsymbol{r\text{-}rad}(I)\subseteq I$. Sea $a\in \boldsymbol{r\text{-}rad}(I)$, entonces existe $m\geq 0$ y $\sigma\in\sum\mathbf{A}^{\mathbf{2}}$ tal que $a^{2m}+\sigma\in I$. Dado que I es real, se sigue que $a^{m}\in I$ luego $a\in I$. Por lo tanto $\boldsymbol{r\text{-}rad}(I)\subseteq I$. □

Si I es un ideal en un anillo A, se sabe que el radical de I es la intersección de todos los ideales primos que contienen a I. En el caso del radical real se tiene un resultado similar, es decir,

TEOREMA 3.4.18. Sea I un ideal en un anillo A, entonces $\boldsymbol{r\text{-}rad}(I)=\cap P$, con P ideal primo real que contiene a I. El radical real es el ideal real más pequeño que contiene a I.

DEMOSTRACIÓN

Sea J un ideal real que contiene al ideal I en A. Entonces $\boldsymbol{r\text{-}rad}(I)\subseteq \boldsymbol{r\text{-}rad}(J)=J$,[†] luego $\boldsymbol{r\text{-}rad}(I)\subseteq J$ para todo ideal J real en A con $I\subseteq J$. Por lo tanto $\boldsymbol{r\text{-}rad}(I)\subseteq\cap J$, con $I\subseteq J$; en particular $\boldsymbol{r\text{-}rad}(I)\subseteq\cap P$, P ideal primo real que contiene a I. Para establecer la otra contención se tendrá que probar que si $a\notin \boldsymbol{r\text{-}rad}(I)$, entonces existe un ideal primo real P que contiene a I tal que $a\notin P$. En efecto, supóngase que $a\notin \boldsymbol{r\text{-}rad}(I)$; para este elemento a se construye el conjunto $\mathrm{S}=\{a^{2m}+\sigma \mid m\in\mathbb{N}\cup\{0\},\ \sigma\in\sum\mathbf{A}^{\mathbf{2}}\}$. S es un sistema multiplicativo en A[‡] que satisface $\mathrm{S}+\sum\mathbf{A}^{\mathbf{2}}\subseteq\mathrm{S}$. Dado que $a\notin \boldsymbol{r\text{-}rad}(I)$ e $I\subseteq \boldsymbol{r\text{-}rad}(I)$, se sigue que $a\notin I$, luego $I\cap\mathrm{S}=\varnothing$. Por el lema 1.1.18., existe un ideal maximal $\mathfrak{m}\supsetneq I$ tal que $\mathrm{S}\cap\mathfrak{m}=\varnothing$. Así, el ideal I se ha extendido a un ideal primo $\mathfrak{m}$ ajeno de S. Por el teorema 1.1.19., el campo $qf(\mathrm{A}/\mathfrak{m})$ es real; sea $\varphi:\mathrm{A}/\mathfrak{m}\to qf(\mathrm{A}/\mathfrak{m})$; $\varphi(\overline{a})=\overline{(a,1)}$. Dado que φ es un homomorfismo inyectivo, por 1.2.17., se sigue que $\mathrm{A}/\mathfrak{m}$ es real, luego $\mathfrak{m}$ es un ideal primo real ajeno de S. De esta forma $a\notin\mathfrak{m}$ y existe un ideal primo real $P\supseteq I$ tal que $a\notin P$. Así, $\cap P\subseteq \boldsymbol{r\text{-}rad}(I)$ con $I\subseteq P$. Finalmente, como intersección de ideales reales es un ideal real, se sigue que el radical real es un ideal real. □

TEOREMA 3.4.19. (*fuerte de los ceros de Hilbert real*). Sea k un campo cerrado real e I un ideal en el anillo $k[x_1,\ldots,x_n]$, entonces $\mathbb{I}\big(\mathbf{V}_k(I)\big)=\boldsymbol{r\text{-}rad}(I)$.

DEMOSTRACIÓN ($\subseteq$)

Sea $f\in\mathbb{I}\big(\mathbf{V}_k(I)\big)$, entonces $f(x)=0$ para todo $x\in\mathbf{V}_k(I)$. Sea P un ideal primo real con

---

[†] Si $a\in \boldsymbol{r\text{-}rad}(I)$, entonces existe $m\in\mathbb{N}\cup\{0\}$ y $\sigma\in\sum\mathbf{A}^{\mathbf{2}}$ tal que $a^{2m}+\sigma\in I$. Como $I\subseteq J$, se sigue que $a^{2m}+\sigma\in J=\boldsymbol{r\text{-}rad}(I)$.

[‡] 1°) Claramente $0\notin\mathrm{S}$, 2°) Si $\alpha_1,\alpha_2\in\mathrm{S}$ con $\alpha_1=a^{2m}+\sigma_1$ y $\sigma_2=a^{2n}+\sigma_2$, entonces $\sigma_1\sigma_2=a^{2(m+n)}+(\sigma_1+\sigma_2)\in\mathrm{S}$ y 3°) $1=a^{2(0)}+0^2+\cdots+0^2\in\mathrm{S}$.

$I \subseteq P$, entonces se tiene que $\mathbf{V}_k(P) \subseteq \mathbf{V}_k(I)$. Como P es un ideal real, por el teorema de los ceros de Hilbert real (teorema 3.4.15.), se sigue que $\mathbb{I}(\mathbf{V}_k(P)) = P$. Como $\mathbf{V}_k(P) \subseteq \mathbf{V}_k(I)$, se tiene $\mathbb{I}(\mathbf{V}_k(I)) \subseteq \mathbb{I}(\mathbf{V}_k(P))$ e $\mathbb{I}(\mathbf{V}_k(I)) \subseteq P$. Esto se cumple para todo ideal primo real que contiene a I; así, $\mathbb{I}(\mathbf{V}_k(I)) \subseteq \cap P$, P ideal primo real que contiene a I. Por el teorema 3.4.18., ***r-rad***$(I) = \cap P$, P ideal primo real que contiene a I, luego $\mathbb{I}(\mathbf{V}_k(I)) \subseteq r\text{-}rad(I)$.

($\supseteq$)

Sea $f \in$ ***r-rad***(I), entonces existe $m \in \mathbb{N} \cup \{0\}$ y $g \in \sum \mathbf{A^2}$ tal que $f^{2m} + g \in I$. Para todo elemento $a \in \mathbf{V}_k(I)$, $f^{2m}(a) + g(a) = 0 \in k$, $f^{m}(a) = 0$ por ser k un campo real y $f(a) = 0$; así, $f \in \mathbb{I}(\mathbf{V}_k(I))$. Por tanto ***r-rad***$(I) \subseteq \mathbb{I}(\mathbf{V}_k(I))$. □

Se observa que si I es un ideal real en A, entonces $\mathbb{I}(\mathbf{V}_k(I)) = I$. Como una consecuencia del teorema 3.4.19., se tiene el siguiente,

COROLARIO 3.4.20. Si $A = k[x_1, \ldots, x_n]/I$ es una álgebra k-afín real con k un campo cerrado real, entonces $\mathbf{V}_k(I)$ es denso Zariski en $V(I\bar{k}[x_1, \ldots, x_n])$

DEMOSTRACIÓN

Se tiene que probar que $\overline{\mathbf{V}_k(I)^*} = \mathbf{V}(I\bar{k}[x_1, \ldots, x_n])$, donde $\overline{\mathbf{V}_k(I)^*}$ es la cerradura de $\mathbf{V}_k(I)$ con respecto al espacio afín $\bar{k}^n$ donde $\bar{k} = k(\sqrt{-1})$ es la cerradura algebraica de k. Primero se probará que $\overline{\mathbf{V}_k(I)^*} \subseteq \mathbf{V}(I\bar{k}[x_1, \ldots, x_n])$. En efecto, como $\mathbf{V}_k(I) \subseteq \mathbf{V}(I\bar{k}[x_1, \ldots, x_n])$ y $\overline{\mathbf{V}_k(I)^*} \subseteq \mathbf{V}(I\bar{k}[x_1, \ldots, x_n])$; por ser $\overline{\mathbf{V}_k(I)^*}$ el menor cerrado en k^n que contiene a $\mathbf{V}_k(I)$, se sigue la contención. Ahora se probará que $\mathbf{V}(I\bar{k}[x_1, \ldots, x_n]) \subseteq \overline{\mathbf{V}_k(I)^*}$ o equivalentemente que $\mathbb{I}(\overline{\mathbf{V}_k(I)^*}) \subseteq \mathbb{I}(\mathbf{V}(I\bar{k}[x_1, \ldots, x_n]))$. En efecto, sea $f \in \mathbb{I}(\overline{\mathbf{V}_k(I)^*})$, es decir, $f \in \bar{k}[x, \ldots, x_n]$ donde $f = f_1 + \sqrt{-1} f_2$ es un polinomio que se anula en $\mathbf{V}_k(I)$, con $f_1, f_2 \in k[x_1, \ldots, x_n]$ entonces para cada $p \in \mathbf{V}_k(I)$, $f(p) = f_1(p) + \sqrt{-1} f_2(p) = 0$. Luego $f_1(p) = 0$, $f_2(p) = 0$ ya que $f_1(p), f_2(p) \in k$, es decir, $f_1, f_2 \in \mathbb{I}(\mathbf{V}_k(I))$. Por el teorema fuerte de los ceros de Hilbert real se tiene que $f_1, f_2 \in$ ***r-rad***(I). Como I es un ideal real, se sigue que $f_1, f_2 \in I$ y $f \in I + \sqrt{-1} I = I\bar{k}[x_1, \ldots, x_n]$. Por lo tanto $f \in \mathbb{I}(\mathbf{V}(I\bar{k}[x_1, \ldots, x_n]))$. □

Sea k un campo algebraicamente cerrado y $f \in k[x_1, \ldots, x_n]$ un polinomio irreducible con $f \notin k$. Considérese la variedad k-afín $\mathbf{V} = \mathbf{V}(f)$ en k^n y un punto $a = (a_1, \ldots, a_n) \in \mathbf{V}$. Sea $l = \{(a_1, \ldots, a_n) + t(b_1, \ldots, b_n) \mid t \in k\}$ una recta que contiene el punto a y $g \in k[x_1, \ldots, x_n]$ el polinomio $g = f \mid l = f(a_1 + b_1 t, \ldots, a_n + b_n t)$ en la indeterminada t. El polinomio g tiene como una raíz a 0; luego 0 es una raíz múltiple de g si y sólo si $\partial f(0)/\partial t = 0$, esto último es equivalente a $\sum_i b_i \, \partial f(a)/\partial x_i = 0$ lo cual también equivale a que la recta l esté contenida en el subespacio lineal afín

$$T_a\mathbf{V}=\{(x_1,\ldots,x_n)\in\mathbf{V} \mid \sum_i b_i\, \partial f(x_i-a_i)/\partial x_i=0\}\subseteq k^n.$$

$T_a\mathbf{V}$ se denomina espacio tangente de $\mathbf{V}$ en a y es un subespacio de dimensión n-1 en k^n. Se recuerda que las derivadas $\partial f(0)/\partial t$ y $\partial f(a)/\partial x_i$ son operaciones algebraicas formales.

Se dice que un punto $a\in\mathbf{V}$ es un **punto regular** o **punto simple** o también llamado **no singular** si $\partial f(a)/\partial x_i\neq 0$ para alguna i=1, 2,…, n. Y un punto $a\in\mathbf{V}$ es **singular** o una **singularidad** si a no es regular. Los puntos en una variedad algebraica pueden ser así divididos en puntos regulares (en los cuales la variedad es suave) y las singularidades. Si *Reg*(**V**) es el conjunto de todos los puntos regulares de una variedad y *Sing*(**V**) el conjunto de singularidades de **V**, entonces *Sing*(**V**)=**V** \ *Reg*(**V**) y *Sing*(**V**) es un conjunto cerrado Zariski de codimensión ≥1, esto es, es cerrado Zariski denso en ninguna parte, es decir,

PROPOSICIÓN 3.4.21. *Reg*(**V**) es un conjunto abierto denso en **V** en la topología de Zariski.

DEMOSTRACIÓN

Como *Sing*(**V**)=**V**($f, \partial f/\partial x_1,\ldots,\partial f/\partial x_n)\subseteq k^n$ es cerrado Zariski y **V** es irreducible, para probar que el abierto *Reg*(**V**) es denso se tendrá que probar que no es vacío. Supóngase lo contrario, esto es, que **V**=*Sing*(**V**), entonces cada uno de los polinomios $\partial f / \partial x_i$ se anula en **V**, luego ellos son divisibles por f. Visto $\partial f/\partial x_i$ como un polinomio en $x_1,\ldots,x_n$, $\partial f/\partial x_i$ tiene grado estrictamente menor que f, de esta forma $f \mid \partial f\ (x)/\partial x_1$ implica que $\partial f/\partial x_i=0$ como un polinomio. Lo anterior es posible si f es un polinomio inseparable en x_i, esto es, $car(k)=p$ y x_i solamente aparece en f como la p-ésima potencia x_i^p. Si esto es valido para toda i, entonces f es una potencia p-ésima en $k[x_1,\ldots,x_n]$. Esto último contradice el hecho de que f es irreducible. □

Como ya se vio, el teorema débil de los ceros de Hilbert real afirma que si una álgebra afín A es semireal, ello equivale a que la variedad $\mathbf{V}_k(I)$ de cualquier ideal propio de A sea no vacía. Un resultado similar se tiene cuando el álgebra afín es real, es decir,

PROPOSICIÓN 3.4.22. (*Criterio débil del punto regular*). Sea k un campo cerrado real, P un ideal primo en el anillo $k[x_1,\ldots,x_n]$ y A=$k[x_1,\ldots,x_n]$ /P una k-álgebra afín. Entonces el anillo A es real si y sólo si $Reg\big(\mathbf{V}\big(P\,\overline{k}\,[x_1,\ldots,x_n]\big)\big)\cap\mathbf{V}_k(P)\neq\varnothing$.

DEMOSTRACIÓN ($\Rightarrow$)

Si A es un anillo real, es decir, P es un ideal primo real, entonces por 3.4.6., $\mathbf{V}\big(P\,\overline{k}\,[x_1,\ldots,x_n]\big)$ es una variedad algebraica irreducible. Por la proposición 3.4.21., $Reg\big(\mathbf{V}\big(P\,\overline{k}\,[x_1,\ldots,x_n]\big)\big)$ es un conjunto abierto y denso Zariski en $\mathbf{V}\big(P\,\overline{k}\,[x_1,\ldots,x_n]\big)$; por 3.4.20., la variedad $\mathbf{V}_k(P)$ es denso Zariski en $\mathbf{V}\big(P\,\overline{k}\,[x_1,\ldots,x_n]\big)$. Luego $Reg\big(\mathbf{V}\big(P\,\overline{k}\,[x_1,\ldots,x_n]\big)\big)\neq\varnothing$

($\Leftarrow$)

Si $\mathbf{V}\left(\mathrm{P}\,\overline{k}\,[x_1,\ldots,x_n]\right)$ tiene un punto regular real $a=(a_1,\ldots,a_n)$ y $m=<\overline{x_1-a_1},\ldots,\overline{x_n-a_n}>$ es el ideal maximal de A correspondiente al punto a, entonces A_m es un anillo local regular. Como $\mathrm{A}_m/m\mathrm{A}_m \cong qf(\mathrm{A}/m)=\mathrm{A}/m\cong k$ y k es un campo real, se sigue que A/m es real y también $\mathrm{A}_m/m\mathrm{A}_m$ es real. Luego A y A_m son anillos locales reales. De 1.2.32., A_m es real y por tanto semireal. Por 1.2.33., se sigue que A es real. □

LEMA 3.4.23. Sea I un ideal en un anillo A. Entonces I es un ideal radical si y sólo si $nil(\mathrm{A}/I)=0$[†)].

DEMOSTRACIÓN ($\Rightarrow$)

Sea $\overline{a}\in nil(\mathrm{A}/I)$, entonces existe $m\in\mathbb{N}$ tal que $\overline{a^m}=\overline{0}$, es decir, $a^m\in I$. Esto significa que $a\in rad(I)$. Como $I=rad(I)$, se sigue que $a\in I$ y $\overline{a}=\overline{0}$; luego $nil(\mathrm{A}/I)=0$.

($\Leftarrow$)

Dado que $I\subseteq rad(I)$, bastará probar que $rad(I)\subseteq I$. Sea $a\in rad(I)$, entonces existe $m\in\mathbb{N}$ tal que $a^m\in I$; de esto se sigue que $\overline{a^m}=\overline{0}$, con $\overline{a}\in\mathrm{A}/I$. Como $nil(\mathrm{A}/I)=0$, se tiene que $\overline{a}=\overline{0}$; y esto último significa que $a\in I$. □

A continuación se da la versión de la proposición 3.4.22., cuando I es un ideal arbitrario en el anillo $k[x_1,\ldots,x_n]$.

TEOREMA 3.4.24. (*Criterio fuerte del punto regular*). Sea k un campo cerrado real, I un ideal en el anillo $k[x_1,\ldots,x_n]$, $P_1,\ldots,P_m$ ideales primos minimales de I y $\mathrm{A}=k[x_1,\ldots,x_n]/I$ una álgebra k-afín. Entonces A es real si y sólo si $I=rad(I)$ y $Reg(\mathbf{V}(P_i\,\overline{k}\,[x_1,\ldots,x_n]))\cap\mathbf{V}_k(P_i)\neq\varnothing$; para cada $i=1,2,\ldots,m$.

DEMOSTRACIÓN

Que A es real, por 1.2.28., es equivalente a que $nil(\mathrm{A})=0$ y P_i/I son ideales primos minimales reales de A.[‡)] Que los ideales P_i/I, $i=1,2,\ldots,m$ sean reales, significa que $(k[x_1,\ldots,x_n]/I)/(P_i/I)$ son reales y por consecuencia $k[x_1,\ldots,x_n]/P_i$ también son reales; para $i=1,2,\ldots,m$. Por el criterio débil del punto regular y el lema 3.4.23., se sigue que I es un ideal radical y cada variedad $\mathrm{V}\left(P_i\,\overline{k}\,[x_1,\ldots,x_n]\right)$; $i=1,2,\ldots,m$ tiene un punto regular real. □

En la sección anterior se introdujo la noción de topología intervalo en un campo ordenado F y se probaron algunos resultados necesarios; aquí se darán unos pocos más. Se sabe que para un campo ordenado F, las operaciones binarias de suma y multiplicación en F son funciones continuas con respecto a la topología intervalo en F, esto es, F con la topología intervalo es un campo topológico. De esta forma, las funciones polinomiales son

---

[†)] Si $nil(\mathrm{A}/I)=0$ se dice que A es un anillo **reducido**.

[‡)] Que P_i/I sean primos minimales reales, $i=1,2,\ldots,n$ se sigue de la correspondencia biyectiva entre los ideales $P_i\supseteq I$ y P_i/I y de la equivalencia $k[x_1,\ldots,x_n]/P_i\cong(k[x_1,\ldots,x_n]/I)/(P_i/I)$.

continuas en esta topología. Sea ahora $F^n=F\times F\times\cdots\times F$ (n veces) el conjunto de n-adas $(x_1,\ldots,x_n)$ de elementos en F. Se puede dotar a F^n con la topología producto τ_{F^n} y convertir al conjunto F^n en un espacio topológico donde una base para esta topología τ_{F^n} viene dada como

$$\mathcal{B}=\{(a_1\,,b_1)\times\cdots\times(a_n\,,b_n)\mid a_i,\,b_i\in F\ a_i<b_i\ i=1,2,\ldots,n\}.$$

Un resultado que se puede enunciar en el espacio $(F^n\,,\ \tau_{F^n})$ es el

TEOREMA 3.4.25. (*del valor intermedio*) Sea k un campo cerrado real, $f:U\subseteq k^n\to k$ una función continua en un conjunto abierto y conexo U y $f(a)<f(b)$ para $a,\,b\in U$. Entonces para cada $\mu\in k$ con $f(a)<\mu<f(b)$ existe un elemento $c\in U$ tal que $f(c)=\mu$.

DEMOSTRACIÓN

Sea $\Gamma=\{x\in U\mid f(x)<\mu\}$ y $\Lambda=\{x\in U\mid f(x)>\mu\}$. Como $a\in\Gamma$ y $b\in\Lambda$, se sigue que $\Gamma\neq\varnothing$, $\Lambda\neq\varnothing$ y $\Gamma\cap\Lambda=\varnothing$. Sea $x\in\Gamma$, como $f(x)<\mu$ y f es continua en x, existe un básico $\mathcal{B}_x$ contenido en U tal que $f(y)<\mu$ para todo $y\in\mathcal{B}_x$; luego Γ es abierto en U. En forma similar se obtiene que Λ es abierto en U. De esta manera $\Gamma\cup\Lambda\subsetneq U$ ya que U es conexo. Entonces existe al menos un punto $c\in U$ tal que $c\notin\Gamma\cup\Lambda$, lo cual es equivalente a que $f(c)\leq\mu$ y $f(c)\geq\mu$, esto es, $f(c)=\mu$. □

Antes de finalizar este capítulo con el criterio del cambio de signo, se probarán las siguientes:

OBSERVACIÓN. 3.4.26. Sea A un D.F.U. y $F=qf(A)$. Si $f\in A[x]$ es un polinomio irreducible en el anillo $A[x]$, con $grad(f)>0$, entonces f es irreducible en $F[x]$.

DEMOSTRACIÓN

Supóngase que $f\in A[x]$ es un polinomio no constante que se factoriza en polinomios $g,\ h\in F[x]$ de grados menores que el grado de f, es decir, $f=gh$. Como F es un campo de cocientes de A, cada coeficiente en g y h es de la forma a/b para algunos $a,\,b\in A$. Haciendo las operaciones con los coeficientes de los polinomios g, h y eliminando denominadores, se obtiene $df=g_1h_1$ para $d\in A$, $g_1,\ h_1\in A[x]$ donde los grados de g_1 y h_1 son los mismos que los grados de g, h respectivamente. Ahora, se sabe que $f=cf_1$, $g_1=c_1g_2$, $h_1=c_2h_2$ donde c, c_1, $c_2\in A$ y f_1, g_2, $h_2\in A[x]$ tienen el mismo grado que f, g y h respectivamente, y sus únicos divisores comunes de todos sus coeficientes son unidades en A.[†)] Entonces $df=g_1h_1$ toma la forma $cdf_1=c_1c_2g_2h_2$, donde g_2h_2 también es un polinomio que satisface que los únicos divisores comunes de todos sus coeficientes son unidades en A.[‡)] Por la unicidad en la igualdad $cdf_1=c_1c_2g_2h_2$ (es decir, un polinomio que satisface que los únicos divisores

[†)] Un polinomio en un D.F.U. cuyos únicos divisores comunes de sus coeficientes son unidades en el anillo base, se denomina **polinomio primitivo**.

[‡)] Este resultado se sigue del lema de Gauss que dice: ***Si A es un D.F.U., entonces el producto de dos polinomios primitivos es un polinomio primitivo.***

comunes de todos sus coeficientes son unidades en A es único salvo un factor unidad $u\in$A) se tiene que $c_1c_2=ucd$ para alguna unidad $u\in$A, luego, $cdf_1=ucdg_2h_2$. De modo que $f_1=ug_2h_2$ y $f=udg_2h_2$. Como g_2h_2 tiene el mismo grado que gh, se concluye que f es irreducible en F[x]. □

OBSERVACIÓN. 3.4.27. Sea A un D.F.U. y F=qf(A). Si f, $g\in$A[x] tal que $f\nmid g$ en A[x], entonces $f\nmid g$ en F[x].

DEMOSTRACIÓN

Supóngase que f, $g\in$F[x] son polinomios tales que $g=hf$ con $h\in$F[x]. Como los coeficientes de h son de la forma a/b con a, $b\in$A, haciendo las operaciones con los coeficientes de h y eliminando el denominador, se obtiene $dg=h_1f$ con $d\in$A, $h_1\in$A[x] un polinomio que tiene el mismo grado que h. Por otro lado, se sabe que $g=cg_1$, $h_1=c_1h_2$ y $f=c_2f_1$ con c, c_1, $c_2\in$A, g_1, h_2, $f_1\in$A[x] polinomios primitivos con el mismo grado que g, h y f respectivamente (ver pie de nota en esta pagina para la definición de polinomio primitivo). Entonces la igualdad $dg=h_1f$ se puede escribir como $cdg_1=c_1c_2h_2f_1$ donde h_2f_1 es un polinomio primitivo que es único salvo un factor unidad. De esta forma se tiene que $c_1c_2=ucd$ para alguna unidad $u\in$A, luego $g=uh_2f_1$. Esto último significa que $f\mid g$ en A[x] lo cual constituye una contradicción a la hipótesis. Por lo tanto $f\nmid g$ en F[x]. □

LEMA. 3.4.28. Sea k un campo cerrado real y f, $g\in k[x_1,\ldots,x_n]$ polinomios con f indefinido e irreducible tal que $\mathbf{V}_k(f)\subseteq\mathbf{V}_k(g)$. Entonces $f\mid g$.

DEMOSTRACIÓN

Como f es indefinido, existen puntos $(a_1',\ldots,a_{n-1}',b_1)$, $(a_1'',\ldots,a_{n-1}'',b_2)\in k^n$ tal que

$$f(a_1',\ldots,a_{n-1}',b_1)<0<f(a_1'',\ldots,a_{n-1}'',b_2)$$

en el único orden de k. Haciendo un cambio de coordenadas tal que las primeras n-1 componentes queden fijas, es decir, existen puntos $(a_1,\ldots,a_{n-1},b_1)$, $(a_1,\ldots,a_{n-1},b_2)\in k^n$ tal que $f(a_1,\ldots,a_{n-1},b_1)<0<f(a_1,\ldots,a_{n-1},b_2)$ en el único orden de k. Sea A=$k[x_1,\ldots,x_{n-1}]$ y F=qf(A), entonces A[x_n]=$k[x_1,\ldots,x_{n-1}][x_n]=k[x_1,\ldots,x_{n-1},x_n]$. Considérese los polinomios f y g en la indeterminada t (=x_n) en el anillo A[t] (=$k[x_1,\ldots,x_{n-1},t]$). Como f es irreducible en el anillo A[t] y $f\nmid g$ también en A[t], entonces por las observaciones 3.4.26. y 3.4.27., se sigue que f es irreducible en F[t] y $f\nmid g$ en F[t]. Como F[t] es un D.I.P., el máximo común divisor de f y g existe y es único salvo la multiplicación por una constante no cero en F. Sea l el máximo común divisor de f y g, entonces l es constante; de no serlo, f sería un múltiplo constante de l ya que f es irreducible y se tendría que $f\mid g$ lo cual no puede ser posible. Por consiguiente, l es constante y se puede suponer que l=1. Luego existen polinomios p, $q\in$F[t] tal que $fp+gq=1$. Sea $p=p_0/h_1$ y $q=q_0/h_2$ con p_0, $q_0\in$A[t] y h_1, $h_2\in$A, $h_1\neq0$, $h_2\neq0$. De esta forma se tiene que $f(p_0/h_1)+g(q_0/h_2)=1$, es decir, $(h_2fp_0+h_1gq_0)/h_1h_2=1$ y $fp_0'+gq_0'=h$, con $p_0'=h_2p_0$, $q_0'=h_1q_0$ y $h_1h_2=h$. Ahora, sea U_1 una vecindad del punto $a\in k^{n-1}$

y $(b_1-\varepsilon_1,\ b_1+\varepsilon_1)$ una vecindad de b_1. Luego $U_1\cap(b_1-\varepsilon_1,\ b_1+\varepsilon_1)$ es una vecindad del punto $(a,\ b_1)$ tal que $f(x,\ b_1)<0$ para cada $x\in U_1\cap(b_1-\varepsilon_1,\ b_1+\varepsilon_1)$. Similarmente, sea U_2 una vecindad del punto $a\in k^{n-1}$ y $(b_2-\varepsilon_2,\ b_2+\varepsilon_2)$ una vecindad de b_2. Entonces $U_2\cap(b_2-\varepsilon_2,\ b_2+\varepsilon_2)$ es una vecindad del punto $(a,\ b_2)$ tal que $f(x,\ b_2)>0$ para cada $x\in U_2\cap(b_2-\varepsilon_2,\ b_2+\varepsilon_2)$. Tomando $U=U_1\cap U_2$, se cumple que $f(x,\ b_1)<0<f(x,\ b_2)$ para todo elemento $x\in U$. Sea $f:k^n\cap[b_1,\ b_2]\subset k^n\to k$, $f(x,\ b)=F_0+F_1b+\cdots+F_nb^n$ una función polinomial (con $F_0,F_1,\ldots,F_n\in A$, $b\in[b_1,\ b_2]$ y $x\in U$ fijo) continua en el conexo $k^n\cap[b_1,\ b_2]$, dado que $f(x,\ b_1)<0<f(x,\ b_2)$ con $(x,\ b_1),\ (x,\ b_2)\in U\times[b_1,\ b_2]$ y por el teorema del valor intermedio, existe un punto $(x,\ b_x)$ en la vecindad $U\times[b_1,\ b_2]$ con $x\in U$ fijo tal que $f\ (x,\ b_x)=0$ donde $b_x\in[b_1,\ b_2]$. Como por hipótesis $\mathbf{V}_k(f\ )\subseteq\mathbf{V}_k(g)$, se sigue que $g(x,\ b_x)=0$ y $f(x,\ b_x)p_0'(x,\ b_x)+g(x,\ b_x)q_0'(x,\ b_x)=h(x)$. De esto se obtiene que $h(x)=0$ para cada $x\in U$ y $h(x_1,\ldots,x_{n-1})$ se anula en un conjunto abierto no vacío en k^{n-1}. Luego h se anula en todo punto de k^{n-1} lo cual es una contradicción. □

Si $f\in k[x_1,\ldots,x_n]$, se define la **reducción** de f, denotada f_{red} como el polinomio que satisface $rad(<f>)=<f_{red}>$. Un polinomio es **reducido** o **libre de cuadrados** si $f=f_{red}$; es decir, si $rad(<f>)=f$.

Se termina este capítulo con un resultado de Dubois y Efroymson.

PROPOSICIÓN. 3.4.29. (*Criterio del cambio de signo*) Sea k un campo cerrado real y $f\in k[x_1,\ldots,x_n]$ un polinomio no cero. Entonces $<f>$ es real si y sólo si f es un producto de polinomios indefinidos e irreducibles libre de cuadrados.

DEMOSTRACIÓN ($\Rightarrow$)

La condición necesaria fue probada en 3.3.33..

($\Leftarrow$)

Sea $f=f_1^{\alpha_1}f_2^{\alpha_2}\cdots f_m^{\alpha_m}$ un producto de polinomios indefinidos e irreducibles libre de cuadrados, luego $f=f_1\cdot f_2\cdots f_m$. Sea $g_1^2+\cdots+g_m^2\in<f>$, entonces existen $h_i\in k[x_1,\ldots,x_n]$ tal que $g_1^2+\cdots+g_m^2=h_if_i$ con f_i indefinido e irreducible $i=1,\ldots,m$; así, $\mathbf{V}_k(f_i)\subseteq\mathbf{V}_k(g_i);i=1,\ldots,m$.[†)] Por el lema 3.4.28., se tiene que $f_i\mid g_i$; $i=1,\ldots,m$, es decir, $g_i=h_if_i$ para algún $h_i\in k[x_1,\ldots,x_n]$ y esto significa que $g_i\in<f>$. Por lo tanto $<f>$ es un ideal real. □

[†)] Si $x\in V_k(f\ )$, entonces $f(x)=0$ y $f(x)h(x)=g_1^2(x)+\cdots+g_m^2(x)=0$ implica $g_1(x)=\cdots=g_m(x)=0$ ya que $g_1(x),\ldots,g_m(x)\in k$. $x\in V_k(g_i)$; $i=1,2,\ldots,m$.

4. APLICACIONES DEL ÁLGEBRA A LA TEORÍA DE SINGULARIDADES.

INTRODUCCIÓN

Se introducen los conceptos de anillo y módulo graduados, y filtración de un módulo. Se presentan algunos resultados que permiten establecer el lema de Artin-Rees. Posteriormente se introduce el concepto de anillo de gérmenes en cero, de funciones C^∞ de $\mathbb{R}^n$ en $\mathbb{R}$; se dan algunas propiedades de este anillo y se exponen algunos resultados tales como el teorema de Tougeron y el lema de Borel. Estas dos afirmaciones junto con el concepto de germen de conjunto, permiten establecer la versión del lema de Artin-Rees en el anillo $\mathcal{E}(n)$.

4.1. LEMA DE ARTIN-REES.

Sea G un monóide abeliano y A un anillo. Una **graduación** de A es una familia $(A_i)_{i\in G}$ de subgrupos A_i del grupo abeliano de A tal que

i) $A=\oplus_{i\in G}A_i$

ii) $A_iA_j\subseteq A_{i+j}$ para cada $i, j\in G$.

La noción de graduación de un anillo A más frecuentemente usada, es cuando G es el monóide $\mathbb{N}^*=\mathbb{N}\cup\{0\}$.

DEFINICIÓN 4.1.1. Sea G un monóide abeliano. Un **anillo G-graduado** o **anillo graduado**, es un anillo A con una graduación $(A_i)_{i\in G}$.

Sea $A=B[x_1,\ldots,x_n]$ el anillo de polinomios en n indeterminadas con coeficientes en un anillo B. La familia $(A_n)_{n\in\mathbb{N}^*}$ donde A_k es el conjunto de polinomios homogéneos de grado k (o también llamados formas de grado k), es una graduación de A. Claramente $A=A_0\oplus A_1\oplus\cdots$ y $A_mA_n=A_{m+n}$ para cada $m, n\in\mathbb{N}^*$ (el grado de un producto de polinomios es la suma de sus grados). Como se sabe, todo elemento $f\in A$ puede escribirse en forma única (salvo el orden) como una suma de polinomios homogéneos, esto es, $f=\sum f_i$ con $f_i\in A_i$; f_i se llama componente homogénea de grado i de f. A, junto con esta graduación se convierte en un anillo graduado.

Sea G un monóide abeliano y A un anillo G-graduado. Como en el ejemplo anterior, los elementos de un A_i en la familia $(A_i)_{i\in G}$ se denominan **elementos homogéneos** de grado i y un elemento $a\in A$ puede ser escrito en forma única como $a=\sum_{i\in G} a_i$ con $a_i\in A_i$ y solamente un número finito de las a_i son diferentes de cero; a_i se denomina **componente homogénea** de grado i de a.

De la definición de graduación $(A_i)_{i\in G}$ de un anillo A, se observa que $A_0\subseteq A$ es un subanillo de A, y cada A_i, $i\in G$ es un A_0-módulo. En efecto, por definición A_0 es un subgrupo de A, es decir, *i*) $1_A\in A_0$, también *ii*) siempre que $a, b\in A_0$, entonces $a+b\in A_0$. Que

$ab \in A_0$ con a, $b \in A_0$ se sigue de $A_iA_j \subseteq A_{i+j}$ para $i=0$, $j=0$. Por otro lado, A_i para toda $i \in G$ son grupos abelianos, es decir, satisfacen que $A_i \neq \varnothing$ para cada $i \in G$, y si a, $b \in A_0$, x, $y \in A_i$, entonces ax, $by \in A_i$ para toda $i \in G$ ya que $A_0A_i \subseteq A_i$. Por lo tanto $ax+by \in A_i$ y A_i es un A_0-módulo para cada $i \in G$.

Similarmente, una **graduación de un A-módulo M**, con A un anillo graduado es una familia $(M_i)_{i \in G}$ de subgrupos M_i del grupo abeliano de M tal que

i) $M=\oplus_{i \in G} M_i$

ii) $A_iM_j \subseteq M_{i+j}$ para cada $i, j \in G$.

Se observa que cada $M_i \in (M_i)_{i \in G}$ es un A_0-submódulo de M.

DEFINICIÓN 4.1.2. Sea G un monóide abeliano y A un anillo graduado. Un **A-módulo graduado** o un **A-módulo G-graduado** es un A-módulo M con una graduación $(M_i)_{i \in G}$.

Como en el caso de anillos, los elementos de M_i, con $i \in G$ son llamados elementos homogéneos de grado i, y todo elemento en M puede escribirse de manera única como suma de elementos homogéneos donde un número finito de ellos son diferentes de cero.

DEFINICIÓN 4.1.3. Un ideal I de un anillo G-graduado A es **homogéneo** (también se denomina ideal G-graduado o ideal graduado) si I es generado por elementos homogéneos.

Para ideales homogéneos en anillos graduados se tienen las siguientes dos

OBSERVACIÓN 4.1.4. Un ideal I de un anillo graduado A es homogéneo si y sólo si para cada $a \in I$, las componentes homogéneas a_i ($i \in G$) de a también pertenecen a I.

DEMOSTRACIÓN ($\Rightarrow$)

Sea $(x_\lambda)_{\lambda \in \Lambda}$ un conjunto de generadores de I, donde x_λ es un elemento homogéneo de grado k_λ. Sea $a \in I$ con $a=\sum_{j=1}^{n} s_{\lambda_j} x_{\lambda_j}$, donde $s_{\lambda_j} = \sum_{i \in G} s_{\lambda_j}{}^{(i)}$ es la descomposición de s_{λ_j} [†)] en componentes homogéneas, donde el elemento s_{λ_j} es homogéneo de grado $grad(s_{\lambda_j}) = grad(a_i) - grad(x_{\lambda_j})$; esto es, $grad(s_{\lambda_j}) = (i - k_{\lambda_j})$. De esta forma $a = \sum_{i \in G} a_i$ con $a_i = s_{\lambda_1}{}^{(i-k_{\lambda_1})} x_{\lambda_1} + \cdots + s_{\lambda_n}{}^{(i-k_{\lambda_n})} x_{\lambda_n}$ donde a_i es de grado i; luego $a_i \in I$ para cada $i \in G$.

($\Leftarrow$)

Si un conjunto de generadores de I está dado, las componentes homogéneas de todos los elementos del conjunto de generadores también constituyen un conjunto de generadores de I. Así, I es un ideal homogéneo. □

OBSERVACIÓN 4.1.5. Un ideal I de un anillo graduado A es homogéneo si y sólo si A /I es un anillo graduado, con graduación $((A/I)_i)_{i \in G}$ donde $(A/I)_i=(A_i+I)/I$.

[†)] Cada s_{λ_j} es homogeneo de grado $grad(s_{\lambda_j})$=grad(a_i)-$grad(x_{\lambda_j})$; esto es, $grad(s_{\lambda_j})=(i-k_{\lambda_j})$.

DEMOSTRACIÓN ($\Rightarrow$)

Como $A/I=\sum_{i\in G}(A/I)_i$, por 4.1.4., será suficiente probar que la representación de un elemento de A/I como suma de elementos en $(A/I)_i$ es única. En efecto, supóngase que $\sum_{i\in G}\overline{a}_i=\overline{0}$ con $\overline{a}_i\in(A/I)_i$, es decir, $\overline{a}_i=a_i+I$ para algún $a_i\in A_i$. Entonces $\sum_{i\in G}a_i\in I$ y así, $a_i\in I$; por lo tanto $\overline{a}_i=\overline{0}$ para cada $i\in G$.

($\Leftarrow$)

Sea $a=\sum_{i\in G}a_i$ un elemento de I, $a_i\in A_i$ para cada $i\in G$. Entonces $\sum_{i\in G}\overline{a}_i=\overline{0}$ en A/I si $\overline{a}_i$ es la clase de a_i. De esto se sigue que $a_i\in I$ para cada $i\in G$. Por 4.1.4., se concluye que I es homogéneo. □

Se observa que si I es un ideal homogéneo finitamente generado, entonces I tiene un conjunto finito de generadores que consiste de elementos homogéneos únicamente. Además si I, J son ideales homogéneos de A, se sigue que $I+J$, IJ, $I\cap J$, la imagen de J en A/I y la imagen inversa de un ideal homogéneo en A/I son homogéneos.

En forma similar a como se define el concepto de homomorfismo para anillos o módulos, se define el concepto de homomorfismo entre módulos graduados, es decir, un **homomorfismo de A-módulos graduados** $\varphi:M\to N$ es un homomorfismo de módulos que satisface $\varphi(M_i)\subseteq N_i$ para cada $i\in G$.

Se recuerda que un anillo A es **noetheriano** si equivalentemente se satisface que todo ideal I de A es finitamente generado, toda familia de ideales en A tiene un elemento maximal (ahí) o toda cadena ascendente de ideales es estacionaria; en forma análoga se define módulo noetheriano. A continuación se dan algunos resultados referentes al concepto de noetherianidad útiles en esta sección. Se empieza con el teorema de la base de Hilbert.

TEOREMA 4.1.6. (*de la base de Hilbert*). Si A es un anillo noetheriano, entonces el anillo $A[x]$ es noetheriano.

DEMOSTRACIÓN

Sea $I_0\subseteq I_1\subseteq\cdots\subseteq I_j\subseteq I_{j+1}\subseteq\cdots$ una cadena ascendente de ideales en el anillo $A[x]$. Considérese el conjunto $C_i(I)=\{a\in A \mid \text{existen } a_0,\ldots,a_{i-1}\in A \text{ con } a_0+a_1x+\cdots+a_{i-1}x^{i-1}+ax^i\in I\}$ de coeficientes principales de polinomios de grado $i\in\mathbb{N}^*$ en el ideal I de $A[x]$. Claramente $C_i(I)$ es un ideal de A para toda $i\in\mathbb{N}^*$, $C_i(I_j)\subseteq C_i(I_{j+1})$ y $C_i(I_j)\subseteq C_{i+1}(I_j)$[†)] para toda $i, j\in\mathbb{N}^*$. Luego

$$C_i(I_0)\subseteq C_i(I_1)\subseteq\cdots\subseteq C_i(I_j)\subseteq C_i(I_{j+1})\subseteq\cdots \text{ y}$$
$$C_0(I_j)\subseteq C_1(I_j)\subseteq\cdots\subseteq C_i(I_j)\subseteq C_{i+1}(I_j)\subseteq\cdots$$

para toda $i, j\in\mathbb{N}^*$. Como A es noetheriano, existen $r, s\in\mathbb{N}^*$ tal que $C_r(I_s)$ es un elemento máximo del conjunto $\{C_i(I_j)\mid i, j\in\mathbb{N}^*\}$. Así, para toda $i\in\mathbb{N}^*$ con $i\geq r$, se tiene que

---

[†)] $C_i(I_j)\subseteq C_{i+1}(I_j)$ se sigue del hecho de que si $a\in C_i(I_j)$, entonces existen elementos $a_0,\ldots,a_{i-1}\in A$ tal que $a_0+a_1x+\cdots+ax^i\in I_i$. Como $x(a_0+a_1x+\cdots+ax^i)\in I_i$, se sigue que $a_0x+a_1x^2+\cdots+ax^{i+1}\in I_i$. Así, $a\in C_{i+1}(I_j)$.

$C_i(I_j)=C_i(I_s)=C_r(I_s)$ para cada $j\geq s$. Usando la condición de cadena ascendente en $C_0(I_j)\subseteq C_1(I_j)\subseteq\cdots\subseteq C_i(I_j)\subseteq C_{i+1}(I_j)\subseteq\cdots$ existe $s'\in\mathbb{N}^*$ tal que para toda $i=0,1,\ldots,r\text{-}1$, $C_i(I_j)\subseteq C_i(I_{s'})$ para cada $j\geq s'$. Haciendo $t=max\{s, s'\}$, se sigue que $C_i(I_j)=C_i(I_t)$ para toda i, $j\in\mathbb{N}^*$ con $i\geq r$ y $j\geq t$. Se afirma que $I_j=I_t$ para cada $j\geq t$; en efecto, por hipótesis $I_j\subseteq I_t$. Supóngase que $I_j\neq I_t$, es decir supóngase que $I_j\subsetneq I_t$, entonces existe al menos un polinomio no cero en $I_t \setminus I_j$. De estos polinomios se elige aquel que tiene grado más pequeño. Sea $g=b_0+b_1x+\cdots+b_ix^i$ con $b_i\neq 0$ este polinomio, luego $b_i\in C_i(I_j)=C_i(I_t)$. Entonces existe un polinomio $h=c_0+c_1x+\cdots+c_{i-1}x^{i-1}\in I_t$, con $g\text{-}h\in I_t \setminus I_j$; como $grad(g\text{-}h)\leq i\text{-}1$, se sigue que g no tiene grado mínimo ¡contradicción! Así, $I_j=I_t$ para toda $j\geq t$; luego la cadena ascendente

$$I_0\subseteq I_1\subseteq\cdots\subseteq I_j\subseteq I_{j+1}\subseteq\cdots$$

de ideales en A[x] es estacionaria. Por lo tanto A[x] es un anillo noetheriano. □

COROLARIO 4.1.7. Si A es un anillo noetheriano, entonces A[$x_1,\ldots,x_n$] es un anillo noetheriano.

DEMOSTRACIÓN (La demostración es por inducción)

El resultado para $n=1$ es el teorema de la base de Hilbert. Para $n>1$, el corolario se sigue de A[$x_1,\ldots,x_n$]=A[$x_1,\ldots,x_{n-1}$][x_n] y la hipótesis de inducción. □

LEMA 4.1.8. Sea A un anillo, M_1 y M_2 A-módulos. Si $\varphi:M_1 \rightarrow M_2$ es un epimorfismo y M_1 es noetheriano, entonces M_2 es noetheriano.

DEMOSTRACIÓN

Sea N_2 un A-submódulo de M_2, entonces $N_1=\varphi^{-1}(N_2)$ es un A-submódulo de M_1. Como M_1 es noetheriano, N_1 es finitamente generado; sea B un conjunto generador de N_1, dado que φ es un epimorfismo se sigue que $\varphi(B)$ es un conjunto generador de $\varphi(N_1)=N_2$. Luego N_2 es finitamente generado y M_2 es noetheriano. □

COROLARIO 4.1.9. Si A es un anillo noetheriano e I un ideal de A. Entonces A /I es noetheriano.

DEMOSTRACIÓN

El resultado se sigue de 4.1.8., considerando que $\pi:A \rightarrow A/I$ es un epimorfismo. □

PROPOSICIÓN 4.1.10. Sea A un anillo, M un A-módulo y N un A-submódulo de M. Entonces M es noetheriano si y sólo si N y M/N son noetherianos.

DEMOSTRACIÓN ($\Rightarrow$)

Dado que todo submódulo de N es un submódulo de M, se sigue que todo submódulo de N es finitamente generado, luego N es un módulo noetheriano. Ahora, sea

$$N_1/N\subseteq N_2/N\subseteq\cdots\subseteq N_n/N\subseteq\cdots$$

una cadena ascendente de submódulos de M/N, con $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n \subseteq \cdots$ una cadena ascendente de submódulos de M donde cada uno de ellos contiene a N. Como esta última cadena es estacionaria, se sigue que existe $n_0 \in \mathbb{N}$ tal que $N_{n_0} = N_{n_0+i}$ para toda $i \in \mathbb{N}$, y $N_{n_0}/N = N_{n_0+i}/N$ para cada $i \in \mathbb{N}$. Así, la primera cadena es estacionaria y M/N es noetheriano.

($\Leftarrow$)

Sea $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ una cadena ascendente de submódulos del módulo M y $N \cap M_1 \subseteq N \cap M_2 \subseteq \cdots \subseteq N \cap M_n \subseteq \cdots$ una cadena ascendente de submódulos de N. Como N es noetheriano, existe $k_1 \in \mathbb{N}$ tal que $N \cap M_{k_1} = N \cap M_{k_1+i}$ para cada $i \in \mathbb{N}$. También, se sabe que

$$N+M_1 \subseteq N+M_2 \subseteq \cdots \subseteq N+M_n \subseteq \cdots$$

es una cadena ascendente de submódulos de M donde cada término contiene a N, y así,

$$(N+M_1)/N \subseteq (N+M_2)/N \subseteq \cdots \subseteq (N+M_n)/N \subseteq \cdots$$

es una cadena ascendente de submódulos de M/N. Como M/N es noetheriano, existe $k_2 \in \mathbb{N}$ tal que $(N+M_{k_2})/N = (N+M_{k_2+i})/N$ para cada $i \in \mathbb{N}$, luego, $N+M_{k_2} = N+M_{k_2+i}$ para toda $i \in \mathbb{N}$. Sea $k = max\{k_1, k_2\}$; por demostrar que $M_k = M_{k+i}$ para cada $i \in \mathbb{N}$. Como $M_k \subseteq M_{k+i}$ restará probar que $M_{k+i} \subseteq M_k$ para toda $i \in \mathbb{N}$. Sea $x \in M_{k+i}$, como $N+M_k = N+M_{k+i}$, se sigue que $x \in N+M_k$ ya que $M_{k+i} \subseteq N+M_{k+i} = N+M_k$, entonces existen elementos $a \in N$ y $b \in M_k$ tal que $x = a+b$ y $a = x-b \in N \cap M_{k+i} = N \cap M_k$. Así, $a, b \in M_k$ y $a+b \in M_k$. □

Se recuerda que una sucesión de A-módulos y A-homomorfismos

$$\cdots \longrightarrow M_{j-1} \xrightarrow{\varphi_j} M_j \xrightarrow{\varphi_{j+1}} M_{j+1} \longrightarrow \cdots$$

es **exacta** en M_j si $Im(\varphi_j) = Ker(\varphi_{j+1})$; y es **exacta,** si es exacta en cada módulo M_j. Una **sucesión exacta corta** es una sucesión

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

donde φ es inyectiva, ψ suprayectiva e $Im(\varphi) = Ker(\psi)$. Los siguientes dos resultados son consecuencia de 4.1.10..

COROLARIO 4.1.11. Sea A un anillo y

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

una sucesión exacta corta de A-módulos y A-homomorfismos. Entonces M es noetheriano si y sólo si M' y M'' son noetherianos.

DEMOSTRACIÓN

Que la sucesión sea exacta corta, significa que φ es inyectiva y ψ suprayectiva, es decir, $M' \cong Im(\varphi) = Ker(\psi)$. Por el primer teorema del isomorfismo, $M/Ker(\psi) \cong M''$; luego por 4.1.10., M es noetheriano si y sólo si $Ker(\psi)$ y $M/Ker(\psi)$ son noetherianos, de esta forma M' y M'' son noetherianos. □

COROLARIO 4.1.12. Sean $M_1, \ldots, M_n$ módulos sobre un anillo A. Entonces la suma directa finita $\bigoplus_{i=1}^{n} M_i$ es noetheriano si y sólo si $M_1, \ldots, M_n$ son noetherianos.

DEMOSTRACIÓN

El resultado se prueba por inducción. Para $n=1$, se tiene que $\bigoplus_{i=1}^{n} M_i \cong M_1$. Sea $n>1$, entonces existe una sucesión exacta corta

$$0 \longrightarrow M_1 \xrightarrow{\alpha} \bigoplus_{i=1}^{n} M_i \xrightarrow{\beta} \bigoplus_{i=2}^{n} M_i \longrightarrow 0$$

Del corolario 4.1.11., se sigue que $\bigoplus_{i=1}^{n} M_i$ es noetheriano si y sólo si M_1 y $\bigoplus_{i=2}^{n} M_i$ son noetherianos. Por la hipótesis de inducción $\bigoplus_{i=2}^{n} M_i$ es noetheriano si y sólo si $M_2, \ldots, M_n$ son noetherianos. □

PROPOSICIÓN 4.1.13. Si A es un anillo noetheriano y M es un A-módulo finitamente generado, entonces M es noetheriano.

DEMOSTRACIÓN

Sean $b_1, \ldots, b_n$ generadores de M y considérese el homomorfismo

$$\varphi: A^n \to M;\ (a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i b_i .$$

φ es un epimorfismo, por el corolario 4.1.12. A^n es un A-módulo noetheriano. De esta forma, se sigue que M es un A-módulo noetheriano. □

DEFINICIÓN 4.1.14. Sea A un anillo y M un A-módulo. Una **filtración** de M es una cadena descendente $(M_n)_{n \in \mathbb{N}^*}$ de A-submódulos M_n de M. $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$.

DEFINICIÓN 4.1.15. Sea A un anillo, I un ideal de A y M un A-módulo. Una filtración $(M_n)_{n \in \mathbb{N}^*}$ de M es una ***I*-filtración** si $IM_n \subseteq M_{n+1}$ para cada $n \in \mathbb{N}^* = \mathbb{N} \cup \{0\}$.

DEFINICIÓN 4.1.16. Sea A un anillo, I un ideal de A y M un A-módulo. Una I-filtración $(M_n)_{n \in \mathbb{N}^*}$ es ***I*-estable** o **estable** si existe $n_0 \in \mathbb{N}$ tal que $IM_n = M_{n+1}$ para cada $n \geq n_0$.

EJEMPLO 4.1.17. Sea A un anillo, I un ideal de A y M un A-módulo. Entonces la familia $(I^n\mathrm{M})_{n\in\mathbb{N}^*}$ es una I-filtración estable.

La filtración $(\mathrm{M}_n)_{n\in\mathbb{N}^*}=(I^n\mathrm{M})_{n\in\mathbb{N}^*}$ se denomina **filtración canónica** de M o también **filtración *I*-ádica**.

OBSERVACIÓN 4.1.18. Sea A un anillo, I un ideal de A, M un A-módulo y $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$ una I-filtración de M. Entonces $I^n\mathrm{M}_m\subseteq\mathrm{M}_{n+m}$ para toda $m, n\in\mathbb{N}^*$.

DEMOSTRACIÓN

La demostración se hace por inducción. □

PROPOSICIÓN 4.1.19. Sea A un anillo, I un ideal de A y M un A-módulo. Si $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$ y $(\mathrm{M}_n')_{n\in\mathbb{N}^*}$ son I-filtraciones de M y $(\mathrm{M}_n')_{n\in\mathbb{N}^*}$ es I-estable, entonces existe $n_0\in\mathbb{N}$ tal que $\mathrm{M}'_{n+n_0}\subseteq\mathrm{M}_n$ para cada $n\in\mathbb{N}^*$.

DEMOSTRACIÓN

Por la estabilidad de $(\mathrm{M}_n')_{n\in\mathbb{N}^*}$ y por la observación 4.1.18., existe $n_0\in\mathbb{N}$ tal que para cada $n\in\mathbb{N}^*$, $\mathrm{M}'_{n+n_0}=I^n\mathrm{M}'_{n_0}\subseteq I^n\mathrm{M}\subseteq\mathrm{M}_n$. □

Se dice que dos filtraciones $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$ y $(\mathrm{M}_n')_{n\in\mathbb{N}^*}$ de un A-módulo M tienen **diferencia acotada** si existe $n_0\in\mathbb{N}$ tal que $\mathrm{M}_{n+n_0}\subseteq\mathrm{M}_n'$ y $\mathrm{M}'_{n+n_0}\subseteq\mathrm{M}_n$ para cada $n\in\mathbb{N}$.

El siguiente resultado se desprende directamente de 4.1.19.,

COROLARIO 4.1.20. Sea A un anillo, I un ideal de A, M un A-módulo y $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$, $(\mathrm{M}'_n)_{n\in\mathbb{N}^*}$ dos I-filtraciones estables de M. Entonces ellas tienen diferencia acotada. □

En el caso en que A es un anillo $\mathbb{N}^*$-graduado, es decir, $\mathrm{A}=\mathrm{A}_0\oplus\mathrm{A}_1\oplus\mathrm{A}_2\oplus\cdots$ se tiene

OBSERVACIÓN 4.1.21. $\mathrm{A}_+:=\mathrm{A}_1\oplus\mathrm{A}_2\oplus\cdots\oplus\mathrm{A}_n\oplus\cdots$ es un ideal de A.

DEMOSTRACIÓN

Sean $(x_i)_{i\in\mathbb{N}}$, $(y_i)_{i\in\mathbb{N}}\in\mathrm{A}_+$, donde casi todos los x_i, y_i son cero excepto un número finito de ellos. Como $x_i, y_i\in\mathrm{A}_i$ para cada $i\in\mathbb{N}$ y $\mathrm{A}_1, \mathrm{A}_2, \ldots$ son grupos, se sigue que $(x_i+y_i)_{i\in\mathbb{N}}\in\mathrm{A}_+$. Sea $(a_i)_{i\in\mathbb{N}^*}\in\mathrm{A}$ y $(x_j)_{j\in\mathbb{N}}\in\mathrm{A}_+$, entonces $a_i\in\mathrm{A}_i$ para cada $i\in\mathbb{N}^*$ con $x_j\in\mathrm{A}_j$ para toda $j\in\mathbb{N}$; como $\mathrm{A}_i\mathrm{A}_j\subseteq\mathrm{A}_{i+j}$ para toda $i\in\mathbb{N}^*$ y $j\in\mathbb{N}$, se sigue que $a_ix_j\in\mathrm{A}_{i+j}$, es decir, $(a_ix_j)\in\mathrm{A}_+$. □

Los anillos graduados tienen propiedades interesantes cuando ellos son noetherianos, es decir,

PROPOSICIÓN 4.1.22. Sea A un anillo $\mathbb{N}^*$-graduado. Entonces A es noetheriano si y sólo si A_0 es noetheriano y A es finitamente generado como A_0-álgebra.

DEMOSTRACIÓN ($\Rightarrow$)

Como A_+ es un ideal de A, A/A_+ es un anillo neotheriano que es isomorfo a A_0 ya que A_0 es una imagen homomorfa de A. Por otro lado, A_+ es un ideal finitamente generado. Sean $x_1,\ldots, x_s$ generadores de A_+, como todo elemento en A_+ puede escribirse de manera única como suma finita de elementos homogéneos en A_i, para cada $i\in\mathbb{N}$, es decir, $x_i=\sum_{j=1}^{t} y_j^{(i)}$, se puede suponer que $y_1,\ldots,y_t$ son los elementos homogéneos correspondientes a $x_1,\ldots,x_s$ de grados $k_1,\ldots,k_t$ respectivamente con $k_j>0$, $j=1,\ldots,t$. Sea B el subanillo de A generado por $y_1,\ldots,y_t$ sobre A_0, esto es, B es el menor subanillo de A que contiene a $y_1,\ldots,y_t$ y A_0, es decir, $B=A_0[y_1,\ldots,y_t]$; se tiene que probar que A=B. Para ello se probará por inducción sobre n que $A_n\subseteq B$ para cada $n\in\mathbb{N}^*$. De como se ha definido B, es claro que $A_0\subseteq B$. Sea $n>0$, si $y\in A_n$, entonces $y\in A_+$ y es un elemento homogéneo de grado n. Luego existen elementos $a_j\in A_{n-k_j}$; $j=1,\ldots,t$ tal que $y=\sum_{i=1}^{t} a_i y_i$. Como cada $k_j>0$, por la hipótesis de inducción se tiene que $a_j\in A_0[y_1,\ldots,y_t]$, $j=1,\ldots,t$, es decir, cada a_j es un polinomio en las indeterminadas $y_1,\ldots,y_t$ con coeficientes en A_0. Esto último significa que $y\in A_0[y_1,\ldots,y_t]$ y $A_n\subseteq B$ para todo $n\in\mathbb{N}^*$. Por lo tanto A es finitamente generado como una A_0-álgebra.

($\Leftarrow$)

Como A es una A_0-álgebra finitamente generada, A es una imagen homomorfa de $B=A_0[x_1,\ldots,x_r]$ para algún $r\in\mathbb{N}$. Por el teorema de la base de Hilbert, se tiene que B es noetheriano ya que A_0 es noetheriano; y como toda imagen homomorfa de un anillo noetheriano es noetheriana, se sigue que A es noetheriano. □

Sea A un anillo no graduado, I un ideal de A, M un A-módulo y $(M_n)_{n\in\mathbb{N}^*}$ una I - filtración de M. Se define

1) $A^*:=I^0\oplus I\oplus I^2\oplus\cdots\oplus I^n\oplus\cdots$

2) $M^*:=M_0\oplus M_1\oplus M_2\oplus\cdots\oplus M_n\oplus\cdots$

A^* es un anillo con las operaciones de suma y multiplicación:

$$(a_i)_{i\geq 0}+(b_i)_{i\geq 0}=(a_i+b_i)_{i\geq 0} \text{ y}$$
$$(a_i)_{i\geq 0}\cdot(b_i)_{i\geq 0}=(a_ib_0+\cdots+a_0b_i)_{i\geq 0}$$

con $(a_i)_{i\geq 0}$, $(b_i)_{i\geq 0}\in A^*$, donde todas las a_i, b_i con $i\geq 0$ son cero excepto un número finito de ellas. El módulo M^* es un A^*-módulo con las operaciones de suma y multiplicación escalar

$$(x_i)_{i\geq 0}+(y_i)_{i\geq 0}=(x_i+y_i)_{i\geq 0} \text{ y}$$
$$(a_i)_{i\geq 0}\cdot(x_i)_{i\geq 0}=(a_ix_0+\cdots+a_0x_i)_{i\geq 0}$$

con $(a_i)_{i\geq 0}\in A^*$, $(x_i)_{i\geq 0}$, $(y_i)_{i\geq 0}\in M^*$; x_i, y_i, a_i, cero excepto un número finito. A^* es un anillo graduado (ya que $I^m\cdot I^n\subseteq I^{m+n}$ para cada $m, n\in\mathbb{N}^*$) y M^* es un A^*-módulo graduado (de 4.1.18., se sigue que $I^mM_n\subseteq M_{m+n}$ para cada $m, n\in\mathbb{N}^*$). En el caso en que A es un anillo noetheriano, se tiene

OBSERVACIÓN 4.1.23. Sea A un anillo noetheriano no graduado e I un ideal de A. Entonces A* es un anillo noetheriano.

DEMOSTRACIÓN

Como A es noetheriano, el ideal I es finitamente generado. Sean $a_1,\ldots,a_s$ generadores de I; considérese el anillo de polinomios $A[x_1,\ldots,x_s]$ en las indeterminadas $x_1,\ldots,x_s$ con coeficientes en A. Sea $\varphi: A[x_1,\ldots,x_s] \to A^*$, $x_i \mapsto a_i$, $x_1^{j_1}\ldots x_s^{j_s} \mapsto a_1^{j_1}\ldots a_s^{j_s}$. φ es un homomorfismo suprayectivo. Por el teorema de la base de Hilbert, $A[x_1,\ldots,x_s]$ es noertheriano y por el lema 4.1.8., A* es noetheriano. □

Sea A un anillo noetheriano no graduado, I un ideal de A, M un A-módulo finitamente generado y $(M_n)_{n\in\mathbb{N}^*}$ una I-filtración de M, entonces se puede considerar la suma directa finita $\bigoplus_{i=0}^{n} M_i$ (para cada $n\in\mathbb{N}^*$) de A-submódulos de M. La suma finita $\bigoplus_{i=0}^{n} M_i$ es un subgrupo del A*-módulo M* que en general no es un A*-submódulo de M* (ya que si $a_i x_i \in A_i\cdot M_i \subseteq M_{i+i}$, $a_i\in A$, $x_i\in M_i$, entonces $(a_i\cdot x_i)_{i\geq 0} \notin \bigoplus_{i=0}^{n} M_i$ para al menos un $n\in\mathbb{N}^*$). Pero el generado por $\bigoplus_{i=0}^{n} M_i$ en A*; $<\bigoplus_{i=0}^{n} M_i>_{A^*}$ es un A*-submódulo de M*. Se afirma que

$$<\bigoplus_{i=0}^{n} M_i>_{A^*} = M_0\oplus M_1\oplus\cdots\oplus M_n\oplus IM_n\oplus I^2M_n\oplus\cdots$$

En efecto, como A es noetheriano y M es finitamente generado, se tiene que M_i es finitamente generado para toda $i\in\mathbb{N}^*$, entonces $\bigoplus_{i=0}^{n} M_i$ es finitamente generado. Como $M_0, M_1,\ldots,M_n$ son finitamente generados, existen conjuntos

$$\{m_0^0, m_1^0,\ldots,m_{k_0}^0\},\ \{m_0^1, m_1^1,\ldots,m_{k_1}^1\},\ldots,\ \{m_0^n, m_1^n,\ldots,m_{k_n}^n\}.$$

Entonces

$\{(m_0^0,0,\ldots,0),(m_1^0,0,\ldots,0),\ldots,(m_{k_0}^0,0,\ldots,0),(0,m_0^1,0,\ldots,0),(0,m_1^1,0,\ldots,0),\ldots,(0,m_{k_1}^1,0,\ldots,0),\cdots,(0,\ldots,m_0^n),(0,\ldots,m_1^n),\ldots,(0,\ldots,m_{k_n}^n)\}$ es un conjunto de generadores de la suma directa finita $\bigoplus_{i=0}^{n} M_i$. Todo elemento $(x_i)_{i\geq 0}$ en $<\bigoplus_{i=0}^{n} M_i>_{A^*}$ se puede escribir como $(x_i)_{i\geq 0}=(a_i^{00})_{i\geq 0}\cdot(m_0^0,0,\ldots,0)+(a_i^{01})_{i\geq 0}\cdot(m_1^0,0,\ldots,0)+\cdots+(a_i^{0k_0})_{i\geq 0}\cdot(m_{k_0}^0,0,\ldots,0)+(a_i^{10})_{i\geq 0}\cdot(0,m_0^1,0,\ldots,0)+(a_i^{11})_{i\geq 0}\cdot(0,m_1^1,0,\ldots,0)+\cdots+(a_i^{1k_1})_{i\geq 0}\cdot(0,m_{k_1}^1,0,\ldots,0)+\cdots+(a_i^{n0})_{i\geq 0}(0,\ldots,m_0^n)+(a_i^{n1})_{i\geq 0}\cdot(0,\ldots,m_1^n)+\cdots+(a_i^{nk_n})_{i\geq 0}\cdot(0,\ldots,m_{k_n}^n)$.

Considérese un sumando arbitrario, $(a_i^{jk})_{i\geq 0}\cdot(0,\ldots,m_k^j,\ldots,0)$ con $j=0,1,\ldots,n$; $k=0,1,\ldots,k_j$. Este sumando es igual a

$$(0,\dots,0,\ a_0{}^{jk}m_k{}^{j},\ a_1{}^{jk}m_k{}^{j},\dots,a_n{}^{jk}m_k{}^{j},\ a_{n+1}{}^{jk}m_k{}^{j},\dots)$$

donde $a_0{}^{jk}m_k{}^{j}\in \mathrm{M}_{k,}$, $a_1{}^{jk}m_k{}^{j}\in \mathrm{M}_{k,+1},\dots,a_n{}^{jk}m_k{}^{j}\in I^{n}\mathrm{M}_k\subseteq I^{n-1}\mathrm{M}_{k+1}\subseteq I^{n-2}\,\mathrm{M}_{k+2}\subseteq\cdots\subseteq I^{k}\,\mathrm{M}_n$. Así, $(a_i{}^{jk})_{i\geq 0}\ (0,\dots,m_k{}^{j},\dots,0)\in \mathrm{M}_0\oplus\mathrm{M}_1\oplus\cdots\oplus\mathrm{M}_n\oplus I\mathrm{M}_n\oplus I^2\mathrm{M}_n\oplus\ \cdots$ y $(x_i)_{i\geq 0}\in\mathrm{M}$. Luego se tiene $<\bigoplus_{i=0}^{n}\mathrm{M}_i>_{\mathrm{A}^*}\subseteq\mathrm{M}_n$. Recíprocamente, considérese un generador en M, esto es, $(0,\dots,m_n,\dots)$ y sea $(0,\dots,am_n,\dots)=(a_i)_{i\geq 0}(x_0,x_1,\dots,x_n,0,\dots)=(a_0x_0,a_0x_1+a_1x_0,a_0x_2+a_1x_1+a_2x_0,\dots,a_0x_n+\cdots+a_nx_0,a_0x_{n+1}+a_1x_n+\cdots+a_{n+1}x_0,a_0x_{n+2},a_1x_{n+1},a_2x_n+\cdots+a_{n+2}x_0,\cdots)=(a_0x_0,a_0x_1+a_1x_0,a_0x_2+a_1x_1+a_2x_0,\dots,a_0x_n+\cdots+a_nx_0,\ a_1x_n+\cdots+a_{n+1}x_0,\ a_2x_n+\cdots+a_{n+2}x_0,\dots)$ ya que $a_{n+1}=x_{n+2}=\cdots=0$.

De la igualdad se sigue que

$$\left.\begin{aligned} a_0x_0 &= 0\\ a_0x_1+a_1x_0 &= 0\\ &\vdots\\ a_0x_n+\cdots+a_nx_0 &= 0\\ a_1x_n+\cdots+a_nx_1+a_{n+1}x_0 &= am_n\\ a_2x_n+\cdots+a_nx_2+a_{n+1}x_1+a_{n+2}x_0 &= 0\\ &\vdots \end{aligned}\right\}$$

De $a_1x_n+\cdots+a_nx_1+a_{n+1}x_0=am_n$ se obtiene que $a_{n+1}x_0=am_n$, esto es, $a=a_{n+1}$ y $x_0=m_n$. De $a_{n+1}x_1+a_{n+2}x_0=0$, se sigue que $a_{n+1}=a_{n+2}=0$. Así, $(0,\dots,am_n,\dots)$ es un elemento de $<\bigoplus_{i=0}^{n}\mathrm{M}_i>_{\mathrm{A}}$ y por consiguiente $\mathrm{M}_n\subseteq<\bigoplus_{i=0}^{n}\mathrm{M}_i>_{\mathrm{A}^*}$. Por lo tanto $<\bigoplus_{i=0}^{n}\mathrm{M}_i>_{\mathrm{A}^*}=\mathrm{M}_n$ para toda $n\in\mathbb{N}^*$.

En el caso en que A sea un anillo noetheriano y M un A-módulo finitamente generado, la estabilidad de cualquier filtración del módulo M será equivalente a que el módulo M* sea finitamente generado como un A*-módulo, es decir,

LEMA 4.1.24. Sea A un anillo noetheriano, I un ideal de A, M un A-módulo finitamente generado y $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$ una I-filtración de M. Entonces el A*-módulo M* es finitamente generado si y sólo si $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$ es estable.

DEMOSTRACIÓN $(\Rightarrow)$

Sea $\mathrm{M}_n{}^*=\mathrm{M}_0\oplus\mathrm{M}_1\oplus\cdots\oplus\mathrm{M}_n\oplus I\mathrm{M}_n\oplus I^2\mathrm{M}_n\oplus\cdots$ Por lo anterior, se tiene que

$$<\bigoplus_{i=0}^{n}\mathrm{M}_i>_{\mathrm{A}^*}=\mathrm{M}_n{}^*$$

es un A*-submódulo de M*. $\mathrm{M}_n{}^*\subseteq\mathrm{M}_{n+1}{}^*$ para toda $n\in\mathbb{N}^*$ ya que $I^m\mathrm{M}_n\subseteq\mathrm{M}_{m+n}$ para cada $m\in\mathbb{N}$ y $(\mathrm{M}_n{}^*)_{n\in\mathbb{N}^*}$ forma una cadena ascendente con $\cup_{n\in\mathbb{N}^*}\mathrm{M}_n{}^*=\mathrm{M}$. Como A* es noetheriano y M* es finitamente generado, M* es noetheriano. Entonces la cadena $\mathrm{M}_0{}^*\subseteq\mathrm{M}_1{}^*\subseteq\cdots\subseteq\mathrm{M}_n{}^*\subseteq\cdots$ es estacionaria, esto es, existe $n_0\in\mathbb{N}$ tal que $\mathrm{M}_{n_0}^{*}=\mathrm{M}$, es decir, $\mathrm{M}_{n_0}=\mathrm{M}^*$ y $\mathrm{M}_{n_0+k}=I^k\mathrm{M}_{n_0}$ para cada $k\in\mathbb{N}^*$. Esto último significa que $(\mathrm{M}_n)_{n\in\mathbb{N}^*}$ es estable.

($\Leftarrow$)

Si $(M_n^*)_{n\in\mathbb{N}^*}$ es estable, entonces $M_{n_0+j} = I^j M_{n_0}$ para alguna $n_0\in\mathbb{N}$ y para cada $j\in\mathbb{N}$. Luego M* es generado por la unión de todos los conjuntos de generadores para $M_0,\ldots,M_n$. Por lo tanto, M* es finitamente generado. □

PROPOSICIÓN 4.1.25. (*lema de Artin-Rees*) Sea A un anillo noetheriano, *I* un ideal de A, M un A-módulo finitamente generado y $(M_n)_{n\in\mathbb{N}^*}$ una *I*-filtración estable de M. Si N es un A-submódulo de M, entonces la filtración inducida $(N\cap M_n)_{n\in\mathbb{N}^*}$ es una *I*-filtración estable, es decir, existe $n_0\in\mathbb{N}$ tal que para toda $n\in\mathbb{N}^*$, se tiene que $N\cap M_{n+n_0} = I^n(N\cap M_{n_0})$.

DEMOSTRACIÓN

$(N\cap M_n)_{n\in\mathbb{N}^*}$ es una *I*-filtración ya que $I(N\cap M_n)\subseteq IN\cap IM_n\subseteq N\cap M_{n+1}$ para cada $n\in\mathbb{N}^*$. Esta filtración inducida define un A*-submódulo

$$N^*=(N\cap M_0)\oplus(N\cap M_1)\oplus(N\cap M_2)\oplus\cdots\oplus(N\cap M_n)\oplus\cdots$$

de M*. Dado que $(M_n)_{n\in\mathbb{N}^*}$ es una *I*-filtración estable del módulo M, por el lema anterior, M* es un A*-módulo finitamente generado. Como A* es noetheriano, M* es noetheriano y N* es un A*-submódulo finitamente generado, nuevamente por 4.1.24., se tiene que la filtración inducida $(N\cap M_n)_{n\in\mathbb{N}^*}$ es una *I*-filtración estable de N. □

Como una consecuencia inmediata del lema de Artin-Rees, se tiene el

COROLARIO 4.1.26. Sea A un anillo noetheriano, *I* un ideal de A, M un A-módulo finitamente generado y N un A-submódulo de M. Entonces existe $n_0\in\mathbb{N}$ tal que para cada $n\in\mathbb{N}^*$, se tiene que $I^{n+n_0}M\cap N = I^n(I^{n_0}M\cap N)$.

DEMOSTRACIÓN

Por el lema de Artin-Rees, existe $n_0\in\mathbb{N}$ tal que para cada $n\in\mathbb{N}^*$, se tiene que $M_{n+n_0}\cap N = I^n(M_{n_0}\cap N)$. Tomando $M_n = I^n M$, se sigue el resultado

$$I^{n+n_0}M\cap N = I^n(I^{n_0}M\cap N).\ \square$$

Para cerrar esta sección, se tiene el siguiente

TEOREMA 4.1.27. Sea A un anillo noetheriano, *I* un ideal de A, M un A-módulo finitamente generado y N un A-submódulo de M, entonces las filtraciones $(I^nN)_{n\in\mathbb{N}^*}$ y $((I^nM)\cap N)_{n\in\mathbb{N}^*}$ tienen diferencia acotada.

DEMOSTRACIÓN

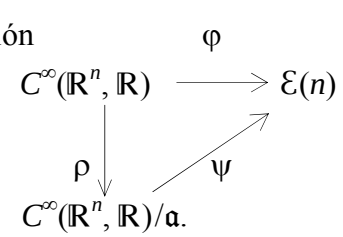
Por 4.1.17., y por el lema de Artin-Rees, las filtraciones $(I^nN)_{n\in\mathbb{N}^*}$ y $((I^nM)\cap N)_{n\in\mathbb{N}^*}$ son filtraciones estables. El resultado se sigue de 4.1.20.. □

4.2 EL LEMA DE ARTIN-REES EN EL ANILLO $\mathcal{E}(n)$.

Sea $C^\infty(\mathbb{R}^n, \mathbb{R}^m)$ el anillo de funciones C^∞ de $\mathbb{R}^n$ en $\mathbb{R}^m$. Si $f, g \in C^\infty(\mathbb{R}^n, \mathbb{R}^m)$, se define una relación en el conjunto $C^\infty(\mathbb{R}^n, \mathbb{R}^m)$ como: f es equivalente a g en el punto x, escrito $f \sim_x g$ si existe $V(x)$ vecindad de x en $\mathbb{R}^n$ tal que $f|_{V(x)} = g|_{V(x)}$ con $f|_{V(x)}$, $g|_{V(x)}$ las restricciones de f y g a la vecindad $V(x)$. $\sim_x$ es una relación de equivalencia en $C^\infty(\mathbb{R}^n, \mathbb{R}^m)$.

DEFINICIÓN 4.2.1. Sea $f \in C^\infty(\mathbb{R}^n, \mathbb{R}^m)$ y $x \in \mathbb{R}^n$. El **germen** de f en x es la clase de equivalencia de f en x dada por la relación $\sim_x$ y se escribe como $\overline{f}$, $[f]$, $[f]_x$ o simplemente f como su representante. De aquí en adelante se usará esta última notación a menos que se especifique otra cosa.

Sea $\mathcal{E}(n)$ el conjunto de gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$. $\mathcal{E}(n)$ es un anillo (conmutativo con unitario) y un $\mathbb{R}$-espacio vectorial de dimensión infinita; esto es, $\mathcal{E}(n)$ es una $\mathbb{R}$-álgebra. Las operaciones en el conjunto de gérmenes $\mathcal{E}(n)$ están inducidas por las operaciones en $\mathbb{R}$. Se puede extender el concepto de germen en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$ a gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R}^m)$ de la siguiente forma: Si $f : \mathbb{R}^n \to \mathbb{R}^m$ es una función C^∞, $f=(f_1, \ldots, f_m)$, entonces el germen de f en cero es dado por $f=(f_1, \ldots, f_m)$, $f_j \in \mathcal{E}(n)$, $j=1, \ldots, m$ y $V(0)=\cap V_i(0)$ es la vecindad en cero de f con $V_j(0)$ vecindad de $f_j \in \mathcal{E}(n)$, $j=1, \ldots, n$. El conjunto de gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R}^m)$ es denotado por $\mathcal{E}(n, m)$. Este conjunto es isomorfo al producto de los m factores $\mathcal{E}(n) \times \cdots \times \mathcal{E}(n)$ (el isomorfismo viene dado por $(f_1, \ldots, f_m) \mapsto f$ donde $f=(f_1, \ldots, f_m)$), lo cual significa que $\mathcal{E}(n, m)$ es un espacio vectorial de dimensión infinita. Las operaciones en el conjunto $\mathcal{E}(n, m)$ están inducidas coordenada a coordenada por las operaciones de $\mathcal{E}(n)$. Sea $\varphi : C^\infty(\mathbb{R}^n, \mathbb{R}) \to \mathcal{E}(n)$; $f \mapsto f$, φ es suprayectiva y su núcleo es



$$\mathfrak{a} = Ker(\varphi) = \{f \in C^\infty(\mathbb{R}^n, \mathbb{R}) \mid f \text{ se anula en una vecindad del cero}\}.$$

En este caso, se cumple que $\mathcal{E}(n) \cong C^\infty(\mathbb{R}^n, \mathbb{R})/\mathfrak{a}$. Este hecho se puede utilizar para definir la estructura de $\mathcal{E}(n)$, es decir, en forma similar a como se ha introducido $\mathfrak{a}$ se define el subconjunto $m(n)$ de $\mathcal{E}(n)$ como el conjunto de gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$ que se anulan en cero esto es, $m(n)=\{ f \in \mathcal{E}(n) \mid f(0)=0\}$. De la estructura de $\mathcal{E}(n)$, se sigue que $m(n)$ es un ideal de $\mathcal{E}(n)$. Más concretamente

OBSERVACIÓN 4.2.2. $\mathcal{E}(n)$ es un anillo local real y $m(n)$ su ideal maximal real.

DEMOSTRACIÓN

Primero se probará que $\mathcal{E}(n)$ es un anillo local con $m(n)$ su ideal maximal. En efecto, supóngase que $f \notin m(n)$, entonces $f(0)\neq 0$ y existe una vecindad del cero, V(0) tal que el representante $f(x)\neq 0$ para toda $x \in V(0)$, luego considerando el germen $1/f$, el representante $1/f$, esta definido en la misma vecindad V(0); así, $(f\ )(1/f\ )$ es el germen de la función constante 1. De esta forma, $\mathcal{E}(n)\setminus m(n)$ contiene únicamente unidades. Por otro lado, como $\mathcal{E}(n)/m(n) \cong \mathbb{R}$, esto es, $m(n)$ es un ideal real, se sigue que $\mathcal{E}(n)$ es un anillo local real. □

De 1.2.31., se sigue que $(\mathcal{E}(n), m(n))$ es un anillo semireal y por el teorema de Artin-Schreier (teorema 2.2.27.) $\mathcal{E}(n)$ es un anillo ordenado; un orden T en $\mathcal{E}(n)$ viene dado como $T = \{ f \in \mathcal{E}(n) \mid f(0) \geq 0 \}$, con centro el ideal $\mathcal{C}(T)=m(n)$. Como ya se comentó, no todo anillo ordenado es un anillo real, pero en este caso $\mathcal{E}(n)$ es un anillo real.

Antes de ver que $m(n)$ es finitamente generado, se probará el siguiente resultado preliminar.

LEMA 4.2.3. Sea $f: U \subseteq \mathbb{R}^n \to \mathbb{R}$ una función C^∞ en un conjunto abierto U estrellado de centro cero en $\mathbb{R}^n$,[†)] entonces existen funciones $g_i: U \subseteq \mathbb{R}^n \to \mathbb{R}$, $i=1, 2, \ldots, n$ tal que $f(x)-f(0)=\sum_{i=1}^{n} x_i\ (x) g_i(x)$ con $x_i: \mathbb{R}^n \to \mathbb{R}$; $x_i(x_1, \ldots, x_n)=x_i$ la función proyección.

DEMOSTRACIÓN

Sea $h:[0\ ,\ 1]\times U \subsetneq \mathbb{R}^{n+1} \to \mathbb{R}^n$; $h(t, x)=tx$ y $g:[0\ ,\ 1]\times U \subsetneq \mathbb{R}^{n+1} \to \mathbb{R}$; $g(t, x)=f(tx)$ la función composición de f y h, esto es, $g=f\circ h$. Por la regla de la cadena, se tiene que

$$Dg(t, x)=Df\,(h(t, x))Dh(t, x)$$

entonces, $\dfrac{\partial g(t,x)}{\partial t} = \sum_{i=1}^{n} \dfrac{\partial f\,(tx)}{\partial x_i} x_i(x)$. Por el teorema fundamental del cálculo, se sigue que

$$\begin{aligned} f\,(x) - f\,(0) &= \int_0^1 \frac{\partial g(t,x)}{\partial t}\, dt \\ &= \int_0^1 \sum_{i=1}^{n} \frac{\partial f\,(tx)}{\partial t} x_i(x)\, dt \\ &= \sum_{i=1}^{n} x_i(x) \int_0^1 \frac{\partial f\,(tx)}{\partial t} dt \end{aligned}$$

[†)] Se recuerda que un subconjunto U de $\mathbb{R}^n$ es **estrellado** con centro en un punto p si para cada punto x en U, el segmento con puntos extremos p y x está enteramente contenido en U.

Sean g_i: $\mathbb{R}^n \to \mathbb{R}$; $g_i(x) = \int_0^1 \frac{\partial f(tx)}{\partial x_i} dt$, $g_i(0) = \int_0^1 \frac{\partial f(0)}{\partial x_i} dt = \frac{\partial f(0)}{\partial x_i}$; $i=1,\ldots,n$, donde las $g_i(x)$ son funciones C^∞ ya que tanto f como $\frac{\partial f(tx)}{\partial x_i}$ son funciones C^∞. Por lo tanto

$$f(x)\text{-}f(0)=\sum_{i=1}^{n} x_i(x) g_i(x). \square$$

Si $f\in m(n)$, por el lema anterior, $f(x)\text{-}f(0)=\sum_{i=1}^{n} x_i(x) g_i(x)$ para $g_i(x)\in \mathcal{E}(n)$, $i=1,\ldots,n$. Entonces f es generado por los gérmenes $x_1,\ldots,x_n$, esto es,

OBSERVACIÓN 4.2.4. El ideal $m(n)$ es finitamente generado por los gérmenes en cero de las coordenadas $x_1,\ldots,x_n$; con x_i: $\mathbb{R}^n \to \mathbb{R}$, $x_i(x_1,\ldots,x_n)=x_i$, la proyección i-ésima. □

De esta observación se sigue que, $m(n)^k$ con $k\in\mathbb{N}$ es el ideal generado por todos los monomios en x_i de grado k, es decir, $m(n)^k$ es finitamente generado por todos los gérmenes en cero de la forma $x^{\mathrm{I}}= x_1^{i_1}\cdots x_n^{i_n}$ con $|\mathrm{I}|=i_1+\cdots+i_n=k$. También, se observa que $m(n)\supsetneq m(n)^2\supsetneq\cdots\supsetneq m(n)^k\supsetneq m(n)^{k+1}\supsetneq\cdots$. Si un germen $f\in m(n)^k$ para toda $k\in\mathbb{N}$, ello será equivalente a: $f(0)=0$ y $\partial^{|\mathrm{I}|}f(0)/\partial x^{\mathrm{I}}=0$ para todo multiíndice I con $|\mathrm{I}|\leq k$-1. Es decir, todas las derivadas parciales de orden $\leq k$-1 se anulan en cero, esto significa que, $\partial f/\partial x_i\in m(n)^{k-1}$. Se define $m(n)^\infty := \cap_{k=1}^{\infty} m(n)^k \subseteq \mathcal{E}(n)$. Al igual que $m(n)$, el ideal $m(n)^\infty$ es un ideal primo real. Un germen $f\in\mathcal{E}(n)$ está en $m(n)^\infty$ si para cada $k\in\mathbb{N}$, existe una representación $f=\sum f_{\mathrm{I}} x^{\mathrm{I}}$, esto es, si todos los gérmenes $\partial^{|\mathrm{I}|}f(0)/\partial x^{\mathrm{I}}=0$, $|\mathrm{I}|\leq k$ para toda $k\in\mathbb{N}$. De lo anterior se observa que $m(n)m(n)^\infty=m(n)^\infty$. En efecto, si $\sum x_i\, h_i\in m(n)m(n)^\infty$, con $x_i\in m(n)$ y $h_i\in m(n)^\infty$; por el lema 4.2.3., la función $f\text{-}f(0)$ está en $m(n)m(n)^\infty$. Dado que $f\text{-}f(0)$ es de clase C^∞ y sus derivadas de todos los ordenes se anulan en cero, se concluye que $f\text{-}f(0)\in m(n)^\infty$. Claramente se tiene que $m(n)^\infty\subseteq m(n)m(n)^\infty$. Por inducción sobre k, se sigue que $m(n)^k m(n)^\infty=m(n)^\infty$ para toda $k\in\mathbb{N}$. Un resultado más general que a primera vista parece sencillo de probar es $m(n)^\infty m(n)^\infty=m(n)^\infty$. Este resultado, se sigue del siguiente lema.

LEMA (*Tougeron*). Si $f\in m(n)^\infty$, entonces existen gérmenes g, $h\in m(n)^\infty$ con $g(x)>0$ para cada $x\neq 0$ tal que $f=gh$.

DEMOSTRACIÓN

Sea $(\mathrm{B}(0,\ 1/2^{i-1}))_{i\in\mathbb{N}}$, la familia anidada de bolas esféricas con centro cero y radios $r=1/2^{i-1}$, $(\mathrm{K}_i)_{i\in\mathbb{N}}$; $\mathrm{K}_i=\overline{\mathrm{B}(0,\ 1/2^{i-1})}\setminus\mathrm{B}(0,\ 1/2^i)$ una familia de compactos y $(\mathrm{F}_i)_{i\in\mathbb{N}}$, $\mathrm{F}_i=(\mathbb{R}^n\setminus\mathrm{B}(0,\ 1/2^{i-1}))\cup\overline{\mathrm{B}(0,\ 1/2^{i+2})}$ una familia de cerrados que contienen al cero. Por el lema de Malgrange (ver apéndice C) existen gérmenes ρ_i en $\mathcal{E}(n)$, para $i\in\mathbb{N}$

$$\rho_i(x)=\begin{cases}1 & \text{si} \quad x\in \mathrm{K}_{i+1}\\ 0 & \text{si} \quad x\in \mathrm{F}_i\end{cases}$$

$\rho_i(x) \geq 0$ para cada $x \in \mathbb{R}^n$; y constantes C_r que no dependen de $i \in \mathbb{N}$ tal que

$$\left|\rho_i\right|_r \leq C_r 2^{ir} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\left|\rho_i\right|_r = \sup_{|\mathrm{I}|\leq r} \left| D^{|\mathrm{I}|} \rho_i(x) \right| .$$

Como $f \in m(n)^{\infty}$, se pueden construir dos sucesiones $(\alpha(r))_{r\in\mathbb{N}}$ y $(\beta(i))_{i\in\mathbb{N}}$ con $(\alpha(r))_{r\in\mathbb{N}}$ creciente y diverge a $+\infty$ y $(\beta(i))_{i\in\mathbb{N}}$ que satisface: $\beta(i) = r$ si $\alpha(r) \leq i < \alpha(r+1)$ tal que para cada $x \in \mathrm{B}(0,\ 1/2^{\alpha(r)})$ y para todo $i \in \{0,1,2,...,r^2+1\}$ (por Taylor) se tiene que

$$\left| f \right|_r^x \leq \left| x \right|^{r^2}$$

De las desigualdades (1), se sigue que la serie $\lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \left(\frac{1}{2^i}\right)^{\beta(i)} \rho_i$ converge uniformemente en $\mathbb{R}^n$, así como todas sus derivadas. En efecto, considérese la serie de derivadas

$$\left| \lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \frac{\partial^{|\mathrm{I}|}}{\partial x^{\mathrm{I}}} \left(\frac{1}{2^i}\right)^{\beta(i)} \rho_i(x) \right|$$

la cual es igual a la serie

$$\lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \left(\frac{1}{2^i}\right)^{\beta(i)} \left| \frac{\partial^{|\mathrm{I}|}}{\partial x^{\mathrm{I}}} \rho_i(x) \right|$$

Como ρ_i es C^{∞} en una bola $\mathrm{B}(0,\ 1/2^{\alpha(r)})$, significa que sus derivadas parciales de todos los órdenes existen y son continuas. Luego ellas están acotadas en toda vecindad compacta del origen contenida en la bola $\mathrm{B}(0,\ 1/2^{\alpha(r)})$. De esto y del hecho de que $\rho_i(x) = 0$ en F_i, $i \in \mathbb{N}$, se sigue que

$$\sup_{|\mathrm{I}|\leq r} \left| \frac{\partial^{|\mathrm{I}|}}{\partial x^{\mathrm{I}}} \rho_i(x) \right| \leq C_r 2^{ir}$$

para cada $i \in \mathbb{N}$. Entonces

$$\lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \left(\frac{1}{2^i}\right)^{\beta(i)} C_r 2^{ir} = C_r \lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \frac{1}{2^{i(\beta(i)-r)}}$$

como $\alpha(r) \geq r$, se sigue que esta serie converge en $\mathbb{R}^n$. Así, la serie

$$\lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \frac{\partial^{|\mathrm{I}|}}{\partial x^{\mathrm{I}}} \left(\frac{1}{2^i}\right)^{\beta(i)} \rho_i(x)$$

converge uniformemente.

Sea $g = \lim_{j\to\infty} \sum_{i=\alpha(1)}^{\alpha(j)} \left(\frac{1}{2^i}\right)^{\beta(i)} \rho_i$; claramente g es C^{∞} con $g(x) > 0$ para cada $x \neq 0$.

Como g y sus derivadas de todos los órdenes se anulan en cero, se tiene que $g \in m(n)^{\infty}$. Dado que el cociente f/g está bien definido y es C^{∞} para cada $x \neq 0$, restará probar que este cociente puede ser extendido a un germen $h \in m(n)^{\infty}$. En efecto, sea

$x \in \mathrm{B}(0,\ 1/2^{\alpha(r)}) \setminus \mathrm{B}(0,\ 1/2^{\alpha(r+1)})$; entonces por como se ha definido la sucesión $(\beta(i))_{i\in\mathbb{N}}$, se tiene que $x \in K_j$ con $\alpha(r) \le j < \alpha(r+1)$. Luego

$$g(x) \ge \left(\frac{1}{2^j}\right)^{\beta(j)} = \left(\frac{1}{2^j}\right)^{r} \ge |x|^r \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (3)$$

También, para cualquier $s \in \mathbb{N} \cup \{0\}$, existen constantes C'_s tal que para cada $x \in \mathrm{B}(0,\ 1) \setminus \{0\}$, se tiene que

$$\left|\frac{f}{g}\right|_s^x \le C'_s \frac{|f|_s^x}{g(x)^{s+1}} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (4)$$

Si $r \ge s$ y si $x \in \mathrm{B}(0,\ 1/2^{\alpha(r)}) \setminus B(0,\ 1/2^{\alpha(r)})$; de (2), (3) y (4) se sigue que

$$\left|\frac{f}{g}\right|_s^x \le C'_s |x|^{r(r-s-1)}$$

De esta forma, si $|x| \to 0$, entonces $\left|\frac{f}{g}\right|_s^x \to 0$ lo cual significa que el cociente f/g puede extenderse a un germen $h \in m(n)^\infty$. □

Sea $\mathfrak{I}(n)^k = \mathcal{E}(n)/m(n)^{k+1}$, $J(n)^k = m(n)/m(n)^{k+1}$ y $\mathcal{J}: \mathcal{E}(n) \to \mathfrak{I}(n)^k$ la proyección canónica. Se observa que $\mathfrak{I}(n)^k$ es un anillo local y $J(n)^k$ su ideal maximal. Más aun, $\mathfrak{I}(n)^k$ es un $\mathbb{R}$-espacio vectorial de dimensión finita, donde los monomios x^{I} de grado $\le k$ generan a $\mathfrak{I}(n)^k$. La dimensión de $\mathfrak{I}(n)^k$ como $\mathbb{R}$-espacio vectorial es $(n+k)!/n!k!$.[†)] Sea $f \in \mathcal{E}(n)$ un germen y $f_0+f_1+\cdots+f_k$ el germen que se obtiene al truncar a orden k el desarrollo en series de Taylor de f en el punto cero. f_0 es el término constante y $f_j = \sum_{\mathrm{I}} \frac{\partial^{|\mathrm{I}|} f(0)}{\partial x^{\mathrm{I}}} \frac{x^{\mathrm{I}}}{\mathrm{I}!}$, donde $\mathrm{I}=(i_1,\ldots,i_n)$ y $|\mathrm{I}|=j$, es el germen que contiene a todos los monomios de grado j. El polinomio $f_0+f_1+\cdots+f_k$ se denomina ***k-jet*** de f en cero y se denota como

$$\mathcal{J}^k(f);\ \mathcal{J}^k(f) = f_0+f_1+\cdots+f_k.$$

$\mathfrak{I}(n)^k$ se denomina **espacio de *k-jets*** y es isomorfo al anillo de polinomios en n indeterminadas con coeficientes en $\mathbb{R}$ de grado $\le k$, esto es,

$$\mathfrak{I}(n)^k \cong \mathbb{R}[[x_1,\ldots,x_n]] / \langle x_1,\ldots,x_n \rangle^{k+1}\ ^{\dagger)}.$$

En efecto, la función que asocia

$$\mathcal{J}^k(f) \mapsto \mathrm{P}_0(x)+\mathrm{P}_1(x)+\cdots+\mathrm{P}_k(x).$$

[†)] La demostración de que $(n+k)!/n!k!$ es la dimensión de $\mathfrak{I}(n)^k$ se hace por inducción.

[†)] Estos polinomios se suman en la forma usual y se multiplican también en la forma usual excepto que los términos de orden mayor que k son omitidos.

con $x\in\mathbb{R}^n$, donde $P_0(x)$ es el polinomio constante $f(0)$ y $P_j(x)$ es el polinomio homogéneo de grado j, cuyos coeficientes están determinados por las derivadas parciales de f de orden j evaluadas en cero, es un homomorfismo. También se tiene que $\mathcal{J}^k(f)\mapsto 0$ si y sólo si $f\in m(n)^{k+1}$; además

$$\mathcal{J}^k(P_0(x)+P_1(x)+\cdots+P_k(x))=P_0(x)+P_1(x)+\cdots+P_k(x).$$

De esta forma, este homomorfismo es en verdad un isomorfismo.[‡)] Cuando $k=\infty$, $\mathcal{J}^\infty(f)$ es la serie de Taylor de f en el punto x y $\mathfrak{I}(n)^\infty$ será identificado con el anillo $\mathbb{R}[[x_1,\ldots,x_n]]$ de series de potencias formales, es decir

TEOREMA 4.2.6. (*lema de Borel*) $\mathcal{E}(n)/m(n)^\infty\cong\mathbb{R}[[x_1,\ldots,x_n]]$.

DEMOSTRACIÓN

Sea $\varphi:\mathcal{E}(n)\to\mathbb{R}[[x_1,\ldots,x_n]]$; $f\mapsto\sum a_I\,(x^I/I!)$ con $a_I=\partial^{|I|}f(0)/\partial x^I$ para cada multiíndice $I\in(\mathbb{N}^*)^n$ y cada número real a_I. Si g es otro representante del germen f, entonces se tendrá que $\partial^{|I|}f(0)/\partial x^I=\partial^{|I|}g(0)/\partial x^I$ para todo multiíndice I, esto es, f y g coinciden en una vecindad del cero; luego φ está bien definida. También, φ es un homomorfismo; en efecto, considérese

$$\begin{aligned}\varphi(f+g)&=\sum_I\frac{\partial^{|I|}(f+g)(0)}{\partial x^I}\frac{x^I}{I!}\\&=\sum_I\frac{\partial^{|I|}f(0)}{\partial x^I}\frac{x^I}{I!}+\sum_I\frac{\partial^{|I|}g(0)}{\partial x^I}\frac{x^I}{I!}\\&=\varphi(f)+\varphi(g).\end{aligned}$$

Por la regla de Leibnitz, se tiene que

$$\begin{aligned}\varphi(fg)&=\sum_I\frac{\partial^{|I|}(fg)(0)}{\partial x^I}\frac{x^I}{I!}\\&=\sum_I\sum_{J+K=I}\left(\frac{I!}{(I-J)!J!}\right)\left(\frac{\partial^{|J|}f(0)}{\partial x^J}\right)\left(\frac{\partial^{|I-J|}g(0)}{\partial x^{I-J}}\right)\left(\frac{x^I}{I!}\right)\end{aligned}$$

Como $J\le I$ y $J+K=I$ para algún multiíndice K, entonces

$$\begin{aligned}&=\sum_I\sum_{J+K=I}\left(\frac{1}{J!}\right)\left(\frac{\partial^{|J|}f(0)}{\partial x^J}\right)\left(\frac{1}{K!}\right)\left(\frac{\partial^{|K|}g(0)}{\partial x^K}\right)\left(\frac{x^I}{I!}\right)\\&=\varphi(f)\varphi(g).\end{aligned}$$

[‡)] Para más información sobre el concepto de germen y conceptos relacionados con él, ver el apéndice A.

A continuación se probará que la función φ es suprayectiva, es decir, existe un germen $f\in\mathcal{E}(n)$ tal que $\partial^{|I|}f(0)/\partial x^I=a_I$. Sea $g_I:\mathbb{R}^n\to\mathbb{R}$; $g_I(x)=a_I(x^I/I!)\rho(x/\mu_I)$, donde

$$\rho:\mathbb{R}^n\to\mathbb{R};\ \rho(x)=\begin{cases}1 & \text{si } \|x\|\le 1/2\\ 0 & \text{si } \|x\|\ge 1\end{cases}$$ y (μ_I) es una sucesión que converge

rápidamente a cero. Para mostrar que la suma $\sum_I g_I$ define una función C^∞; $f:\mathbb{R}^n\to\mathbb{R}$, cuyas derivadas parciales $\partial^{|J|}f/\partial x^J$; $J\ge 0$ son dadas por la serie $\sum_I \partial^{|J|}g_I/\partial x^J$, será suficiente probar que esta serie converge uniformemente en $\mathbb{R}^n$.†) Por la regla de Leibnitz, se tiene que

$$\frac{\partial^{|J|}g_I(x)}{\partial x^J}=\sum_{0\le J\le I}a_I\left(\frac{J!}{(J-K)!K!}\right)\left(\frac{\partial^{|K|}(x^I/I!)}{\partial x^K}\right)\left(\frac{\partial^{|J-K|}\rho(x/\mu_I)}{\partial x^{J-K}}\right)$$

$$=a_I\sum_{0\le J\le I}\left(\frac{J!}{(J-K)!K!}\right)\left(\frac{1}{(I-K)!}\right)x^{I-K}\frac{\partial^{|J-K|}\rho(x/\mu_I)}{\partial x^{J-K}}$$

con $0\le J\le I$. Considérese

..

$$\left|\frac{\partial^{|J|}g_I(x)}{\partial x^J}\right|\le|a_I|\sum_{0\le J\le I}\frac{J!}{(J-K)!K!}\frac{1}{(I-K)!}\left\|x^{I-K}\right\|\left|\frac{\partial^{|J-K|}\rho(x/\mu_I)}{\partial x^{J-K}}\right|$$

$$\le|a_I|\sum_{0\le J\le I}\frac{J!}{(J-K)!K!}\frac{1}{(I-K)!}\left\|x^{I-K}\right\|\left(1/\mu_I^{|J-K|}\right)|\rho(x/\mu_I)|$$

Como ρ es C^∞ en una vecindad V(0) del origen, significa que sus derivadas parciales de todos los ordenes existen, son continuas y están acotadas en toda vecindad compacta del origen contenida en V(0). Así, el supremo de cada una de estas funciones existe en cualquier compacto K que contiene al origen y que está contenido en V(0). De esto y del hecho de que $\rho(x/\mu_I)=0$ para $\|x\|\ge\mu_I$, se sigue que

$$M_J=max\left\{sup\left\{\left|\frac{\partial^{|L|}\rho(x)}{\partial x^L}\right|\ \middle|\ \forall x\in K\right\}\forall\ L,J\ \middle|\ 0\le L\le J\right\}$$

Es una cota superior de $\left|\frac{\partial^{|J-K|}\rho(x/\mu_I)}{\partial x^{J-K}}\right|$. Como $\|x^{I-K}\|\le\mu_I^{|J-K|}$, se tiene que

$$\left|\frac{\partial^{|J|}g_I(x)}{\partial x^J}\right|\le J!|a_I|M_J\sum_{0\le J\le I}\left(\mu_I^{|I-K|}/\mu_I^{|J-K|}\right)$$

†) Ver el teorema del apéndice B.

$$\left|\frac{\partial^{|J|} g_I(x)}{\partial x^J}\right| \le J!|a_I| M_J \sum_{0\le J\le I}\left(\mu_I^{|I|}/\mu_I^{|J|}\right)$$

Considerando la sucesión (μ_I) tal que $\mu_I = \begin{cases} 1/2 & \text{si } |a_I| \le 1 \\ 1/(2|a_I|) & \text{si } |a_I| > 1 \end{cases}$

entonces

$$|a_I|\left(\mu_I^{|I-K|}/\mu_I^{|J-K|}\right) = |a_I|\left(\mu_I^{|I|}/\mu_I^{|J|}\right) \le \left(2^{|J|}/2^{|I|}\right)$$

Para J<I. De esta forma

$$\left|\frac{\partial^{|J|} g_I(x)}{\partial x^J}\right| \le J!M_J \sum_{0\le J\le I}\left(2^{|J|}/2^{|I|}\right) \le (J!M_J \sum_{0\le J\le I} 2^{|J|}) \Big/ 2^{|I|}$$

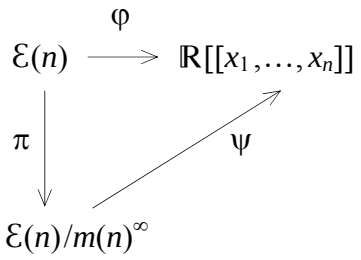
para J<I donde $J!M_J \sum 2^{|J|}$ no depende de I o de *x*. Dado que la serie $\sum_I (1/2^{|I|})$ converge, se sigue que la serie $\sum_I \frac{\partial^{|J|} g_I(x)}{\partial x^J}$ converge uniformemente en $\mathbb{R}^n$ para todo multiíndice I.

Como $\sum_I \frac{\partial^{|K|}\rho(0)}{\partial x^K} = 0$ para K≠0, se tiene que

$$\frac{\partial^{|J|} f(0)}{\partial x^J} = \sum_I \frac{\partial^{|J|} g_I(0)}{\partial x^J} = \sum_I \frac{\partial^{|J|} g_I(0)}{\partial x^J} = a_J$$

Así, existe un germen $f \in \mathcal{E}(n)$ tal que $\varphi(f) = \sum_I \frac{\partial^{|J|} g_I(0)}{\partial x^J}(x^I/I!)$ y φ es suprayectiva. Por otro lado, el núcleo de φ es el conjunto de todos los gérmenes *f* tal que $f(0)=0$ y $\partial^{|J|} f(0)/\partial x^J = 0$ para todo multiíndice I con $|I| \le \infty$, es decir, todas las derivadas parciales de cualquier orden se anulan en cero. Así, se tiene que $Ker(\varphi) = m(n)^\infty$ y $\mathcal{E}(n)/m(n)^\infty \cong \mathbb{R}[[x_1, \ldots, x_n]]$. □

OBSERVACIÓN 4.2.7. El anillo de series de potencias formales $\mathbb{R}[[x_1, \ldots, x_n]]$ es un anillo local real y $\mathcal{M}(n)$ (=$\{f \in \mathbb{R}[[x_1, \ldots, x_n]] \mid f(0)=0\}$) su ideal real maximal real.



DEMOSTRACIÓN

Claramente $\mathcal{M}(n)$ es un ideal de $\mathbb{R}[[x_1, \ldots, x_n]]$. Sea $f \notin \mathcal{M}(n)$, entonces $f = f_0(1-f_1)$ con $f_0 \in \mathbb{R}$, $f_0 \neq 0$ y $f_1 \in \mathcal{M}(n)$. Luego $(1/f) = (1/f_0)(1+f_1+f_1^2+\cdots)$ y $(f)(1/f) = 1$ es la serie

de potencias 1; de esta forma, $\mathbb{R}[[x_1,\ldots,x_n]]\setminus\mathcal{M}(n)$ contiene únicamente unidades. Así, $\mathcal{M}(n)$ es el ideal maximal de $\mathbb{R}[[x_1,\ldots,x_n]]$. □

Se sabe que el anillo de series de potencias formales $\mathbb{R}[[x_1,\ldots,x_n]]$ ($\cong\mathcal{E}(n)/m(n)^\infty$) es un anillo noetheriano, pero

OBSERVACIÓN 4.2.8. $\mathcal{E}(n)$ no es un anillo noetheriano.

DEMOSTRACIÓN

Si se supone que $\mathcal{E}(n)$ es noetheriano, entonces $m(n)^\infty$ es un ideal finitamente generado. Dado que $m(n)m(n)^\infty=m(n)^\infty$, por el lema de Nakayama (ver apéndice A pag 150.) se sigue que $m(n)^\infty=(0)$, siendo $m(n)=jac(\mathcal{E}(n))$. Por otro lado, la función

$$f:\mathbb{R}\to\mathbb{R};\ f(x)=\begin{cases}\exp(-1/x^2) & \text{si}\quad x\neq 0\\ 0 & \text{si}\quad x=0\end{cases}$$

es C^∞ no cero cuyas derivadas de todos los ordenes se anulan en cero, esto es, $f\in m(1)^\infty$ lo cual no puede ser posible. □

Considérese la familia $\mathcal{N}_0=\{X\subseteq\mathbb{R}^n \mid 0\in X\}$ de todos los subconjuntos de $\mathbb{R}^n$ que contienen al cero. Se define una relación en $\mathcal{N}_0$ como sigue: se dice que X~Y para X, Y en $\mathcal{N}_0$ si existe una vecindad U del cero tal que $U\cap X=U\cap Y$. La relación ~ es de equivalencia y las clases de equivalencia se denominan ***gérmenes de conjunto.*** Si X está en $\mathcal{N}_0$, el germen de conjunto de X se denota como $\mathcal{X}$ o *germ*(X).

Se dice que una función $f:U\subseteq\mathbb{R}^n\to\mathbb{R}$ definida en un conjunto abierto U en $\mathbb{R}^n$ es **analítica real** si es de clase C^∞ y coincide con su serie de Taylor en una vecindad de cada punto de U. Sea U un conjunto abierto en $\mathcal{N}_0$ y considérese un conjunto cerrado X en U que contiene al cero. X es un **conjunto analítico real** si es el conjunto de ceros comunes de una familia finita de funciones analíticas reales, esto es,

$$X=\{x\in\mathbb{R}^n \mid f_1(x)=\cdots=f_s(x)=0\}^{\dagger)}$$

Si X es un conjunto analítico real, se define el germen de conjunto de X denominado **germen de conjunto analítico real** como

$$\mathcal{X}=germ\{x\in\mathbb{R}^n \mid f_1(x)=\cdots=f_s(x)=0\}$$

---

†) Se pudo haber definido X como el conjunto de ceros comunes de todas las funciones en un cierto ideal I de $C^\infty(\mathbb{R}^n,\mathbb{R})$; pero dado que este conjunto es muy complicado se ha preferido no considerarlo.

con $f_1,\ldots,f_s$ funciones analíticas reales. Se observa que unión e intersección finitas de gérmenes de conjunto analíticos reales también son gérmenes de conjunto analíticos reales. Para cualquier germen de conjunto $\mathcal{X}$, se define el ideal $\mathcal{I}(\mathcal{X})$ en $\mathcal{E}(n)$ de gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$ las cuales se anulan en el representante X, esto es, si V es una vecindad del cero, se tiene que

$$\mathcal{I}(\mathcal{X})=\{g\in\mathcal{E}(n) \mid \text{existe V (que depende de } g) \text{ con } g|_{X\cap V}\equiv 0\}.$$

Se observa que si X′ es otro representante del germen $\mathcal{X}$, entonces existe una vecindad U del cero tal que $U\cap X=U\cap X'$, luego g se anula en $(U\cap V)\cap X'$. De esta forma la definición anterior es independiente de los representantes de $\mathcal{X}$.

Sea I un ideal en $\mathcal{E}(n)$ finitamente generado por gérmenes $f_1,\ldots,f_s$ cuyos representantes son funciones analíticas reales. Se denota por $\mathcal{U}(I)$ el germen de los ceros comunes de los representantes $f_1,\ldots,f_s$, esto es,

$$\mathcal{U}(I)=germ\{x\in\mathbb{R}^n \mid f_1(x)=\cdots=f_s(x)=0\}$$

Se observa que $\mathcal{U}(I)$ no depende de los representantes. En efecto, si I es también generado por los gérmenes $g_1,\ldots,g_s$ con $f_i=g_i$ para cada $i=1,\ldots,s$, entonces existen vecindades $V_1,\ldots,V_s$ tal que $f_i(x)=g_i(x)$ para cada $x\in V_i$, $i=1,\ldots,s$. De esta forma, los ceros comunes del conjunto $\{f_1,\ldots,f_s\}$ coinciden con los ceros comunes del conjunto $\{g_1,\ldots,g_s\}$ en $V_1\cap\ldots\cap V_s$. También se cumple que $\mathcal{U}(I)$ no depende de los generadores del ideal I; esto es, si $I=<f_1,\ldots,f_s>=<g_1,\ldots,g_t>$, y $x\in\mathcal{U}(f_1,\ldots,f_s)$, se sigue que $f_i(x)=0$ para cada $i=1,2,\ldots,s$. Dado que $g_j=\sum_{i=1}^{s} h_{ij} f_i$, esto último implica que $g_j(x)=0$ para toda $j=1,\ldots,t$; de esta forma, $x\in\mathcal{U}(g_1,\ldots,g_t)$. Similarmente se tiene que $\mathcal{U}(g_1,\ldots,g_t)\subseteq\mathcal{U}(f_1,\ldots,f_s)$.

OBSERVACIÓN 4.2.9. Sean I y J ideales en $\mathcal{E}(n)$, entonces

1) $\mathcal{I}(\mathcal{U}(I))\supseteq I$.
2) Si $I\subseteq J$, entonces $\mathcal{U}(I)\supseteq\mathcal{U}(J)$.
3) Si $\mathcal{U}(I)\subseteq\mathcal{U}(J)$, entonces $\mathcal{I}(\mathcal{U}(I))\supseteq\mathcal{I}(\mathcal{U}(J))$.
4) $\mathcal{U}(\mathcal{I}(\mathcal{U}(I)))=\mathcal{U}(I)$.

DEMOSTRACIÓN

1) Si $f\in I$, entonces $f(x)=0$ para cada $x\in\mathcal{U}(I)$, esto es, $f\in\mathcal{I}(\mathcal{U}(I))$. 2) Sea $x\in\mathcal{U}(J)$, entonces se tiene que $f(x)=0$ para cada $f\in J$, luego $f(x)=0$ para toda $f\in I$, esto es, $x\in\mathcal{U}(I)$.

3) Si $f\in\mathcal{I}(\mathcal{U}(J))$, entonces $f(x)=0$ para cada $x\in\mathcal{U}(J)$; luego $x\in\mathcal{U}(I)$ y $f\in\mathcal{I}(\mathcal{U}(I))$. 4) ($\supseteq$) Sea $x\in\mathcal{U}(I)$, entonces $f(x)=0$ para toda $f\in\mathcal{I}(\mathcal{U}(I))$; esto significa que $x\in\mathcal{U}(\mathcal{I}(\mathcal{U}(I)))$. ($\subseteq$) Como $\mathcal{I}(\mathcal{U}(I))\supseteq I$, se tiene que $\mathcal{U}(\mathcal{I}(\mathcal{U}(I)))\subseteq\mathcal{U}(I)$. □

Se dice que un germen de conjunto analítico real $\mathcal{X}$ es irreducible si siempre que $\mathcal{X}=\mathcal{X}_1\cup\mathcal{X}_2$ con $\mathcal{X}_1$, $\mathcal{X}_2$ gérmenes de conjunto analíticos reales, se tiene que $\mathcal{X}=\mathcal{X}_1$ o $\mathcal{X}=\mathcal{X}_2$.

OBSERVACIÓN 4.2.10. Un germen de conjunto analítico real $\mathcal{X}$ es irreducible si y sólo si $\mathcal{I}(\mathcal{X})$ es primo.

DEMOSTRACIÓN ($\Leftarrow$)

Supóngase que $\mathcal{X}$ no es irreducible. Sea $\mathcal{X}=\mathcal{X}_1\cup\mathcal{X}_2$ con $\mathcal{X}_1$, $\mathcal{X}_2$ gérmenes de conjunto analíticos reales con $\mathcal{X}_1\subsetneq\mathcal{X}$, y $\mathcal{X}_2\subsetneq\mathcal{X}$. Luego $\mathcal{I}(\mathcal{X}_1)\supsetneq\mathcal{I}(\mathcal{X})$ e $\mathcal{I}(\mathcal{X}_2)\supsetneq\mathcal{I}(\mathcal{X})$; entonces existen gérmenes $f\in\mathcal{I}(\mathcal{X}_1)\setminus\mathcal{I}(\mathcal{X})$ y $g\in\mathcal{I}(\mathcal{X}_2)\setminus\mathcal{I}(\mathcal{X})$. Es claro que $f\,g\in\mathcal{I}(\mathcal{X})$ ya que el representante $f\,g$ se anula en todos los puntos de X ($\mathcal{X}=germ(\mathrm{X})$). Por lo tanto, $\mathcal{I}(\mathcal{X})$ no es primo.

($\Rightarrow$)

Si $\mathcal{I}(\mathcal{X})$ no es un ideal primo, entonces existen gérmenes $f\notin\mathcal{I}(\mathcal{X})$ y $g\notin\mathcal{I}(\mathcal{X})$ tal que $f\,g\in\mathcal{I}(\mathcal{X})$. Considerese los ideales $I_1=\mathcal{I}(\mathcal{X})+<f>$ e $I_2=\mathcal{I}(\mathcal{X})+<g>$. Es claro que $\mathcal{X}_1=\mathcal{U}(I_1)$ y $\mathcal{X}_2=\mathcal{U}(I_2)$ satisfacen que $\mathcal{X}_1\subsetneq\mathcal{X}$, y $\mathcal{X}_2\subsetneq\mathcal{X}$. Ahora, si $x\in\mathcal{X}$ y $x\notin\mathcal{X}_1$, se obtiene que $f(x)\neq 0$, pero $f(x)g(x)=0$, entonces $g(x)=0$ y $x\in\mathcal{X}_2$. Luego $\mathcal{X}=\mathcal{X}_1\cup\mathcal{X}_2$, $\mathcal{X}_1\neq\varnothing$ y $\mathcal{X}_2\neq\varnothing$; así, $\mathcal{X}$ no es irreducible. □

Se observa que no todo ideal primo P en $\mathcal{E}(n)$ es necesariamente de la forma $\mathcal{I}(\mathcal{X})$ con $\mathcal{X}$ un germen de conjunto analítico real, esto es, el nullstellensatz es falso en general. Por ejemplo considérese el ideal primo generado por el germen x^2+y^2. Claramente se tiene que $f(x,y)=x^2+y^2$ es irreducible e $\mathcal{I}(\mathcal{U}(<f>))=m(2)$. Aun así, se puede uno fijar en aquellos ideales I en $\mathcal{E}(n)$ que satisfacen $\mathcal{I}(\mathcal{U}(I))=I$. Si I es un ideal en $\mathcal{E}(n)$, se define el **radical** de I como el ideal $\mathcal{I}(\mathcal{U}(I))$. Se dirá que I es un ideal **radical** si $\mathcal{I}(\mathcal{U}(I))=I$.

Si $I_1,\ldots,I_r$ son ideales radicales de $\mathcal{E}(n)$, entonces su intersección $\cap I_i$ es un ideal radical. En efecto, como $\bigcap_{j=1}^{r} I_j\subseteq I_i$ para cada $i\in\{1,2,\ldots,r\}$, se sigue que

$$\mathcal{I}(\mathcal{V}(\bigcap_{j=1}^{r} I_j)) \subseteq \mathcal{I}(\mathcal{V}(I_i)) \text{ e } \mathcal{I}(\mathcal{V}(\bigcap_{j=1}^{r} I_j)) \subseteq \bigcap_{j=1}^{r} \mathcal{I}(\mathcal{V}(I_j))$$

para toda $i \in \{1,2,\ldots,r\}$. Dado que

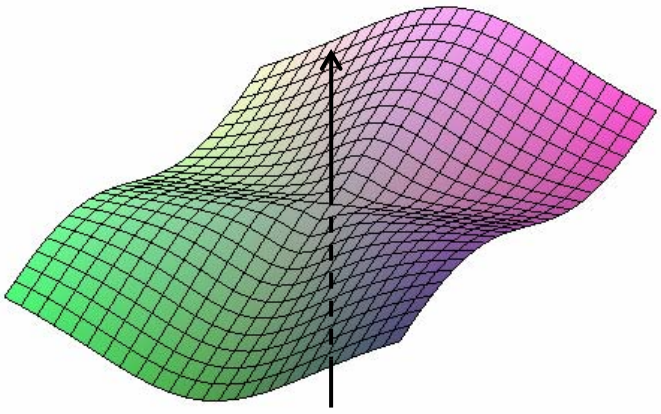
$$\bigcap_{j=1}^{r} I_j \subseteq \mathcal{I}(\mathcal{V}(\bigcap_{j=1}^{r} I_j)), \text{ entonces } \bigcap_{j=1}^{r} \mathcal{I}(\mathcal{V}(I_j)) \subseteq \mathcal{I}(\mathcal{V}(\bigcap_{j=1}^{r} I_j)).$$

Por lo tanto $\mathcal{I}(\mathcal{V}(\bigcap_{j=1}^{r} I_j)) = \bigcap_{j=1}^{r} I_j$.

DEFINICIÓN 4.2.11. Sea U un conjunto abierto en $\mathbb{R}^n$ y X un conjunto analítico en U. X es **coherente** en un punto x en X si existen una vecindad V_x del punto x y funciones analíticas $f_1,\ldots,f_s$ en V_x que se anulan en X tal que para cada $y \in V_x \cap X$ se tiene que $\mathcal{I}(\mathcal{X}_y) = \langle f_1{}^y,\ldots,f_s{}^y \rangle$, donde $f_i{}^y$ es el germen de f_i en el punto y; $i=1,\ldots,s$.

DEFINICIÓN 4.2.12. Un conjunto analítico X en un abierto U en $\mathbb{R}^n$ es coherente si el es coherente en cada uno de sus puntos.

EJEMPLO 4.2.13. Se sabe que todo conjunto analítico en $\mathbb{C}^n$ es coherente pero en general no todo conjunto analítico en $\mathbb{R}^n$ es coherente. Un ejemplo de esto es la superficie conexa e irreducible en $\mathbb{R}^3$; $z(x^2+y^2)-x^3=0$ denominada *paraguas de Whitney*. Ella no es coherente en cero y tiene al eje z como un generador aislado.



Se denota por $\mathcal{O}(n)$ el anillo de gérmenes en cero de funciones analíticas reales en $\mathbb{R}^n$. $\mathcal{O}(n)$ es un anillo local noetheriano

OBSERVACIÓN 4.2.14. Sea $\mathcal{X}$ el germen de conjunto analítico real en cero, $\mathcal{I}_*(\mathcal{X})$ su ideal analítico en el anillo $\mathcal{O}(n)$ e $\mathcal{I}(\mathcal{X})$ el ideal en $\mathcal{E}(n)$. Entonces $\mathcal{X}$ es coherente en 0 si y sólo si $\mathcal{I}(\mathcal{X})=\mathcal{I}_*(\mathcal{X})\mathcal{E}(n)$.

DEMOSTRACIÓN

Para la demostración ver [14] (teorema 3.10. pagina 95). □

DEFINICIÓN 4.2.15. Un ideal I en $\mathcal{E}(n)$ es un **ideal de Malgrange** si

i) I es finitamente generado por gérmenes de funciones analíticas reales y

ii) $\mathcal{V}(I)$ es un conjunto coherente en cero

Se observa que para ideales de Malgrange, la observación 4.2.14., asegura que $\mathcal{I}(\mathcal{X})$ es finitamente generado.

Considérese los conjuntos

$$\mathfrak{M}=\{I \mid I \text{ ideal radical y de Malgrange }\}$$
$$\mathcal{C}=\{\ \mathcal{V}(I)\mid\ \mathcal{V}(I) \text{ germen coherente}\}.$$

Se pueden definir los siguientes mapeos

$$\mathcal{I}:\mathcal{C}\to\mathfrak{M} \quad \text{y} \quad \mathcal{V}:\mathfrak{M}\to\mathcal{C}$$

Se afirma que estos mapeos están bien definidos y uno es el inverso del otro. En efecto, como I es un ideal radical y de Malgrange, se sigue que $\mathcal{V}(I)$ es coherente e $\mathcal{I}(\mathcal{V}(I))=I$. También, si $\mathcal{V}(I)$ está en $\mathcal{C}$, $\mathcal{I}(\mathcal{V}(I))$ es finitamente generado y $\mathcal{V}(\mathcal{I}(\mathcal{V}(I)))=\mathcal{V}(I)$ es coherente. Además se tiene que $\mathcal{I}(\mathcal{V}(\mathcal{I}(\mathcal{V}(I))))=\mathcal{I}(\mathcal{V}(I))$. De esta forma, $\mathcal{I}$ y $\mathcal{V}$ son mapeos biyectivos y uno es el inverso del otro.

Así, se tiene una correspondencia entre gérmenes de conjuntos coherentes e ideales radicales y de Malgrange

$$\{I \mid I \text{ ideal radical y de Malgrange}\} \xleftrightarrow{\ \mathcal{I}\ \mathcal{V}\ } \{\ \mathcal{V}(I)\mid \mathcal{V}(I) \text{ germen coherente}\}$$

Considérese un ideal I en el anillo local real $\mathcal{E}(n)$. De acuerdo al teorema 3.4.18., el radical real de I, *r-rad*(I) es la intersección de todos los ideales primos reales en el anillo $\mathcal{E}(n)$ que contienen a I. En el caso en que un ideal radical I sea un ideal real, se tendrá que $\mathcal{I}(\mathcal{V}(I))=$*r-rad*$(I)=I$ es decir, los conceptos de ideal radical real e ideal radical coinciden.

Si I es un ideal arbitrario en $\mathcal{E}(n)$, entonces se cumple que $\mathcal{V}(r\text{-}rad(I))=\mathcal{V}(I)$ y $r\text{-}rad(I)\subseteq\mathcal{I}(\mathcal{V}(I))$. La contención recíproca en esta última expresión no es valida en general. Por ejemplo, $\mathcal{I}(\mathcal{V}(m(n)^{\infty}))=m(n)$ y $r\text{-}rad(m(n)^{\infty})=m(n)^{\infty}$.

PROPOSICIÓN 4.2.16. Si I en $\mathcal{E}(n)$ es un ideal radical, entonces $Im(n)^{\infty}=I\cap m(n)^{\infty}$.

DEMOSTRACIÓN

Dado que $Im(n)^{\infty}\subseteq I\cap m(n)^{\infty}$, restará probar únicamente que $I\cap m(n)^{\infty}\subseteq I\,m(n)^{\infty}$. Sea $f\in I\cap m(n)^{\infty}$, entonces por el lema de Tougeron (lema 4.2.5.), existen gérmenes g, $h\in m(n)^{\infty}$ con $g(x)>0$ para toda $x\neq 0$ tal que $f=hg$. Ahora, como $f\,|\,\mathcal{V}(I)\equiv 0$, se sigue que $h(x)=0$ para cada $x\in\mathcal{V}(I)$ y $h\in\mathcal{I}(\mathcal{V}(I))=I$. De esta forma, $f\in Im(n)^{\infty}$. □

OBSERVACIÓN 4.2.17. Sea $\pi:\mathcal{E}(n)\rightarrow\mathbb{R}[[x_1,\ldots,x_n]]$ el homomorfismo proyección, $\mathcal{M}(n)$ el ideal maximal de $\mathbb{R}[[x_1,\ldots,x_n]]$. Entonces $\pi^{-1}(\mathcal{M}(n))$ es el ideal maximal $m(n)$ de $\mathcal{E}(n)$.

DEMOSTRACIÓN

Sea $f\in\pi^{-1}(\mathcal{M}(n))\subseteq\mathcal{E}(n)$, entonces $\pi(f)\in\mathcal{M}(n)$, esto es, $\pi(f(0))=0$. Luego $\pi^{-1}(\pi(f(0))=0$; así, $f(0)=0$ y $f\in m(n)$. Recíprocamente, si $f\in m(n)$, entonces $f(0)=0$ y $\pi(f(0))=\pi(0)=0$, luego $\pi(f)\in\mathcal{M}(n)$. □

A continuación se prueba un resultado análogo del lema de Artin–Rees para el anillo $\mathcal{E}(n)$.

TEOREMA 4.2.18. (*lema de Artin-Rees*) Sea I un ideal radical en $\mathcal{E}(n)$, entonces existe $k_0\in\mathbb{N}$ tal que para todo entero no negativo k se cumple que

$$m(n)^{k+k_0}\cap I=m(n)^{k}(m(n)^{k_0}\cap I).$$

DEMOSTRACIÓN

Sea I un ideal radical en el anilo $\mathcal{E}(n)$ y considérese el ideal J en $\mathbb{R}[[x_1,\ldots,x_n]]$ tal que $\pi(I)=J$ [†)] con π la proyección del lema de Borel. Por el corolario al lema de Artin-Rees (ver 4.1.26.), existe $k_0\in\mathbb{N}$ tal que para toda $k\in\mathbb{N}^*$

$$\mathcal{M}(n)^{k+k_0}\cap J=\mathcal{M}(n)^{k}(\mathcal{M}(n)^{k_0}\cap J)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(1)$$

Tomando imagen inversa en (1)

$$\pi^{-1}(\mathcal{M}(n)^{k+k_0}\cap J)=\pi^{-1}[\,\mathcal{M}(n)^{k}(\mathcal{M}(n)^{k_0}\cap J)]$$

[†)] Si I es un ideal en $\mathcal{E}(n)$, entonces $\pi(I)$ es un ideal en $\mathbb{R}[[x_1,\ldots,x_n]]$ por ser π suprayectiva.

$$\pi^{-1}(\mathcal{M}(n)^{k+k_0}) \cap \pi^{-1}(J)=\pi^{-1}(\mathcal{M}(n)^k)\pi^{-1}(\mathcal{M}(n)^{k_0}\cap J) \text{ y}$$
$$\pi^{-1}(\mathcal{M}(n))^{k+k_0}\cap\pi^{-1}(J)=\pi^{-1}(\mathcal{M}(n))^k[\pi^{-1}(\mathcal{M}(n)^{k_0}\cap\pi^{-1}(J)].$$ ‡)

Ya que $\pi(I)=J$, se tiene que

$$\pi^{-1}(\mathcal{M}(n))^{k+k_0}\cap\pi^{-1}(\pi(I))=\pi^{-1}(\mathcal{M}(n))^k[\pi^{-1}(\mathcal{M}(n)^{k_0}\cap\pi^{-1}(\pi(I))].$$

Como $\pi^{-1}(\mathcal{M}(n))=m(n)$ (ver observación 4.1.14.), entonces

$$m(n)^{k+k_0}\cap(I+m(n)^\infty)=m(n)^k\,[m(n)^{k_0}\cap(I+m(n)^\infty)].$$ ††)

Dado que $m(n)^\infty\subseteq m(n)^{k+k_0}$, por la ley modular‡‡) se tiene que

$$(m(n)^{k+k_0}\cap I)+m(n)^\infty=m(n)^k[(m(n)^{k_0}\cap I)+m(n)^\infty]$$

y

$$(m(n)^{k+k_0}\cap I)+m(n)^\infty=m(n)^k(m(n)^{k_0}\cap I)+m(n)^\infty\cdots\cdots\cdots\cdots\cdots\cdots(2)$$

donde $m(n)^k m(n)^\infty=m(n)^\infty$. Intersecando (2) con I y dado que

$$m(n)^{k+k_0}\cap I\subseteq I\cap m(n)^k(m(n)^{k_0}\cap I)\subseteq I,$$

se sigue que

$$(m(n)^{k+k_0}\cap I)+(m(n)^\infty\cap I)=m(n)^k(m(n)^{k_0}\cap I)+(m(n)^\infty\cap I).$$

Dado que $I\,m(n)^\infty=I\cap m(n)^\infty$ (ver proposición 4.2.16.) se tiene que

$$(m(n)^{k+k_0}\cap I)+Im(n)^\infty=m(n)^k(m(n)^{k_0}\cap I)+Im(n)^\infty.$$

Como $I\,m(n)^\infty\subseteq I\cap m(n)^{k+k_0}$ e $I\,m(n)^\infty\subseteq m(n)^k\,(m(n)^{k_0}\cap I)$ se obtiene finalmente el resultado

$m(n)^{k+k_0}\cap I=m(n)^k\,(m(n)^{k_0}\cap I)$. □

Se observa que si I es un ideal arbitrario en $\mathcal{E}(n)$, entonces en general la igualdad en el lema de Artin-Rees, puede escribirse como

$$m(n)^{k+k_0}\cap I=m(n)^k\,(m(n)^{k_0}\cap I)+(m(n)^\infty\cap I).$$

Se termina este capítulo probando cuatro resultados a cerca de generación finita de ideales en $\mathcal{E}(n)$. Por la observación 4.2.8., se sabe que no todo ideal en $\mathcal{E}(n)$ es finitamente generado (por ejemplo $m(n)^\infty$ es un ideal que no es finitamente generado) pero para un ideal arbitrario de $\mathcal{E}(n)$, se tiene

---

‡) $\pi^{-1}[\mathcal{M}(n)^k(\pi^{-1}(\mathcal{M}(n)^{k_0}\cap J]=\pi^{-1}(\mathcal{M}(n))^k[\pi^{-1}(\mathcal{M}(n)^{k_0}\cap\pi^{-1}(J)]$ ya que π es suprayectiva.

††) Como $\pi^{-1}(\pi(I))=I+Ker(\pi)$ y $Ker(\pi)=m(n)^\infty$, se sigue que $\pi^{-1}(\pi(I))=I+m(n)^\infty$.

‡‡) $\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c})=\mathfrak{b}+\mathfrak{a}\cap\mathfrak{c}$ si $\mathfrak{a}\supseteq\mathfrak{b}$ y $\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c})=\mathfrak{a}\cap\mathfrak{b}+\mathfrak{c}$ si $\mathfrak{a}\supseteq\mathfrak{c}$.

OBSERVACIÓN 4.2.19. Sea I un ideal de $\mathcal{E}(n)$, entonces existen gérmenes $f_1,\ldots,f_s$ en I tal que $I=<f_1,\ldots,f_s>+(m(n)^\infty\cap I)$.

DEMOSTRACIÓN

Sea $\pi:\mathcal{E}(n)\to\mathbb{R}[[x_1,\ldots,x_n]]$ la proyección natural del teorema de Borel. Sean $h_1,\ldots,h_s$ generadores del ideal $\pi(I)$ y gérmenes $f_i\in\mathcal{E}(n)$ tal que $\pi(f_i)=h_i$; $i=1,2,\ldots,s$. Entonces

$$\begin{aligned}\pi(I)&=<h_1,\ldots,h_s>.\\&=<\pi(f_1),\ldots,\pi(f_s)>.\\&=\pi(<f_1,\ldots,f_s>).\end{aligned}$$

Luego

$$I+m(n)^\infty=<f_1,\ldots,f_s>+m(n)^\infty.$$

Intersecando esta igualdad con I, se obtiene

$$(I+m(n)^\infty)\cap I=(<f_1,\ldots,f_s>+m(n)^\infty)\cap I.$$

Por la ley modular (aquí, $<f_1,\ldots,f_s>\subseteq I$) se tiene que

$$I+(m(n)^\infty\cap I)=<f_1,\ldots,f_s>+(m(n)^\infty\cap I).$$

esto es,

$$I=<f_1,\ldots,f_s>+m(n)^\infty\cap I.$$

donde $m(n)^\infty\cap I\subseteq I$. □

Con la notación de la observación anterior, se tiene la siguiente

OBSERVACIÓN 4.2.20. Sea I un ideal radical en $\mathcal{E}(n)$. Entonces I es finitamente generado si y sólo si $I\cap m(n)^\infty\subseteq<f_1,\ldots,f_s>$.

DEMOSTRACIÓN ($\Rightarrow$)

Por la observación anterior, se tiene que $I=<f_1,\ldots,f_s>+I\cap m(n)^\infty$ para $f_1,\ldots,f_s$ en I. Como I es finitamente generado, por el lema de Nakayama se tiene que $I=<f_1,\ldots,f_s>$. Entonces $I\cap m(n)^\infty+<f_1,\ldots,f_s>=<f_1,\ldots,f_s>$; luego $I\cap m(n)^\infty\subseteq<f_1,\ldots,f_s>$.

($\Leftarrow$)

Sea $I=<f_1,\ldots,f_s>+I\cap m(n)^\infty$ e $I\cap m(n)^\infty\subseteq<f_1,\ldots,f_s>$, entonces

$$I=<f_1,\ldots,f_s>+I\cap m(n)^\infty=<f_1,\ldots,f_s>,$$

Así, I es un ideal finitamente generado de $\mathcal{E}(n)$. □

OBSERVACIÓN 4.2.21. Sea I un ideal de $\mathcal{E}(n)$ tal que $\pi(I)=\pi(\hat{I})$ con $\hat{I}$ un ideal radical (π, la proyección natural del lema de Borel). Entonces I es un ideal radical.

DEMOSTRACIÓN

Como $\pi(I)=\pi(\hat{I})$, se tiene que $I+m(n)^{\infty}=\hat{I}+m(n)^{\infty}$. Intersecando esta igualdad con $\hat{I}$, se obtiene

$$(I+m(n)^{\infty})\cap\hat{I}=(\hat{I}+m(n)^{\infty})\cap\hat{I}.$$

Por la ley modular, la anterior igualdad se puede escribir como

$$I+(m(n)^{\infty}\cap\hat{I})=\hat{I}+(m(n)^{\infty}\cap\hat{I}).$$

Dado que $m(n)^{\infty}\cap\hat{I}=\hat{I}m(n)^{\infty}$ y como $m(n)^{\infty}\cap\hat{I}\subseteq\hat{I}$, se sigue que $\hat{I}=I+\hat{I}m(n)^{\infty}$. Ya que $\hat{I}$ es finitamente generado, por el lema de Nakayama se tiene que $I=\hat{I}$. □

Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales finitamente generados en un anillo A, entonces se sabe que en general, $\mathfrak{a}\cap\mathfrak{b}$ no es un ideal finitamente generado. Para ideales en el anillo $\mathcal{E}(n)$, se tiene

OBSERVACIÓN 4.2.22. Si I es un ideal finitamente generado de $\mathcal{E}(n)$, entonces $I\cap m(n)^{k+1}$ es finitamente generado para cada $k\in\mathbb{N}$.

DEMOSTRACIÓN

Sean $f_1,\ldots,f_s$ generadores del ideal I y $f\in I$. Entonces $f=f_1\,g_1+\cdots+f_s\,g_s$, con $g_i\in\mathcal{E}(n)$, $i=1,\ldots,s$. f se puede escribir como

$$f=f_1\,\mathcal{J}^k(g_1)+\cdots+f_s\,\mathcal{J}^k(g_s)+[(g_1-\mathcal{J}^k(g_1))f_1+\cdots+(g_s-\mathcal{J}^k(g_s))f_s]$$

donde $\mathcal{J}^k(g_i)$ es el *k-jet* de $g_i\in\mathcal{E}(n)$, $i=1,\ldots,s$. Considérese $J=\{\sum_{i=1}^{s} f_i\,\mathcal{J}^k(g_i)\mid g_i\in\mathcal{E}(n)\}$. J es un $\mathcal{E}(n)$-módulo y como $\mathbb{R}$-espacio vectorial es generado por $\{x^L g_i\}$ con $|L|\leq k$. Como

$$\sum_{i=1}^{s}(g_i-\mathcal{J}^k(g_i))f_i\in Im(n)^{k+1}\text{ se sigue que}$$

$$I=J+Im(n)^{k+1}.\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(1)$$

Intersecando esta igualdad con $m(n)^{k+1}$, se obtiene

$$I\cap m(n)^{k+1}=(J+Im(n)^{k+1})\cap m(n)^{k+1}$$

lo cual se puede escribir como (con $Im(n)^{k+1}\subseteq m(n)^{k+1}$)

$$I\cap m(n)^{k+1}=J\cap m(n)^{k+1}+Im(n)^{k+1}$$

Como I y $m(n)^{k+1}$ son ideales finitamente generados, $Im(n)^{k+1}$ es generado por el conjunto de todos los productos de generadores de I y $m(n)^{k+1}$, esto es, el conjunto de generadores de $Im(n)^{k+1}$ es finito. Ahora, si se considera a los ideales en (1) como espacios vectoriales, $J\cap m(n)^{k+1}$ es un subespacio vectorial de J cuya base unida al conjunto de generadores de $Im(n)^{k+1}$ que es un conjunto finito, genera a $I\cap m(n)^{k+1}$. □

APÉNDICE A

En el capítulo 1 se ha hecho uso de algunas propiedades de anillos locales regulares. En este apéndice se presentan en forma más extensa los conceptos y resultados necesarios para la comprensión de lo expuesto ahí. Como siempre, anillo significa anillo conmutativo con unitario.

Como ya se comentó en el capítulo 1, una expresión de la forma $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ es una **cadena** de ideales primos de A cuya **longitud** se define como el número de ideales en la cadena menos 1; y es un entero no negativo o ∞.[†)] Una cadena $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ de ideales primos de un anillo A está **saturada** si no se puede construir una cadena de longitud $n+1$ agregando un ideal primo de A entre dos términos vecinos; y la cadena es **maximal** si ella está saturada, P_n es un ideal maximal de A y P_0 un ideal primo minimal de cero. También, en el capítulo 1 se definió la **dimensión** de un anillo A como el supremo de longitudes de cadenas de ideales primos de A. Como todo ideal primo de A está contenido en un ideal maximal de A y contiene un ideal primo minimal de cero, se sigue que para calcular la dimensión de A no es necesario considerar todas las cadenas de ideales primos de A si no únicamente las cadenas maximales en A. Si A es un anillo y P un ideal primo de A, se define la **altura** de P escrita $ht_{\mathrm{A}}(P)$ como el supremo de longitudes de cadenas $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ de ideales primos de A con $P_n = P$. Al igual que la longitud, la altura es un entero no negativo o ∞. Si A es un anillo de dimensión finita, entonces

$$dim(\mathrm{A}) = sup\{ht_{\mathrm{A}}(m) \mid m \text{ es un ideal maximal de A}\}.$$

Dado que los ideales maximales en un anillo A son primos, se tiene también que

$$dim(\mathrm{A}) = sup\{ht_{\mathrm{A}}(P) \mid P \text{ es un ideal primo de A}\}.$$

De esto se sigue

OBSERVACIÓN A.1. Si (A, m) es un anillo local, entonces $dim(\mathrm{A}) = ht_{\mathrm{A}}(m)$. □

Como se recordará, un anillo A es **noetheriano** si toda cadena ascendente de ideales de A es estacionaria (condición de cadena ascendente) [‡)] o todo subconjunto no vacío de ideales de A ordenado parcialmente por inclusión tiene un elemento maximal (condición maximal) o todo ideal de A es finitamente generado. También se dice que A es un **anillo de Artin** (o artiniano) si toda cadena descendente de ideales de A es estacionaria (condición de cadena descendente) o todo subconjunto no vacío de ideales de A ordenado parcialmente por inclusión tiene un elemento minimal (condición minimal). En forma análoga se definen módulo noetheriano y módulo artiniano.

Para un ideal I ($\neq$A) de un anillo noetheriano A, se define la altura de I como

---

[†)] Las cadenas de longitud cero son aquellas que constan de un único ideal primo P de A.

[‡)] La **condición de cadena ascendente** establece que si $(I_i)_{i\in\mathbb{N}}$ es una familia de ideales de A tal que $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq I_{i+1} \subseteq \cdots$, entonces existe $k \in \mathbb{N}$ tal que $I_k = I_{k+i}$ para todo $i \in \mathbb{N}$.

$$ht_{\mathrm{A}}(I)=min\{ht_{\mathrm{A}}(P) \mid P\supseteq I \text{ es un ideal primo}\}.$$

Como todo ideal primo de A que contiene a I contiene un ideal primo minimal de I, se sigue que

$$ht_{\mathrm{A}}(I)=min\{ht_{\mathrm{A}}(P) \mid P \text{ es un ideal primo minimal de } I\}.$$

Sea $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ una cadena de ideales primos de un anillo A tal que $I\subseteq P_0$ con I un ideal de A. Entonces $P_0/I\subsetneq P_1/I\subsetneq\cdots\subsetneq P_n/I$ es una cadena de ideales primos del anillo A/I. De la biyección que existe entre los ideales $J\supseteq I$ del anillo A y J/I en el anillo A/I, se sigue que $dim(\mathrm{A}/I)$ es igual al supremo de longitudes de cadenas $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ de ideales primos de A donde $I\subseteq P_0$. Por otro lado, si el ideal P es un ideal primo de A con $I\subseteq P$, $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ y $P'_0\subsetneq P'_1\subsetneq\cdots\subsetneq P'_m$ cadenas de ideales primos de A donde $P_n=P=P'_0$, entonces $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n\subsetneq P'_1\subsetneq\cdots\subsetneq P'_m$ es una cadena de longitud $m+n$ de ideales primos de A. Así, se tiene

OBSERVACIÓN A.2. Sean $I\subseteq P$ ideales de un anillo A con P primo. Entonces
$dim(\mathrm{A}/I)=sup\{ht_{\mathrm{A}}(P) \mid I\subseteq P\}$, $ht_{\mathrm{A}/I}(P/I)\le ht_{\mathrm{A}}(P)$ y $ht_{\mathrm{A}}(P)+dim(\mathrm{A}/I)\le dim(\mathrm{A})$. □

OBSERVACIÓN A.3. Sea P un ideal primo de un anillo A y S un subconjunto multiplicativamente cerrado en A tal que $P\cap\mathrm{S}=\varnothing$. Entonces $ht_{\mathrm{S}^{-1}\mathrm{A}}(\mathrm{S}^{-1}P)=ht_{\mathrm{A}}(P)$.

DEMOSTRACIÓN

Sea $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ una cadena de ideales primos del anillo A con $P_n=P$. De la biyección que existe entre los ideales P en el anillo A con $P\cap\mathrm{S}=\varnothing$ y los ideales $\mathrm{S}^{-1}P$ en el anillo de cocientes $\mathrm{S}^{-1}\mathrm{A}$, se sigue que $\mathrm{S}^{-1}P_0\subsetneq\mathrm{S}^{-1}P_1\subsetneq\cdots\subsetneq\mathrm{S}^{-1}P_n$ es una cadena de ideales primos en $\mathrm{S}^{-1}\mathrm{A}$ con $\mathrm{S}^{-1}P_n=\mathrm{S}^{-1}P$. Luego $ht_{\mathrm{S}^{-1}\mathrm{A}}(\mathrm{S}^{-1}P)\ge ht_{\mathrm{A}}(P)$. Por otro lado, si $\wp_0\subsetneq\wp_1\subsetneq\cdots\subsetneq\wp_n$ es una cadena de ideales primos del anillo de cocientes $\mathrm{S}^{-1}\mathrm{A}$ con $\wp_n=\mathrm{S}^{-1}P$ y $\varphi^{-1}(\wp_0)\subsetneq\varphi^{-1}(\wp_1)\subsetneq\cdots\subsetneq\varphi^{-1}(\wp_n)$ es una cadena de ideales primos de A (con $\varphi:\mathrm{A}\to\mathrm{S}^{-1}\mathrm{A}$ el homomorfismo natural), donde $\varphi^{-1}(\wp_n)\subsetneq\varphi^{-1}(\mathrm{S}^{-1}P)=P$. Así, $ht_{\mathrm{S}^{-1}\mathrm{A}}(\mathrm{S}^{-1}P)\le ht_{\mathrm{A}}(P)$. □

Sea A un anillo y P un ideal primo de A, luego $dim(\mathrm{A}_P)=ht_{\mathrm{A}}(P)$ con A_P la localización de A en P. Esto se sigue de que $dim(\mathrm{A}_P)=ht_{\mathrm{A}}(P\mathrm{A}_P)$ y $ht_{\mathrm{A}}(P\mathrm{A}_P)=ht_{\mathrm{A}}(P)$.

LEMA DE NAKAYAMA. Sea I un ideal de un anillo A con $I\subseteq Jac(\mathrm{A})$, M un A-módulo finitamente generado y N un A-submódulo de M. Si $\mathrm{N}+I\mathrm{M}=\mathrm{M}$, entonces $\mathrm{N}=\mathrm{M}$.[†)]

DEMOSTRACIÓN

Si el A-módulo M es generado por $\mathrm{m}_1,\ldots,\mathrm{m}_n$, entonces el A-módulo M/N es

[†)] ***Jac*(A)** se denomina **radical de Jacobson** y se define como la intersección de todos los ideales maximales de A. *Jac*(A) tiene la propiedad de que $x\in Jac(\mathrm{A})\Leftrightarrow 1-xy$ es una unidad de A para cada y en A.

generado por $m_1+N,\ldots,m_n+N$. Como $N+IM=M$, se sigue que $I(M/N)=(N+IM)/N=M/N$; se afirma que $M/N=0$. Supóngase lo contrario; sea $L=\{g_1,\ldots,g_n\}$ un conjunto generador minimal para $M/N=I(M/N)$. Dado que $g_1\in I(M/N)$, existen $a_1,\ldots,a_n\in I$ tal que $g_1=\sum_{i=1}^{n} a_i g_i$, entonces $g_1(1-a_1)=\sum_{i=2}^{n} a_i g_i$. Como $a_1\in I\subseteq Jac(A)$, $1-a_1$ es una unidad de A con inverso b, luego se tiene que $g_1=\sum_{i=2}^{n} ba_i g_i$ y M es generado por $\{g_2,\ldots,g_n\}$, lo cual es una contradicción. Por lo tanto $M/N=0$ y $N=M$. □

OBSERVACIÓN A.4. Sea (A, m) un anillo local con $K=A/m$ su campo residual. Si M es un A-módulo finitamente generado y si $m_1,\ldots,m_n\in M$ son tales que $m_1+M,\ldots,m_n+M$ forman una base del K-espacio vectorial M/mM, entonces $m_1,\ldots,m_n$ generan a M.

DEMOSTRACIÓN
Sea N el A-submódulo de M generado por los elementos $m_1,\ldots,m_n$; se afirma que $N+mM=M$. Sea $m\in M$, entonces existen elementos $a_1,\ldots,a_n\in A$ tal que

$$m+mM=a_1(m_1+mM)+\cdots+a_n(m_n+mM),$$

luego $m-\sum_{i=1}^{n} a_i m_i\in mM$ y $M\subseteq N+mM$. La otra contención es por construcción. Así, $M=N+mM$ y por el lema de Nakayama se sigue que $M=N$. □

Como se recordará, un ideal propio I de un anillo A es un ideal **primario** de A si siempre que $a, b\in A$ con $ab\in I$, entonces $a\in I$ o $b^n\in I$ para algún $n\in\mathbb{N}$. Esto es, I es primario si y sólo si el anillo A/I es no trivial y cada divisor de cero en A/I es nilpotente. Se observa que todo ideal primo de A es un ideal primario de A, También, se dice que un ideal I en A es ***P*-primario** si $rad(I)=P$ con P ideal primo de A.

OBSERVACIÓN A.5. Sean I y m ideales de un anillo A tal que m es un ideal maximal de A. Si $rad(I)=m$, entonces I es un ideal primario de A y toda potencia m^n, con n número natural es m-primario.

DEMOSTRACIÓN

$I\neq A$ ya que $I\subsetneq m$. Ahora sean $a, b\in A$ tal que $ab\in I$ pero $b^n\notin I$ para cada $n\in\mathbb{N}$, entonces $b\notin rad(I)=m$ y $rad(I)+rad(\langle b\rangle_A)=A$. Luego $I+\langle b\rangle_A=A$, y existen $d\in I$ y $c\in A$ tal que $d+cb=1$; así, $a=a1=a(d+cb)=ad+a(cb)\in I$ ya que $d\in I$ y $ab\in I$. Por lo tanto I es primario. La última afirmación se sigue del hecho de que $rad(m^n)=m$ para toda $n\in\mathbb{N}$. □

OBSERVACIÓN A.6. Sea I un ideal de un anillo A. Si $rad(I)$ es finitamente generado, entonces existe $n\in\mathbb{N}$ tal que $rad(I)^n\subseteq I$.

DEMOSTRACIÓN

Supóngase que $rad(I)$ es generado por $a_1,\ldots,a_k$. Luego para cada $i=1,\ldots,k$, existe $n_i\in\mathbb{N}$ tal que $a_i^{n_i}\in I$. Sea $n=1+\sum_{i=1}^{k}(n_i-1)$; se sigue que $rad(I)^n$ es el ideal generado por el conjunto

$$L=\{\, a_1^{r_1}\cdots a_k^{r_k} \mid r_1,\ldots,r_k\in\mathbb{N}\cup\{0\},\ \sum_{i=1}^{k} r_i=n\}.$$

Por como se ha definido n, se tiene que $r_j\geq n_j$ para al menos un índice j, con $j=1,\ldots,k$; luego $a_1^{r_1}\cdots a_k^{r_k}\in I$. De aquí, $L\subseteq I$ y $rad(I)^n\subseteq AL\subseteq I$. □

Sea I un ideal de un anillo A. Se dice que I admite una **descomposición primaria** si existen ideales primarios $Q_1,\ldots, Q_n$ en A tal que $I=Q_1\cap\cdots\cap Q_n$ con $rad(Q_i)=P_i$, $i=1,\ldots, n$; e I admite una **descomposición primaria minimal** si $P_1,\ldots,P_n$ son ideales diferentes de A e $I\neq Q_1\cap\cdots\cap Q_{j-1}\cap Q_{j+1}\cap\cdots\cap Q_n$ o equivalentemente $Q_j\not\supseteq Q_1\cap\cdots\cap Q_{j-1}\cap Q_{j+1}\cap\cdots\cap Q_n$ para toda $j=1,\ldots, n$. Los ideales P_i se denominan **ideales primos asociados** de I. Si I es un ideal de A que admite una descomposición primaria minimal, entonces para un ideal primo P de A, se tiene que $rad(I)\subseteq rad(P)=P$ si y sólo si $I\subseteq P$.[†)] Dado que $rad(I)=\bigcap_{i=1}^{n} rad(Q_i)=\bigcap_{i=1}^{n} P_i$, se sigue que $I\subseteq P$ si y sólo si $P_{j_0}\subseteq P$ para algún índice j_0 en $\{1,\ldots,n\}$, es decir, $P'\subseteq P$ para algún $P'\in\{P_1,\ldots,P_n\}$.

LEMA A.7. Sea I un ideal de un anillo noetheriano A y $J=\bigcap_{n=1}^{\infty} I^n$. Entonces $J=IJ$.

DEMOSTRACIÓN

Si $I=A$, el resultado se sigue. Por otro lado, si $I\neq A$, como A es noetheriano y $IJ\subseteq J\subseteq I$, entonces que $IJ\neq A$, luego IJ tiene una descomposición primaria minimal, esto es, existen ideales primarios $Q_1,\ldots,Q_n$ en el anillo A tal que $IJ=Q_1\cap\cdots\cap Q_n$ con $rad(Q_i)=P_i$, $i=1,\ldots,n$; se afirma que $J\subseteq Q_i$ para cada $i=1,\ldots,n$. Supóngase que existe un índice i_0 en $\{1,\ldots,n\}$ tal que $J\not\subseteq Q_{i_0}$ y sea $a\in J\setminus Q_{i_0}$. Como $a\in J$ se sigue que $aI\subseteq IJ=Q_1\cap\cdots\cap Q_n\subseteq Q_{i_0}$. Dado que Q_{i_0} es P_{i_0}-primario y $a\notin Q_{i_0}$, se tiene que $I\subseteq P_{i_0}$. Como $P_{i_0}=rad(Q_{i_0})$, se sigue de A.6., que existe $t\in\mathbb{N}$ tal que $P_{i_0}^{\,t}\subseteq Q_{i_0}$ Luego se obtiene que $J=\bigcap_{i=1}^{\infty} I^n\subseteq I^n\subseteq P_{i_0}^{\,t}\subseteq Q_{i_0}$ lo cual es una contradicción. Así, $J\subseteq Q_i$ para cada $i=1,\ldots,n$ y $J=IJ$. □

[†)] $\{P_1,\ldots, P_n\}$ es independiente de la elección de la descomposición primaria minimal de I. Esto es, si $I=Q_1\cap\cdots\cap Q_n$ con $rad(Q_i)=P_i$, $i=1,\ldots,n$ e $I=Q_1'\cap\cdots\cap Q_m'$ con $rad(Q_i')=P_i'$, $i=1,\ldots, m$ son dos descomposiciones primarias minimales de I entonces $n=m$ y $\{P_1,\ldots,P_n\}=\{P_1',\ldots, P_m'\}$.

TEOREMA A.8. (*Krull*) Sea I un ideal de un anillo noetheriano A tal que $I \subseteq Jac(A)$. Entonces $\bigcap_{i=1}^{\infty} I^n = 0$

DEMOSTRACIÓN

Sea $J = \bigcap_{i=1}^{\infty} I^n$; por A.7, $J = IJ$. Como A es noetheriano y J es un ideal finitamente generado de A, se sigue del lema de Nakayama que $J = 0$. □

Se observa que si (A, m) es un anillo local noetheriano, se sigue de A.8, que $\bigcap_{i=1}^{\infty} m^n = 0$.

COROLARIO A.9. Sean I y m ideales de un anillo noetheriano A, con m un ideal maximal. Entonces las siguientes afirmaciones son equivalentes.

i) I es m-primario

ii) $rad(I) = m$.

iii) $m^n \subseteq I \subseteq m$ para algún $n \in \mathbb{N}$.

DEMOSTRACIÓN

i)$\Rightarrow$*ii*) por definición. *ii*)$\Rightarrow$*iii*) se sigue de A.5 y A.6. *iii*)$\Rightarrow$*i*) tomando radicales; $rad(m^n) \subseteq rad(I) \subseteq rad(m)$. Así, $rad(I) = m$. □

OBSERVACIÓN A.10. Sea (A, m) un anillo local noetheriano e I un ideal de A (con $I \neq 0$, $I \neq A$). Entonces I es m-primario y $m^n \subseteq I$.

DEMOSTRACIÓN

Se sigue directamente de A.9. □

OBSERVACIÓN A.11. Sea A un anillo local noetheriano que no es un campo. Entonces $m^n \neq m^{n+1}$ para cada $n \in \mathbb{N} \cup \{0\}$.

DEMOSTRACIÓN

Supóngase que $m^n = m^{n+1}$ para algún $n \in \mathbb{N} \cup \{0\}$. Por el lema de Nakayama se tiene que $m = 0$, lo cual no es posible. □

OBSERVACIÓN A.12. Sea I un ideal de un anillo A que admite una descomposición primaria minimal y P un ideal primo de A. Entonces P es un ideal primo minimal de I si y sólo si P es un elemento minimal (con respecto a la inclusión) del conjunto $\{P_1, \ldots, P_n\}$ de ideales primos asociados de I.

DEMOSTRACIÓN ($\Rightarrow$)

Como $P' \subseteq P$ para algún $P' \in \{P_1, \ldots, P_n\}$ con $rad(Q_i) = P_i$, $i = 1, \ldots, n$ y

$$\{P_1,\ldots,P_n\}=\{P \mid P\supseteq I \text{ ideal primo de A}\}$$

se sigue de la hipótesis que $P=P'$ es un elemento minimal (con respecto a la inclusión) del conjunto $\{P_1,\ldots,P_n\}$ de ideales primos asociados de I.

($\Leftarrow$)

Si P es un elemento minimal de $\{P_1,\ldots,P_n\}$, entonces $I\subseteq P$ y existe un ideal primo minimal P' de I tal que $P'\subseteq P$. Luego existe un ideal primo minimal $P''\in\{P_1,\ldots,P_n\}$ tal que $P''\subseteq P'\subseteq P$; como P es un elemento minimal de $\{P_1,\ldots,P_n\}$, se tiene que $P=P'=P''$. Por lo tanto $P=P'$ es un ideal primo minimal de I. □

Como una consecuencia de este resultado, se obtiene que todos los ideales primos minimales de I pertenecen a $\{P_1,\ldots,P_n\}$, luego I tiene solamente un número finito de ideales primos minimales.

Sean I, J ideales de un anillo A, M un A-módulo y N un A-submódulo de M. Se definen los **ideales cociente** $(I : J)=\{a\in A \mid <a>J\subseteq I\}$ y $(N : J)=\{a\in A \mid ab\in J$ para todo $b\in J\}$ si $J\subseteq M$, $J\neq\emptyset$. $(I : J)$ y $(N : J)$ son ideales de A. En el caso particular de que $J=0$ y $N=0$, $(0 : J)=\{a\in A \mid ab=0$ para todo $b\in J\}$ (en ambos casos) se denominan **anulador** de J y se escribe $Ann(J)$. Si I es un ideal de un anillo A, M es un A-módulo e $I\subseteq Ann(M)$, entonces a M se le puede dar la estructura de un A/I-módulo, definiendo el mapeo $(A/I)\times M\to M$; $(a+I, m)\mapsto am$ con $a\in A$ y $m\in M$. De esta forma, las estructuras de A-módulo y A/I-módulo están relacionadas como: $(a+I)m=am$ para cada $a\in A$ y $m\in M$; y un subconjunto de M es un A-submódulo si y sólo si él es un A/I-submódulo. Entonces M es un A-módulo noetheriano (artiniano) si y sólo si M es un A/I-módulo noetheriano (artiniano). También, se tiene que A/I es un A-módulo noetheriano (artiniano) si y sólo si A/I es un anillo noetheriano (artiniano).

OBSERVACIÓN A.13. Sea A un anillo, $m_1,\ldots,m_n$ ideales maximales de A y M un A-módulo tal que $m_1\cdots m_nM=0$. Entonces M es un A-módulo noetheriano si y sólo si M es un A-módulo de Artin.

DEMOSTRACIÓN (por inducción sobre n)

Para $n=1$; como $m_1M=0$, M es anulado por m_1 y se puede considerar a M como un A/m_1-módulo, esto es, como un A/m_1-espacio vectorial. Entonces M es un A/m_1-espacio vectorial noetheriano (artiniano) si y sólo si M es un A-módulo noetheriano (artiniano). Pero si M es un A/m_1-espacio vectorial noetheriano si y sólo si M es un A/m_1-espacio vectorial de Artin. Luego M es un A-módulo noetheriano si y sólo si M es un A-módulo de Artin. Supóngase que $n>1$ y considérese la sucesión exacta

$$0\longrightarrow m_nM\xrightarrow{\ i\ }M\xrightarrow{\ \pi\ }M/m_nM\longrightarrow 0$$

Por la proposición 4.1.11., se tiene que M es un A-módulo noetheriano (artiniano) si y sólo si m_nM y M/m_nM son A-módulos noehterianos (artinianos). Ahora, como el módulo

M/m_nM es anulado por el ideal maximal m_n, se sigue que M/m_nM es un A-módulo noetheriano si y sólo si M/m_nM es un A-módulo de Artin. También, el A-módulo m_nM es anulado por el producto $m_1 \cdots m_{n-1}$ y por la hipótesis de inducción se tiene que m_nM es un A-módulo noetheriano si y sólo si m_nM es un A-módulo de Artin. □

PROPOSICIÓN A.14. Sea A un anillo noetheriano en el que todo ideal primo de A es maximal, entonces A es un anillo semilocal de Artin.[†)]

DEMOSTRACIÓN

Primero se probará que A es semilocal. Supóngase que A≠0 y sea m un ideal maximal de A. Como todo ideal primo de A es maximal, m es un ideal primo minimal que contiene al cero. Por A.12., se tiene que $m \in \{P_1, \ldots, P_n\}$, P_i, $i=1, \ldots, n$ ideales primos asociados de cero. Luego el conjunto $\{P \mid P$ ideal primo de A$\}$ está contenido en $\{P_1, \ldots, P_n\}$; pero $\{P_1, \ldots, P_n\}$, está contenido en $\{P \mid P$ ideal primo de A$\}$. De esta forma se tiene que, $\{P \mid P$ ideal primo de A$\}=\{P_1, \ldots, P_n\}$ es finito. Por lo tanto A es semilocal. A continuación se probará que A es un anillo de Artin. Sean $m_1, \ldots, m_n$ ideales maximales de A, entonces $rad(0)=\bigcap_{i=1}^{n} m_i$. Por A.6., existe $t \in \mathbb{N}$ tal que $rad(0)^t=0$, luego $m_1^t \cdots m_n^t \subseteq (\bigcap_{i=1}^{n} m_i)^t = rad(0)^t = 0$; entonces $m_1^t \cdots m_n^t A = 0$. Como A es, noetheriano se sigue de A.13., que A es un A-módulo de Artin. Por lo tanto A es un anillo de Artin. □

LEMA A.15. Sea A un anillo de Artin, entonces todo ideal primo de A es maximal.

DEMOSTRACIÓN

Sea P un ideal primo de A y $\overline{A} = A/P$. A es un dominio entero de Artin. Se probará que $\overline{A}$ es un campo. Sea $b \in \overline{A}$ con $b \neq 0$, entonces

$$\langle b \rangle_{\overline{A}} \supseteq \langle b^2 \rangle_{\overline{A}} \supseteq \cdots \supseteq \langle b^i \rangle_{\overline{A}} \supseteq \langle b^{i+1} \rangle_{\overline{A}} \supseteq \cdots$$

es una cadena descendente de ideales de $\overline{A}$, luego existe $n \in \mathbb{N}$ tal que $\langle b^n \rangle_{\overline{A}} = \langle b^{n+1} \rangle_{\overline{A}}$. De aquí, $b^n = cb^{n+1}$ para algún $c \in \overline{A}$. Dado que $\overline{A}$ es un dominio entero, $1=cb$ y b es una unidad de $\overline{A}$. Por lo tanto $\overline{A} = A/P$ es un campo y P es un ideal maximal de A. □

LEMA A.16. Sea A un anillo de Artin, entonces A tiene solamente un número finito de ideales maximales.

DEMOSTRACIÓN

Supóngase que A≠0 y sea $\Im$ el conjunto de todos los ideales de A que son expresados como intersecciones de un número finito de ideales maximales de A. Por la condición minimal, $\Im$ tiene un elemento minimal J. Entonces existen ideales maximales

[†)] Se dice que un anillo es **semilocal** si tiene solamente un número finito de ideales maximales.

$m_1,\ldots,m_n$ de A tal que $J=m_1\cap\cdots\cap m_n$. Se afirma que $m_1,\ldots,m_n$ son los únicos ideales maximales de A. En efecto, sea m un ideal maximal de A, entonces

$$J=m_1\cap\cdots\cap m_n\supseteq m\cap m_1\cap\cdots\cap m_n\in\mathfrak{I}.$$

Por la minimalidad de J en $\mathfrak{I}$, se tiene que

$$J=m_1\cap\cdots\cap m_n=m\cap m_1\cap\cdots\cap m_n.$$

Luego $m_1\cap\cdots\cap m_n\subseteq m$ y como m es primo, se sigue que $m_j\subseteq m$ para algún j con $j=1,\ldots,n$. Dado que m_j y m son ideales maximales de A, se deduce que $m_j=m$. Por lo tanto $m,\ldots,m_n$ son los únicos ideales maximales de A. □

PROPOSICIÓN A.17. Sea A un anillo de Artin, entonces existe $t\in\mathbb{N}$ tal $rad(0)^t=0$.

DEMOSTRACIÓN

Considérese la cadena

$$rad(0)\supseteq rad(0)^2\supseteq\cdots\supseteq rad(0)^i\supseteq rad(0)^{i+1}\supseteq\cdots$$

Como A es un anillo de Artin, existe un número natural t tal que $rad(0)^{t+i}=rad(0)^t$ para cada $i\in\mathbb{N}$; se afirma que $rad(0)^t=0$. Supóngase lo contrario, considérese la familia

$$\mathfrak{I}=\{I \mid I \text{ es un ideal de A e } I\cdot rad(0)^t\neq 0\}.$$

Entonces $rad(0)^i\in\mathfrak{I}$ para cada $i\in\mathbb{N}$; ya que $rad(0)^i rad(0)^t=rad(0)^{t+i}=rad(0)^t\neq 0$. Como A es de Artin, se sigue de la condición minimal que $\mathfrak{I}$ tiene un elemento minimal J. Como $J\cdot rad(0)^t\neq 0$, existe $a\in J$ tal que $rad(0)^t\neq 0$, $\langle a\rangle_A rad(0)^t\neq 0$ y $\langle a\rangle_A\subseteq J$. Por la minimalidad de J en $\mathfrak{I}$, se tiene que $\langle a\rangle_A=J$. Se observa que el ideal $a\cdot rad(0)^t$ $(=\langle a\rangle_A rad(0)^t)$ de A satisface

$$a\cdot rad(0)^t rad(0)^t=\langle a\rangle_A rad(0)^{2t}=\langle a\rangle_A rad(0)^t=J\cdot rad(0)^t\neq 0.$$

Dado que $a\cdot rad(0)^t\subseteq\langle a\rangle_A=J$, también se sigue de la minimalidad que $a\cdot rad(0)^t=\langle a\rangle_A=J$. En particular $a=ab$ para algún $b\in rad(0)^t\subseteq rad(0)$. Así, existe $r\in\mathbb{N}$ tal que $b^r=0$, y ya que $a=ab=(ab)b=ab^2=\cdots=ab^r=0$ se tiene que $J\cdot rad(0)^t=\langle a\rangle_A rad(0)^t=0$, lo cual es una contradicción. Por lo tanto $rad(0)^t=0$. □

Cuando un ideal I de un anillo A satisface $I^t=0$ para algún $t\in\mathbb{N}$, se dice que I es **nilpotente**.

TEOREMA A.18. Todo anillo de Artin es noetheriano.

DEMOSTRACIÓN

Supóngase que $A\neq 0$; por A.15., todo ideal primo de A es maximal y por A.16., A tiene solamente un número finito de ideales maximales $m_1,\ldots,m_n$. Como $rad(0)=\bigcap_{i=1}^{n} m_i$, por la proposición A.17., existe $t\in\mathbb{N}$ tal que $rad(0)^t=0$. Luego $m_1{}^t\cdots m_n{}^t\subseteq(\bigcap_{i=1}^{n} m_i)^t=rad(0)^t=0$; así, $m_1{}^t\cdots m_n{}^t A=0$. Dado que A es de Artin, de A.13., se sigue que A es noetheriano. □

COROLARIO A.19. A es de Artin si y sólo si A es noetheriano y todo ideal primo de A es maximal.

DEMOSTRACIÓN

La condición necesaria se sigue de A.15. y A.16.. La condición suficiente se sigue de A.14.. □

LEMA A.20. Sea A un anillo, P un ideal primo minimal de un ideal propio I de A y S un subconjunto multiplicativamente cerrado en A tal que $S\cap P=\varnothing$, entonces $S^{-1}P$ es un ideal primo minimal del ideal $S^{-1}I$ de $S^{-1}A$.

DEMOSTRACIÓN

Supóngase que existe un ideal primo $\wp'$ de $S^{-1}A$ tal que $S^{-1}I\subseteq\wp'\subsetneq S^{-1}P$. Luego existe un ideal primo P' del anillo A con $S\cap P'=\varnothing$ tal que $S^{-1}P'=\wp'$; entonces $S^{-1}I\subseteq S^{-1}P'\subsetneq S^{-1}P$ .Tomando imagen inversa, se tiene que

$$I\subseteq\varphi^{-1}(S^{-1}I)\subseteq\varphi^{-1}(S^{-1}P')=P'\subsetneq\varphi^{-1}(S^{-1}P)=P,$$

como P es un ideal primo minimal de I, se sigue que $P'=P$ y $S^{-1}P'=\wp'=S^{-1}P$. Luego $S^{-1}P$ es un ideal primo minimal de $S^{-1}I$. □

TEOREMA A.21. Sea A un anillo noetheriano e $I=\langle x_1,\ldots,x_n\rangle$ un ideal de A. Entonces $ht_A(P)\leq n$ para todo ideal primo minimal P de I.

DEMOSTRACIÓN (por inducción sobre n.)

Si $n=0$, $I=0$ y P es un ideal primo minimal del ideal cero, entonces $ht_A(P)=0$. Si $n=1$, dado que el ideal maximal PA_P del anillo local A_P es un ideal primo minimal del ideal $\langle x\rangle_A A_P$ y $ht_{AP}(PA_P)=ht_A(P)$, será suficiente probar el resultado para anillos locales (A, m) y $P=m$. Supóngase que $ht_A(m)>1$, entonces existe una cadena $P'\subsetneq P\subsetneq m$ de ideales primos de A de longitud 2. Como m es el único ideal maximal de A, y es un ideal primo minimal del ideal $\langle x\rangle_A$, se tiene que $m/\langle x\rangle_A$ es el único ideal primo del anillo $A/\langle x\rangle_A$, luego por A.14., $A/\langle x\rangle_A$ es un anillo de Artin. Considérese la n-ésima potencia simbólica del ideal P; es decir, $P^{(n)}=\varphi^{-1}(S^{-1}P^{\,n})$ ($\varphi:A\to A_P$ el homomorfismo natural) que es un ideal P-primario de A. Se observa que $P^{(n)}\supseteq P^{(n+1)}$ para cada $n\in\mathbb{N}$. Como $A/\langle x\rangle_A$ es de Artin, se tiene

$$(P^{(1)}+\langle x\rangle_A)/\langle x\rangle_A \supseteq (P^{(2)}+\langle x\rangle_A)/\langle x\rangle_A \supseteq \cdots \supseteq (P^{(n)}+\langle x\rangle_A)/\langle x\rangle_A \supseteq \cdots$$

Luego, existe $k\in\mathbb{N}$ tal que $P^{(k)}+\langle x\rangle_A=P^{(k+1)}+\langle x\rangle_A$. Ahora sea $r\in P^{(k)}$, entonces $r=s+xc$ para algún $s\in P^{(k+1)}$ y $c\in A$. Pero $xc=r-s\in P^{(k)}$ con $P^{(k)}$ un ideal P-primario de A y $x\notin P$ ya que m es un ideal primo minimal de $\langle x\rangle_A$; así, $c\in P^{(k)}$. De esto se obtiene que $P^{(k)}=P^{(k+1)}+\langle x\rangle_A$, pero $x\in m$ y $P^{(k)}/P^{(k+1)}=m(P^{(k)}/P^{(k+1)})$. Por el lema de Nakayama, se tiene que $P^{(k)}=P^{(k+1)}$. Ahora, sea $(S^{-1}P)^k=(S^{-1}P)^{k+1}$; nuevamente, por el lema de Nakayama aplicado ahora al A_P-módulo finitamente generado $(S^{-1}P)^k$, se sigue que $(S^{-1}P)^k=0$. De lo anterior, en el anillo A_P, el ideal maximal $S^{-1}P$ es nilpotente y como $rad(P^n)=P$ para toda $n\in\mathbb{N}$, $S^{-1}P$ está contenido en todo ideal primo de A_P. Esto último contradice que $S^{-1}P'\subsetneq S^{-1}P$ sea una cadena de ideales primos de A_P.

Supóngase que $n>1$. Como IA_P es un ideal de A_P que puede ser generado por n elementos, y como en el caso $n=1$, será suficiente probar el resultado para anillos locales noetherianos (A, m) con $P=m$. Sea P' un ideal no maximal de P, entonces existe un ideal primo P'' de A no maximal tal que $P'\subseteq P''$ y la cadena $P''\subsetneq m$ de ideales primos de A está saturada. Se afirma que para un ideal primo Q de A no maximal, la cadena de ideales primos está saturada y $ht_A(Q)\leq n-1$. Para el ideal Q, se tiene que $I\nsubseteq Q$, luego existen elementos $x_1,\ldots,x_n\in I$ con $x_n\notin Q$ e $I=\langle x_1,\ldots,x_n\rangle$. Ahora, m es el único ideal primo de A que contiene a $Q+\langle x_n\rangle_A$ y así, por la proposición A.14., el anillo $A/(Q+\langle x_n\rangle_A)$ es un anillo local de Artin. Por A.17. y A.15. y del hecho de que $rad(0)=\cap P$, (P ideal primo de A) su ideal maximal $m/(Q+\langle x_n\rangle_A)$ es nilpotente. Luego existe $k\in\mathbb{N}$ tal que $x_i^k\in(Q+\langle x_n\rangle_A)$ para cada $i=1,\ldots,n-1$. Entonces existen $q_1,\ldots,q_{n-1}\in Q$ y $a_1,\ldots,a_{n-1}\in A$ con $x_i^k=q_i+a_ix_n$ para cada $i=1,\ldots,n-1$. Se observa que $\langle x_1,\ldots,x_n\rangle_A\subseteq Q$; se probará que Q es un ideal primo minimal de $\langle q_1,\ldots,q_{n-1}\rangle_{\overline{A}}$. Sea $\overline{A}=A/\langle q_1,\ldots,q_{n-1}\rangle_{\overline{A}}$; luego todo ideal P' de A que contiene todas las $q_1,\ldots,q_{n-1}$, x_n contiene también a $x_1,\ldots,x_n$, así, m es el único ideal primo de A que contiene todas las $q_1,\ldots,q_{n-1}$, x_n. De esta forma, el ideal maximal $m/\langle q_1,\ldots,q_{n-1}\rangle_A$ del anillo $\overline{A}$ es un ideal primo minimal de ideal principal $\langle x_n\rangle_{\overline{A}}$. Por el caso $n=1$, se tiene que $ht_A(m/\langle q_1,\ldots,q_{n-1}\rangle_{\overline{A}})\leq 1$, de esto Q es un ideal primo minimal de $\langle q_1,\ldots,q_{n-1}\rangle_{\overline{A}}$ o la cadena $Q/\langle q_1,\ldots,q_{n-1}\rangle_{\overline{A}}\subseteq m/\langle q_1,\ldots,q_{n-1}\rangle_{\overline{A}}$ de ideales primos del anillo A puede ser extendida hacia abajo. Por lo tanto se sigue de la hipótesis de inducción que $ht_A(Q)\leq n-1$. □

Como una consecuencia del teorema anterior, se tiene que todo ideal primo de un anillo noetheriano tiene altura finita y en consecuencia todo anillo local noetheriano tiene dimensión finita. Por otro lado, si P y P' son ideales primos de un anillo noetheriano A con $P\subsetneq P'$, entonces $ht_A(P)\leq ht_A(P')$ y $ht_A(P)=ht_A(P')$ si y sólo si $P=P'$. También si $P_1\supsetneq P_2\supsetneq\cdots\supsetneq P_n$ es una cadena descendente de ideales primos de A, entonces se tiene que $n\leq ht_A(P_1)+1$ lo cual significa que A satisface la condición de cadena descendente.

OBSERVACIÓN A.22. Sean $I\subseteq P$ ideales de un anillo noetheriano A con P un ideal primo de A. Si $ht_A(I)=ht_A(P)$, entonces P es un ideal primo minimal de I.

DEMOSTRACIÓN

Supóngase que P no es un ideal primo minimal de I. Entonces existe un ideal primo minimal P' de I tal que $I\subseteq P'\subsetneq P$. Por los comentarios hechos antes de esta observación, $ht_{\mathrm{A}}(I)\leq ht_{\mathrm{A}}(P')< ht_{\mathrm{A}}(P)$, lo cual contradice la hipótesis. □

LEMA A.23. Sean H, H_1 y H_2 grupos aditivos contenidos en un cierto grupo G. Si $H\subseteq H_1\cup H_2$, entonces $H\subseteq H_1$ o $H\subseteq H_2$.

DEMOSTRACIÓN

Supóngase que $H\nsubseteq H_1$ y $H\nsubseteq H_2$, entonces existen elementos $h_1\in H\setminus H_1$ y $h_2\in H\setminus H_2$. Como $H\subseteq H_1\cup H_2$ se tiene que $h_1\in H_2$ y $h_2\in H_1$. Como $h_1+h_2\in H\subseteq H_1\cup H_2$, luego $h_1+h_2\in H_1$ o $h_1+h_2\in H_2$ pero ninguna de las dos situaciones es posible ya que $h_1=(h_1+h_2)-h_2\in H_1$ o $h_2=(h_1+h_2)-h_1\in H_2$ conducen a contradicciones. Por lo tanto $H\subseteq H_1$ o $H\subseteq H_2$. □

PROPOSICIÓN A.24. Sean $I_1,\ldots,I_n$ con $n\geq 2$ ideales de un anillo A tal que a lo más dos de ellos son no primos. Sea B un subanillo de A (B puede no tener al neutro multiplicativo de A) con $\mathrm{B}\subseteq\bigcup_{i=1}^{n} P_i$, entonces $\mathrm{B}\subseteq I_j$ para algún $j=1,\ldots,n$.

DEMOSTRACIÓN (Por inducción sobre n)

$n=2$ se sigue directamente del lema A.23.. Supóngase que el resultado es valido para $n=k$ con $k\geq 2$ y se desea probarlo para $n=k+1$. Se sabe que $\mathrm{B}\subseteq\bigcup_{i=1}^{k+1} I_i$, y que a lo mas dos de los ideales $I_1,\ldots,I_{k+1}$ son no primos. Supóngase que I_{k+1} es un ideal primo y que $\mathrm{B}\nsubseteq I_1\cup I_2\cup\cdots\cup I_{j-1}\cup I_{j+1}\cup\cdots\cup I_{k-1}\cup I_k$ para toda $j=1,\ldots,n$, entonces existen elementos $a_1,a_2,\ldots,a_{k+1}$ en el ideal A tal que $a_1\in\mathrm{B}\setminus I_2\cup I_3\cup\cdots\cup I_k\cup I_{k+1}$, $a_2\in\mathrm{B}\setminus I_1\cup I_3\cup\cdots\cup I_k\cup I_{k+1},\ldots,$ $a_{k+1}\in\mathrm{B}\setminus I_1\cup I_2\cup\cdots\cup I_{k-1}\cup I_k$.[†]. Dado que $\mathrm{B}\subseteq\bigcup_{i=1}^{k+1} I_i$, se tiene que $a_1\in I_1,\ldots,a_{k+1}\in I_{k+1}$. Como I_{k+1} es un ideal primo en A, se sigue que $a_1\cdots a_k\notin I_{k+1}$, luego $a_1\cdots a_k\in\bigcap_{i=1}^{k}(I_i\setminus I_{k+1})$ y $a_{k+1}\in I_{k+1}\setminus I_1\cup I_2\cup\cdots\cup I_k$. Considérese el elemento $b=a_1\cdots a_k+a_{k+1}$, entonces $b\notin I_{k+1}$ ya que de lo contrario $a_1\cdots a_k=b-a_{k+1}\in I_{k+1}$ lo cual es una contradicción. También, $b\notin I_j$, para algún j en $\{1,\ldots,k\}$ ya que si $b\in I_j$, para cada $j=1,\ldots,k$ implicaría que $a_{k+1}=b-a_1\cdots a_k\in I_j$ lo cual no puede ser posible. Pero $b\in\mathrm{B}$ ya

que $a_1,\ldots,a_{k+1}\in\mathrm{B}$ y así, se tiene una contradicción a la hipótesis de que $\mathrm{B}\subseteq\bigcup_{i=1}^{k+1} I_i$. Luego existe al menos un j en $\{1,\ldots,k+1\}$ tal que $\mathrm{B}\subseteq I_1\cup I_2\cup\cdots\cup I_{j-1}\cup I_{j+1}\cup\cdots\cup I_{k-1}\cup I_k$. Usando la hipótesis de inducción se obtiene que $\mathrm{B}\subseteq I_i$ para algún i en $\{1,\ldots,k+1\}$ □

A continuación se probará el inverso del teorema A.21..

[†] Si P_{k+1} no es un ideal primo, se elige un ideal primo P_i con i en $\{1,\ldots,n\}$ y reindizando se escribe este ideal en la posición $k+1$.

TEOREMA A.25. Sea A un anillo noetheriano y P un ideal primo de A. Si $ht_A(P)=n$, entonces existe un ideal I de A generado por n elementos tal que $I\subseteq P$ y $ht_A(I)=n$.

DEMOSTRACIÓN (por inducción sobre n.)

Para $n=0$, se elige $I=0$. Sea $n>0$ y $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_{n-1}\subsetneq P_n$ una cadena de ideales primos de A con $P_n=P$. Como $ht_A(P_{n-1})<ht_A(P)$, se tiene que $ht_A(P_{n-1})\leq n$-1 mientras que $ht_A(P_{n-1})\geq n$-1 en virtud de la cadena anterior. Entonces por la hipótesis de inducción aplicada al ideal P_{n-1}, existe un ideal propio J de A tal que $J=<a_1,\ldots,a_{n-1}>$, $J\subseteq P_{n-1}$ y $ht_A(J)=n$-1. Por la observación A.22., P_{n-1} es un ideal primo minimal de J y como tiene un número finito de ideales primos minimales, se sigue del teorema A.21., que todos los ideales primos minimales de J tienen altura n-1. Sean $Q_1,\ldots, Q_t$ los ideales primos minimales de J. Por A.24., se tiene que $P\nsubseteq P_{n-1}\cup Q_1\cup\cdots\cup Q_t$. Si esto no fuera el caso, se seguiría de A.24., que $P\subsetneq P_{n-1}$ o $P\subsetneq Q_i$ para alguna $i=1,\ldots, t$. pero ninguna de estas posibilidades puede ocurrir ya que

$$ht_A(P)=n,\ ht_A(P_{n-1})=ht_A(Q_1)=\cdots=ht_A(Q_t)=n\text{-}1.$$

Por lo tanto existe un elemento

$$a_n\in P\setminus(P_{n-1}\cup Q_1\cup\cdots\cup Q_t).$$

Definiendo

$$I=<a_1,\ldots,a_n>_A=<a_1,\ldots,a_{n-1}>_A+<a_n>_A;$$

se probará que el ideal I tiene las propiedades deseadas. Es claro que I es generado por n elementos e $I=J+<a_n>_A\subseteq P_{n-1}+P\subseteq P$; luego restará probar que $ht_A(I)=n$. Como $J\subseteq I\subseteq P$, $ht_A(J)=n$-1 y $ht_A(P)=n$, se sigue que $ht_A(I)$ es n-1 o n. Si $ht_A(I)=n$-1, existe un ideal primo minimal P' de I tal que $ht_A(P')=n$-1. Ahora $J\subseteq I\subseteq P'$ y $ht_A(J)\subseteq ht_A(P')=n$-1. Luego se sigue de A.22., que P' es uno de los ideales primos minimales de J, esto es, P' es uno de los ideales primos minimales $P_{n-1}, Q_1,\ldots, Q_t$. Pero esto no es posible ya que $a_n\in I\subseteq P'$, donde a_n no pertenece a ningúno de los ideales $P_{n-1}, Q_1,\ldots, Q_t$. Por lo tanto $ht_A(I)=n$. □

Como una consecuencia de esta proposición se tiene

OBSERVACIÓN A.26. Sea A un anillo noetheriano, $I\subseteq P$ ideales de A con $I=<x_1,\ldots,x_n>$ y P un ideal primo de A. Entonces $ht_{A/I}(P/I)\leq ht_A(P)\leq ht_{A/I}(P/I)+n$.

DEMOSTRACIÓN

De A.2., se sigue que $ht_{A/I}(P/I)\leq ht_A(P)$. Ahora, sean $x_1,\ldots, x_n$ generadores de I y considérese $\bar{A}=A/I$; supóngase que $ht_{A/I}(P/I)=t$. Por la observación A.22. y el teorema A.25., existen elementos $a_1,\ldots, a_t\in A$ tal que en el anillo A, el ideal primo P/I es un ideal primo minimal de $<a_1,\ldots, a_t>$. Ahora, como $<a_1,\ldots, a_t>=(<a_1,\ldots, a_t>+I)/I$, por la biyección

que existe entre ideales primos P en A e ideales primos P/I en A con $I\subseteq P$, y como dim(A) es el supremo de longitudes de cadenas $P_0\subsetneq P_1\subsetneq\cdots\subsetneq P_n$ de ideales primos de A que contienen a I (ver A.2.), se sigue que P es un ideal primo minimal del ideal $<a_1,\ldots,a_t>+I=<a_1,\ldots,a_t>+<x_1,\ldots,x_n>$ que es generado por $t+n$ elementos. Por el teorema A.21., $ht_A(P)\leq t+n$ y dado que $ht_{A/I}(P/I)\leq ht_A(P)$ se sigue el resultado. □

OBSERVACIÓN A.27. Sea (A, m) un anillo local noetheriano, entonces

$$dim(A)=min\{n\in\mathbb{N}\cup\{0\}\mid \text{existen } a_1,\ldots,a_n\in A \text{ con } <a_1,\ldots,a_t>\ m\text{-primario}\}.$$

DEMOSTRACIÓN

Supóngase que $n=min\{n\in\mathbb{N}\cup\{0\}\mid$ existen elementos $a_1,\ldots,a_n\in A$ con $<a_1,\ldots,a_t>$ m-primario$\}$. Se sigue de la observación A.1. que $dim(A)=ht_A(m)$ y del teorema A.21. que $dim(A)\leq n$ ya que un ideal m-primario tiene a m como su único ideal primo minimal. Por A.22. y A.25., existe un ideal primo Q de A que tiene a m como un ideal primo minimal y es generado por $dim(A)=ht_A(m)$ elementos. Como todo ideal primo de A está contenido en m y m es el único ideal primo asociado, se sigue que Q es m-primario y existe un ideal m-primario de A que es generado por dim(A) elementos con $dim(A)\geq n$. □

Sea (A, m) un anillo local noetheriano de dimensión d. Por un **sistema de parámetros** para A se entiende un conjunto de d elementos de A que generan un ideal m-primario. Si (A, m) es un anillo local noetheriano de dimensión d y $a_1,\ldots,a_t\in m$, se sigue de A.1., que $dim(A)=ht_A(m)$ y $dim(\overline{A})=ht_A(\overline{m})$ donde $\overline{A}=A/<a_1,\ldots,a_t>$ y $\overline{m}=m/<a_1,\ldots,a_t>$. Luego, de A.26., se tiene que

$$dim(A)-t\leq dim(\overline{A})\leq dim(A) \cdots\cdots\cdots\cdots\cdots(1)$$

Si $a_1,\ldots,a_t\in m$ son elementos de un sistema de parámetros para A, entonces

PROPOSICIÓN A.28. Sea (A, m) un anillo local noetheriano de dimensión d. Entonces $\{a_1,\ldots,a_t\}$ es un subconjunto de un sistema de parámetros donde todos los elementos son diferentes si y sólo si $dim(\overline{A})=dim(A)-t$ con $\overline{A}=A/<a_1,\ldots,a_t>$.

DEMOSTRACIÓN ($\Rightarrow$)

Supóngase que $t\leq d$ y que existen $a_{t+1},\ldots,a_d\in m$ tal que $a_1,\ldots,a_t, a_{t+1},\ldots,a_d$ forman un sistema de parámetros para A. Esto significa que $<a_{t+1},\ldots,a_d>$ es un ideal m-primario de A. Entonces $<\overline{a}_{t+1},\ldots,\overline{a}_d>$ es un ideal $\overline{m}$-primario de $\overline{A}$. Por A.27., $dim(\overline{A})\leq d-t$, pero se sigue de (1) que $dim(\overline{A})\geq d-t$.

($\Leftarrow$)

Supóngase que $dim(\overline{A})=d-t$, entonces $t\leq d$ y por A.27., existen $a_{t+1},\ldots,a_d\in m$ tal que $\{\overline{a}_{t+1},\ldots,\overline{a}_d\}$ es un sistema de parámetros para el anillo $\overline{A}$. Esto significa que el ideal $<a_1,\ldots,a_t,a_{t+1},\ldots,a_d>/<a_1,\ldots,a_t>$ es un ideal $\overline{m}$-primario de $\overline{A}$. Luego $<a_1,\ldots,a_d>$ es un

ideal m-primario de A. De A.27., se sigue que $\{a_1,\ldots,a_d\}$ con $a_1,\ldots,a_t$ todos diferentes, es un sistema de parámetros para A. □

Si (A, m) es un anillo local noetheriano de dimensión d y K=A/m su campo residual, se sigue del hecho de que $dim_K(m/m^2)$ es el número de elementos en cada conjunto generador minimal para m, que m es generado por al menos $dim(A)=d$ elementos (ver A.27.) y A es un anillo local regular (*se recuerda que un anillo local noetheriano* (A, m) *es un anillo local regular si* $dim(A)=dim_K(m/m^2)$). Si A es un anillo local regular y los elementos $a_1,\ldots,a_d\in m$ generan a m, ello es equivalente a que $a_1+m^2,\ldots,a_d+m^2$ formen una base en el K-espacio vectorial m/m^2. También, si A es un anillo noetheriano y P un ideal primo de A con $ht_A(P)=n$ y $P=<a_1,\ldots,a_n>$, entonces la localización A_P es un anillo local regular de dimensión n, esto se sigue del hecho de que la localización A_P es un anillo local noetheriano, tiene dimensión n y su ideal maximal $PA_P=<a_1,\ldots,a_n>A_P=<a_1,\ldots,a_n>_{A_P}$ es generado por n elementos.

LEMA A.29. Si (A, m) es un anillo local noetheriano de dimensión d, K=A/m su campo residual y $x\in m\setminus m^2$. Entonces $dim_{\overline{K}}(m/m^2)=dim_K(\overline{m}/\overline{m}^2)+1$, donde $\overline{K}=\overline{A}/\overline{m}$ es el campo residual del anillo local noetheriano $\overline{A}=A/<x>_A$ y $\overline{m}=m/<x>_A$ su ideal maximal.

DEMOSTRACIÓN

Supóngase que $dim_{\overline{K}}(\overline{m}/\overline{m}^2)=n$. Sean $a_1,\ldots,a_n\in m$ elementos tal que sus imágenes $a_1+m^2,\ldots,a_n+m^2$ forman una base para el K-espacio vectorial $\overline{m}/\overline{m}^2$. Luego $a_1+m^2,\ldots,a_n+m^2$ generan al ideal $\overline{m}$, entonces

$$\overline{m}=m/<x>_A=<a_1+m^2,\ldots,a_n+m^2>_A=(<a_1,\ldots,a_n>_A+<x>_A)/<x>_A.$$

y se sigue que $m=<a_1,\ldots,a_n>_A+<x>_A$. Así, el K-espacio vectorial m/m^2 es generado por $a_1+m^2,\ldots,a_n+m^2$. Resta probar que estos $n+1$ elementos son linealmente independientes sobre K. En efecto, supóngase que $b_1,\ldots,b_n,c\in A$ son elementos tales que en el K-espacio vectorial m/m^2, $\sum_{i=1}^{n}(b_i+m)(a_i+m^2)+(c+m)(x+m^2)=0$. Entonces $\sum_{i=1}^{n}(\overline{b_i}+\overline{m})(\overline{a_i}+\overline{m}^2)=0$. Pero $\overline{a_1}+\overline{m}^2,\ldots,\overline{a_n}+\overline{m}^2$ son linealmente independientes en $\overline{K}$ y así, $\overline{b_1},\ldots,\overline{b_n}\in\overline{m}$ y $b_1,\ldots,b_n\in m$. De $\sum_{i=1}^{n}a_ib_i+cx\in m^2$ se tiene que $cx\in m^2$, entonces $c\in m$ ya que si $c\notin m$, c sería una unidad de A y $x=c^{-1}cx\in m^2$ lo cual no es posible. Por lo tanto $a_1+m^2,\ldots,a_n+m^2$, $x+m^2$ son linealmente independientes en K. □

OBSERVACIÓN A.30. Sea (A, m) un anillo local regular con campo residual K=A/m y $x\in m\setminus m^2$. Entonces $\overline{A}=A/<x>_A$ es un anillo local regular de dimensión $dim(\overline{A})=dim(A)-1$.

DEMOSTRACIÓN

De A.26., se sigue que $ht_A(\bar{m})\geq ht_A(m)$-1 con $\bar{m}=m/<x>_A$ el ideal maximal de $\bar{A}$. Como $dim(\bar{A})=ht_{\bar{A}}(\bar{m})$ se tiene $dim_{\bar{K}}(\bar{m}/\bar{m}^2)\geq dim(\bar{A})=ht_{\bar{A}}(\bar{m})\geq ht_{\bar{A}}(\bar{m})$-1=$dim$(A)-1 donde $\bar{K}=\bar{A}/\bar{m}$ es el campo residual de $\bar{A}$. Pero de A.29. y dado que A es regular, resulta que dim(A)-1=$dim_K(m/m^2)$-1=$dim_{\bar{K}}(\bar{m}/\bar{m}^2)$+1-1. Luego

$$dim_K(\bar{m}/\bar{m}^2)\geq dim(\bar{A})\geq dim(A)\text{-}1=dim_{\bar{K}}(\bar{m}/\bar{m}^2),$$

esto es, $dim(\bar{A})=dim$(A)-1 y $dim(\bar{A})=dim_{\bar{K}}(\bar{m}/\bar{m}^2)$, lo cual significa que $\bar{A}$ es un anillo local regular de dimensión dim(A)-1. □

Sea A un subanillo de un anillo B; como se recordará, un elemento $x\in$B es entero sobre A si x satisface $x^n+a_1x^{n-1}+\cdots+a_n=0$ con $a_i\in$A, $i=1,\ldots,n$. Claramente todo elemento de A es entero sobre A. El conjunto X de todos los elementos de B que son enteros sobre A, se denomina **cerradura entera** de A en B y es un subanillo de B que contiene A. Cuando X=A, se dice que A es **enteramente cerrado** en B[†)]. Sea φ:A$\to$B un homomorfismo de anillos y M un B-módulo; a M se le puede dar una estructura de A-módulo donde la operación de multiplicación escalar se define como $\cdot$:A×M$\to$M; $(a, m)\mapsto \varphi(a)m$; de esta forma, se dice que M es considerado un A-módulo por medio de φ o por **restricción de escalares**. También se dice que un A-módulo M es **fiel** si Ann(A)=0.

PROPOSICIÓN A.31. Sea A un subanillo de un anillo B y $x\in$B. Entonces las siguientes afirmaciones son equivalentes.

i) x es entero sobre A.

ii) el subanillo A[x] de B es finitamente generado como un A-módulo.

iii) existe un subanillo A′ de B tal que A[x]$\subsetneq$A′; A′ es finitamente generado como un A-módulo.

iv) existe un A[x]-módulo fiel que es considerado como un A-módulo por restricción de escalares

DEMOSTRACIÓN

i) $\Rightarrow$ *ii*) A[x] es generado como un A-módulo por el conjunto $\{x^i \mid i\in\mathbb{N}\cup\{0\}\}$. Entonces existe $m\in\mathbb{N}$ y $a_0,\ldots, a_{m-1}\in$A tal que $x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0=0$, esto es, $x^m\in$A[1,$x,\ldots,x^{m-1}$] lo cual implica que $x^n\in$A[1,$x,\ldots,x^{m-1}$] para $n\geq m$. Será suficiente probar que $x^{m+n}\in<1, x,\ldots,x^{m-1}>_A$ para toda $n\in\mathbb{N}\cup\{0\}$. Luego existe un número entero no negativo con $x^n(x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0)=0$, esto es, $x^{m+n}=-(a_mx^n+\cdots+a_1x^{m+n-1})$. Por inducción sobre n se tiene que, efectivamente, todas las potencias positivas de x están en el A-módulo generado por 1,$x,\ldots,x^{m-1}$. Por lo tanto, A[x] es generado (como A-módulo) por 1, $x,\ldots,x^{m-1}$. *ii*) $\Rightarrow$ *iii*) Se sigue al tomar A′=A[x]. *iii*) $\Rightarrow$ *iv*) Tomando M=A′, el cual es un A[x]-módulo fiel ya que $a\in(0:, A')$ implica $a1_A=0$. *iv*) $\Rightarrow$ *i*) Sea M un A[x]-módulo fiel que es

[†)] Como se recordará, un campo K es algebraicamente cerrado si todo polinomio no constante en K[x] tiene una raíz en K. Luego enteramente cerrado implica algebraicamente cerrado pero no recíprocamente.

finitamente generado como un A-módulo. Dado que $x\mathrm{M}\subseteq\mathrm{AM}$, existe $n\in\mathbb{N}$ y $a_1,\ldots,a_n\in\mathrm{A}$ tal que $x^n+a_1x^{n-1}+\cdots+a_n\in(0\colon \mathrm{M})=0$. Luego x es entero sobre A. □

Si K es un campo, una **valoración discreta** es una función $v\colon \mathrm{K}\setminus\{0\}\to\mathbb{Z}$ que satisface

i) $v(xy)=v(x)+v(y)$

ii) $v(x+y)\geq min[v(x), v(y)]$.

El conjunto constituido por 0 y todos los $x\in \mathrm{K}\setminus\{0\}$ con $v(x)\geq 0$ es un anillo de valoración, llamado **anillo de valoración de *v***. Un dominio entero A es un **anillo de valoración discreta** si existe una valoración discreta v de su campo de cocientes K tal que A es el anillo de valoración de v. A es un anillo local y su ideal maximal m es el conjunto de todas las $x\in\mathrm{K}$ tal que $v(x)>0$. A continuación se establece la conexión que existe entre anillos de valoración discreta y anillos locales regulares.

PROPOSICIÓN A.32. Sea (A, m) un dominio entero local noetheriano de dimensión 1. Entonces las siguientes afirmaciones son equivalentes.

i) A es un anillo local regular.

ii) Todo ideal no cero de A es una potencia de m.

iii) existe $a\in\mathrm{A}$ tal que cada ideal no cero de A es de la forma $<a^k>$, para algún $k\in\mathbb{N}\setminus\{0\}$.

iv) A es un anillo de valoración discreta.

v) A es enteramente cerrado.

vi) m es principal.

DEMOSTRACIÓN

i) $\Rightarrow$ *ii*) Sea I un ideal de A diferente de cero. Por A.10., se sigue que $m^n\subseteq I$ para algún $n\in\mathbb{N}$. Por A.19., el anillo A/m^n es de Artin y su ideal maximal es principal, I/m^n es una potencia de m/m^n e I es una potencia de m. *ii*) $\Rightarrow$ *iii*) Por A.11., $m\neq m^2$, esto es, $m^2\subseteq m$. Sea $a\in m\setminus m^2$, por hipótesis $<a>=m^n$ para algún $n\in\mathbb{N}$. Como $a\notin m^2$, se tiene que $n=1$ y así, $m=<a>$. Dado que todo ideal no cero de A es una potencia de m, se sigue que cada ideal no cero de A tiene la forma $<a^k>=m^k$ para algún $k\in\mathbb{N}\cup\{0\}$. *iii*) $\Rightarrow$ *iv*) Como $m=<x>$, por A.11., $<x^k>\neq<x^{k+1}>$. Sea $a\in\mathrm{A}$ con $a\neq 0$, luego $<a>=<x^k>$ para exactamente un valor de k. Sea $v\colon \mathrm{K}\to\mathbb{Z}$, $v(a)=k$ y se extiende v a $\mathrm{K}\setminus\{0\}$ definiendo $v(a/b)=v(a)-v(b)$. v está bien definida, es una valoración discreta, y A es un anillo de valoración de v. *iv*) $\Rightarrow$ *v*) Sea $x\in\mathrm{K}$ entero sobre A, entonces $x^n+a_1x^{n-1}+\cdots+a_n=0$ con $a_i\in\mathrm{A}$, $i=1,\ldots,n$. Si x está en A, la demostración termina; si el inverso $x^{-1}\in\mathrm{A}$, entonces $x=-(a_1+a_2x^{-1}+\cdots+a_nx^{1-n})\in\mathrm{A}$. *v*) $\Rightarrow$ *vi*) Sea $a\in m$ con $a\neq 0$. Por A.10., $<a>$ es m-primario y contiene una potencia de m. Sea n el menor $i\in\mathbb{N}$ tal que $m^i\subseteq<a>$, entonces $m^{n-1}\nsubseteq<a>$. Sea $b\in m^{n-1}$ pero $b\notin<a>$ y $x=a/b\in\mathrm{K}$ con K el campo de funciones de A. Se observa que $x^{-1}=a/b\in\mathrm{K}\setminus\mathrm{A}$ (ya que $b\notin<a>$). Luego, por hipótesis x^{-1} no es entero sobre A. También se observa que $x^{-1}m=\{x^{-1}r \mid r\in m\}$ es un A-submódulo del campo K y $x^{-1}m\subseteq\mathrm{A}$ ya que $bm\subseteq m^n\subseteq<a>$. Luego $x^{-1}m$ es un ideal de A; se afirma que $x^{-1}m=\mathrm{A}$. En efecto, supóngase lo contrario; entonces $x^{-1}m\subseteq m$, esto significa que el A-módulo finitamente generado m es cerrado bajo la multiplicación por elementos del subanillo $\mathrm{A}[x^{-1}]$ del campo K y así, tiene una estructura natural como $\mathrm{A}[x^{-1}]$-módulo. Como

A es un dominio entero, por A.31., m es un A[x^{-1}]-módulo fiel y entonces x^{-1} es entero sobre A., luego $x^{-1}m$=A. Por lo tanto m=<x>. *vi*) $\Rightarrow$ *i*) Por A.4.,se tiene que $dim_K(m/m^2)\leq 1$ y por A.11., se sigue que $m/m^2\neq 0$. Luego $dim_K(m/m^2)=1$. □

Se sabe que no todo anillo local noetheriano es un dominio entero. Pero en el caso de los anillos locales noetherianos que son regulares esto si es cierto. Antes de ver esto, se prueba el siguiente

LEMA A.33. Sea (A, m) un anillo local noetheriano que no es un dominio entero y P=<x> un ideal primo de A. Entonces P es un ideal primo minimal del cero, esto es, $ht(P)$=0.

DEMOSTRACIÓN

Supóngase que P no es un ideal primo minimal de cero, entonces existe $P'\subseteq P$ ideal primo de A. Se observa que x$\notin P'$ o $P\subseteq P'$ lo cual no es posible; se afirma que $P'\subsetneq P^n$ para cada $n\in\mathbb{N}$. Por inducción sobre n; se observa que para n=1 se cumple. Ahora, sea $a\in P'$, como P=<x>, se tiene P^n=<x^n> y existe $b\in$A tal que $a=bx^n$. Como $a\in P'$ y $x\notin P'$, se sigue que $b\in P'\subsetneq P$, luego $a=bx^n\in P^{n+1}$; así, se ha probado que $P'\subseteq\bigcap_{n=1}^{\infty}P^n$. Por el teorema A.8., P'=0 pero esto contradice el hecho de que A no es un dominio entero. □

TEOREMA A.34. Todo anillo local regular es un domino entero.

DEMOSTRACIÓN

Sea (A, m) un anillo local regular de dimensión d, la demostración se hace por inducción sobre d. Si d=0, m es generado por 0 elementos y m=0, luego A es un campo y por tanto un dominio entero. d=1, se sigue de A.32.. Supóngase que d>1 y que el resultado es cierto para todo anillo local regular de dimensión < d. Supóngase también que A no es un dominio entero. Dado que $dim_K(m/m^2)=dim(A)=d>0$ se tiene que $m^2\subsetneq m$. Sea $x\in m\setminus m^2$, Por el lema A.30., A /<x>$_A$ es regular de dimensión d-1. Por la hipótesis de inducción, se tiene que <x>$_A$ es un ideal primo de A y por A.33.,se sigue que $ht(\langle x\rangle_A)=0$, esto es, <x>$_A$ es un ideal primo minimal de cero. Luego existe solamente un número finito de ideales primos minimales de cero; sean $P_1,\ldots,P_s$ tales ideales primos minimales de cero, entonces $m\setminus m^2\subseteq P_1\cup\cdots\cup P_s$ y $m\subseteq m^2\cup P_1\cup\cdots\cup P_s$. Por A.24., se deduce que $m\subsetneq m^2$ o $m\subseteq P_i$ para algúna i con $1\leq i\leq s$. No obstante, ninguna de las dos es posible: $m\subsetneq m^2$ es una contradicción al hecho de que $m^2\subsetneq m$ y $m\subseteq P_i$ para algún $i=1,\ldots,n$ significaría que $d=dim(A)=ht(m)\leq ht(P_i)=0$ lo cual también es una contradicción. Por lo tanto, A es un dominio entero. □

Sea (A, m) un anillo local regular de dimensión d. Un **sistema regular de parámetros para** A es un conjunto de d elementos que generan a m. Se termina este apéndice con el siguiente resultado que generaliza la observación A.30..

PROPOSICIÓN A.35. Sea (A, m) un anillo local regular de dimensión $d> 0$, $\{x_1,\ldots,x_d\}$ un sistema regular de parámetros para A. Entonces $\overline{A}=A/<x_1,\ldots,x_i>$ es un anillo local regular de dimensión d-i para toda $i=1,\ldots,d$ y

$$0\subsetneq<x_1>\subsetneq<x_1, x_2>\subsetneq\cdots\subsetneq<x_1,\ldots,x_i>\subsetneq\cdots\subsetneq<x_1,\ldots,x_d>$$

es una cadena saturada de ideales primos de A de longitud d.

DEMOSTRACIÓN

Sea $i\in\{1,\ldots,d\}$, por A.28., el anillo $\overline{A}$ tiene dimensión d-i y su ideal maximal $\overline{m}=m/<x_1,\ldots,x_i>$ es generado por d-i elementos $\overline{x}_{i+1},\ldots,\overline{x}_d$. Luego $\overline{A}$ es un anillo local regular y por A.34., es un dominio entero. Entonces el ideal $<x_1,\ldots,x_i>$ es un ideal primo de A para cada $i=1,\ldots,d$. Como $dim(\overline{A})=d$-i para toda $i=1,\ldots,d$, se sigue que

$$0\subsetneq<x_1>\subsetneq<x_1, x_2>\subsetneq\cdots\subsetneq<x_1,\ldots,x_i>\subsetneq\cdots\subsetneq<x_1,\ldots,x_d>.$$

Así, se tiene una cadena de ideales primos de A y es saturada porque su longitud es $dim(A)=d$. □

APÉNDICE B

TEOREMA B. Sea (f_n) una sucesión de funciones diferenciables f_n:U$\subseteq\mathbb{R}^n \to \mathbb{R}$, U abierto y conexo. Si

(i) existe al menos un $x_0\in$U tal que la sucesión $(f_n(x_0))$ converge en $\mathbb{R}$ y

(ii) para cada $x\in$U y para toda vecindad esférica $B_r(x)$ contenida en U, la sucesión de derivadas (Df_n) converge uniformemente en $B_r(x)$ a una función g.

Entonces para cada $x\in$U, la sucesión (f_n) converge uniformemente en $B_r(x)$ a una función f que es diferenciable en U y $g(x)=Df(x)$ para todo $x\in$U.

Para la demostración véase: Dieudonné, J., Fundamentos de Análisis Moderno, Editorial Reverté. (8.6.3) pagina 159.

APÉNDICE C

LEMA (*de Malgrange*) Existen constantes $C_k\geq 0$ que dependen únicamente de $k\in\mathbb{N}^n$ con la siguiente propiedad: Si K es un subconjunto compacto de $\mathbb{R}^n$ y $\varepsilon>0$ es un número real, entonces existe una función C^∞ α_ε en $\mathbb{R}^n$ la cual satisface:

1) $\alpha_\varepsilon=1$ en una vecindad de K, $\alpha_\varepsilon=0$ si $d(x, K)\geq\varepsilon$ y $0\leq\alpha_\varepsilon\leq 1$.
2) Para cada $x\in\mathbb{R}^n$ y para toda k, $|D^k\alpha_\varepsilon(x)|\leq C_k/\varepsilon^{|k|}$.

Para la demostración, véase (lema 3.3.) en [18], pagina 77 o (lema 4.2.) en [14], pag 11.

APÉNDICE D.

DETERMINACIÓN DE GERMENES.

Las propiedades cualitativas de una función $f:\mathbb{R}^n\to\mathbb{R}$ en una vecindad $V(x_0)$ de un punto x_0 en $\mathbb{R}^n$, usualmente son determinadas analizando los primeros términos del desarrollo en series de Taylor de f en torno a x_0.

$$f(x_0+h)=f(x_0)+f(x_0)_1+f(x_0)_2+\cdots+f(x_0)_k+\cdots$$

donde $f(x_0)$ es el término constante de f y $f_j(x_0)$ viene dado como

$$f_j(x_0)=\sum_{\mathrm{I}}\frac{\partial^{|\mathrm{I}|}f(x_0)}{\partial x^{\mathrm{I}}}\frac{h^{\mathrm{I}}}{\mathrm{I}!};\ \mathrm{I}=(i_1,...,i_n),\ |\mathrm{I}|=j.$$

El proceso de determinar las propiedades cualitativas de una función f cuando su desarrollo en series de Taylor puede ser truncado en algún término de cierto grado, es llamado el **problema de determinación**.

Como se recordará (ver capítulo 4), $\mathcal{E}(n)$ es el anillo de gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R})$. $\mathcal{E}(n)$ es un $\mathbb{R}$-espacio vectorial de dimensión infinita y un anillo local con ideal maximal $m(n)$ que consta de los gérmenes en $\mathcal{E}(n)$ que se anulan en cero (ver observación 4.2.2.). También, para el anillo $\mathcal{E}(n)$ se definieron $\mathfrak{I}(n)^k=\mathcal{E}(n)/m(n)^{k+1}$, $\boldsymbol{J}(n)^k=m(n)/m(n)^{k+1}$ y $\mathcal{J}^k:\mathcal{E}(n)\to\mathfrak{I}(n)^k$, donde $\mathfrak{I}(n)^k$ es el espacio de *k-jets* en cero de gérmenes en $\mathcal{E}(n)$ que es isomorfo al anillo de polinomios en n indeterminadas con coeficientes en $\mathbb{R}$ de grado $\le k$. El producto de los m factores $\mathcal{E}(n)\times\cdots\times\mathcal{E}(n)$ es isomorfo al $\mathbb{R}$-espacio vectorial de dimensión infinita $\mathcal{E}(n, m)$ de los gérmenes en cero de funciones en $C^\infty(\mathbb{R}^n, \mathbb{R}^m)$.

Sea $G(n)$ en $\mathcal{E}(n, n)$ el conjunto de los gérmenes en cero de difeomorfismos locales que mandan cero en cero. Si $f, g\in G(n)$ se define la composición de f y g escrita $f\circ g$ como la clase de la composición de los representantes f y g. $G(n)$ con esta operación es un grupo donde el germen de la identidad es el neutro, y el inverso de un germen $g\in G(n)$ es el germen g^{-1} (ya que el representante g es un difeomorfismo). El espacio de *k-jets* en cero de gérmenes en $\mathcal{E}(n, m)$ que se denotará por $\mathfrak{I}(n, m)^k$ es isomorfo al producto de m factores $\mathfrak{I}(n)^k\times\cdots\times\mathfrak{I}(n)^k$. Como $\mathfrak{I}(n)^k$ $(=\mathcal{E}(n)/m(n)^{k+1})$ es un espacio vectorial de dimensión finita, $\mathfrak{I}(n, m)^k$ también es un espacio vectorial de dimensión finita. Si $f=(f_1,\ldots,f_m)$ es un germen en $\mathfrak{I}(n, m)^k$, entonces el *k-jet* en cero de f viene dado como

$$\mathcal{J}^k(f)=(\mathcal{J}^k(f_1),\ldots,\mathcal{J}^k(f_m)).$$

Sea $G(n)^k$ el conjunto de *k-jets* en cero de gérmenes de difeomorfismos de $\mathbb{R}^n$ que se anulan en cero. En $G(n)^k$ se puede definir una operación $\star$ como sigue: si $f_1, f_2 \in G(n)$,

$$\mathcal{J}^k(f_1) \star \mathcal{J}^k(f_2) = \mathcal{J}^k(f_1 \circ f_2).$$

$\star$ está bien definida ya que si $f_1, f_2 \in G(n)$, entonces $f_1 \circ f_2 \in G(n)$; luego $\mathcal{J}^k(f_1 \circ f_2) \in G(n)^k$. Como $\mathcal{J}^k(f_1 \circ f_2)$ involucra solamente derivadas parciales de orden $\leq k$ de los gérmenes f_1 y f_2, entonces $\mathcal{J}^k(f_1 \circ f_2)$ coincidirá con $\mathcal{J}^k(g_1 \circ g_2)$ para aquellos gérmenes $g_1, g_2 \in G(n)$ tal que $\mathcal{J}^k(g_1) = \mathcal{J}^k(f_1)$ y $\mathcal{J}^k(g_2) = \mathcal{J}^k(f_2)$. Así, $\star$ no depende de los representantes. Como la composición de gérmenes es asociativa, se sigue que $\star$ es asociativa. El elemento neutro de $G(n)^k$ es el *k-jet* de la identidad en $\mathcal{E}(n, n)$ y si $\mathcal{J}^k(f)$ es cualquier otro elemento de $G(n)^k$, el *k-jet* $\mathcal{J}^k(f^{-1})$ es el inverso de $\mathcal{J}^k(f)$ ya que $\mathcal{J}^k(f) \star \mathcal{J}^k(f^{-1}) = \mathcal{J}^k(f \circ f^{-1}) = \mathcal{J}^k(id)$. Así, se puede escribir $\mathcal{J}^k(f^{-1}) = \mathcal{J}^k(f)^{-1}$; de esta forma $(G(n)^k, \star)$ es un grupo.

DEFINICIÓN D.1. Un grupo de *Lie* es un grupo que también es una variedad diferenciable y las operaciones de grupo; $(x, y) \mapsto xy$, $x \mapsto x^{-1}$ como funciones son C^∞.

Sea G un grupo de *Lie*. (H, φ) es un subgrupo cerrado de *Lie* de G si H es un grupo de *Lie*, (H, φ) es una subvariedad de G, $\varphi: H \to G$ es un homomorfismo de grupos y $\varphi(H)$ es un subconjunto cerrado de G. A continuación se prueba que $G(n)^k$ es un grupo de *Lie*. La operación $\star$ vista como una función es C^∞; en efecto, sean $f, g \in G(n)$ con $f = (f_1, \ldots, f_n)$ y $g = (g_1, \ldots, g_n)$, entonces $\mathcal{J}^k(f)$, $\mathcal{J}^k(g) \in G(n)^k$. Será suficiente probar que en cada coordenada, $\star$ depende polinomialmente de las derivadas parciales en cero de ordenes $\leq k$ de los gérmenes f_i, g_i; $i = 1, 2, \ldots, n$. Del isomorfismo que existe entre $\mathfrak{I}(n)^k$ y el anillo de polinomios en n indeterminadas con coeficientes en $\mathbb{R}$ de grado $\leq k$, se tiene que

$$\mathcal{J}^k(f_i) = \sum_{0 \leq |\mathrm{I}| \leq k} \frac{\partial^{|\mathrm{I}|} f_i(0)}{\partial x^{\mathrm{I}}} \frac{x^{\mathrm{I}}}{\mathrm{I}!} \text{ y } \mathcal{J}^k(g_i) = \sum_{0 \leq |\mathrm{I}| \leq k} \frac{\partial^{|\mathrm{I}|} g_i(0)}{\partial x^{\mathrm{I}}} \frac{x^{\mathrm{I}}}{\mathrm{I}!} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Del isomorfismo, de (1) y dado que $\mathcal{J}^k(f) \star \mathcal{J}^k(g) = (\mathcal{J}^k(f_1 \circ g), \ldots, \mathcal{J}^k(f_n \circ g))$, se sigue que $\mathcal{J}^k(f_i \circ g)$, coincide con el *k-jet* de

$$\sum_{\mathrm{I}} \frac{1}{\mathrm{I}!} \frac{\partial^{|\mathrm{I}|} f_i(0)}{\partial x^{\mathrm{I}}} \left[\prod_{j=1}^{n} \sum_{\mathrm{J}} \frac{1}{\mathrm{J}!} \frac{\partial^{|\mathrm{J}|} g_i(0)}{\partial x^{\mathrm{J}}} \frac{x^{\mathrm{J}}}{\mathrm{J}!} \right]^{\mathrm{I}}$$

$i = 1, 2, \ldots, n$, el cual depende polinomialmente de los coeficientes $\frac{1}{\mathrm{I}!} \frac{\partial^{|\mathrm{I}|} f_i(0)}{\partial x^{\mathrm{I}}}$ y $\frac{1}{\mathrm{J}!} \frac{\partial^{|\mathrm{J}|} g_i(0)}{\partial x^{\mathrm{J}}}$ para cada par de índices $i, j = 1, 2, \ldots, n$.

Como los elementos de $G(n)^k$ son los *k-jets* en cero de gérmenes de difeomorfismos en $\mathbb{R}^n$, esto es, de gérmenes en $\mathcal{E}(n, n)$ que se anulan en cero, entonces $G(n)^k$ está contenido en el $\mathbb{R}$-espacio vectorial de dimensión finita $\boldsymbol{J}(n)^k\times\cdots\times\boldsymbol{J}(n)^k\cong\boldsymbol{J}(n, n)^k$. Como el *k-jet* del germen constante cero no pertenece a $G(n)^k$, esta contención es propia, es decir, $G(n)^k\subsetneq\boldsymbol{J}(n)^k\times\cdots\times\boldsymbol{J}(n)^k$. Dado que $G(n)^k$ puede ser identificado con el grupo lineal general $GL(n, \mathbb{R})$; el grupo de todas las matrices no singulares reales $n\times n$ [†)]. $GL(n, \mathbb{R})$ se considera como un subconjunto de $\mathbb{R}^n$ y es abierto en $\mathbb{R}^n$ (como la función determinante det: $\mathbb{R}^n\to\mathbb{R}$ es un mapeo polinomial, se tiene que $det^{-1}(\mathbb{R}\setminus\{0\})=GL(n, \mathbb{R})$ es abierto). Luego $G(n)^k$ es un conjunto abierto en la variedad diferenciable $\boldsymbol{J}(n)^k\times\cdots\times\boldsymbol{J}(n)^k$ [‡)] y por tanto $G(n)^k$ es una variedad diferenciable de dimensión finita. Así, se tiene el primer resultado.

PROPOSICIÓN D.2. $G(n)^k$ es un grupo de *Lie* de dimensión finita.

DEMOSTRACIÓN

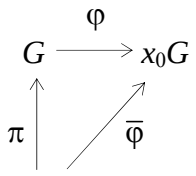
De la siguiente afirmación: *Si G es un grupo y una variedad diferenciable y la operación de grupo* $(x, y)\mapsto xy$ *vista como una función es* C^∞*, entonces* $x\mapsto x^{-1}$ *también es* C^∞, se sigue el resultado. □

Otros resultados de la teoría de grupos de *Lie* que serán necesarios aquí y cuya demostración se omite (para las demostraciones ver [17] y [19]) son los siguientes:

TEOREMA D.3. Sea G un grupo de *Lie*, H un subgrupo cerrado de *Lie*, $G/H\equiv\{aH\}$ clases laterales izquierdas y $\pi: G\to G/H$ la proyección natural. Entonces G/H tiene una única estructura de variedad diferenciable tal que π es una sumersión C^∞. □

Se recuerda que una acción de un grupo G en un conjunto M es una función de $M\times G$ a M que satisface que *i*) $xe=x$ para cada $x\in M$ y *ii*) $x(fg)=(xf)g$ para toda $x\in M$ y cada f, $g\in G$. Esta acción, induce una partición en el conjunto M y a las clases de equivalencia se les denomina **órbitas** de M bajo el grupo G, y se denotan como xG para $x\in M$.

TEOREMA D.4. Sea G un grupo de *Lie* que actúa en una variedad M y $x_0\in M$. Si $\pi: G\to G/Est(x_0)$ (con $Est(x_0)$ el estabilizador de x_0) y $\varphi: G\to x_0G$ es el mapeo orbita. Entonces existe una única φ tal que el siguiente diagrama conmuta y φ es una inmersión 1 a 1 y por consiguiente es una subinmersión. □



Como una consecuencia de este teorema, se tiene el

[†)] Los *k-jets* en $G(n)^k$ tienen término constante cero y por el teorema de la función inversa, sólo dependen de la parte lineal. Luego, se le puede considerar como una matriz invertible $n\times n$, esto es, como un elemento en el grupo $GL(n, \mathbb{R})$.

[‡)] Se sabe que todo espacio vectorial de dimensión finita es una variedad diferenciable y que todo abierto en una variedad diferenciable es una variedad diferenciable.

COROLARIO D.5. Con las hipótesis del teorema anterior; φ tiene el mismo rango constante en cada una de las componentes conexas. □

Se dice que dos gérmenes f y g en el anillo $\mathcal{E}(n)$ son ***k*-equivalentes** escrito $f \sim_k g$ si $\mathcal{J}^k(f)=\mathcal{J}^k(g)$. La relación $\sim_k$ es una relación de equivalencia. Se observa que

1) si $f \sim_k g$, entonces $f\text{-}g \in m(n)^{k+1}$ y

2) $f+c \sim_k g+c$ para todo germen constante c en $\mathcal{E}(n)$.

Dos gérmenes f y g en el anillo $\mathcal{E}(n)$ son **equivalentes por la derecha**, lo cual se escribe $f \sim_D g$ si existe un germen $H \in G(n)$ tal que $g=f\circ H$. La relación $\sim_D$ es una relación de equivalencia. Se observa que si $f \sim_D g$, entonces $f+c \sim_D g+c$ para todo germen constante c en $\mathcal{E}(n)$. La acción del grupo $G(n)$ sobre el anillo $\mathcal{E}(n)$, $\varphi:\mathcal{E}(n)\times G(n)\to\mathcal{E}(n)$ induce como ya se sabe una partición en $\mathcal{E}(n)$, donde las clases de equivalencia son las clases dadas por $\sim_D$. La clase de equivalencia de f es la **órbita** de f bajo el grupo $G(n)$ y se escribe $\mathcal{O}_f$, esto es, $\mathcal{O}_f=\{g\in\mathcal{E}(n) \mid f \sim_D g\}$. Entonces $f \sim_D g$ si y sólo si $\mathcal{O}_f=\mathcal{O}_g$.

DEFINICIÓN D.6. Un germen $f\in\mathcal{E}(n)$ es ***k*-determinado** si para cada $g\in\mathcal{E}(n)$, con $f\sim_k g$, se tiene que $f\sim_D g$.

De D.6, se sigue que si $f\in\mathcal{E}(n)$ es k-determinado, entonces f es l-determinado para toda $k\leq l$. Se observa que si $f\in\mathcal{E}(n)$ es k-determinado y $f \sim_k g$, entonces g es k-determinado. Lo mismo se cumple si $f \sim_D g$. En efecto, si $g \sim_k h$ y $f \sim_k g$, se sigue que $f \sim_k h$. Dado que f es k-determinado; $f \sim_D g$ y $f \sim_D h$, luego $g \sim_D h$ y g es k-determinado. Así, que $f \sim_D g$, significa que $g=f\circ H$ para algún $H\in G(n)$, luego $\mathcal{J}^k(g)=\mathcal{J}^k(f\circ H)$ y $g \sim_k f\circ H$. Si $g \sim_k h$, entonces $f\circ H \sim_k h$ y $\mathcal{J}^k(f\circ H)=\mathcal{J}^k(h)$, de esta forma

$$\mathcal{J}^k(f\circ H)\mathcal{J}^k(H^{-1})=\mathcal{J}^k(h)\mathcal{J}^k(H^{-1}),$$

esto es, $\mathcal{J}^k(f)=\mathcal{J}^k(h\circ H^{-1})$. Como f es k-determinado, se sigue que $f \sim_D h\circ H^{-1}$; de $h \sim_D h\circ H^{-1}$ se tiene $f \sim_D h$. Dado que $g \sim_D f$, se sigue que $g \sim_D h$; así, g es k-determinado. También, $f\in\mathcal{E}(n)$ es k-determinado, será equivalente a que $f+c$ es k-determinado para todo germen constante c. Sea $f\in\mathcal{E}(n)$ un germen y $\{x_1,\ldots,x_n\}$ un sistema de coordenadas en $\mathbb{R}^n$; considérese el ideal en $\mathcal{E}(n)$ generado por las parciales $\partial f/\partial x_j$, $j=1, 2,\ldots,n$. Este ideal, se denomina ideal **jacobiano** y es denotado como

$$\Delta(f)=<\frac{\partial f}{\partial x_1},\ldots,\frac{\partial f}{\partial x_n}>_{\mathcal{E}(n)}.$$

Sea $\Delta_x(f)=<\frac{\partial f}{\partial x_i}>_{\mathcal{E}(n)}$ y $\Delta_y(f)=<\frac{\partial f}{\partial y_j}>_{\mathcal{E}(n)}$, $i, j=1, 2,\ldots, n$ el ideal jacobiano de f con respecto a dos diferentes sistemas de coordenadas. Sea $H\in G(n)$ el germen del difeomorfismo $H:\mathbb{R}^n\to\mathbb{R}^n$ tal que $H(y_1,\ldots,y_n)=(x_1,\ldots,x_n)$, entonces $f\circ H$ es un germen en $\mathcal{E}(n)$ y por la regla de la cadena se tiene que

$$\frac{\partial f}{\partial y_j}=\sum_{i=1}^{n}\frac{\partial f}{\partial x_i}\frac{\partial x_i}{\partial y_j}.$$

Dado que $\partial f/\partial x_i\in\Delta_x(f)$ para toda $i=1,\ldots,n$ y como $\partial x_i/\partial y_j$ es un germen en $\mathcal{E}(n)$, entonces $\partial f/\partial y_j\in\Delta_x f$ para toda, $j=1, 2,\ldots,n$. De esta forma se tiene que $\Delta_y(f)\subseteq\Delta_x(f)$; la otra contención es análoga; así, se ha obtenido que el ideal jacobiano de un germen f, $\Delta(f)$ no depende del cambio de coordenadas. También, se observa que $\Delta(f)=\Delta(f+c)$ donde $c\in\mathcal{E}(n)$, es un germen constante.

Sea $\mathfrak{A}$ el conjunto de gérmenes en $(0, t_0)$ de funciones en $C^\infty(\mathbb{R}^n\times\mathbb{R}, \mathbb{R})$. Como en el caso del anillo $\mathcal{E}(n)$, $\mathfrak{A}$ es un anillo local y su ideal maximal $\mathfrak{a}$ consta de todos los gérmenes en $\mathfrak{A}$ que se anulan en $(0, t_0)$. Sea $\pi:\mathbb{R}^n\times\mathbb{R}\to\mathbb{R}^n$; $\pi(x, t)=x$ la proyección canónica; π induce un homomorfismo inyectivo $\pi^*:\mathcal{E}(n)\to\mathfrak{A}$; $f\mapsto f\circ H$. Así, cuando se trabaje con el ideal $m(n)^k$ en $\mathcal{E}(n)$, $\pi^*(m(n)^k)$ corresponderá a un ideal en $\mathfrak{A}$.

Considérese el germen H en $\{0\}\times\mathbb{R}$ de una función $H: \mathbb{R}^n\times\mathbb{R}\to\mathbb{R}$; definida como $H(x, t)=(1-t)f(x)+tg(x)$ con $f, g\in m(n)$ y $f\sim_k g$.

OBSERVACIÓN D.7. Si $m(n)^{k+1}\subseteq m(n)^2\Delta(f)$, entonces $\pi^*(m(n)^{k+1})\subseteq\pi^*(m(n)^2)\Delta(H)$ donde $\Delta(H)$ $(=<\frac{\partial H}{\partial x_1},\ldots,\frac{\partial H}{\partial x_n}>)$ es el ideal jacobiano de H generado por las parciales $\frac{\partial H}{\partial x_1},\ldots,\frac{\partial H(x,t)}{\partial x_n}$ sobre $\mathfrak{A}$.

DEMOSTRACIÓN

Considérese

$$\frac{\partial H(x,t)}{\partial x_i}=(1-t)\frac{\partial f(x)}{\partial x_i}+t\frac{\partial g(x)}{\partial x_i}$$
$$=\frac{\partial f(x)}{\partial x_i}+t\frac{\partial}{\partial x_i}\big(g(x)-f(x)\big)$$

Como $f\sim_k g$, se tiene que $g-f\in m(n)^{k+1}$ y $\frac{\partial}{\partial x_i}(g-f)\in m(n)^k$. Luego

$$\frac{\partial f(x)}{\partial x_i}=\frac{\partial H(x,t)}{\partial x_i}-t\frac{\partial}{\partial x_i}\big(g(x)-f(x)\big)\in<\frac{\partial H(x,t)}{\partial x_i}>+\pi^*(m(n)^k))\subseteq\Delta(H)+\pi^*(m(n)^k).$$

Así,

$$\frac{\partial f(x)}{\partial x_i} \in \Delta(\mathrm{H})+\pi^*(m(n)^k).$$

para cada i=1, 2,…, n, y

$$\pi^*(\Delta(f))\subseteq\Delta(\mathrm{H})+\pi^*(m(n)^k).$$

Como $\pi^*(m(n))\subseteq\mathfrak{a}$ y por hipótesis $m(n)^{k+1}\subseteq m(n)^2\Delta(f)$, se sigue que

$$\pi^*(m(n)^{k+1})\subseteq\pi^*(m(n)^2\Delta(f)).$$

Ahora, dado que

$$\pi^*(\Delta(f))\subseteq\Delta(\mathrm{H})+\pi^*(m(n)^k)$$

se tiene

$$\pi^*(m(n)^2\Delta(f))\subseteq\pi^*(m(n)^2)[\Delta(\mathrm{H})+\pi^*(m(n)^k)]=\pi^*(m(n)^2)(\Delta(\mathrm{H}))+\pi^*(m(n)^{k+2})=$$

$$=\pi^*(m(n)^2)\Delta(\mathrm{H})+\pi^*(m(n))\pi^*(m(n)^{k+1})\subseteq\pi^*(m(n)^2)\Delta(\mathrm{H})+\mathfrak{a}\pi^*(m(n)^{k+1}).$$

Así,

$$\pi^*(m(n)^{k+1})\subseteq\pi^*(m(n)^2)\Delta(\mathrm{H})+\mathfrak{a}\pi^*(m(n))\pi^*(m(n)^{k+1}).$$

Por el lema de Nakayama, con $\pi^*(m(n)^{k+1})$ finitamente generado, se obtiene

$$\pi^*(m(n)^{k+1})\subseteq\pi^*(m(n)^2)\Delta(\mathrm{H}).\ \square$$

La observación D.7., implica la siguiente

PROPOSICIÓN D.8. Para cada $t_0\in[0, 1]$, existe un germen F en $(0, t_0)$ de una función en $C^\infty(\mathbb{R}^n\times\mathbb{R}, \mathbb{R})$ que satisface

a) $\mathrm{F}(0, t_0)=0$

b) $\sum_{i=1}^{n}\frac{\partial \mathrm{H}(x,t)}{\partial x_i}\mathrm{F}_i(x,t)+\frac{\partial \mathrm{H}(x,t)}{\partial t}=0$.

para todo punto (x, t) en una vecindad de $(0, t_0)$.

DEMOSTRACIÓN

Sea $\mathrm{H}: \mathbb{R}^n\times\mathbb{R}\to\mathbb{R}$; una función definida como $\mathrm{H}(x, t)=(1-t)f(x)+tg(x)$; se afirma que $\frac{\partial \mathrm{H}(x,t)}{\partial t}\in\pi^*(m(n)^2)\subseteq\Delta(\mathrm{H})$. En efecto, dado que $\frac{\partial \mathrm{H}(x,t)}{\partial t}=\frac{\partial}{\partial t}[(1-t)f(x)+tg(x)]=g(x)-f(x)$ y como $f\sim_k g$, se sigue que $g-f\in m(n)^{k+1}$. Por D.7., se tiene que $f-g\in\pi^*(m(n)^2)\Delta(\mathrm{H})$, esto es, $\frac{\partial \mathrm{H}(x,t)}{\partial t}\in\pi^*(m(n)^2)\Delta(\mathrm{H})$. De esta forma, $\frac{\partial \mathrm{H}(x,t)}{\partial t}=\sum_{j=1}^{n}a_j(x)\,u_j(x, t)$ donde $a_j(x)\in\pi^*(m(n)^2)$ y $u_j(x, t)\in\Delta(\mathrm{H})$. Como $u_j(x, t)=\sum_{i=1}^{n}b_{ij}(x,t)\,\frac{\partial \mathrm{H}(x,t)}{\partial x_i}$, donde $b_{ij}(x, t)$ son gérmenes en $\mathfrak{A}$. Entonces $\frac{\partial \mathrm{H}(x,t)}{\partial t}=\sum_{i=1}^{n}\sum_{j=1}^{n}a_i(x)\,b_{ij}(x, t)\frac{\partial \mathrm{H}(x,t)}{\partial x_i}$; haciendo $\mathrm{F}_i(x, t)=-\sum a_j(x)b_{ij}(x, t)$; i=1,…, n.

F_i así definido, es un germen en el anillo $\mathfrak{A}$ ya que $b_{ij}\in\mathfrak{A}$ y $a_j\in\mathfrak{a}$. Luego, al sustituir F_i en la expresión anterior, se obtiene:

$$\frac{\partial H(x,t)}{\partial t}=\sum_{i=1}^{n}\sum_{j=1}^{n}a_j(x)\,b_{ij}(x,t)\,\frac{\partial H(x,t)}{\partial x_i}$$

$$=-\sum_{i=1}^{n}F_i(x,t)\,\frac{\partial H(x,t)}{\partial x_i}\qquad \text{y}$$

$$\frac{\partial H(x,t)}{\partial t}+\sum_{i=1}^{n}F_i(x,t)\,\frac{\partial H(x,t)}{\partial x_i}=0.$$

Esto último satisface el inciso *b*). Por otro lado, como F_i para $i=1,\ldots,n$ es un germen de $\mathfrak{A}$; si se hace $F=(F_1,\ldots, F_n)$ se obtiene un germen en $(0, t_0)$ de funciones en $C^\infty(\mathbb{R}^n\times\mathbb{R}, \mathbb{R}^n)$ con $F(0, t_0)=0$, ya que $F_i(x, t)=-\sum_{j=1}^{n}a_i(x)\,u_j(x, t)$ con $a_j(0)=0$; $j=1,\ldots,n$; así, $F_i(x,t)=-\sum_{j=1}^{n}a_j(0)u_j(0,t)=0$; $i=1,\ldots,n$. Por lo tanto $F_i(0, t)=0$ y aquí termina la demostración. □

La proposición D.8., implica la siguiente

PROPOSICIÓN D.9. Dado $t_0\in[0, 1]$, existe un germen G en $(0, t_0)$ de una función G en $C^\infty(\mathbb{R}^n\times\mathbb{R}, \mathbb{R}^n)$ tal que para cada punto (x, t) en una vecindad de $(0, t_0)$ se cumple

c) $G(x, t_0)=x$.
d) $G(0, t)=0$.
e) $H(G(x, t), t)=H(x, t_0)$.

DEMOSTRACIÓN

Como F es diferenciable, el teorema de existencia y unicidad de ecuaciones diferenciales ordinarias asegura la existencia de una solución $G(x, t)$ de la ecuación diferencial $\frac{\partial H(x,t)}{\partial t}=F(G(x, t), t)$ que pasa por x en el tiempo t_0, es decir, $G(x, t_0)=x$; esto corresponde al inciso *c*). Del inciso *a*) de la proposición D.8., se obtiene que $F(0, t)=0$ lo que implica que el sistema

$$\frac{\partial H(x,t)}{\partial t}=F_i(G(x, t), t)$$

tiene como solución a $G(0, t)=0$ para cada t en una vecindad de t_0. Esto último satisface *d*). Ahora, en el inciso *d*) de la proposición D.9., poner $G(x, t)$ en donde está escrita x (esto es, la función que manda x a $F(x, t)$ es un difeomorfismo), entonces se obtiene:

$$\sum_{i=1}^{n} \frac{\partial H(G(x,t),t)}{\partial x_i} F_i(G(x, t), t) + \frac{\partial H(G(x,t),t)}{\partial t} = 0,$$

esto es,

$$\sum_{i=1}^{n} \frac{\partial H(G(x,t),t)}{\partial x_i} \frac{\partial G_i(x,t)}{\partial t} + \frac{\partial H(G(x,t),t)}{\partial t} = 0.$$

Por la regla de la cadena, lo anterior es equivalente a

$$\frac{\partial}{\partial t}[H\circ(G(x, t), t)] = 0.$$

Esto significa que $H(G(x, t), t)$ es una función constante en una vecindad del punto $(0, t_0)$ en $\mathbb{R}^n\times\mathbb{R}$. Del inciso *c*), $G(x, t_0)=x$ para cada (x, t_0) en una vecindad del punto $(0, t_0)$; lo cual significa que $H\circ(G(x, t), t)$ toma el valor constante $H(G(x, t_0), t_0)=H(x, t_0)$ para todo (x, t) en una vecindad de $(0, t_0)$. Así, $H(G(x, t), t)=H(x, t_0)$ y el inciso *e*) se cumple. □

Finalmente, la proposición D.9., implica el siguiente

LEMA D.10. Sea $t_0\in[0, 1]$ un número real fijo, entonces existe una familia (G^t) de difeomorfismos G^t en $G(n)$ definidos para toda t en una vecindad de t_0 en $\mathbb{R}$ tal que

f) $G^{t_0}(x) = x$.

g) $H^t(x, t)\circ G^t(x) = H^{t_0}(x,t)$.

DEMOSTRACIÓN

Defínase $G^t:V(0)\subsetneq\mathbb{R}^n\to\mathbb{R}^n$; $G^t(x)=G(x, t)$; G^t es la restricción de G en $\mathbb{R}^n\times\{t\}$. G^t es un germen en cero cuyo representante satisface $G^t(0)=0$ ($G^t(0)$ coincide con $G(0, t)=0$). Por el inciso *c*) de la proposición D.9., se tiene que $G^{t_0}(x)=G(x, t_0)=x$, es decir, G^{t_0} es el germen de la identidad en $\mathbb{R}^n$. De esta forma, se cumple el inciso f) del lema D.9.. Por el inciso *e*) se tiene que $H(G(x, t), t)=H(x, t_0)$ para toda x en una vecindad del cero en $\mathbb{R}^n$, esto es, $H^t(x, t)\circ G^t(x)=H^t\circ(x, t)$ que corresponde al inciso g) del lema. □

A continuación se enuncia el primer teorema de Mather

TEOREMA D.11. Si $f\in m(n)$ y $m(n)^{k+1}\subseteq m(n)^2\Delta(f)$ donde $\Delta(f)$ es el ideal jacobiano de *f*, entonces *f* es *k*-determinado.

DEMOSTRACIÓN

Como antes, sea H el germen en $\{0\}\times\mathbb{R}$ de una función $H: \mathbb{R}^n\times\mathbb{R}\to\mathbb{R}$; definida como $H(x, t)=(1-t)f(x)+tg(x)$ para toda $x\in\mathbb{R}^n$ y $t\in\mathbb{R}$. Considérese la restricción $H^t=H|\,\mathbb{R}^n\times\{t\}:\mathbb{R}^n\times\{t\}\subseteq\mathbb{R}^n\times\mathbb{R}\to\mathbb{R}$; $H^t(x)=H(x, t)$; se sigue que $H^0(x)=f(x)$ y $H^1(x)=g(x)$, esto es, $H(x, 0)=f(x)$ y $H(x, 1)=g(x)$.

La idea de la demostración es ir modificando continuamente el germen *f* a través de la homotopia H en el germen *g*, suponiendo que $f\sim_k g$. Como [0, 1] es compacto, existe un

número finito de vecindades $V(t_0)$, $V(t_1)$,…,$V(t_m)$ donde $V(t_i)$ es una vecindad de centro el punto t_i; $i=1,,\ldots,m$ y $0=t_0<t_1<\cdots<t_m=1$. También se tiene que $V(t_i)\cap V(t_{i+1})\neq\varnothing$ para toda $i=1,\ldots,m$. Por el lema anterior se sigue que en cada vecindad $V(t_i)$ existe una familia (G_i^t) con $G_i^t \in G(n)$ tal que

1) $G_i^{t_i}(x)=x$
2) $H^t(x,t)\circ G_i^t(x)=H^{t_i}(x,t)$.

Si $t\in V(t_i)\cap V(t_{i+1})$, entonces se obtiene que

$$H^t(x,t)\circ G_i^t(x)=H^{t_i}(x,t) \text{ y } H^t(x,t)\circ G_{i+1}^t(x)=H^{t_i+1}(x,t).$$

Sea

$$H^t(x,t)\circ G_i^t(x)\circ G_i^t(x)^{-1}=H^{t_i}(x,t)\circ G_i^t(x)^{-1}$$

donde

$$G_i^t(x)^{-1}\in G(n),$$

luego

$$H^t(x,t)=H^{t_i}(x,t)\circ G_i^t(x)^{-1}.$$

De esta última igualdad y de $H^t(x,t)\circ G_{i+1}^t(x)= H^{t_i+1}(x,t)$ se obtiene

$$H^{t_i}(x,t)\circ G_i^t(x)^{-1}\circ Gi_{+1}^t(x)=H^{t_i+1}(x,t).$$

Así, se sigue que

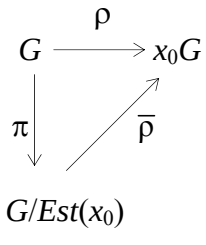
$$H^{t_i+1}(x,t)=H^{t_i}(x,t)\circ G_i(x) \text{ con } G_i(x)=G_i^t(x)^{-1}\circ G_{i+1}^t(x)\in G(n).$$

Por lo tanto $H^{t_i}\sim_D H^{t_i+1}$ para toda $i=1,\ldots,m$-1, esto es, $f\sim_D g$ y f es k-determinado. □

El siguiente resultado que es una consecuencia del teorema D.4., será útil en lo que sigue.

COROLARIO D.12. Sea G un grupo de *Lie*, x_0G la orbita del punto x_0, $\pi:G\to G/Est(x_0)$ una sumersión con $Est(x_0)$ el estabilizador de x_0 y $c:(-1,1)\to x_0G$ una curva con $c(0)=x_0$. Entonces existe una curva $C(-\varepsilon,\varepsilon)\to G$ con $C(0)=id$ tal que $c'(0)=d/dt(x_0C(t))\big|_{t=0}$.

DEMOSTRACIÓN



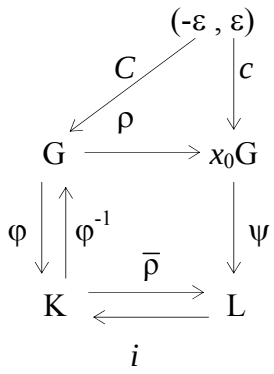
Por el teorema D.4., la orbita x_0G es la imagen de una inmersión inyectiva $(Est(x_0),\rho)$. Esto significa que el mapeo; órbita $\rho:G\to x_0G$ tiene rango constante; digamos r. Del teorema del rango, existen difeomorfismos φ de una vecindad abierta U de la identidad en G sobre el cubo unitario abierto K con $\varphi(id)=0$ y ψ de una vecindad abierta V de x_0g con $g\in G$ sobre el cubo unitario abierto L con $\psi(x_0g)=0$ tal que $\psi\circ\rho\circ\varphi^{-1}(x,y)=(x,0)$. Definiendo $C(t)=\varphi^{-1}\circ(i)\circ\psi(c(t))$, se tiene que

$\psi(\rho(C(t)))=(\psi\circ\rho\circ\varphi^{-1})\circ(i)\circ\psi(c(t))=\psi(c(t))$. lo cual implica que $\rho\circ C(t)=c(t)$, para cada elemento $t\in(-\varepsilon\ ,\ \varepsilon)$. Por lo tanto $c'(0)=(\rho\circ C)'(0)$. □

Considérese la función

$$\pi=\mathcal{J}^{k+1}\,|\,m(n):m(n)\to m(n)/m(n)^{k+2};\ f\mapsto \mathcal{J}^{k+1}(f)$$

con f k-determinado, donde $\mathcal{J}^{k+1}:\mathcal{E}(n)\to\mathcal{E}(n)/m(n)^{k+2}$ es el homomorfismo canónico.



Sea

$$P=\{g\in m(n)\mid f\sim_k g\}\ \text{y}\ Q=\{g\in m(n)\mid f\sim_D g\}.$$

Q es la órbita de f bajo el grupo $G(n)$. Se observa que $\mathcal{J}^{k+1}(P)\subseteq\mathcal{J}^{k+1}(Q)$; $P\subseteq Q$ y también se tiene que $P=f+m(n)^{k+1}$. Si $z=\mathcal{J}^{k+1}(f)$, entonces se sigue que $\mathcal{J}^{k+1}(P)=\mathcal{J}^{k+1}(f+m(n)^{k+1})=\mathcal{J}^{k+1}(f)+\mathcal{J}^{k+1}(m(n)^{k+1})$ y $\mathcal{J}^{k+1}(P)=z+\mathcal{J}^{k+1}(m(n)^{k+1})$. Como $\mathcal{J}^{k+1}(m(n)^{k+1})$ es un $\mathbb{R}$-espacio vectorial de dimensión finita, $\mathcal{J}^{k+1}(P)$ es un espacio afín de $\mathcal{J}^{k+1}(m(n)^{k+1})$. De esta forma, el espacio tangente de $\mathcal{J}^{k+1}(P)$ en z es lo mismo que el espacio tangente de $\mathcal{J}^{k+1}(m(n)^{k+1})$ en z, esto es,

$$T_z\mathcal{J}^{k+1}(P))=\mathcal{J}^{k+1}(m(n)^{k+1}).$$

Por otro lado, como $G(n)^k$ es un grupo de *Lie* de dimensión finita, por el teorema D.3., la órbita de z bajo el grupo $G(n)^{k+1}$; $\mathcal{O}_z$ es una variedad de dimensión finita. Dado que $\mathcal{J}^{k+1}(Q)=\mathcal{O}_z$, esto significa que $T_z(\mathcal{J}^{k+1}(Q))$ existe. Como $\mathcal{J}^{k+1}(P)\subseteq\mathcal{J}^{k+1}(Q)$, entonces $T_z(\mathcal{J}^{k+1}(P))\subseteq T_z(\mathcal{J}^{k+1}(Q))$, donde $T_z(\mathcal{J}^{k+1}(P))=\mathcal{J}^{k+1}(m(n)^{k+1})$ y $T_z(\mathcal{J}^{k+1}(Q))$ satisface el

LEMA D.13. $T_z(\mathcal{J}^{k+1}(Q))=\mathcal{J}^{k+1}(m(n))\Delta(f)$.

DEMOSTRACIÓN

Sea $G=id+F$ un germen en $G(n)$ tal $F(0)=0$. Sea $H:\mathbb{R}^n\times\mathbb{R}\to\mathbb{R}^n$; $H(x,t)=x+tF(x)$ y considérese la restricción H^t: $\mathbb{R}^n\times[0,\ 1]\subsetneq\mathbb{R}^n\times\mathbb{R}\to\mathbb{R}^n$; $H^t(x)=H(x,\ t)$. Se tiene que $H^0(x)=H(x,0)=0$, $H^1(x)=H(x,\ 1)=G$ y $H^0,\ H^1\in G(n)$. Escogiendo una vecindad U de la identidad H^0 con $U\subseteq G(n)$ y un $t_0>0$ que dependa de U tal que para cada $t\in\mathbb{R}$ con $0\le t\le t_0$ se tenga que $H^t\in G(n)$ con $0<t<t_0$, esto es, H^t es un germen en el grupo $G(n)$; luego, $\{H^t\}$ es una curva contenida en $G(n)$ que empieza en H^0. Por otro lado, si $0<t<t_0$ y si también $H^t\in G(n)$, se tiene que, $f\sim_D f\circ H^t$. Luego $f\circ H^t\in Q$ y $f\circ H^0=f$. De esta forma $\{f\circ H^t\}$ es una curva en Q que empieza en f en $t=0$. De lo anterior se sigue que $\{\mathcal{J}^{k+1}(f\circ H^t)\}$ es una curva en $\mathcal{J}^{k+1}(Q)$ que empieza en $z=\mathcal{J}^{k+1}(f)$ en $t=0$. La tangente a la curva $\{\mathcal{J}^{k+1}(f\circ H^t)\}$ en el punto $t=0$ viene dada por el vector $\partial/\partial t(\mathcal{J}^{k+1}(f\circ H^t))|_{t=0}$; se afirma que $\partial/\partial t(\mathcal{J}^{k+1}(f\circ H^t))|_{t=0}\in\mathcal{J}^{k+1}(m(n)\Delta(f))$. En efecto, sea

$$\frac{\partial}{\partial t}(\mathcal{J}^{k+1}(f\circ \mathrm{H}^{\mathrm{t}}))|_{t=0}=\frac{\partial}{\partial t}\sum_{|\mathrm{I}|=1}^{k+1}\left.\frac{\partial^{|\mathrm{I}|} f\circ \mathrm{H}^{\mathrm{t}}}{\partial x^{\mathrm{I}}}\right|_{t=0}\left(\frac{x^{\mathrm{I}}}{\mathrm{I}!}\right)$$

$$=\sum_{|\mathrm{I}|=1}^{k+1}\frac{\partial}{\partial t}\left.\frac{\partial^{|\mathrm{I}|} f\circ \mathrm{H}^{\mathrm{t}}}{\partial x^{\mathrm{I}}}\right|_{t=0}\left(\frac{x^{\mathrm{I}}}{\mathrm{I}!}\right)$$

$$=\frac{\partial}{\partial t}\sum_{|\mathrm{I}|=1}^{k+1}\left.\frac{\partial^{|\mathrm{I}|}}{\partial x^{\mathrm{I}}}\frac{\partial f\circ \mathrm{H}^{\mathrm{t}}}{\partial t}\right|_{t=0}\left(\frac{x^{\mathrm{I}}}{\mathrm{I}!}\right)$$

$$=\mathcal{J}^{k+1}\left.\left(\frac{\partial^{|\mathrm{I}|} f\circ \mathrm{H}^{\mathrm{t}}}{\partial x^{\mathrm{I}}}\right)\right|_{t=0}$$

Como $\mathrm{H}^{\mathrm{t}}(x)=x+\mathrm{F}(x)$, donde $\mathrm{F}(x)=(\mathrm{F}_1(x),\ldots,\mathrm{F}_n(x))$ es un germen en $\mathcal{E}(n, n)$ que se anula en cero, se tiene que

$$\frac{\partial}{\partial t}(f\circ \mathrm{H}^{t})|_{t=0}=\frac{\partial}{\partial t}[f\circ(id+\mathrm{F})]|_{t=0}.$$

$$=\sum_{i=1}^{n}\frac{\partial f}{\partial x_i}\ (id+\mathrm{F})\mathrm{F}_i\,|_{t=0}.$$

$$=\sum_{i=1}^{n}\frac{\partial f}{\partial x_i}(\mathrm{F}_i).$$

Así,

$$\frac{\partial}{\partial t}(\mathcal{J}^{k+1}(f\circ \mathrm{H}^{t}))|_{t=0}=\mathcal{J}^{k+1}(\sum_{i=1}^{n}\frac{\partial f}{\partial x_i}(\mathrm{F}_i))\in\mathcal{J}^{k+1}(m(n)\Delta(f)),$$

esto es, $\frac{\partial}{\partial t}(\mathcal{J}^{k+1}(f\circ \mathrm{H}^{t}))|_{t=0}\in\mathcal{J}^{k+1}(m(n)\Delta(f))$ y $\mathrm{T}_z(\mathcal{J}^{k+1}(\mathrm{Q}))=\mathcal{J}^{k+1}(m(n)\Delta(f))$. Recíprocamente, si $g\in m(n)\Delta(f)$, entonces $g=\sum_{i=1}^{n}\frac{\partial f}{\partial x_i}\mathrm{F}_i$, donde $\mathrm{F}_i\in m(n)\Delta(f)$. Si $\mathrm{F}(x)=(\mathrm{F}_1(x),\ldots,\mathrm{F}_n(x))$, entonces F es un germen en $\mathcal{E}(n, n)$ que se anula en cero (ya que $\mathrm{F}_i\in m(n)$). Además, F determina una curva en $G(n)$ definida como antes $\mathrm{H}^{t}(x)=x+\mathrm{F}(x)$. Por lo tanto,

$$\mathcal{J}^{k+1}(m(n)\Delta(f))=\mathrm{T}_z(\mathcal{J}^{k+1}(\mathrm{Q})).\ \square$$

A continuación se enuncia y demuestra el segundo teorema de Mather.

TEOREMA D.14. Si $f\in m(n)$ es k-determinado, entonces $m(n)^{k+1}\subseteq m(n)\Delta(f)$.

DEMOSTRACIÓN.

Dado que $\mathrm{T}_z(\mathcal{J}^{k+1}(\mathrm{P}))\subseteq\mathrm{T}_z(\mathcal{J}^{k+1}(\mathrm{Q}))$ y como $\mathrm{T}_z(\mathcal{J}^{k+1}(\mathrm{P}))=\mathcal{J}^{k+1}(m(n)^{k+1})$ se sigue $\mathcal{J}^{k+1}(m(n)^{k+1})\subseteq\mathrm{T}_z(\mathcal{J}^{k+1}(\mathrm{Q}))$. Por el lema D.13., se tiene que $\mathcal{J}^{k+1}(m(n)^{k+1})\subseteq\mathcal{J}^{k+1}(m(n)\Delta(f))$. Lo anterior implica que $m(n)^{k+1}+ker(\mathcal{J}^{k+1})\subseteq m(n)\Delta(f)+ker(\mathcal{J}^{k+1})=m(n)\Delta(f)+m(n)^{k+2}$ y como

$m(n)^{k+1}\subseteq m(n)^{k+1}+ker(\mathcal{J}^{k+1})$ se concluye que $m(n)^{k+1}\subseteq m(n)\Delta(f)+m(n)^{k+2}$. Por el lema de Nakayama con $m(n)^{k+1}$ finitamente generado, se tiene que $m(n)^{k+1}\subseteq m(n)\Delta(f)$. □

DEFINICIÓN D.15. Un germen $f\in\mathcal{E}(n)$ es **finitamente determinado** si es k-determinado para algún $k\in\mathbb{N}$.

La **determinación** de un germen $f\in\mathcal{E}(n)$ es el mínimo de los $k\in\mathbb{N}$ para el cual f es k-determinado y se escribe como ***deter*(*f*)**=k.

COROLARIO D.16. Un germen $f\in\mathcal{E}(n)$ es finitamente determinado si y sólo si $m(n)^{k+1}\subseteq\Delta(f)$ para algún $k\in\mathbb{N}$.

DEMOSTRACIÓN ($\Rightarrow$)

Por hipótesis f es k-determinado para algún $k\in\mathbb{N}$. Por el teorema D.14., $m(n)^{k+1}\subseteq m(n)\Delta(f)$, luego $m(n)^{k+1}\subseteq m(n)\Delta(f)\subseteq\Delta(f)$. Así, $m(n)^{k+1}\subseteq\Delta(f)$.

($\Leftarrow$)

Si $m(n)^{k+1}\subseteq\Delta(f)$ para alguna $k\in\mathbb{N}$, entonces $m(n)^{k+2}\subseteq m(n)^2\Delta(f)$. Por el teorema D.11., se sigue que f es $(k+1)$-determinado y por tanto finitamente determinado. □

COROLARIO D.17. $f\in m(n)\backslash m(n)^2$, si y sólo si f es 1-determinado.

DEMOSTRACIÓN ($\Rightarrow$)

Si $f\in m(n)\backslash m(n)^2$, esto significa que $f\notin m(n)^2$, es decir, existe un índice $i_0\in\{1,\ldots,n\}$ tal que la derivada $\frac{\partial f(0)}{\partial x_{i_0}}\neq 0$, luego $\frac{\partial f}{\partial x_{i_0}}\notin m(n)$; entonces $\frac{\partial f}{\partial x_{i_0}}\in\mathcal{E}(n)\backslash m(n)$. Dado que $\frac{\partial f}{\partial x_{i_0}}$ es una unidad en $\mathcal{E}(n)$, se sigue que $\Delta(f)=\mathcal{E}(n)$. Así, $m(n)^2\Delta(f)=m(n)^2$; en particular $m(n)^2\subseteq m(n)^2\Delta(f)$. Por D.11., se sigue que f es 1-determinado.

($\Leftarrow$)

Si f es 1-determinado, entonces $T_f^1\neq 0$ lo cual significa que al menos una derivada parcial $\partial f(0)/\partial x\neq 0$, luego $f\in m(n)\backslash m(n)^2$. □

A continuación se pasa a enunciar y probar el último resultado importante; el teorema de Stefan que da una condición necesaria y suficiente para la k-determinación. Al final de la sección se ven dos ejemplos que muestran que los recíprocos de los teoremas D.11. y D.14., no se verifican en general.

TEOREMA D.18. (*de Stefan*) $f\in\mathcal{E}(n)$ es k-determinado si y sólo si $m(n)^{k+1}\subseteq m(n)\Delta(f+h)$ para todo germen $h\in m(n)^{k+1}$.

DEMOSTRACIÓN ($\Rightarrow$)

Sea $h\in m(n)^{k+1}$, luego $\mathcal{J}^k(h)=0$ y $\mathcal{J}^k(f+h)=\mathcal{J}^k(f)+\mathcal{J}^k(h)$, esto es, $\mathcal{J}^k(f+h)=\mathcal{J}^k(f)$, es decir, $f+h\sim_k f$. Como f es k-determinado se sigue que $f+h$ es k-determinado. Por el teorema D.14., se concluye que $m(n)^{k+1}\subseteq m(n)\Delta(f+h)$ para todo germen $h\in m(n)^{k+1}$.

($\Leftarrow$)

Sea g un germen en el anillo $\mathcal{E}(n)$, con $g-f\in m(n)^{k+1}$, esto es, $g=f+h$ para algún germen $h\in m(n)^{k+1}$. Defínase el germen H en $\{0\}\times\mathbb{R}$ de una función en $C^\infty(\mathbb{R}^n\times\mathbb{R}, \mathbb{R})$ como H: $\mathbb{R}^n\times\mathbb{R}\to\mathbb{R}$; con regla de correspondencia $H(x, t)=(1-t)f+tg(x)$. H es un germen del anillo local $\mathfrak{A}$ que satisface $\frac{\partial H}{\partial t}=g-f$, es decir, $\frac{\partial H}{\partial t}\in m(n)^{k+1}$. Sea

$$H^t=H|\,\mathbb{R}^n\times\{t\}:\mathbb{R}^n\times\{t\}\subseteq\mathbb{R}^n\times\mathbb{R}\to\mathbb{R};\ H^t(x)=H(x, t).$$

H^t es un germen en $\mathcal{E}(n)$ que satisface

$$\begin{aligned}\mathcal{J}^k(H^t)&=\mathcal{J}^k[(1-t)f+tg]\\&=(1-t)\mathcal{J}^k(f)+t\mathcal{J}^k(g)\\&=\mathcal{J}^k(f)+t[\mathcal{J}^k(g)-\mathcal{J}^k(f)]\end{aligned}$$

Como $f\sim_k g$ y t es un germen constante en $\mathfrak{A}$, se sigue que $\mathcal{J}^k(H^t)=\mathcal{J}^k(f)$; esto es, $H^t\sim_k g$ y como f es k-determinado, por el teorema D.14., se sigue $m(n)^{k+1}\subseteq m(n)\Delta(H^t)$, luego $m(n)^{k+1}\subseteq m(n)\Delta(H^t)+m(n)^{k+2}$. Sea $\frac{\partial H^{t_0}(x)}{\partial x_i}=\frac{\partial H(x,t_0)}{\partial x_i}$ con t_0 un número real fijo y considérese

$$\begin{aligned}\frac{\partial H(x,t_0)}{\partial x_i}-\frac{\partial H(x,t)}{\partial x_i}&=[(1-t_0)\frac{\partial f(x)}{\partial x_i}+t_0\,g(x)]-[(1-t)\frac{\partial f(x)}{\partial x_i}+t\,g(x)].\\&=(t_0-t)\frac{\partial}{\partial x_i}(g(x)-f(x))\\&=(t_0-t)\frac{\partial}{\partial x_i}\frac{\partial H(x,t_0)}{\partial t}.\end{aligned}$$

Así, $\frac{\partial H^{t_0}(x)}{\partial x_i}=\frac{\partial H(x,t)}{\partial x_i}+(t_0-t)\frac{\partial}{\partial x_i}(g(x)-f(x))$. Dado que (t_0-t) puede considerarse como un germen en $\mathfrak{A}$ que se anula en t_0 y $\frac{\partial}{\partial x_i}(g(x)-f(x))\in m(n)^k$ un germen en $\mathfrak{A}$ y un elemento en $m(n+1)^k$, se tiene que $\frac{\partial H^{t_0}(x)}{\partial x_i}\in<\frac{\partial H}{\partial x_i}>+m(n)m(n)^k$. Así, de esta forma se cumple que $\frac{\partial H^{t_0}(x)}{\partial x_i}\in\Delta(H)+m(n)^{k+1}$ y $\Delta(H^{t_0})\subseteq\Delta(H)+m(n+1)^{k+1}$. Sustituyendo esta última expresión en $m(n)^{k+1}\subseteq m(n)\Delta(H^t)+m(n)^{k+2}$ y considerando a cada uno de los ideales en $\mathfrak{A}$, se obtiene

$$\mathfrak{A}m(n)^{k+1}\subseteq\mathfrak{A}m(n)\Delta(\mathrm{H}^{t_0})+\mathfrak{A}m(n)^{k+2}\subseteq\mathfrak{A}m(n)[\Delta(\mathrm{H})+\mathfrak{A}m(n+1)^{k+1}]+\mathfrak{A}m(n)^{k+2}$$

$$\subseteq\mathfrak{A}m(n)\Delta(\mathrm{H})+m(n)^{k+2},$$

esto es,

$$\mathfrak{A}m(n)^{k+1}\subseteq\mathfrak{A}m(n)\Delta(\mathrm{H})+\mathfrak{A}m(n)^{k+2}.$$

Por el lema de Nakayama con $\mathfrak{A}m(n)^{k+1}$ el módulo finitamente generado se obtiene $\mathfrak{A}m(n)^{k+1}\subseteq\mathfrak{A}m(n)\Delta(\mathrm{H})$. Como $\dfrac{\partial \mathrm{H}}{\partial t}\in\mathfrak{A}m(n)^{k}$, entonces $\dfrac{\partial \mathrm{H}}{\partial t}\in\mathfrak{A}m(n)\Delta(\mathrm{H})$, esto es,

$$\frac{\partial \mathrm{H}(x,t)}{\partial t}=\sum_{i=1}^{n}\mathrm{F}_i(x,t)\,\frac{\partial \mathrm{H}(x,t)}{\partial x_i}$$

y $\mathrm{F}_i\in\mathfrak{A}m(n)\subseteq\mathfrak{a}$ donde, como se recordará, $\mathfrak{a}$ es el ideal maximal de $\mathfrak{A}$ que consta de todos los gérmenes en $\mathfrak{A}$ que se anulan en $(0, t_0)$. Así, $\mathrm{F}=(\mathrm{F}_1,\ldots,\mathrm{F}_n)$ es un germen en $(0, t_0)$ de funciones en $C^{\infty}(\mathbb{R}^n\times\mathbb{R}, \mathbb{R}^n)$ tal que $\mathrm{F}(0, t_0)=0$ y para cada punto (x, t) en una vecindad de $(0, t_0)$ se cumple que

$$\sum-\mathrm{F}_i(x, t)\frac{\partial \mathrm{H}(x,t)}{\partial x_i}\,\partial \mathrm{H}(x, t)/\partial x_i+\frac{\partial \mathrm{H}(x,t)}{\partial x_i}\,\partial \mathrm{H}(x, t)/\partial t=0.$$

y esto último implica la proposición D.9., que a su vez implica el lema D.10.; y esto a su vez implica el teorema D.11., que garantiza que f es k-determinado. □

OBSERVACIÓN D.19. El recíproco del teorema D.14., no es valido en general.

En efecto, considérese el germen f en $\mathcal{E}(1)$ dado por $f(x)=x^{k+1}$, con k un número natural. Aquí, $m(1)=\langle x\rangle$ y $\Delta(f)=\langle x^k\rangle=m(1)^k$. Así, se tiene que

$$m(1)^{k+1}\subseteq m(1)\Delta(f)\text{ y }m(1)^{k+2}\subseteq m(1)^2\Delta(f).$$

por el teorema D.11., se sigue que f es $(k+1)$-determinado. □

OBSERVACIÓN D.20. El recíproco del teorema D.11., no es valido en general.

En efecto, considérese el germen f en $\mathcal{E}(2)$; $f(x, y)=(x^3/3)+xy^3$; aquí, $m(2)=\langle x, y\rangle$ y $\Delta(f)=\langle x^2+y^3, xy^2\rangle$. Se afirma que $m(2)^6\subseteq m(2)^2\Delta(f)$ pero $m(2)^5\not\subseteq m(2)^2\Delta(f)$.

Se tiene que:

$$m(2)^2=\langle x^2, xy, y^2\rangle,$$
$$m(2)^2\Delta(f)=\langle x^2, xy, y^2\rangle\langle x^2+y^3, xy^2\rangle=\langle x^4+x^2y^3, x^3y^2, x^3y+xy^4, x^2y^3, x^2y^2+y^5, xy^4\rangle,$$
$$m(2)^5=\langle x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5\rangle,$$
$$m(2)^6=\langle x^6, x^5y, x^4y^2, x^3y^3, x^2y^4, xy^5, y^6\rangle.$$

Se probará que

$$m(2)^6 \subseteq m(2)^2\Delta(f)$$

o equivalentemente (por Nakayama) que

$$m(2)^6 \subseteq m(2)^2\Delta(f)+m(2)^7.$$

$x^6 \in m(2)^2\Delta(f)$ ya que al multiplicar x^2 por $x^4+x^2y^3$ se obtiene $x^6+x^4y^3 \in m(2)^2\Delta(f)+m(2)^7$. $x^5y \in m(2)^2\Delta(f)$ ya que al multiplicar xy por $x^4+x^2y^3$ se obtiene $x^5y+x^3y^4$ que es un elemento de $m(2)^2\Delta(f)+m(2)^7$. x^4y^2, x^3y^3, x^2y^4, xy^5 y y^6 se obtienen multiplicando y^2 por $x^4+x^2y^3$, y por x^3y^2, y por x^3y+xy^4, y por x^2y^3, y por $x^2y^2+y^5$, y por xy^4. Así, $m(2)^6 \subseteq m(2)^2\Delta(f)$. En forma similar se puede ver que x^5, x^4y, x^3y^2, x^2y^3 y xy^4 están en $m(2)^2\Delta(f)$ pero y^5 no está en $m(2)^2\Delta(f)$. En efecto, considérese la combinación

$$y^5=\alpha_1(x, y)(x^4+x^2y^3)+\alpha_2(x, y)(x^3y^2)+\alpha_3(x, y)(x^3y+xy^4)+\alpha_4(x, y)(x^2y^3)+$$
$$+\alpha_5(x, y)(x^2y^2+x^5)+\alpha_6(x, y)(xy^4).$$

Evaluando en $(0, y)$ se obtiene que $y^5=\alpha_5(0, y)\, y^5$, luego $\alpha_5(0, y)=1$. Por el teorema fundamental del cálculo, se sigue que $\alpha_5(x, y)-\alpha_5(0, y)=x\,\overline{\alpha}_5$ y $\alpha_5(x, y)=\alpha_5(0, y)+x\,\overline{\alpha}_5$, esto es, $\alpha_5(x, y)=1+x\,\overline{\alpha}_5$; así, se tiene que $m(2)^6 \subseteq m(2)^2\Delta(f)$ y $m(2)^5 \not\subseteq m(2)^2\Delta(f)$. Por el teorema D.11., se obtiene que f es 5-determinado pero no se puede saber utilizando este teorema si f es 4-determinado. Se afirma que f es 4-determinado. En efecto, por el teorema D.18., de Stefan, se tendrá que verificar que $m(2)^5 \subseteq m(2)\Delta(f+h)$ para cualquier germen $h \in m(2)^5$ o equivalentemente que $m(2)^5 \subseteq m(2)\Delta(f+h)+m(2)^6$ para cada $h \in m(2)^5$. Como

$$m(2)\Delta(f+h)=\left\langle x\frac{\partial f}{\partial x}+x\frac{\partial h}{\partial x}, y\frac{\partial f}{\partial x}+y\frac{\partial h}{\partial x}, x\frac{\partial f}{\partial y}+x\frac{\partial h}{\partial y}, y\frac{\partial f}{\partial y}+y\frac{\partial f}{\partial y}\right\rangle.$$
$$=\left\langle x^3+xy^3+x\frac{\partial h}{\partial x}, x^2y+y^4+y\frac{\partial h}{\partial x}, x^2y^2+x\frac{\partial h}{\partial y}, xy^3+y\frac{\partial h}{\partial y}\right\rangle.$$

En forma similar, como ya se hizo antes, si se multiplica x^2 por $x^3+xy^3+x\dfrac{\partial h}{\partial x}$, se obtiene $x^5+x^3y^3+x^3\dfrac{\partial h}{\partial x}$ que está en $m(2)\Delta(f+h)+m(2)^6$ ya que x^3y^3 y $x^3\partial h/\partial x$ están en $m(2)^6$ ($h \in m(2)^5$ y $\dfrac{\partial h}{\partial x}$, $\dfrac{\partial h}{\partial y}$ están en $m(2)^4$); así, $x^5 \in m(2)\Delta(f+h)$. En forma similar se obtiene que x^4y, x^3y^2, x^2y^3, xy^4 están en $m(2)\Delta(f+h)$. Finalmente, y^5 también está en $m(2)\Delta(f+h)$ ya que multiplicando y por $x^2y+y^4+y\dfrac{\partial h}{\partial x}$ se obtiene que $y^5+x^2y^2+y^2\dfrac{\partial h}{\partial x}$. Así, $m(2)^5 \subseteq m(2)\Delta(f+h)$ y por el teorema de Stefan, se sigue que el germen $f(x, y)=(x^3/3)+xy^3$ es 4-determinado y el recíproco del teorema D.11., es falso en general. □

REFERENCIAS.

1. Atiyah, M. D., Macdonald, I. G.: Introducción al Álgebra Conmutativa. Editorial Reverté, 1989.

2. Becker, E.: Extended Artin-Schreier Theory of Fields. Rocky Mountain Journal of Mathematics Vol 14, Number 4 1984.

3. Bierstone, E.: An Introducton to Singularities Smooth Functions. Notas de Curso.

4. Bochnak, K. J., Coste, M. y Roy, M-F.: Géométrie Algébrique Réelle. Springer-Verlag, 1987.

5. Cassels, J. W. S., Ellison, W. J. y Pfister, A.: On Sums of Squares and Elliptic Curves over Function Fields. Journal of Number Theory 3, 125-149, 1971.

6. Huneke, C.: Uniform Bounds in Noetherian Ring. Invent Math, 107, 203-223, 1992.

7. Kunz, E.: Introduction to Commutative Algebra and Algebraic Geometry. Birkhauser, 1985.

8. Kushner, L.: Finite Determination on Algebraic Sets. Transactions of the American Mathematical Society Vol 331, Number 2, 1992.

9. Kushner, L. y Terra L. B.: Finite Relative Determination and Relative Stability. Pacific Journal of Mathematics Vol 192, Number 2, 2000.

10. Lam, T. Y.: An Introduction to Algebra Real. Rocky Mountain Journal of Mathematics. Vol 14, Num 4, 1984.

11. Lam, T. Y.: The Algebraic Theory. of Quadratics Form. Benjamin, Inc. 1973.

12. Lang, S.: Algebra. Addison-Wesley publishing company. 2^a Edition 1984.

13. Lang, S.: The Theory of Real Places. Annals of Mathematics Vol 57, Number 2 1953.

14. Malgrange, B:. Ideals of Differentiable Functions. Oxford University Press, 1966.

15. Prestel, A.: Lectures on Formally Real Fields. IMPA. Lecture Notes, No 22, Rio de Janeiro, 1975.

16. Prestel, A y Delzell, C.: Positive Polynomials. From Hilbert's 17ht Problems to Real Algebra. Springer Monographs in Mathematics, 2001.

17. Spivak, M.: A Comprehensive Introduction to Differential Geometry. Vol 1 Second Edition Publish or Perish, Inc.

18. Tougeron, J. C.: Idéaux de Fonctions Différentiables, Springer-Verlag, 1972.

19. Warner, F. W:. Foundations of Differentiable Manifolds and Lie Groups. Springer-Verlag 1983.

20. Zeeman, E. C.: Catastrophe Theory: Selected Papers 1972-1977. pags 501-561