Introducción a la geometría algebraica

Maximiliano Riddick, Paula Vizzarri

23 de diciembre de 2008

Índice

1. Introducción **3**

2. Preliminares **4**

3. Variedades **12**
3.1. Problemas propuestos 17

4. El teorema central de Hilbert **21**
4.1. Problemas propuestos 25

5. Teorema de los ceros de Hilbert **27**
5.1. Problemas propuestos 33

6. El teorema de los ceros: Versiones equivalentes **37**
6.1. Problemas propuestos 41

7. Localización **46**
7.1. Problemas propuestos 54

8. Descomposición primaria **56**
8.1. Problemas propuestos 60

1. Introducción

Con la idea de que el presente trabajo pueda ser utilizado como material de consulta en un futuro, nos hemos esforzado especialmente en detallar al máximo cada idea...

Mediante esta breve introducción, buscaremos adelantarle al lector lo que encontrará a lo largo del trabajo.

Cada sección constará de una pequeña intro, se desarrollarán luego los temas principales y se concluirá con una serie de problemas resueltos, que buscarán clarificar conceptos y en ocaciones, brindar una idea geométrica de los temas tratados.

Comenzaremos recordando definiciones y propiedades básicas que nos serán de utilidad a lo largo del presente.

Definiremos luego lo que es una variedad y daremos un sencillo enfoque topológico, al hablar de la ¨Topología de Zarisky¨, pues como veremos en dicha topología las variedades y los conjuntos cerrados coinciden.

Definiremos también lo que llamaremos ¨ideal de un conjunto¨y a partir de esto, ideal de una variedad entre otros. Daremos además algunas propiedades de utilidad que cumplen estas estructuras.

Pasaremos luego a demostrar un importante resultado conocido como ¨Teorema Central de Hilbert¨, y daremos una breve reseña acerca del anillo de Series Formales de Potencias.

Introduciremos la noción de ideal radical, y estableceremos relaciones entre variedades e ideales, al remitirnos al Teorema de los ceros de Hilbert, en sus diversas versiones.

Dedicaremos las últimas dos secciones a desarrollar los dos siguientes temas: Localización y descomposición Primaria; pues como veremos, todo ideal en un anillo Noetheriano puede expresarse como intersección finita de ideales primarios.

2. Preliminares

Definición. Sea R un conjunto dotado de dos operaciones binarias,¨+¨ y ¨∗¨, a las que llamaremos ¨suma¨y ¨producto¨ respectivamente.
Diremos que $(R, +, *)$, es un *Anillo* sii:

1. $(R, +)$ es grupo abeliano, esto es:
   - $(a + b) + c = a + (b + c)\ \forall a, b, c \in R$ *(Asociatividad)*;
   - $\exists\ 0 \in R$ tal que $\forall a \in R, a + 0 = 0 + a = a$ *(Existencia de neutro)*;
   - $\forall a \in R, \exists(-a) \in R : a + (-a) = (-a) + a = 0$ *(Existencia de opuesto)*;
   - $a + b = b + a \forall a, b \in R$ *(Conmutatividad)*
2. $(a * b) * c = a * (b * c), \forall a, b, c \in R$ *(Asociatividad de ∗)*;
3. $a * (b + c) = a * b + a * c$ y
   $(b+c)*a = b*a+c*a, \forall a, b, c \in R$ *(Distributividad de ∗ respecto de +, a derecha e izquierda)*

Observación 2.1. .

- Es usual escribir ab en vez de $a * b$;
- Es frecuente nombrar al anillo, por R en vez de $(R, +, *)$;
- Si existe 1 en R tal que $a * 1 = 1 * a = a, \forall a \neq 0 \in R$, entonces R se dice anillo con unidad;
- Si $*$ es una operación conmutativa, entonces R se dirá anillo conmutativo

Definición. Si a, b son elementos distintos de 0 en R, cumpliendo que ab=0, diremos que a y b son *Divisores de cero del anillo R*

Definición. .

1. Un anillo R, se dirá un *Dominio Íntegro* si es un anillo conmutativo con unidad, cumpliendo que si $ab = 0 \Rightarrow a = 0 \vee b = 0$ (i.e, sin divisores de cero).
2. Un anillo conmutativo con unidad R se dirá un *Anillo de División*, si todo elemento distinto de 0, tiene inverso multiplicativo.
   i.e Si $\forall a \neq 0 \in R, \exists a^{-1} \in R$ tal que, $aa^{-1} = a^{-1}a = 1$
3. Un *Cuerpo* es un anillo conmutativo de división.

Proposición 2.2. Un Dominio Íntegro finito, es un cuerpo

Definición. Diremos que un subconjunto S de un anillo R, es un *Subanillo de* R, con las operaciones definidas en R, sii es un subgrupo aditivo de R, en el que la multiplicación es cerrada.
Esto es:

- $S \subseteq R$;
- $S \neq \emptyset$;
- $\ddot{+}$ cerrada en S;
- $\forall s \in S, \exists -s \in S : s + (-s) = 0$ *(Existencia de opuesto en S)*
- $*$ cerrada en S

Definición. Sea S un subconjunto de un anillo R, diremos que S es *multiplicativo*, sii:

- $0 \notin S$;
- $1 \in S$;
- si $a, b \in S$, entonces $ab \in S$ *(Multiplicativamente cerrado)*

Definición. Sean R y S dos anillos, y sea $f : R \to S$ una función.
Diremos que f es un *Morfismo de anillos* si $\forall a, b \in R$:

(a) $f(a +_R b) = f(a) +_S f(b)$;

(b) $f(a._R b) = f(a)._S f(b)$

Definición. Como siempre, hablaremos de:

- *Monomorfismo*, en el caso f morfismo inyectivo;
- *Epimorfismo*, en el caso f morfismo suryectivo;
- *Isomorfismo*, f biyectivo;
- *Endomorfismo*, si $R = S$;
- *Automorfismo*, si f es isomorfismo y $R = S$.

Definición. Sean R un anillo e $I \subseteq R$ un subgupo de $(R, +)$.
Si $bI \subseteq I, \forall b \in R$, diremos que I es un *ideal a izquierda del anillo* R;
Si $Ib \subseteq I, \forall b \in R$, diremos que I es un *ideal a derecha del anillo* R;
Si se verifican las dos condiciones anteriores, diremos que I es un *ideal bilátero*, o simplemente un ideal del anillo R.

Observación 2.3. .

- A menudo nos referiremos a la propiedad de que $\forall a \in I, r \in R$ el elemento $ar \in I$, como *Propiedad de absorvencia del ideal*;
- Si R es anillo con unidad y $1 \in I$, entonces $R = I$.

Definición. Sean R un anillo conmutativo con unidad, y X un subconjunto de R.
Definimos el *Ideal Generado por X* como:

$$\begin{aligned} \langle X \rangle &= RX \\ &= \{\sum_{i=1}^{n} r_i x_i : r_i \in R, x_i \in X, n \in \mathbb{N}\} \\ &= \bigcap_{I} I, I \text{ ideal que contiene a X} \end{aligned}$$

Observar entonces, que el ideal generado por X, resulta ser el conjunto de todas las combinaciones lineales finitas de elementos de X, y además es el menor ideal que contiene a X.

Definición. Sea R un anillo conmutativo con unidad, y sea X=$\{$a$\} \subset R$, un conjunto unitario;
El ideal generado por X, recibe el nombre de *Ideal Principal*, siendo:

$$\langle X \rangle = \{ra : r \in R\}$$

Definición. Un dominio íntegro en el que todo ideal es principal, es llamado un *Dominio de Ideales Principales*

Definición. Sea R un anillo, y sean $I_1, ..., I_n$ ideales de R.
Definimos la *Suma de los ideales* $I_1, ..., I_n$ como:

$$\sum_{i=1}^{n} I_i = \{\ a_1 + ... + a_n : a_i \in I_i, \text{ con } 1 \leq i \leq n\ \}$$

Definición. Sean R un anillo, e $I_1, ..., I_n$ ideales de R.
Definimos *El Producto de los ideales* $I_1, ..., I_n$ como:

$$\prod_{i=1}^{n} I_i = \{\ \sum_{j=1}^{m} a_{1_j} a_{2_j} ... a_{n_j} : a_{i_j} \in I_i (1 \leq i \leq n); m \text{ arbitrario }\}$$

Nota: Tanto la suma, como el producto de ideales, resultan ser ideales. Más aún, puede probarse que $\sum_{i=1}^{n} I_i = \langle \bigcup_{i=1}^{n} I_i \rangle$

Definición. Diremos que un ideal P en un anillo conmutativo R es *Primo* sii
$P \neq R$ y si $ab \in P \Rightarrow a \in P \vee b \in P$

Definición. Un elemento $p \in P$ se dirá *Primo* sii el ideal generado por p es primo.

Definición. Un ideal M en un anillo R se dirá *Maximal* si
$M \neq R$, y si es tal que si I es otro ideal cumpliendo que $M \subseteq I \subseteq R$, entonces $I = M \vee I = R$

Teorema 2.4. Sea R un anillo con unidad, y sea $I \neq R$ un ideal de R.
Luego, existe un ideal maximal de R que contiene a I.

Corolario 2.5. En un anillo con unidad, siempre hay ideales maximales

Teorema 2.6. Sean R un anillo conmutativo con unidad, y $M \subseteq R$ un ideal. Luego:
M es un ideal maximal $\Leftrightarrow R/M$ es un cuerpo

Teorema 2.7. Sean R un anillo conmutativo con unidad, y $M \subseteq R$ un ideal. Luego:
M es un ideal primo $\Leftrightarrow R/M$ es un dominio íntegro.

Teorema 2.8. Sea R un anillo conmutativo con unidad, y sea I un ideal de R.
Luego, si I es maximal $\Rightarrow I$ es primo

Teorema 2.9. Sea R un Dominio Íntegro, y sea $I \neq 0 \subseteq R$ un ideal.
Luego, I es primo $\Leftrightarrow I$ es maximal

Definición. Sea R un anillo, e $I \subseteq R$ un ideal;
Definimos en R la relación de equivalencia $b \sim c \Leftrightarrow b - c \in I$; anotaremos la clase de equivalencia del elemento $a \in R$ según esta relación, como $a + I$.
El conjunto cociente será $R/I = \{a + I : a \in R\}$.

Se afirma que tal conjunto adquiere estructura de anillo con la suma de clases dada por $(a + I) + (b + I) = a + b + I$, y el producto de clases definido como $(a + I)(b + I) = ab + I$

Teorema 2.10. *(Teorema de correspondencia: Versión para ideales)*
Sea R un anillo, $I \subseteq R$ un ideal.
Afirmamos que la función $\pi : \{J \text{ ideal de } R : I \subseteq J\} \to R/I$, dada por $\pi(J) = R/J$, es biyectiva.
Más aún, bajo esta correspondencia, los ideales de R que contiene a I se corresponden con ideales de R/I

Definición. Sea C un conjunto.
Diremos que $\ddot{\leq}$ es una relación de *Orden Parcial* si:

- Es *Reflexiva*. i.e $a \leq a \forall a \in C$;
- Es *Transitiva*. i.e si $a \leq b \wedge b \leq c \Rightarrow a \leq c (\forall a, b, c \in C)$;
- Es *Antisimétrica*. i.e $a \leq b \wedge b \leq a \Rightarrow a = b$

Definición. Diremos que ¨$\leq$¨ es un *Orden Total* sobre un conjunto C, si:
Dos elementos cualesquiera de C están relacionados, i.e $\forall a, b \in C, a \leq b \vee b \leq a$

Definición. Una *Cadena* es un subconjunto totalmente ordenado, de un conjunto ordenado.
i.e Si $(X, \leq)$, es un conjunto en el que se ha definido una relación de orden, entonces $C \subseteq X$ se dirá ¨Una cadena¨ sii $(C, \leq)$ es un conjunto totalmente ordenado.

Definición. Dado $(X, \leq)$ un conjunto ordenado,
diremos que $m \in X$ es un *Elemento maximal respecto a la relación de orden* si:
$\forall a \in X : a \geq m, a = m$

Lema 2.11. *Lema de Zorn*
Sea C un conjunto ordenado y no vacío;
Si toda cadena en C tiene una cota superior en C, entonces C tiene elementos maximales.

Definición. Dado un anillo R, diremos que este cumple *La Condición de la Cadena Ascendente (C.C.A)* si:
Dada una sucesión de ideales $(I_n)_n$ tales que $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq I_{n+1} \subseteq ...$ Esta se ¨estaciona¨,
en el sentido de que $\exists n_0 \in \mathbb{N}$, tal que $I_n = I_{n_0}, \forall n \geq n_0$.

Definición. Diremos que un anillo R es *Noetheriano* si cumple la condición de la cadena ascendente.

Teorema 2.12. Sea R un anillo. Son equivalentes:

- R es Noetheriano;
- R cumple la condición de la cadena ascendente;
- Todo ideal $I \subseteq R$ está finitamente generado;
- Para toda familia $(I_\alpha)_{\alpha \in A}$ de ideales en R, $\exists \tilde{\alpha} \in A$ tal que $\tilde{\alpha}$ es maximal, (entre los elementos de la familia), con la inclusión.

Definición. Un Dominio íntegro D, se dirá *Dominio de Factorización Única (D.F.U)* si:
Todo $a \neq 0 \in D$ puede expresarse en forma única salvo unidades y orden, como producto de factores irreducibles de D.

Lema 2.13. Sea R ún $D.F.U$;
Un elemento $a \in R$ es irreducible sii es primo.

Teorema 2.14. Si R es DFU, entonces $R[X]$ es DFU

Corolario 2.15. Si R es DFU, entonces $R[X_1, ..., X_n]$ es DFU. En particular, $K[X_1, ..., X_n]$ para todo cuerpo K.

Definición. Sea R un dominio íntegro conmutativo, y consideremos $a, b, c \in R - \{0\}$

1. Llamaremos *Unidades de* R, a aquellos elementos de R que tienen inverso multiplicativo. Anotaremos $\mathcal{U}(R) = R^* = \{$ Elementos inversibles de $R\}$
2. a y b se dirán *asociados* y anotaremos $a \sim b$, si $\exists u \in \mathcal{U}(R) : a = bu$
3. Diremos que a *divide* a b, y anotaremos $a \mid b$, si $\exists c \in R : b = ac$
4. diremos que a es *Irreducible* si:
   - $a \notin R^*$
   - $a = bc \Rightarrow b \in R^* \vee c \in R^*$
5. Diremos que $a \in R$ es *Primo* si:
   - $a \notin R^*$
   - si $a \mid bc \Rightarrow a \mid b \vee a \mid c$

Observación 2.16. .

1. $a \sim b \Rightarrow a \mid b \wedge b \mid a$
2. $a \mid b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$
3. $a \sim b \Leftrightarrow \langle a \rangle = \langle b \rangle$
4. a es primo $\Leftrightarrow \langle a \rangle$ es primo
5. Si $a \mid b \Rightarrow au \mid vb \forall u, v \in R^*$
6. Si $a \mid b \wedge a \notin R^* \Rightarrow b \notin R^*$
7. Si a es primo y $a \mid b_1 ... b_r \Rightarrow \exists i \in \{1, .., r\} : a \mid b_i$

Definición. Sea $(R, +_R, *)$ un anillo con unidad, y sea $(M, +)$ un grupo abeliano.
Diremos que M es un R-Módulo a izquierda, si existe un producto externo $\ddot{\cdot}$,
$\cdot : R \times M \to M$, verificando las siguientes propiedades $\forall a, b \in R$; $m, n \in M$:

(1) $a \cdot (m + n) = a \cdot m + a \cdot n$;

(2) $(a +_R b) \cdot m = a \cdot m + b \cdot m$;

(3) $a \cdot (b \cdot m) = (a * b) \cdot m$;

(4) $1 \cdot m = m$

De modo análogo se define R-Módulo a derecha, con $\ddot{\cdot}$esta vez definido de $M \times R$ a M.

Observación 2.17. .

- Si el anillo R es conmutativo, todo R- módulo a derecha lo es también a izquierda (y viceversa) definiendo el producto externo como $a \cdot m = m \cdot a$ (o al revés)
- Todo ideal de R es un R-Módulo, tomando como producto externo, el producto ya definido sobre el anillo.
- La teoría de módulos es una generalización a la teoría de espacios vectoriales, si se piensa que ahora los escalares pueden ser de cualquier anillo en vez de de un cuerpo.

Definición. Sean R un anillo, M un R- Módulo y $X \subseteq M$.
Definimos el *Anulador de* X, como:

$$An(X) = \{a \in R : a \cdot x = 0 \, \forall \, x \in X\}$$

Si $m \in M$, se define de modo análogo el*Anulador de* m, como:

$$An(m) = \{a \in R : a \cdot m = 0\}$$

Definición. Sean A, B, C R-Módulos, y sean f, g homomorfismos de R-Módulos.
Diremos que la sucesión

$$A \xrightarrow{f} B \xrightarrow{g} C$$

es una *Sucesión exacta corta*, si Imag(f)=Nu(g).
De modo análogo, $A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} A_2 ... \xrightarrow{f_n} A_{n+1}$, se dirá una *Sucesión exacta larga*, si cada terna $A_k \xrightarrow{f_k} A_{k+1} \xrightarrow{f_{k+1}} A_{k+2}$, es una sucesión exacta corta.

Definición. Sea A un conjunto. Diremos que A es una *R-álgebra* si:
A es un anillo y un R-módulo , siendo la operación $\ddot{+}$ la misma (como R-módulo y como anillo) y siendo tal que el producto en M $(*)$, y el producto externo por alguien de R $(\cdot)$ verifican la siguiente identidad: $\forall r \in R, m_1, m_2 \in M, r \cdot (m_1 * m_2) = (r \cdot m_1) * m_2 = m_1 * (r \cdot m_2)$.

Definición. Diremos que $\{a_1, ..., a_n\}$ son *algebraicamente independientes sobre* K si:
$\nexists f \in K[X_1, ..., X_n] : f \neq 0 \wedge f(a_1, ..., a_n) = 0$

Definición. Sea A un subanillo de un anillo R y sea $x \in R$.
Diremos que x *es integral sobre* A si x es raíz de un polinomio mónico f, con coeficientes en A.
De modo análogo, si B es otro subanillo de R diremos que B *es integral sobre* A si $\forall b \in B, b$ es integral sobre A.

Teorema 2.18. Sean A, B, C subanillos de un anillo R; Si C es integral sobre B y B es integral sobre A, entonces C es integral sobre A.

Teorema 2.19. Sea A un subanillo de R y $x \in R$, son equivalentes:

(a) x es integral sobre A;

(b) $A[x]$ es finitamente generado como A-módulo;

(c) $x \in B$ siendo este un subanillo de R, tal que $A \subseteq B$, y B es un A-módulo finitamente generado.

Teorema 2.20. Sea A un subanillo de un dominio íntegro B, con B integral sobre A.
Afirmamos que A es cuerpo sii B también lo es.

Definición. Si F y E son dos cuerpos verificando que $E \subseteq F$,
diremos que F *es una extensión del cuerpo* E, y lo anotaremos $E \leq F$
(también es usual anotar F/E)

Observación 2.21. Si F es una extensión del cuerpo E, puede verse a F como un E- espacio vectorial. Pues F es en particular un grupo abeliano con la suma, y podemos definir un producto externo en el que tomamos a los elementos de E como escalares.

Definición. Si $E \leq F$, y vemos a F como un E- espacio vectorial,
definimos el *Grado de la extensión de cuerpos* como la dimensión de F como E- esp. vectorial.
Anotamos $[F : E]$, y nos referimos a esta dimensión como el grado de F sobre E.
Si tal grado resulta finito, decimos que F *es una extensión finita de* E

Teorema 2.22. El grado es multiplicativo, en el siguiente sentido:
Si $E \leq K \leq F$, entonces $[F : E] = [F : K][K : E]$.
Notar que en particular, $[F : E]$ será una extensión finita, sii $[F : K], [K : E]$ lo son.

Un hecho útil que se desprende de la teoría de ¨extensión de cuerpos¨ es el siguiente:
Si f es un polinomio no constante en $E[X]$ sin raíces en E; siempre es posible hallar una extensión de cuerpos, en la que f sí tenga raíces..., enunciamos esto en el siguiente teorema.

Teorema 2.23. Sea f un polinomio no constante sobre el cuerpo E.
Luego existen una extensión $E \leq F$ y un elemento $a \in F$ tal que $f(a) = 0$.

Definición. Sea $E \leq F$,
Diremos que el elemento $a \in F$ es *algebraico sobre* E, si existe un polinomio no constante f en $E[X] : f(a) = 0$.
Si un elemento no es algebraico sobre E, decimos que es *trascendental*.
Si todo elemento de F es algebraico sobre E, decimos que F es una *extensión algebraica de* E.

Teorema 2.24. Si F es una extensión finita de E, entonces F es una extensión algebraica de E.

Teorema 2.25. Si E está generado sobre F por finitos elementos $a_1, ..., a_n$ algebraicos sobre F (es decir, $E = F(a_1, ..., a_n)$), entonces E es una extensión finita de F.

3. Variedades

Nota: A menos que que se especifique lo contrario, todos los anillos serán conmutativos.

Definición. Llamaremos *Espacio Afín n-dimensional de un cuerpo K* al conjunto:

$$A^n = \{\ (k_1, k_2, ..., k_n) : k_i \in K, \forall i = 1, ..., n\ \}$$

Frecuentemente nos referiremos a los elementos de A^n como puntos.

¿Qué diferencia hay entre A^n y K^n?
La diferencia reside en que en A^n se ¨olvida¨ la estructura vectorial de K^n, de manera de que ningún punto desempeña un papel destacado (como ocurre con el $\vec{0}$ en K^n).
De ningún modo esto significa despreciar la estructura vectorial, sino que lo que se pretende es brindar la posibilidad de que el vector $\vec{0}$ sea en cada momento el punto que más convenga.

Definición. Sea $S \subseteq K[X_1, ..., X_n]$. Definimos la ¨Variedad del conjunto S¨ como :

$$\mathrm{V}(S)=\{\ \mathrm{x} \in A^n \text{ tales que } f(x) = 0, \forall\ f \in S\ \}$$

Podemos pensar a una variedad, como el conjunto solución de ecuaciones polinomiales simultáneas. Notemos además, que toda variedad es la variedad de un ideal; en el sentido de que si I es el ideal generado por un conjunto de polinomios S, esto es $I = \langle\ S\ \rangle = \{\ \sum g_i\ f_i$ con $g_i \in K[X_1, ...X_n]$ y $f_i \in S\ \}$, entonces $V(\mathrm{S}) = V(\mathrm{I})$.

Mediante la siguiente proposición, probaremos que A^n, puede ser visto como un espacio topológico, tomando a las variedades como conjuntos cerrados.

Proposición 3.1. .

1. Si $V_\alpha = V(I_\alpha) \forall \alpha \in T \Longrightarrow \bigcap\limits_{\alpha \in T} V_\alpha = V(\bigcup\limits_{\alpha \in T} I_\alpha)$
   (Esto es, la intersección arbitraria de variedades es una variedad)
2. Si V_j=$V(I_j)$, j=1,....r $\Longrightarrow \bigcup\limits_{j=1}^{r} V_j = V(\{f_1 \dots\ f_r$ tales que $f_j \in I_j$, j=1,...,r $\})$
   (Esto es, la unión finita de variedades es una variedad)
3. A^n= $V(0)$ y $\emptyset$=$V(1)$
   (Los espacios, vacío y total, son variedades)

   Demostración. .

1. ($\subseteq$) Sean $x \in \bigcap\limits_{\alpha \in T} V_\alpha$, $f \in \bigcup\limits_{\alpha \in T} I_\alpha$. Deberemos ver que $f(x) = 0$.
   Como $f \in \bigcup\limits_{\alpha \in T} I_\alpha \Rightarrow \exists \alpha_i \in T : f \in I_{\alpha_i}$. Además, como $x \in \bigcap\limits_{\alpha \in T} V_\alpha$, se tiene que en particular $x \in V(I_{\alpha_i})$. Pero entonces $f(x) = 0$, resultando así que $\bigcap\limits_{\alpha \in T} V_\alpha \subseteq V(\bigcap\limits_{\alpha \in T} I_\alpha)$

($\supseteq$) Sea $x \in V(\bigcup I_\alpha) \Rightarrow \forall f \in \bigcup I_\alpha, f(x) = 0$
Como $\forall \alpha, I_\alpha \subset \bigcup I_\alpha$, se tendrá que $f(x) = 0 \, \forall f \in I_\alpha, \alpha \in T$.
Luego x $\in V(I_\alpha) \; \forall \; \alpha \in T$.

Finalmente, afirmamos que x $\in \bigcap(V(I_\alpha))$; con lo que queda probada la doble contención.

2. ($\subseteq$) Sea $x \in \bigcup_{i=1}^{r} V_j \Rightarrow \exists j \in \{1, ..., r\} : x \in V_j = V(I_j) \Rightarrow \forall f_j \in I_j, f_j(x) = 0 \Rightarrow$ todo producto de polinomios que tenga a alguien de I_j entre sus factores, se anulará al ser evaluado en x.
Con esto, $x \in V(\{f_1 ....f_r : f_i \in I_i, i = 1, ..., r\})$.

($\supseteq$) Por el contrarecíproco.
Supongamos que $x \notin \bigcup_{j=1}^{r} V(I_j)$, luego $\forall V_j = V(I_j), x \notin V_j$. Con esto, se tiene que:

- Para $I_1, \exists f_1 \in I_1 : f_1(x) \neq 0$;
- Para $I_2, \exists f_2 \in I_2 : f_2(x) \neq 0$;

$$\vdots$$

- Para $I_r, \exists f_r \in I_r : f_r(x) \neq 0$.

Luego, si consideramos el producto $f_1 ....f_r$ y lo evaluamos en x, se tendrá que este es no nulo; con lo cual, $x \notin V((\{f_1 \dots f_r$ tales que $f_j \in I_j, j = 1, ..., r\})$.
Afirmamos entonces, válida la igualdad.

3. *(Veamos que $A^n = V(0)$)*
($\subseteq$) Sea x $\in A^n$; por definición de polinomio nulo, se tiene que $0(x) = 0$. Con esto $x \in V(0)$
($\supseteq$) Sea $x \in V(0)$, entonces por definición de variedad, $x \in A^n$.
Luego, afirmamos válida la igualdad.

(Veamos que $\emptyset = V(1)$)
$V(1) = \{x \in A^n$ tales que 1(x)=0$\}$
Pero $1(x) = 1 \forall x \in A^n$!!. Luego $V(1) = \emptyset$ ▲

Observación 3.2. La condición 2. puede reescribirse como:

$$\bigcup_{j=1}^{r} V(I_j) = V(\prod_{j=1}^{r} I_j) = V(\bigcap_{j=1}^{r} I_j)$$

Como consecuencia de esta proposición, existe una topología definida sobre A^n, llamada *Topología de Zariski*, en la que los conjuntos cerrados y las variedades coinciden.

Definición. Si $X \subseteq A^n$, definimos *¨El ideal de X ¨* como:

$$I(\text{X}) = \{ \; f \in K[X_1, ..., X_n] \text{ tales que } f(x) = 0, \; \forall \text{ x} \in X\}$$

Proposición 3.3. .

1. Sean X e $Y \subseteq A^n$;
Si $X \subseteq Y \Rightarrow I(Y) \subseteq I(X)$.

2. Sean $S, T \subseteq K[X_1, ..., X_n]$;
   Si $S \subseteq T \Rightarrow V(T) \subseteq V(S)$.

Demostración. .

1. Sea $f \in I(Y)$, entonces $f \in K[X_1, ..., X_n]$ y $f(y) = 0 \, \forall \, y \in Y$, pero como $X \subseteq Y$, en particular vale que $\forall x \in X, f(x) = 0$.
   Con esto, $f \in I(X)$.

2. Sea $x \in V(T)$, luego $x \in A^n$ y $\forall f \in T, f(x) = 0$. Por la contención de S en T, en particular vale que $\forall f \in S, f(x) = 0$.
   Afirmamos entonces, que $x \in V(T)$. ▲

Definición. Sea $S \subseteq K[X_1, ..., X_n]$, definimos *¨El ideal de la Variedad de S ¨*como $IV(S) = I(V(S))$, en donde esto ya es un conjunto conocido, por la definición anterior.

Similarmente, si $X \subseteq A^n$, podemos definir $VI(X)$, $IVI(X)$, $VIV(S)$, y así sucesivamente..., del modo en el que ya todos nos imaginamos.

Proposición 3.4. .

1. *a)* Si $S \subseteq K[X_1, ...X_n]$, entonces $S \subseteq IV(S)$
   b) Si $X \subseteq A^n$, entonces $X \subseteq VI(X)$

   Si se ¨aplican¨ V e I de forma alternada, la sucesión se ¨estabiliza¨, en el siguiente sentido:

2. *a)* $VIV(S) = V(S)$
   b) $IVI(X) = I(X)$

3. $I(\emptyset) = K[X_1, ...X_n]$

4. Si K es un cuerpo con infinitos elementos, entonces $I(A^n) = \{0\}$

5. Si x=$(a_1, a_2, ..., a_n) \in A^n$, entonces $I(\{x\}) = \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n \rangle$

Demostración. .

1. *a)* Sea $f \in S$, luego $\forall \, x \in V(S)$, $f(x)$=0, pero entonces, $f \in I(V(S))$= $IV(S)$.
   Con esto, $S \subseteq IV(S)$
   b) Sea $x \in X$, y sea $f \in I(X)$, luego por definición de $I(X)$, $f(x)$=0, pero entonces $x \in V(I(X))$.
   Con esto, $X \subseteq VI(X)$

2. *a)* ($\subseteq$) Por item 1 (a), de esta misma proposición, sabemos que $S \subseteq IV(S)$, y por el item 2 de la proposición 1.3, concluímos que $VIV(S) \subseteq V(S)$.

   ($\supseteq$) Sea $x \in V(S)$. Queremos ver que $x \in VIV(S)$.
   Consideremos $f \in IV(S)$. Luego, $\forall y \in V(S), f(y) = 0$, pero esto vale en particular, para el x dado, i.e $f(x) = 0$.
   Concluímos entonces, que $x \in V(I(V(S))) = VIV(S)$.

b) ($\subseteq$) Por proposición 1.4, item 4 (b), sabemos que $X \subseteq VI(X)$; pero entonces,por proposición 1.3 insiso 1, $IVI(X) \subseteq I(X)$.

($\supseteq$) Sea $f \in I(X)$, y consideremos $x \in VI(X)$. Luego, por definición de variedad, $\forall\, g \in I(X)$, $g(x) = 0$. Pero entonces, en particular para la f dada, $f(x) = 0$.
Con esto resulta $I(X) \subseteq IVI(X)$.

3. ($\subseteq$) $I(\emptyset) \subseteq K[X_1, ..., X_n]$, por definición de ideal de un conjunto.

   ($\supseteq$) Observemos: $I(\emptyset) = \{f \in K[X_1, ..., X_n] : f(x) = 0\, \forall x \in \emptyset\}$.
   Por el absurdo, supongamos que $K[X_1, ..., X_n]$ no está contenido en $I(\emptyset)$.
   Luego $\exists f \in K[X_1, ..., X_n] : f \notin I(\emptyset)$. Pero entonces, $\exists\, x \in \emptyset : f(x) \neq 0$ ABS!, (pues $\forall x, x \notin \emptyset$).
   Con esto $K[X_1, ..., X_n] \subseteq I(\emptyset)$,resultando así que $K[X_1, ..., X_n] = I(\emptyset)$.

4. Por inducción sobre la cantidad n de variables;

   - Si $n = 1$
     ($\subseteq$) Sea $f \in I(A^1) \Rightarrow \forall x \in K, f(x) = 0$.
     El problema se reduce entonces, a demostrar que si un polinomio en una variable tiene infinitos ceros, debe ser nulo.
     Por el absurdo, supongamos que $f \neq 0$, digamos entonces que Gr(f)=r.
     Ahora, f tiene infinitas raíces, con lo que en particular tiene $r + 2$, digamos $a_1, ..., a_{r+2}$.
     Luego, $(X - a_i)|f, \forall i = 1, ..., r + 2$, resultando así que

     $$f = (X - a_1)...(X - a_{r+2})q, q \in K[X]$$

     Por aditividad del grado, se tiene que $\text{Gr}(f) = (r + 2) + Gr(q) \geq r + 2$ ABS! (pues $\text{Gr}(f) = r$).
     El absurdo provino de suponer $f \neq 0$. Concluímos entonces, $f = 0$.
   - Supongamos que para $k < n$, vale que si K es un cuerpo con infinitos elementos $\Rightarrow$ $I(A^k) = \{0\}$
   - Veamos para $k = n$.
     ($\supseteq$) Trivial!

     ($\subseteq$) Sea $f \in I(A^n) \Rightarrow f \in K[X_1, ..., X_n] \wedge f(a_1, ..., a_n) = 0\, \forall\, (a_1, ..., a_n) \in A^n$.
     Por el absurdo supongamos que $f \neq 0$.
     Como $f \in K[X_1, ..., X_n]$, puede verse a f como una suma (finita) de monomios de $K[X_1, ..., X_n]$, digamos

     $$f = M_1 + ... + M_l, \text{ con los } M_i \text{ monomios de } K[X_1, ..., X_n].$$

     Ahora, cada $M_i = X_1^{m_i} q_i(X_2, ..., X_n)$ con $i = 1, ..., l, m_i \geq 0 \in \mathbb{N}$, con lo que:

     $$f = X_1^{m_1} q_1(X_2, ..., X_n) + X_1^{m_2} q_2 + ... + X_1^{m_l} q_l.$$

     Agrupando, de ser necesario, se llega a que f puede expresarse como:

     $$f = p_0 + p_1 X_1^1 + ... + p_j X_1^j, \text{ en donde } p_i \in K[X_2, ..., X_n] \text{ y } p_j \neq 0$$

     Ahora, como p_j es un polinomio no nulo en (menos de n) variables, se tendrá por Hipótesis Inductiva que, $p_j \notin I(A^{n-1})$; esto es $\exists (a_2, ..., a_n) \in A^{n-1} : p_j(a_2, ..., a_n) \neq 0$.
     Consideremos ahora el polinomio en X_1 dado por:

$$p_0(a_2,...,a_n) + p_1(a_2,...,a_n)X_1 + ... + \underbrace{p_j(a_2,...,a_n)}_{\neq 0} X_1^j$$

Luego, siendo tal polinomio no nulo, se tendrá que por el caso $n = 1, \exists a_1 \in K$:
$p_0(a_2,...,a_n) + p_1(a_2,...,a_n)a_1 + ... + p_j(a_2,...,a_n)a_1^j \neq 0$.
Pero esto dice que $f(a_1, a_2, ..., a_n) \neq 0 \Rightarrow f \notin I(A^n)$. ABS!!! (*pues se supuso* $f \in I(A^n)$).
El absurdo provino de suponer $f \neq 0$. Luego, f debe ser igual al polinomio nulo.
Concluímos finalmente, por el principio de inducción, que $\forall n \in \mathbb{N}, I(A^n) = 0$

5. ($\supseteq$) Sea $f \in \langle X_1 - a_1, ..., X_n - a_n\rangle \Rightarrow \exists P_1, ..., P_n \in K[X_1, ..., X_n]$ tales que

$$f = P_1(X_1 - a_1) + ... + P_n(X_n - a_n).$$

$$\begin{aligned} \text{Luego } f(a_1,...,a_n) &= P_1(a_1,...,a_n)\underbrace{(a_1 - a_1)}_{=0} + ... + P_n(a_1,...,a_n)\underbrace{(a_n - a_n)}_{=0} \\ &= 0. \end{aligned}$$

Con lo cual $f \in I(\{x\})$.

($\subseteq$) Queremos ver que si $f(x) = 0 \Rightarrow f \in \langle X_1 - a_1, ..., X_n - a_n\rangle$.
Por inducción sobre n.

- Si $n = 1$.
  Que $f(a) = 0 \Rightarrow (X - a)|f \Rightarrow \exists P_1 \in K[X] : f = (X - a)P_1 \Rightarrow f \in \langle X - a\rangle$.
- Supongamos que para $k < n$ vale que si $f(a_1, ..., a_k) = 0 \Rightarrow f \in \langle X_1 - a_1, ..., X_k - a_k\rangle$
- Veamos para $k = n$,
  Sea $f \in I(\{x\}) \Rightarrow f \in K[X_1, ..., X_n] \wedge f(x) = 0$.
  Hemos visto en la demostración anterior, que f puede verse como:

  $$f = p_0 + p_1X_1 + ... + p_rX_1^r, \text{ en donde los } p_i \in K[X_2, ..., X_n] \wedge p_r \neq 0.$$

  Dividiendo f entre $X_1 - a_1$ se tiene, por el algoritmo de la división, que $\exists q \in K[X_1, ..., X_n], r \in K[X_2, ..., X_n]$, tales que

  $$f = (X_1 - a_1)q(X_1, ..., X_n) + r(X_2, ..., X_n).$$

  Observación:¿Por qué r no tiene a X_1 entre sus variables?
  Si miramos a f como un polinomio en X_1 con coeficientes en el anillo de polinomios, y aplicamos el algoritmo de la división para dividir a f por $(X_1 - a_1)$, obtendremos que el resto r tiene, en la variable X_1, grado menor que 1.
  Resulta así que r es constante en la variable X_1, o como dijimos antes, r no tiene a X_1 entre sus variables.
  Sigamos con lo nuestro... $f \in I(\{x\}) \Rightarrow f(a_1, ..., a_n) = 0$,
  Pero $f(a_1, ..., a_n) = \underbrace{(a_1 - a_1)}_{=0} q(a_1, ..., a_n) + r(a_2, ..., a_n) = 0$.
  Luego $r(a_2, ..., a_n) = 0$ y por hipótesis inductiva, $r \in \langle X_2 - a_2, ..., X_n - a_n\rangle$.
  Finalmente, siendo $f = (X_1 - a_1)q + r$, afirmamos que $f \in \langle X_1, ..., X_n\rangle$. ▲

Definición. Una variedad se dice *reducible* si puede expresarse como unión de dos subvariedades propias. En caso contrario, diremos que la variedad es *irreducible*.

3.1. Problemas propuestos

En los Ejercicios del 1 al 4 se muestra que:
Una variedad V es irreducible, sii $I(V)$ es un ideal primo.

Problema 3.1. Asumamos que $I(V)$ no es primo, y consideremos $f_1 f_2 \in I(V)$con f_1,$f_2 \notin I(V)$.
Sea $x \in V$, muestre que si $x \notin V(f_1) \Rightarrow x \in V(f_2)$, y viceversa.

$I(V)$ no es un ideal primo, luego $\exists\ f_1,\ f_2$: $f_1\ f_2 \in I(V)$ con $f_1,\ f_2 \notin I(V)$.
Sea $x \in V : x \notin V(f_1)$,
como $f_1\ f_2 \in I(V)$, se tiene que $\forall\ y \in V,\ f_1 f_2(y) = 0$; luego en particular, vale que $f_1 f_2(x) = 0$.
Pero $f_1 f_2(x) = f_1(x) f_2(x)$, y siendo $f_1(x) \neq 0$, se concluye que $f_2(x) = 0$.
Con esto, $x \in V(f_2)$, como queríamos ver.
(Del mismo modo se demuestra que si $x \in V$ y $x \notin V(f_1) \Rightarrow x \in V(f_2)$). □

Observación : Esto muestra que si $x \in V \Rightarrow x \in V(f_1) \vee x \in V(f_2)$
O dicho de otro modo, que $V \subseteq V(f_1) \cup V(f_2)$.

Problema 3.2. Si $I(V)$ no es primo $\Rightarrow V$ es reducible.

Definamos $V_1 = V \cap V(f_1),\ \ V_2 = V \cap V(f_2)$; en donde f_1, f_2 son tales que:

$$f_1 f_2 \in I(V) \wedge f_1, f_2 \notin I(V).$$

Puesto a que la intersección de variedades, es una variedad (prop. 1.1 insiso 1), se tiene que tanto V_1 como V_2 son variedades.

$$\begin{aligned} \text{Ahora}, V_1 \cup V_2 &= (V \cap V(f_1)) \cup (V \cap V(f_2)) \\ &= V \cap (V(f_1) \cup V(f_2)) \\ &= V \text{ (Pues por observación del ejercicio anterior, } V \subseteq V(f_1) \cup V(f_2)). \end{aligned}$$

Serán V_1, V_2 variedades propias?

- *¿$V_1, V_2 \neq$ de vacío?*
  Por el absurdo supongamos que $V_1 = \emptyset$; luego siendo $V = V_1 \cup V_2$, se tiene que $V = V_2$, pero entonces $V \subseteq V(f_2)$, *(pues $V_2 = V \cap V(f_2)$).*
  Con esto, por prop. 2.3 insiso 1, resulta que $I(V(f_2)) \subseteq I(V)$.
  Sin embargo $f_2 \in I(V(f_2))$, y por lo recién dicho, resulta que $f_2 \in I(V)$, pero f_2 fue tomada en $(I(V))^c$.ABS!!
  El absurdo provino de suponer $V_1 = \emptyset$. Concluímos entonces que $V_1 \neq \emptyset$.
  De modo análogo se llega a que $V_2 \neq \emptyset$.

- *¿Son $V_1, V_2 \neq V$?*
  Por el absurdo supongamos que $V_2 = V$; pero entonces siendo $V_2 = V \cap V(f_2)$, se tiene que $V \subseteq V(f_2)$. Con lo que de la prop. 2.3 insiso 1, concluímos que $I(V(f_2)) \subseteq I(V)$, ABS!!
  (pues $f_2 \in I(V(f_2))$ pero $f_2 \notin I(V)$)
  Luego, $V_2 \neq V$
  De modo análogo se prueba lo mismo para V_1.

Se tienen entonces, dos variedades propias, V_1 y V_2: $V = V_1 \cup V_2$. Afirmamos entonces, que V es reducible. □

Problema 3.3. Si V y W son variedades cumpliendo que $V \subset W \Rightarrow I(W) \subset I(V)$.

Sea $f \in I(W)$, entonces $\forall x \in W$ se tiene que $f(x) = 0$.En particular para los $x \in V$, también vale que $f(x) = 0$ *(pues por hip. $V \subset W$)*. Con esto $f \in I(V)$
Concluímos entonces $I(W) \subseteq I(V)$. □

Problema 3.4. Asumamos ahora que $V = V_1 \cup V_2$ con V_1, $V_2 \subset V$. Por el problema 3, podemos elegir $f_i \in I(V_i) : f_i \notin I(V)$.
Muestre que $f_1 f_2 \in I(V)$. Observar que esto muestra que $I(V)$ no es un ideal primo.

Sean $f_i \in I(V_i) : f_i \notin I(V)$, para $i = 1, 2$
Queremos ver que $f_1 f_2 \in I(V)$, es decir que $\forall x \in V, f_1 f_2(x) = 0$
Sea $x \in V$, luego por hip. $x \in V_1 \vee x \in V_2$; con lo cual $f_1(x) = 0 \vee f_2(x) = 0$ *(Pues $f_i \in I(V_i)$ por hip.)*. En cualquiera de los dos casos, vale que $f_1 f_2(x) = 0$.
Luego $f_1 f_2 \in I(V)$.
Observación: Con esto, $\exists\ f_1, f_2 \notin I(V)$, pero tales que $f_1 f_2 \in I(V)$.
Esto dice, que $I(V)$ no es un ideal primo. □

Moraleja: V irreducible $\Leftrightarrow$ $I(V)$ es un ideal primo

Problema 3.5. Toda variedad puede expresarse como unión finita de subvariedades irreducibles.

Sea V una variedad;

- Si V es irreducible *Listo!* (V resulta unión de una variedad irreducible, que es ella misma)
- Si V es reducible $\Rightarrow V = V_1 \cup V_2$, para ciertas subvariedades propias V_1, V_2
  - Si V_1, V_2 son irreducibles. *Listo!* ($V = V_1 \cup V_2$)
  - Si alguna de las subvariedades (o las dos) son reducibles;
    Sin pérdida de demasiada generalidad, supongamos V_1 reducible.
    Luego, $\exists\ V_{1_1}$, V_{1_2} variedades propias : $V_1 = V_{1_1} \cup V_{1_2}$
    - Si ambas son irreducibles (V_{1_1}, V_{1_2}), entonces:
      - $V = (V_{1_1} \cup V_{1_2}) \cup V_2$; en el caso V_2 irreducible; o
      - En el caso V_2 reducible, $\exists\ V_{2_1}, V_{2_2}$, variedades propias : V_2=($V_{2_1} \cup V_{2_2}$), resultando así $V = (V_{1_1} \cup V_{1_2}) \cup (V_{2_1} \cup V_{2_2})$.
        Observar que en ambos casos, hemos sido capaces de descomponer a V, como unión finita de variedades irreducibles.
    - Si alguna fuera reducible, el proceso se continuaría de forma sucesiva...

Notemos ahora lo siguiente, el proceso ¨desarma¨ en forma progresiva a V como unión finita de variedades irreducibles. Luego, si el proceso concluyera en un número finito de iteraciones, habríamos podido descomponer a V, como una unión finita de variedades irreducibles.

¿Puede el proceso continuarse infinitamente?
Por el absurdo, supongamos que si,
Luego, podemos construir una sucesión $(\tilde{V_i})$ de variedades, de modo que $\tilde{V}_{i+1} \subset \tilde{V}_i$. Y con ella, una sucesión de ideales $I(\tilde{V}_i)$, cumpliendo que, $I(\tilde{V}_i) \subseteq I(\tilde{V}_{i+1})$ (*(por prop. 1.3 insiso 1).*
Esta sucesión de ideales, no es más que una cadena ascendente que no se estabiliza nunca!!!
Se contradice así, el hecho de que $K[X_1, ..., X_n]$ es Noetheriano. ABS!!
Luego el proceso debe finalizar en un número finito de pasos. Resulta así que V es unión finita de variedades irreducibles. □

Problema 3.6. Muestre que la descomposición del problema anterior es única, asumiendo que se descartan las subvariedades que estén contenidas en otras.

Supongamos que $V = V_1 \cup V_2 \cup ... \cup V_n$, para ciertas variedades irreducibles $V_1, ..., V_n : V_i$ no está contenida en V_j, para $i \neq j$; y que además $V = W_1 \cup W_2 \cup ... \cup W_m$, con $W_1, .., W_m$ irreducibles cumpliendo que W_i no está contenida en W_j para $i \neq j$.

$$\begin{aligned} \text{Ahora}, V_i &= V_i \cap V, \text{ para cada } i = 1, ..., n \\ &= V_i \cap \bigcup_{j=1}^{m} W_j \\ &= \bigcup_{j=1}^{m} (V_i \cap W_j) \text{ (Recordemos que la intersección de variedades es una variedad)} \end{aligned}$$

Luego, siendo V_i irreducible $\forall\ i$, no puede escribirse como unión de subvariedades propias.
Con esto, deberá existir (para cada i), un $j_i \in \{1, ..., m\} : V_i = V_i \cap W_{j_i}$ (3)
$\Rightarrow V_i \subseteq W_{j_i}$(1)
Del mismo modo, se llega a que $\exists\ k \in \{1,...,n\} : W_{j_i} = W_{j_i} \cap V_k$ (3´)
$\Rightarrow W_{j_i} \subseteq V_k$ (2)
Luego, de (1) y (2), se tiene que $V_i \subseteq V_k$. Pero entonces $V_i = V_k$ *(pues V_i no está contenida en V_j si $i \neq j$)*
Pero entonces, siendo $V_i = V_k$, de (3)+ (3´), resulta $W_{j_i} = V_i$
Observemos ahora lo siguiente,

- Cada V_i es igual a un único W_j *(por el simple hecho de que si $V_i = W_j$ y $V_i = W_t$ con $j \neq t$, entonces por transitividad de la igualdad, $W_j = W_t$)*
- Si $V_i \neq V_j$, entonces, sus correspondientes W_l y W_t también son distintos.

Luego, afirmamos con toda certeza que n=m, y la descomposición resulta única!. □

Problema 3.7. Sea K un cuerpo algebraicamente cerrado. Supongamos que A^n es cubierto por conjuntos abiertos $A^n - V(I_i)$ de la topología de Zariski.
Sea I el ideal generado por los $I_i, (I = \sum I_i) = \{x_{i_1} + ... + x_{i_2}$, con $x_{i_j} \in I_{i_j}\}$.
Muestra que $1 \in I$. (*Sugerencia:* Puede utilizarse el Nullstellensatz débil, que será enunciado y probado más adelante).

Antes que nada enunciemos el llamado ¨*Teorema débil de los ceros.* ¨
Este afirma que si I es un ideal de $K[X_1, ..., X_n] : V(I) = \emptyset$, entonces $I = K[X_1, ..., X_n]$.
Ahora si, volvamos al ejercicio.
Supongamos que $A^n = \bigcup_i A^n - V(I_i) = \bigcup_i (V(I_i))^c$, con $(V(I_i))^c$ abiertos de la topología de Zariski.
Tomando complementos a ambos lados, llegamos a que:

$$\begin{aligned}\emptyset &= \textstyle\bigcap_i (V(I_i)^c)^c \\ &= \textstyle\bigcap_i V(I_i) \\ &= V(\textstyle\bigcup_i I_i) \textit{ Por proposición 2.1 inciso 1} \\ &= V(\langle \textstyle\bigcup_i I_i \rangle) \\ &= V(I).\end{aligned}$$

Luego, por el Teorema Débil de los ceros, $I = K[X_1, ..., X_n]$, y por ende, $1 \in I$. □

Problema 3.8. Muestre que A^n es compacto con la topología de Zariski.

Sea $\{(V(I_i))^c\}$ un cubrimiento por abiertos de la topología de Zariski para A^n.
Llamemos $I = \langle \bigcup_i I_i \rangle = \sum_i I_i$.
Por ejercicio anterior, sabemos que $1 \in I$, con lo cual puede expresarse como una suma finita, digamos $1 = x_{i_1} + x_{i_2} + ... + xi_r$ para ciertos $x_{i_j} \in I_{i_j}$. Luego $1 \in \sum_{j=1}^{r} I_{i_j}$.
Ahora, como el polinomio constante e igual a 1 no se anula nunca, se concluye que
$V(\sum_{j=1}^{r} I_{i_j}) = \emptyset$, esto es $V(\langle \bigcup_{j=1}^{r} I_{i_j} \rangle) = \emptyset$, o lo que es lo mismo, $V(\bigcup_{j=1}^{r} I_{i_j}) = \emptyset$.
Luego, por proposición 2.1, inciso 1, $\bigcap_{j=1}^{r} V_{i_j} = \emptyset$.
Tomemos complementos a ambos lados de la igualdad, para concluir que $A^n = \bigcup_{j=1}^{r} (V_{i_j})^c$.
Queda en evidencia, que todo cubrimiento por abiertos de la topología de Zariski para A^n admite un subcubrimiento finito, revelándose así, la compacidad de A^n. □

4. El teorema central de Hilbert

En la sección anterior, hemos hablado de las variedades, como conjuntos solución de ecuaciones polinomiales simultáneas.
En general, pueden estar involucradas infinitas ecuaciones. Sin embargo en esta sección, veremos que una colección infinita de ecuaciones, puede siempre ser reemplazada por una colección finita.
La razón por la cual puede hacerse esto, es que todo ideal de $K[X_1, ..., X_n]$ tiene un conjunto finito de generadores. O dicho en otras palabras, $K[X_1, ..., X_n]$ es un anillo Noetheriano.
Observemos que el cuerpo K, es un dominio de ideales principales, con lo cual es en particular Noetheriano.
Probaremos entonces, el llamado ¨Teorema Central de Hilbert¨.

Teorema 4.1. *(Teorema Central de Hilbert)* : Si R es un anillo Noetheriano, entonces el anillo de polinomios en n variables $R[X_1, ..., X_n]$ es también Noetheriano.

Demostración.

Basta probarlo para una indeterminada.
Sea I un ideal de $R[X]$, y consideremos J_i, el subconjunto de R formado por todos los coeficientes principales de polinomios de I, con grado i (más el 0).
Es claro que J_i es un ideal de R. Más aún, puede verse que $J_0 \subset J_1 \subset J_3 \subset$... *(Para ver que todo elemento deJ_i es un elemento de J_{i+1}, basta agarrar al polinomio que justifica que el elemento está en J_i, y multiplicarlo por X. El polinomio resultante, tendrá grado $i+1$ y como coeficiente principal al elemento en cuestión. Luego estará en J_{i+1}).*
Siendo R Noetheriano, la cadena ascendente anteriormente mencionada, deberá estabilizarse a partir de un momento. Mas precisamente, $\exists\ r \in \mathrm{N} : J_i = J_r\ \forall\ i \geq r$.
También, por ser R Noetheriano, todo ideal está finitamente generado; digamos $J_i = \langle\ b_{i_1}, b_{i_2}, ..., b_{i_n}\ \rangle$, para $i = 0, ..., r$ *(Obs: No es restricción suponer que el número de generadores es el mismo, pues siempre pueden agregarse generadores redundantes)*. Suponedremos además, que los b_{i_j} son no nulos.
Sea P_{i_j} un polinomio $\in I$ de grado i, cuyo coeficiente (de grado i), es b_{i_j}.
Probaremos que I=$\langle\ P_{i_j}$, con i=0,...,r; j=1,...n $\rangle$. Con lo cual, I estaría finitamente generado.
Es claro, que el ideal generado por los P_{i_j} está contenido en I. Veremos entonces la otra contención.
Sea $f \in I$ un polinomio cualquiera;digamos, de grado ¨d¨.
Veremos que $f \in \langle\ P_{i_j}$, con i=0,...,r; j=1,...n $\rangle$, por inducción sobre ¨d¨.
El coeficiente principal de f, está en b_d.

- Si $d > r$, notemos que los coeficientes principales de $X^{d-r}p_{r_1}$, $X^{d-r}p_{r_2}$, ..., $X^{d-r}p_{r_n}$, son los números $b_{r_1}, b_{r_2}, ..., b_{r_n}$ que generan $b_r = b_d$.
  Luego, existirán $c_1, ..., c_n \in R : f - (c_1X^{d-r}p_{r_1} + c_2X^{d-r}p_{r_2} + ... + c_nX^{d-r}p_{r_n})$; tiene grado menor que d y está en I.Pero entonces, por hipótesis inductiva, $f \in$ al ideal generado por los P_{i_j}
- Si $d \leq r$ obtenemos un polinomio $f - (c_1P_{d_1} + c_2P_{d_2} + ... + c_nP_{d_n})$ de grado menor que d y contenido en I con lo que se concluye igualmente. ■

Corolario 4.2. : Toda variedad es intersección de finitas *hipersuperficies* (conjuntos nulos de polinomios simples). i.e, Si V es una variedad, entonces $\exists f_1, ..., f_r \in K[X_1, ..., X_n] : V = \bigcap_{i=1}^{r} V(f_i)$

Demostración.

Sea $V = V(I)$ *(Recordemos que toda variedad es la variedad de algún ideal)*
Ahora, por teorema anterior, I tiene finitos generadores, digamos $f_1, ..., f_r$.
Veamos que $V(I) = \bigcap_{i=1}^{r} V(f_i)$
($\subseteq$) Sea $x \in V(I) = V(\langle f_1, ..., f_r \rangle) = V(\{f_1, ..., f_r\}) \Rightarrow f_i(x) = 0 \, \forall i = 1, ..., r \Rightarrow x \in V(f_i)$
$\forall i = 1, ..., r \Rightarrow x \in \bigcap_{i=1}^{r} V(f_i)$
($\supseteq$) Sea $x \in \bigcap_{i=1}^{r} V(f_i) = \bigcap_{i=1}^{r} V(\langle f_i \rangle)$, luego, por proposición 2.1 inciso 1, $x \in V(\bigcup_{i=1}^{r} \langle f_i \rangle = V(\{f_1, ..., f_r\})$.
Con esto, $x \in V(I)$. ♣

Definición. *(Series Formales de potencias)*
Sea D un dominio íntegro. Llamaremos *Anillo de series formales de potencias* con n indeterminadas $X_1, ..., X_n$ sobre D, al conjunto $D[[X_1, ..., X_n]]$ formado por todas las sucesiones
$\{ F_m \} \in D[X_1, ..., X_n]$ tales que F_m es una forma de grado m o la forma nula.
En lugar de $\{ F_m \}$, es frecuente escribir $\sum_{m=1}^{\infty} F_m = F_1 + F_2 + F_3 + ...$

Es fácil ver que $D[[X_1, ..., X_n]]$ adquiere estructura de anillo conmutativo con unidad, con las operaciones dadas por:

$$\sum_{m=0}^{\infty} F_m + \sum_{m=1}^{\infty} G_m = \sum_{m=0}^{\infty} (F_m + G_m); \text{ y}$$
$$(\sum_{m=0}^{\infty} F_m)(\sum_{m=1}^{\infty} G_m) = \sum_{m=0}^{\infty} (\sum_{i+j=1}^{\infty} F_i G_j)$$

Podemos identificar al anillo de polinomios $D[X_1, ..., X_n]$ con el subanillo de $D[[X_1, ..., X_n]]$ formado por las series de términos finalmente nulos. También es claro que podemos ver a $D[[X_1, ..., X_{n-1}]]$ como subanillo de $D[[X_1, ..., X_n]]$. La forma no nula de menor grado, de una serie no nula, se llama *término inicial de la serie*. Es claro que el término inicial de un producto, es el producto de los términos iniciales; de donde se sigue en particular que $D[[X_1, ..., X_n]]$ es un Dominio íntegro. Veremos ahora, que si R es un anillo Noetheriano, entonces el anillo de series formales de potencias $R[[X]]$ es también Noetheriano.

Observación 4.3. Si $F = a_r X^r + a_{r+1} X^{r+1} + ...$, con r entero no negativo, y $a_r \neq 0$. Permitámonos decir que F tiene grado r, y coeficiente principal a_r.
Si F fuera la serie nula, diremos que su grado es infinito, y su coeficiente principal 0.

Teorema 4.4. Si R es un anillo Noetheriano, entonces el anillo de series formales de potencias $R[[X]]$ es también Noetheriano.

Demostración.

Sea I un ideal de $R[[X]]$, debemos mostrar que I está finitamente generado.
Construiremos inductivamente una sucesión de elementos f_i de $R[[X]]$ como sigue:
Sea f_1 de grado mínimo entre los elementos de I.
Supongamos que hemos elegido $f_1, ..., f_i$, en donde f_i tiene grado d_i y coeficiente principal a_i.
Elegiremos entonces f_{i+1}, cumpliendo las siguientes tres condiciones:

1. $f_{i+1} \in I$;
2. $a_{i+1} \notin \langle a_1, ..., a_i \rangle$ (ideal de R generado por los a_j $j = 1..., i$);
3. De entre todos los elementos de I que satisfacen las primeras dos condiciones, f_{i+1} es de grado mínimo.

La segunda condición fuerza al procedimiento a terminar en un número finito de pasos.
Pues de otro modo habría en R, una cadena ascendente $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset ...$, que no se estabilizaría. Esto no puede darse, puesto a que por hipótesis, R es Noetheriano.
Veremos que si la estabilización de dicha cadena ocurre en el paso k, entonces I está generado por $f_1, ..., f_k$.
Sea $g = aX^d + ..., \in I$ con coeficiente principal a y grado d.
Luego $a \in \langle a_1, ..., a_k \rangle$ *(Ver problema 1)*

- **Caso 1:** $d \geq d_k$
  Como $d_i \leq d_{i+1}$ *(Ver Problema 2)*; tenemos que $d \geq d_i$ para $i = 1..., k$.
  Ahora, como $a \in \langle a_1, ..., a_k \rangle$, $a = \sum_{i=1}^{k} c_{i_0} a_i$ para ciertos $c_{i_0} \in R$
  Definamos ahora $g_0 = \sum_{i=1}^{k} c_{i_0} X^{d-d_i} f_i$.
  Observemos que g_0 tiene grado d y coeficiente principal a, y por ende, $g - g_0$ tiene grado mayor que d.
  Se definen de este modo $g_0, ..., g_r \in \langle f_1, ..., f_k \rangle$ tales que $g - \sum_{i=0}^{r} g_i$ tiene grado mayor que $d+r$, digamos $g - \sum_{i=0}^{r} g_i = bX^{d+r+1} + ...$ *(el argumento sería análogo si el grado fuera mayor que* $d + r + 1$*)*
  Ahora, $b \in \langle a_1, ..., a_k \rangle$ *(Por problema 1 nuevamente)*. Luego $b = \sum_{i=1}^{k} c_{i_{r+1}} a_i$ para ciertos $c_{i_{r+1}} \in R$
  Definimos $g_{r+1} = \sum_{i=1}^{k} c_{i_{r+1}} X^{d+r+1-d_i} f_i$, de modo que $g - \sum_{i=0}^{r+1} g_i$ tiene grado mayor que $d+r+1$.
  Luego, $g = \sum_{r=0}^{\infty} g_r = \sum_{r=0}^{\infty} (\sum_{i=1}^{k} c_{i_r} X^{d+r-d_i} f_i)$
  Puesto a que la sumatoria interior, es finita, podemos invertir el orden de suma y concluir que $g \in \langle f_1, ..., f_k \rangle$, como queríamos ver.

- **Caso 2:** $d < d_k$
  (Esto es, Gr(g) ¡$máx\{Gr(f_i)$ $i = 1, ..., k\}$*)*
  Como antes, $a \in \langle a_1, ..., a_k \rangle$, así que habrá un m menor, entre 1 y k tal que $a \in \langle a_1, ..., a_m \rangle$.

Se sigue que $d \geq d_m$ *(Ver problema 3)*
Como en el caso 1 tenemos que $a = \sum_{i=1}^{m} c_i a_i$ con $c_i \in R$
Definimos $h = \sum_{i=1}^{m} c_i X^{d-d_i} f_i \in \langle f_1, ..., f_k \rangle$
El coeficiente principal de h es a, con lo cual el grado de $g - h$ es mayor que d.
Reemplacemos g por $g - h$ y repitamos el procedimiento...
Luego de a lo sumo $d_k - d$ iteraciones, habremos conseguido un elemento $g - \sum h_i \in I$ de grado al menos d_k, con todos los $h_i \in \langle f_1, ..., f_k \rangle$.
Luego, por el análisis del caso 1, $g \in \langle f_1, ..., f_k \rangle$. ■

4.1. Problemas propuestos

Problema 4.1. Sea $g = a_{k+1}X^d + a_{k+1}X^{d+1} + ... \in I$.
Justifique: $a_{k+1} \in \langle a_1, ..., a_k \rangle$

Por el absurdo supongamos que $a_{k+1} \notin \langle a_1, ..., a_k \rangle$.
Tenemos entonces, que $g \in I \wedge a_{k+1} \notin \langle a_1, ..., a_k \rangle$.
Luego, g es candidato a extender el proceso inductivo para la construcción de la sucesión $\{ f_i \} \subseteq R[[X]]$, en la demostración del teorema 2.4.
(Si no lo extendiera g, lo extendería otro elemento de I, de grado menor que d, y coeficiente principal a_{k+1}) ABS!!
Pues, si se extiende el proceso inductivo, la estabilización de la cadena ascendente
$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset ...$ mencionada en la demostración del teorema, no ocurriría en el paso k. Con esto, $a_{k+1} \in \langle a_1, ..., a_k \rangle$, como queríamos ver. □

Problema 4.2. Justifique: ¿Por qué $d_i \leq d_{i+1}$?

$d_i = Gr(f_i)$; $d_{i+1} = Gr(f_{i+1})$
a_i es el coeficiente principal de f_i y a_{i+1} el de f_{i+1}. *(en el sentido de que $f_j = a_jX^j + a_{j+1}X^{j+1} + ...$)*
Recordemos:

1) f_i fue elegida de modo de cumplir:
   (a) $f_i \in I$;
   (b) $a_i \notin \langle a_1, ..., a_{i-1} \rangle$;
   (c) f_i es la de menor grado cumpliendo los dos items anteriores;

2) De modo análogo f_{i+1} fue elegida de modo de verificar:
   (a) $f_{i+1} \in I$;
   (b) $a_i \notin \langle a_1, ..., a_i \rangle$;
   (c) f_{i+1} es la de menor grado cumpliendo los dos items anteriores;

Llamemos I_i al ideal generado por $a_1, ..., a_i$ y observemos que $I_i \subseteq I_{i+1}$.
Ahora si, con todas estas consideraciones previas, supongamos por el absurdo que $d_i > d_{i+1}$.
Luego f_{i+1} cumple las condiciones $1(a)$ y $1(b)$ (pues por la contención antes mencionada, si $a_{i+1} \notin I_i \Rightarrow a_{i+1} \notin I_{i-1}$). Más aún, $\text{gr}(f_{i+1}) < gr(f_i)$. Pero entonces f_i no cumple $1(c)$. ABS!!, pues f_i es la de menor grado cumpliendo $1(a)$ y $1(b)$.
El absurdo provino de suponer $d_i > d_{i+1}$; afirmamos luego que $d_i \leq d_{i+1}$. □

Problema 4.3. Justifique: ¿Por qué $d \geq d_m$?

Teníamos $g \in I$, con $\text{Gr}(g) = d$, y coeficiente principal a *(En los sentidos antes especificados).*
Por el problema 1, sabemos que $a \in \langle a_1, ..., a_k \rangle$; más aún, podemos considerar un entero menor m $(1 \leq m \leq k)$: $a \in \langle a_1, ..., a_m \rangle$ y $a \notin \langle a_1, ..., a_{m-1} \rangle$.

Supongamos por el absurdo que $\mathrm{Gr}(g) < \mathrm{Gr}(f_m)$ *(i.e,* $d < d_m$)
Luego, f_m no cumple la condición 3 de la construcción, pues no sería la de menor grado cumpliendo que:

- $f_m \in I$;
- $a_m \notin \langle a_1, ..., a_{m-1} \rangle$

Debido a que existe g de grado menor, cumpliendo los dos items anteriores. ABS!!
Luego $d \geq d_m$. □

5. Teorema de los ceros de Hilbert

Hemos observado que toda variedad define un ideal $I(V)$, y todo ideal define una variedad $V(I)$. Más que eso, si $I(V_1) = I(V_2)$, entonces $V_1 = V_2$.
Vale mencionar, que hay muchos ideales que definen la misma variedad. Por ejemplo, los ideales $\langle f \rangle$ y $\langle f^m \rangle$, no necesariamente coinciden, pero sus variedades son idénticas.
Una variedad V, es siempre expresable como $V(S)$, para cierta colección de polinomios S. Pero un ideal I, no es siempre de la forma especial $I(X)$.
El Teorema de los ceros de Hilbert *(The Hilbert Nullstellensatz)* dice que si dos ideales definen la misma variedad, entonces son iguales salvo potencias.
Más precisamente: Si $V(I_1) = V(I_2) \Rightarrow$ Si g pertenece a uno de los ideales I_i, existirá un entero positivo r, tal que g^r pertenece al otro ideal.
Otro modo de enunciar el mismo hecho es decir que I un ideal de $K[X_1, ..., X_n]$. Luego $IV(I) = \sqrt{I}$ (No se asusten, a estas instancias no conocen la definición de $\sqrt{I}$, pero esta les será dada a la brevedad).
Comencemos mostrando que todo punto de A^n determina un ideal maximal.

Lema 5.1. Si $a = (a_1, a_2, ..., a_n) \in A^n$, entonces $I = \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n \rangle$ es un ideal maximal

Demostración.

Supongamos que existe un ideal J tal que $I \subsetneq J$. Deberá suceder $J = K[X_1, ..., X_n]$.
Sea $f \in J - I$, aplicamos el algoritmo de la división como sigue:

$$\begin{aligned}
f &= A_1(X_1 - a_1) + B_1 \text{ en donde } A_1 \in K[X_1, ..., X_n] \text{ y } B_1 \in K[X_2, ..., X_n] \\
&\quad \text{(Observar que } B_1 \neq 0 \text{ (pues de lo contrario } f \in I) \\
B_1 &= A_2(X_2 - a_2) + B_2, \text{ con } A_2 \in K[X_2, ..., X_n], B_2 \in K[X_3, ..., X_n] \\
&\quad \text{(Otra vez } B_2 \text{ resulta no nulo por las mismas razones.)} \\
&\vdots \\
B_{n-1} &= A_n(X_n - a_n) + B_n, \text{ con } A_n \in K[X_n], B_n \in K \\
&\quad (B_n \neq 0)
\end{aligned}$$

Con esto, se tiene que: $f = A_1(X_1 - a_1) + A_2(X_2 - a_2) + ... + A_n(X_n - a_n) + B_n$
Ahora, como $I \subset J$, $A_1(X_1 - a_1) + A_2(X_2 - a_2) + ... + A_n(X_n - a_n) \in J$, pero además $f \in J$, luego restando llegamos a que $B_n \in J$.
Pero B_n es inversible!!, pues es un elemento no nulo del cuerpo escalar; por lo que $1 \in J$, resultando así $J = K[X_1, ..., X_n]$
Afirmamos entonces, que I es un ideal maximal. $\surd$

Definición. Sea R un anillo conmutativo, y sea I un ideal de R.
Definimos *La Raíz* del ideal I, como:

$$\sqrt{I} = \{ f \in R \text{ tal que } f^r \in I, \text{ para algún entero positivo } r \}$$

Notemos que $\sqrt{I}$ es un ideal.

Teorema 5.2. *(Teorema de los Ceros de Hilbert)*
Sea I un ideal de $K[X_1, ..., X_n]$. Luego $IV(I) = \sqrt{I}$

Demostración.

Dividiremos la demostración en dos. La parte fácil, que es la inclusión $\sqrt{I} \subseteq IV(I)$, será vista a modo de lema; la parte difícil, que es la inclusión restante, necesitará de bastante trabajo.
Para llevarla a cabo, deberemos dar un par de lemas, el llamado *Teorema Débil de los ceros* y una ingeniosa técnica conocida como ¨Truco de Rabinowitsch¨.

Lema 5.3. Si I es un ideal de $K[X_1, ..., X_n]$, entonces $\sqrt{I} \subseteq IV(I)$

Demostración.

Sean $f \in \sqrt{I}$, $x \in V(I)$. Como $f \in \sqrt{I}\, \exists n \in \mathbb{N} : f^n \in I$; y como $x \in V(I)$, $g(x) = 0\, \forall g \in I$.
Luego vale en particular, que $f^n(x) = 0 \Rightarrow f(x) = 0$.
Resulta así que $f \in I(V(I))$ como queríamos ver. $\surd$

Daremos ahora la demostración de que $IV(I) \subseteq \sqrt{I}$
Sea $f \in IV(I)$. Notemos que si I es un ideal de $K[X_1, ..., X_n]$, entonces I está finitamente generado, digamos $I = \langle f_1, ..., f_m \rangle$.
Introduzcamos una variable adicional Y, y trabajemos en $K[X_1, ..., X_n, Y]$.
Sea I^* el ideal de $K[X_1, ..., X_n, Y]$, generado por $\{f_1, ..., f_m, 1 - Yf\}$ (en donde f es la dada).
Aclaremos una ligera ambigüedad..., cuando hablemos de $f_i(X_1, ..., X_n, Y)$, nos estaremos refiriendo a $f_i(X_1, ..., X_n)$, análogamente con f.
Para seguir con la demostración, necesitamos probar los dos lemas siguientes:

Lema 5.4. Si $(a_1, ..., a_n, a_{n+1}) \in A^{n+1}$ y $(a_1, ..., a_n) \in V(I)$, entonces $(a_1, ..., a_n, a_{n+1}) \notin V(I^*)$

Demostración.

Veremos que el polinomio $1 - Yf (\in I^*)$ no se anula en $(a_1, ..., a_n, a_{n+1})$.
$(1 - Yf)((a_1, ..., a_n, a_{n+1})) = 1 - a_{n+1}f((a_1, ..., a_n))$; pero $(a_1, ..., a_n) \in V(I)$ y $f \in IV(I)$, luego $(1 - Yf)((a_1, ..., a_n, a_{n+1})) = 1 - a_{n+1}0 = 1 \neq 0$.
Con esto, $(a_1, ..., a_n, a_{n+1}) \notin V(I^*)$ $\surd$

Lema 5.5. Si $(a_1, ..., a_{n+1}) \in A^{n+1}$ y $(a_1, ..., a_n) \notin V(I)$, entonces $(a_1, ..., a_n, a_{n+1}) \notin V(I^*)$

Demostración.

Como $(a_1, ..., a_n) \notin V(I)$, se tiene que $\exists i \in \{1, ..., m\} : f_i((a_1, ..., a_n)) \neq 0$. Luego $f_i((a_1, ..., a_{n+1})) \neq 0$, pero $f_i \in I^*$, luego se afirma que $(a_1, ..., a_n, a_{n+1}) \notin V(I^*)$. $\surd$

De estos dos lemas se deduce que:
Si $(a_1, ..., a_{n+1}) \in A^{n+1}$ entonces $(a_1, ..., a_n, a_{n+1}) \notin V(I^*)$. O dicho de otro modo, $V(I^*) = \emptyset$
Necesitamos ahora del llamado *Teorema Débil de los ceros.*

Teorema 5.6. Si I es un ideal de $K[X_1, ..., X_n] : V(I) = \emptyset$, entonces $I = K[X_1, ..., X_n]$

Afirmamos entonces, por teorema precedente, que $I^* = K[X_1, ..., X_n, Y]$
Estamos ahora preparados para probar el siguiente resultado.

Lema 5.7. Existen polinomios $g_1, ..., g_m, h \in K[X_1, ..., X_n, Y]$ tales que:

$$1 = \sum_{i=1}^{m} g_i f_i + h(1 - Yf)$$

Demostración.

Hemos visto que, en virtud del teorema débil de los ceros, $I^* = K[X_1, ..., X_n, Y]$. Luego, en particular se tendrá que $1 \in I^*$.
Recordando ahora que $I^* = \langle f_1, ..., f_m, 1 - Yf \rangle$, se tendrá que $\exists g_1, ..., g_m, h \in K[X_1, ..., X_n, Y]$ tales que $1 = \sum_{i=1}^{m} g_i f_i + h(1 - Yf)$ $\surd$

Observación 5.8. La ecuación dada en el lema anterior también es válida en el cuerpo de funciones racionales, llamémoslo $K(X_1, ..., X_n, Y)$, que consiste en cocientes de polinomios de $K[X_1, ..., X_n, Y]$

Ahora sí!, llegó el momento de aplicar el ¨Truco de Rabinowitsch¨ y resolver el problema, concluyendo que $f \in \sqrt{I}$

Teorema 5.9. *(Truco de Rabinowitsch)*
El truco consiste en reemplazar la variable Y, por la variable $1/f$, de modo que la ecuación dada en el lema anterior se transforme en:

$$1 = \sum_{i=1}^{m} g_i(X_1, ..., X_n, \tfrac{1}{f(X_1,...,X_n)}) f_i(X_1, ..., X_n)$$

Observación: Supondremos $f \neq 0$
Si f fuera nula, es claro que $0 \in \sqrt{I}$, (pues $0 \in I, \forall I$ ideal)

Para justificar el reemplazo $Y = \frac{1}{f}$, consideremos el homomorfismo de anillos que va de $K[X_1, ..., X_n, Y]$ en $K(X_1, ..., X_n) : X_i \longmapsto X_i (i = 1, ..., n)$ y $Y \longmapsto \frac{1}{f(X_1,...,X_n)}$.
Aplicamos este mapeo, en la igualdad dada en el lema 4.7, resultando:

$$\begin{aligned} 1 &= (\sum_{i=1}^{m} g_i f_i + h(1 - Yf))(X_1, ..., X_n, \tfrac{1}{f}) \\ &= \sum_{i=1}^{m} g_i f_i(X_1, ..., X_n, \tfrac{1}{f(X_1,...,X_n}) + h(1 - Yf)(X_1, ..., X_n, \tfrac{1}{f(X_1,...,X_n)}) \\ &= \sum_{i=1}^{m} g_i(X_1, ..., X_n, \tfrac{1}{f}) f_i(X_1, ..., X_n) \end{aligned}$$

Pues, observemos que:

$$\begin{aligned} h(1 - Yf)(X_1, ..., X_n, \tfrac{1}{f}) &= h(X_1, ..., X_n, \tfrac{1}{f}) - h(X_1, ..., X_n, \tfrac{1}{f}) \tfrac{1}{f(X_1,...,X_n)} f(X_1, ..., X_n) \\ &= h - h(X_1, ..., X_n, \tfrac{1}{f}) \\ &= 0. \end{aligned}$$

Hemos llegado así, a una suma finita de funciones racionales cuyos denominadores son potencias de f.
Sea r el mayor exponente al que se encuentra elevado f.
Multiplicando a ambos lados de la igualdad obtenida unas líneas arriba, logramos absorver todos los denominadores resultando:

$$f^r = \sum_{i=1}^{m} h_i(X_1, ..., X_n) f_i(X_1, ..., X_n)$$

Luego, como los $h_i\acute{}s \in K[X_1, ..., X_n]$ y los $f_i\acute{}s \in$ el ideal I , concluímos con claridad que $f^r \in I$, con lo cual $f \in \sqrt{I}$ como queríamos ver.

De este modo se afirma que $IV(I) \subseteq \sqrt{I}$, y finalmente que $IV(I) = \sqrt{I}$, quedando así concluida, la demostración del Teorema de los Ceros de Hilbert. ■

Lema 5.10. *(Lema de normalización de Noether)*
Sea A una K-álgebra finitamente generada, siendo K un cuerpo;
Es decir, existen finitos elementos $x_1, ..., x_n$ que generan a A sobre el cuerpo K, en el sentido de que todo elemento de A es un polinomio en las x_i; o equivalentemente, A es imagen del anillo de polinomios $K[X_1, ..., X_n]$ por el homomorfismo determinado por: $X_i \longmapsto x_i, i = 1, ..., n$.
Luego,$\exists\{y_1, ..., y_r\} \subseteq A$ tal que los $y_i\acute{}s$ son algebraicamente independientes sobre K, y A es integral sobre $K[y_1, ..., y_r]$.

Demostración.
Sea $\{x_1, ..., x_r\}$ un subconjunto algebraicamente independiente y maximal de $\{x_1, ..., x_n\}$.

- Si $n = r$, tomamos $y_i = x_i \forall i$ y listo!, pues si $a \in A, \exists p \in K[X_1, ..., X_n] : a = p(x_1, x_2, ..., x_n) \Rightarrow a \in K[x_1, ..., x_n]$. Más aún a es raiz de $X - a$, que claramente es un polinomio mónico con coeficientes en $K[x_1, ..., x_n]$.
  Resulta así que A es integral sobre $K[y_1, ..., y_r]$

- Si $r < n$, resulta que $x_1, ..., x_n$ son algebraicamente dependientes sobre K; luego, $\exists f \in K[X_1, ..., X_n] : f \neq 0 \wedge f(x_1, ..., x_n) = 0$.
  Observación: Supondremos $n > 1$, ya que si $n = 1, r$ sería 0, resultaría $A = K[x_1]$, y podríamos tomar $\{y_1, ..., y_r\} = \emptyset$.

  - Consideraremos primero el caso en el que K es un cuerpo con infinitos elementos.
    Daremos una prueba por inducción sobre n.
    Descompongamos a f en sus componentes homogéneas (cada una de ellas, es suma de monomios de igual grado).
    Llamemos g a la componente homogénea de mayor grado (digamos d).
    Luego, mirando a g como un polinomio en la variable X_n, con coeficientes en el anillo de polinomios $K[X_1, ..., X_{n-1}]$, tenemos (renombrando variables si es necesario), que $g(X_1, ..., X_{n-1}, 1) \neq 0$.
    Ahora, siendo K un cuerpo con infinitos elementos, sabemos por proposición 2.4 inciso 4, que $I(A^n) = \{0\}$ (Esto dice que el único polinomio que se anula en todos lados es el pol. nulo); luego, para g deberán existir $a_1, ..., a_{n-1} \in K : g(a_1, ..., a_{n-1}, 1) \neq 0$
    Definamos $z_i = x_i - a_i x_n, i = 1..., n - 1$, y reemplacemos en $f(x_1, ..., x_n) = 0$, para obtener una ecuación de la forma:

$$g(a_1, ..., a_{n-1}, 1)x_n^d + \text{términos de grado menor que } d \text{ en la variable } x_n = 0$$

Ejemplo 5.11. : Daremos un ejemplo concreto de esta construcción, para intentar clarificar ideas...
Supongamos que tenemos $f(x_1, x_2) = x_1^2 x_2^3 \Rightarrow g(x_1, x_2) = f(x_1, x_2)$
Se tendrá entonces un único z_i, que es $z_1 = x_1 - a_1 x_2$, luego $x_1 = z_1 + a_1 x_2$.
Reemplazando obtenemos:

$$\begin{aligned} x_1^2 x_2^3 &= (z_1 + a_1 x_2)^2 x_2^3 \\ &= (z_1^2 + 2 z_1 a_1 x_2 + a_1^2 x_2^2) x_2^3 \\ &= z_1^2 x_2^3 + 2 z_1 a_1 x_2^4 + a_1^2 x_2^5 \\ &= g(a_1, 1) x_2^5 + \underbrace{(z_1^2 x_2^3 + 2 z_1 a_1 x_2^4)}_{\text{Términos de grado} < 5 \text{ en } x_2} \end{aligned}$$

Sigamos con lo nuestro...

Siendo $g(a_1, ..., a_n, 1) \neq 0$, podemos dividir la expresión obtenida anteriormente por ello, y obtener:

$$x_n^d + \frac{\text{términos de grado menor que } d \text{ en la variable } x_n}{g(a_1, ..., a_n, 1)} = 0$$

Con lo que claramente x_n es raíz de un polinomio mónico con coeficientes en $K[z_1, ..., z_{n-1}]$.
Concluímos así x_n integral sobre $B = K[z_1, ..., z_{n-1}]$
Luego, por hipótesis inductiva, existen $y_1, ..., y_r$ algebraicamente independientes sobre K tal que B es integral sobre $K[y_1, ..., y_r]$. Además los x_i con $i < n$, son integrales sobre B, pues $x_i = z_i + a_i x_n$.
Luego por transitividad, $x_1, ..., x_n$ son integrales sobre $K[y_1, ..., y_r]$ (Teo 1.18 preliminares)
Finalmente concluímos A integral sobre $K[y_1, ..., y_r]$ (Ash 7.1.5)

Ahora, nos ocuparemos del caso general, tomando k arbitrario.
Como antes, $r < n \Rightarrow \exists f \in k[X_1, ..., X_n]$ tq $f(x_1, ..., x_n) = 0$.
Consideremos un escalar s, que sea mayor que la suma de los grados de todos los monomios de f, y definamos el *'peso de cada variable X_i '* como:

$$w_i = s^{n-i} \text{ (notemos que, si } i > j, \Rightarrow w_i < w_j).$$

Definamos ahora, el *'peso de un monomio '*.
Sea $h = b X_1^{a_1} ... X_n^{a_n}$, llamaremos 'peso de h ' a:

$$w(h) = \sum_{i=1}^{n} a_i w_i.$$

Si g es otro monomio, advertimos que $w(h) > w(g) \Leftrightarrow h \succ g$ considerando el orden lexicográfico (i.e., $h \succ g$ si al comparar los grados de las variables en h con los grados de las variables en g en forma ordenada, (primero los de X_1, luego los de X_2....., y por último los de X_n), se tiene que para algún m, las potencias de las variables en h y g son iguales $\forall i \leq m$, y el grado de la variable X_{m+1} en h es mayor que en g).
Con esto, si dos monomios h, g son tales que $h \succ g \wedge g \succ h$, entonces, tendrán diferentes pesos.

Ahora consideramos el monomio de mayor peso, digamos h.
Como antes, planteamos:

$$z_i = x_i - {x_n}^{w_i},\ 1 \leq i \leq n-1$$

e introducimos esto en $f(x_1, ..., x_n)$ para obtener:

$$c{x_n}^{w(h)} + \text{términos de grado menor en la variable } x_n = 0$$

Luego, x_n es integral sobre $B = k[z_1, ..., z_{n-1}]$.
Como en el caso anterior, existirán $y_1, ..., y_r$ algebraicamente independientes sobre k tal que B es integral sobre $k[y_1, ..., y_r]$.
Ahora, siendo $x_i = z_i - {x_n}^{w(h)}$ se tiene que x_i es integral sobre $k[y_1, ..., y_r] \forall i, : 1 \leq i \leq n$.
Luego, como en la demostración anterior, concluimos que $x_1, ..., x_n$ son integrales sobre $k[y_1, ..., y_r]$ y, finalmente, que A es integral sobre $k[y_1, ..., y_r]$ como queríamos ver. $\surd$

Corolario 5.12. Sea B una $k-$álgebra finitamente generada, con k cuerpo.
Se afirma que si I es un ideal maximal de B, entonces B/I es una extensión finita del cuerpo k

Demostración.

Consideremos el mapeo $\sigma : K \to B/I$, definido como $\sigma(c) = c+I$ y veamos que resulta inyectivo.
Supongamos que $\sigma(c) = \sigma(c') \Rightarrow c + I = c' + I \Rightarrow c - c' + I = 0 + I \Rightarrow c - c' \in I$.
Ahora, si $b = c - c'$ fuera distinto de cero, existiría $b^{-1} \in B$ tal que $bb^{-1} = 1$ pertenecería a I por ser este ideal. ABS!!! (pues I maximal implica I propio, por lo que $1 \notin I$).
Luego $c - c' = 0$, con lo que resulta $c = c'$, y por ende σ inyectiva. Esto nos dice, que K puede ser 'visto´dentro de B/I.

Por otro lado, B/I es una k-álgebra finitamente generada, con lo que por teorema anterior, $\exists\{y_1, ..., y_r\} \in B/I$ algebraicamente independientes sobre K, tales que B/I es integral sobre $K[y_1, ..., y_r]$. Además, siendo I maximal, por teorema 1.6, resulta que B/I es cuerpo.
Tenemos entonces que B/I cuerpo y B/I integral sobre $K[y_1, ..., y_r]$. Luego, por teorema 1.20, se deduce que $K[y_1, ..., y_r]$ es cuerpo. Veremos que esto no puede suceder si $r \geq 1$, demostrando que $y_1 \in K[y_1, ..., y_r]$, pero $\frac{1}{y_1}$ no.
Por el absurdo supongamos que $\frac{1}{y_1} \in K[y_1, ..., y_r]$. Luego $\exists g \in K[X_1, ..., X_r] : g(y_1, ..., y_r) = \frac{1}{y_1}$, pero entonces $y_1 g(y_1, ..., y_r) = 1$ y $y_1 g(y_1, ..., y_r) - 1 = 0$.
Es decir, existe un polinomio no nulo, que evaluado en $(y_1, ..., y_r)$ se anula. ABS!!!
pues se contradice el hecho de que $\{y_1, ..., y_r\}$ es algebraicamente independiente.

Se concluye así, que si $K[y_1, ..., y_r]$ es cuerpo, entonces r debe ser 0.
Con esto $K[y_1, ..., y_r] = K$; resultando B/I es integral sobre K, y por teorema ende, B/I algebraico sobre K.

Recapitulando..., hemos llegado a que $K \ \ddot{}\subseteq \ddot{}B/I$, B/I finitamente generado sobre K, y B/I algebraico sobre K.
Luego, por teorema 1.24, se afirma que B/I es una extensión finita de K. $\clubsuit$

Corolario 5.13. Sea A una k-álgebra finitamente generada, con k cuerpo. Afirmamos que:
Si A es un cuerpo, entonces A es una extensión finita de k.

Demostración.

La demostración es análoga a la del corolario anterior, tomando A en lugar de B/I. $\clubsuit$

5.1. Problemas propuestos

Problema 5.1. Sea S un subconjunto multiplicativo del anillo R.
Si I es un ideal disjunto con S, entonces por el lema de Zorn, existe un ideal J que es maximal entre los ideales disjuntos de S.
Muestre que J debe ser primo.

Por el absurdo, supongamos que J no es primo. Luego, existen $x, y \notin J : xy \in J$.
Dado que J es un ideal maximal, de entre todos los ideales disjuntos con S, se tiene que $\forall a \notin J$, el ideal $J + \langle a \rangle$ contendrá al menos un elemento de S.
Consideremos entonces los ideales $I_x = J + \langle x \rangle$ e $I_y = J + \langle y \rangle$.
Por lo dicho anteriormente, deben existir $s_1 \in I_x : s_1 \in S \wedge s_1 \notin J$ y $s_2 \in I_y : s_2 \in S \wedge s_2 \notin J$.
Ahora, $s_1 s_2 \in (J + \langle x \rangle)(J + \langle y \rangle)$, pero observemos que :

(a) $(J + \langle x \rangle)(J + \langle y \rangle) \subseteq J + \langle xy \rangle$

(b) $J + \langle xy \rangle \subseteq J$

Con esto, el elemento $s_1 s_2 \in J$, y además pertenece a S, pues tanto s_1 como $s_2 \in S$, y S es multiplicativo. Pero entonces $s_1 s_2 \in S \cap J$ ABS!! (Recordar que J es disjunto con S).
El absurdo provino de suponer que J no era primo; concluímos finalmente, J ideal primo.
Veamos (a), (b) para tranquilidad del lector.

(a) Sea $z \in (J + \langle x \rangle)(J + \langle y \rangle) \Rightarrow \exists z_1 \in J + \langle x \rangle \wedge z_2 \in J + \langle y \rangle : z = z_1 z_2$
$\Rightarrow \exists j_1 \in J \wedge ax \in \langle x \rangle : z_1 = j_1 + ax \wedge j_2 \in J \wedge by \in \langle y \rangle : z_2 = j_2 + by$
$\Rightarrow z_1 z_2 = (j_1 j_2 + j_1 by + j_2 ax) + (abxy)$, que claramente pertenece a $J + \langle xy \rangle$

(b) Supongamos que $J + \langle xy \rangle \nsubseteq J$
$\Rightarrow \exists z \in J + \langle xy \rangle : z \notin J$
$\Rightarrow z = j_1 + axy$, con $j_1 \in J, \ \ a \in R$
$\Rightarrow z \in J$ ABS!! (No olvidemos que el elemento $xy \in J$) □

Problema 5.2. Muestra que $\sqrt{I}$ es la intersección de todos los ideales primos que contienen a I.
Sugerencia: Si $f^r \in I \subseteq P, P$ primo, entonces $f \in P$. Recíprocamente, asuma que $f \notin \sqrt{I}$; con una elección inteligente de un conjunto multiplicativo S, muestre que para algún ideal primo P que contenga a I, se tiene que $f \notin P$.

Sea A=$\{P_i : P_i$ es un ideal primo que contiene a $I\}$, debemos ver que $\sqrt{I} = \bigcap_{P_i \in A} P_i$.

($\subseteq$) Sea $f \in \sqrt{I}$, y sea $P \in A$. Queremos ver que $f \in P$.
Como $f \in \sqrt{I}, \exists r \in N : f^r \in P$, observemos entonces que:

- Si $r = 1$. Listo! y $f \in P$
- Si $r > 1$, asociamos y $f = f f^{r-1}$.
  Siendo P primo, se tiene que $f \in P \vee f^{r-1} \in P$

- Si $f \in P$ Listo!
- Si $f^{r-1} \in P \Rightarrow f^{r-1} = ff^{r-2}$
  - Si $f \in P$ Listo!
  - Si no, entonces $f^{r-2} \in P$

$$\vdots$$

Continuando el razonamiento, y siendo $r < \infty$, en a lo sumo $r-1$ pasos, afirmaremos con toda certeza que $f \in P$.

($\supseteq$) Por el absurdo, supongamos que $\bigcap_{P_i \in A} P_i \nsubseteq \sqrt{I}$. Luego, $\exists f \in \bigcap_{P_i \in A} P_i : f \notin \sqrt{I}$
Consideremos el conjunto multiplicativo S=$\{ 1, f, f^2, ..., f^r, ...\}$
Observemos que $S \cap I = \emptyset$, pues, si $f^n \in I$ para algún n, entonces f pertenecería a $\sqrt{I}$, y esto no sucede.
Como en el ejercicio anterior, podemos afirmar la existencia de un ideal J primo y maximal entre todos los ideales disjuntos con S; luego siendo I disjunto con S, se tendrá en particular que $I \subseteq J$.
Ahora, por un lado, f debe pertenecer a J, pues J es un ideal primo que contiene a I (con lo cual $J \in A$); pero por otro lado $f \notin J$, pues $f \in S$, y J y S son disjuntos. ABS!!
El absurdo provino de suponer que $\bigcap_{P_i \in A} P_i \nsubseteq \sqrt{I}$. Se tiene entonces que $\bigcap_{P_i \in A} P_i \subseteq \sqrt{I}$ y afirmamos finalmente, válida la igualdad. □

Problema 5.3. Una *Curva algebraica* es una variedad definida por un polinomio no constante en dos variables.
Muestra, usando el Teorema de los Ceros, que dos polinomios f y g, definen la misma curva algebraica sii f divide a alguna potencia de g y g divide a alguna potencia de f (i.e, f y g, tienen los mismos factores irreducibles).

($\Rightarrow$) Sean $f, g \in K[X,Y]$, dos polinomios no constantes tal que $V(f) = V(g)$, entonces, $I(V(f)) = I(V(g))$, y por teorema de los ceros, $\sqrt{\langle f \rangle} = \sqrt{\langle g \rangle}$.
Luego, como $f \in \sqrt{\langle f \rangle}$ (pues, $\exists 1 \in N : f^1 \in \langle f \rangle$); se tendrá que $f \in \sqrt{\langle g \rangle}$, con lo cual $\exists n \in N : f^n \in \langle g \rangle$. Esto es $f^n = qg$, con $q \in K[X,Y]$.
Afirmamos entonces que g divide a una potencia de f.
Del mismo modo, se probaría que f divide a una potencia de g.

($\Leftarrow$) f divide a una potencia de $g \Rightarrow \exists q_1 \in K[X,Y] : g^n = q_1 f$, para algún$n \in N$.
g divide a una potencia de $f \Rightarrow \exists q_2 \in K[X,Y] : f^r = q_2 g$, para algún $r \in N$.
Veamos que $V(f) = V(g)$.
($\subseteq$) Sea $x \in V(\langle f \rangle)$, entonces $\forall h \in \langle f \rangle\, h(x) = 0$, en particular para $q_1 f \in \langle f \rangle$, $q_1 f(x) = 0$.
Luego $g^n(x) = 0$ y por tanto $g(x) = 0$. Finalmente concluimos que $x \in V(\langle g \rangle)$.
($\supseteq$) Se prueba análogamente.

Afirmamos entonces, que f y g definen la misma curva algebraica. □

Problema 5.4. Muestre que la variedad V definida sobre los números complejos por los polinomios $y^2 - xz$ y $z^2 - x^2 y$, es $L \cup W$. Siendo L =$\{(x,y,z) : y = z = 0\}, W$ =$\{(t^3, t^4, t^5), t \in \mathbb{C}\}$.

($\supseteq$) Veamos que $L \cup W \subseteq V$.

- Afirmamos que $L \subseteq V$; veámoslo:
  Sea $(x, y, z) \in L$, luego $y = z = 0 \Rightarrow (x, y, z) = (x, 0, 0)$
  Para ver que tal punto pertenece a V, veremos que las dos ecuaciones polinomiales dadas se anulan en él.

  a) $0^2 - x0 = 0$
  b) $0^2 - x^2 0 = 0$

  Luego $(x, y, z) \in V$. Queda demostrado que $L \subseteq V$

- Afirmamos que $W \subseteq V$;veámoslo:
  Sea $w \in W$, luego $w = (t^3, t^4, t^5)$ para algún $t \in \mathbb{C}$.

  Como antes, verificamos que las dos ecuaciones polinomiales dadas se anulan en w:

  a) $(t^4)^2 - t^3 t^5 = t^8 - t^8 = 0$
  b) $(t^5)^2 - (t^3)^2 t^4 = t^{10} - t^6 t^4 = t^{10} - t^{10} = 0$

  Luego $w \in V$.Queda demostrado que $W \subseteq V$.

Finalmente, $L \subseteq V \wedge W \subseteq V \Rightarrow L \cup W \subseteq V$.

($\subseteq$) Veamos que $V \subseteq L \cup W$.
Sea $(x, y, z) \in V \Rightarrow y^2 - xz = 0 \wedge z^2 - x^2 y = 0$,

- Si $x = 0$
  Como $y^2 - xz = 0 \Rightarrow y^2 = 0 \Rightarrow y = 0$.
  Por otro lado, como $z^2 - x^2 y = 0 \Rightarrow z^2 = 0 \Rightarrow z = 0$.
  Luego, $(x, y, z) = (0, 0, 0) \Rightarrow (x, y, z) \in L \cup W$

- Si $x \neq 0$
  Despejamos z y z^2 de las ecuaciones polinomiales que definen a nuestra variedad, para obtener:
  $z = \frac{y^2}{x}$ (1)
  $z^2 = x^2 y$ (2)

  - Si $y = 0$, entonces $z = 0$ (por(1)) .
    Luego $(x, y, z) = (x, 0, 0)$, con lo cual $(x, y, z) \in L$ y por ende en $L \cup W$.
  - Si $y \neq 0$.
    Definamos $t = \frac{y}{x}$
    Luego (1) y (2), pueden reescribirse como:
    $z = \frac{y^2}{x} = (\frac{y^2}{x^2})x = (\frac{y}{x})^2 x = t^2 x$
    $z^2 = x^2 y$
    Con esto, igualando z^2, $t^4 x^2 = x^2 y$, y siendo $x \neq 0$ resulta, $y = t^4$;
    Por otro lado, $t = \frac{y}{x} \Rightarrow t = \frac{t^4}{x}$ y siendo $y \neq 0 (t \neq 0)$, resulta $x = t^3$;

Por último, podemos reemplazar x e y, en cualquiera de las ecuaciones polinómicas originales, para obtener $z = t^5$.

Finalmente, ha resultado que $v = (t^3, t^4, t^5)$. Con lo cual, $v \in W \Rightarrow v \in L \cup W$.
Luego $V \subseteq L \cup W$, resultando así $V = L \cup W$. □

Problema 5.5. Llamamos *Cubo torcido* a la variedad V, definida sobre los números complejos por $y - x^2$ y $z - x^3$. En forma paramétrica, esta puede expresarse como $V = \{(t, t^2, t^3) : t \in \mathbb{C}\}$.
Muestra que V es irreducible.
(El mismo argumento funciona para cualquier variedad que pueda ser parametrizada sobre un cuerpo infinito).

En los ejercicios 1-4, de la sección 2, hemos demostrado que una variedad V es irreducible sii $I(V)$ es un ideal primo. Demostraremos entonces, este hecho equivalente.
Sea $fg \in I(V)$. Debemos ver que $f \in I(V) \vee g \in I(V)$. Esto es que $\forall x \in V, f(x) = 0 \vee g(x) = 0$.
Como $fg \in I(V)$, se tiene que $\forall x \in V, fg(x) = f(x)g(x) = 0$
Usando la forma paramétrica de V, esto se traduce como, $f(t, t^2, t^3)g(t, t^2, t^3) = 0 \, \forall t \in \mathbb{C}$.
Notemos ahora que tanto $f(t, t^2, t^3)$ como $g(t, t^2, t^3)$, son polinomios en una variable, sobre el cuerpo C, digamos $\tilde{f}, \tilde{g}$.
Luego, siendo $\tilde{f}(t)\tilde{g}(t) = 0 \, \forall t \in \mathbb{C}$, afirmamos que $\tilde{f}(t) = 0 \vee \tilde{g}(t) = 0 \forall t \in \mathbb{C}$.
Esto es $f(t, t^2, t^3) = 0 \vee g(t, t^2, t^3) = 0 \, \forall t \in \mathbb{C}$, o dicho de otro modo, $f(x) = 0 \vee g(x) = 0 \, \forall x \in V$.
Afirmamos así, que $I(V)$ es un ideal primo, y por ende, V es una variedad irreducible. □

6. El teorema de los ceros: Versiones equivalentes

Teorema 6.1. Para cualquier cuerpo K, y para todo entero positivo n, son equivalentes:

1. *Teorema de los ideales maximales*
   Los ideales maximales de $K[X_1, ..., X_n]$, son de la forma:

   $$M = \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n \rangle$$

   Luego, como $(a_1, ..., a_n) \in K^n$, los ideales maximales se corresponden con puntos.

2. *Teorema Débil de los ceros*
   Si I es un ideal de $K[X_1, X_2, ..., X_n]$ y si $V(I) = \emptyset$, entonces $I = K[X_1, X_2, ..., X_n]$.
   Equivalentemente, podemos decir que si I es un ideal propio, etonces $V(I) \neq \emptyset$.

3. *Teorema de los ceros*
   Si I es un ideal de $K[X_1, ..., X_n]$, entonces $\sqrt{I} = I(V(I))$

4. K es algebraicamente cerrado.

Demostración.
(1) $\Rightarrow$ (2) Sea I un ideal propio de$K[X_1, ...X_n]$. (Queremos ver que $V(I) \neq \emptyset$).
Siendo $K[X_1, ..., X_n]$ un anillo conmutativo con unidad y siendo $I \neq K[X_1, ..., X_n]$, sabemos por teorema 1.4 de las preliminares, que $\exists$ un ideal maximal J, tal que $I \subseteq J$.
Luego existirá, por hipótesis, un punto $a = (a_1, ..., a_n) \in A^n$, tal que $J = \langle X_1 - a_1, ..., X_n - a_n \rangle$.
Pero entonces, por proposición 2.3 insiso 2, resulta que $V(J) \subseteq V(I)$; luego para ver que $V(I) \neq \emptyset$, bastará ver que $V(J) \neq \emptyset$. Veamos que $a = (a_1, ..., a_n) \in V(J)$.
Sea $f \in J$, luego $\exists k_1, ..., k_n \in K[X_1, ..., X_n] : f = k_1(X_1 - a_1) + ... + k_n(X_n - a_n)$
$\Rightarrow f(a) = k_1(a)(0_k) + ... + k_n(a)(0_k) = 0_k$
Luego, $a \in V(J)$, y por ende $a \in V(I)$.
Finalmente afirmamos que $V(I) \neq \emptyset$.
Obs:*Puede verse que en realidad* $V(J)$=$\{a\}$

(2) $\Rightarrow$ (3) (Fue probado en la sección anterior).

(3) $\Rightarrow$ (2) Sea I un ideal propio. Queremos ver que $V(I) \neq \emptyset$.
Por teorema 1.4 de las preliminares, sabemos que $\exists$ un ideal maximal J,tal que $I \subseteq J$; además por teorema 1.8, tb de las preliminares, J resulta ser un ideal primo.
Con esto, J es un ideal primo que contiene a I.
Ahora, por ejercicio 2 de la sección anterior, sabemos que $\sqrt{I}$ es igual a la intersección de todos los ideales primos que contienen a I. Luego $\sqrt{I} \subseteq J$, con lo que se sigue, por hipótesis, que $I(V(I)) \subseteq J$.
Supongamos por el absurdo que $V(I) = \emptyset$; luego, por proposición 2.4, inciso 3, resulta que
$I(V(I)) = K[X_1, ..., X_n]$; pero entonces $J = K[X_1, ..., X_n]$. ABS!!
Pues por definición de ideal maximal, $J \neq K[X_1, ..., X_n]$.
Luego, $V(I) \neq \emptyset$, como queríamos ver.

(2) $\Rightarrow$ (1) Sea I un ideal maximal de $K[X_1, ..., X_n]$.
Queremos ver que $I = \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n\rangle$, para ciertos $a_i \in K$.
Observemos que en particular I es un ideal propio, con lo que por hipótesis, resulta $V(I) \neq \emptyset$.
Luego $\exists a = (a_1, ..., a_n) \in A^n : a \in V(I)$, i.e, $\forall f \in I, f(a) = 0$, o dicho de otro modo, tal que $I \subseteq I(\{a\})$.
Si pudiéramos ver que $I(\{a\}) = \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n\rangle$, podríamos concluir que
$I = \langle X_1 - a_1, ..., X_n - a_n\rangle$, pues:
siendo $\langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n\rangle$ maximal (lema 4.1), es en particular distinto de $K[X_1, ..., X_n]$;
Luego aplicando la definición de ideal maximal a I, se deduce lo esperado.

Veamos $I(\{a\}) = \langle X_1 - a_1, X_2 - a_2, ., X_n - a_n\rangle$.
($\subseteq$) Sea $f \in I(\{a\})$, aplicando el algoritmo de la división como en la demostración del lema 4.1, podemos descomponer a f como:
$f = A_1(X_1 - a_1) + A_2(X_2 - a_2) + ... + A_n(X_n - a_n) + b$, con $b \in K$
Ahora, $f(a) = A_1(a)(a_1 - a_1) + ... + A_n(a)(a_n - a_n) + b = 0 \Rightarrow b = 0$.
Luego $f = A_1(X_1 - a_1) + A_2(X_2 - a_2) + ... + A_n(X_n - a_n)$, con lo cual $f \in \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n\rangle$.

($\supseteq$) Sea $f \in \langle X_1 - a_1, X_2 - a_2, ..., X_n - a_n\rangle$, luego $f = A_1(X_1 - a_1) + A_2(X_2 - a_2) + ... + A_n(X_n - a_n)$, pero entonces $f(a) = 0$, con lo cual $f \in I(\{a\})$.
Queda así probada la igualdad, así como también la implicación.

(1) $\Rightarrow$ (4) Queremos ver K algebraicamente cerrado.
Por el absurdo, supongamos que existe un polinomio no constante en $K[X_1]$, sin raíz en K.
Mirando a f como un polinomio en n variables, resulta que f no tiene raíz en A^n.
Consideremos $\langle f\rangle$. Por teorema 1.4 de las preliminares, sabemos que existe un ideal maximal M, tal que $\langle f\rangle \subseteq M$ (notar que esto en particular nos dice que $f \in M$).
Además por hipótesis, deberá existir un $a = (a_1, ..., a_n) \in A^n : M = \langle X_1 - a_1, ..., X_n - a_n\rangle$.
Ahora, hemos observado en a demostración de (2) $\Rightarrow$ (1) que $M = I(\{a\})$. Luego, como $f \in M$, se tiene que $f \in I(\{a\})$, pero entonces $f(a) = 0$! ABS!!, pues f no tenía raíz en A^n.
El absurdo provino de suponer que K no era algebraicamente cerrado.
Concluimos entonces, K algebraicamente cerrado.

(4) $\Rightarrow$ (1) Sea I un ideal maximal de $K[X_1, ..., X_n]$.
Consideremos $B = K[X_1, ..., X_n]/I$ y observemos que siendo I maximal, resulta por teorema 1.6, que B es cuerpo.
Definamos ahora el siguiente mapeo:

$$\sigma : K \to B \text{ dado por } \sigma(c) = c + I$$

Afirmamos que, siendo este inyectivo, B contiene una copia de K, digamos, K '$\subseteq$´B.
Veamos que también, B '$\subseteq$´ K.
Por corolario 4.12, B resulta ser una extensión finita de K, y por teoerma 1.24, B es extensión algebraica de K.
Esto dice que $\forall b \in B, \exists f_b$ polinomio no constante de $K[X] : f_b(b) = 0$
Veamos que siendo K algebraicamente cerrado, resulta que b '$\in$ ´$K(\forall b \in B)$, en el sentido de que todo b de B es imagen por σ de algún $k \in K$.
Supongamos que el grado de f_b es $n > 0$. Siendo K algebraicamente cerrado, se tiene que la descomposición de f_b en polinomios irreducibles de $K[X]$, tiene la forma

$$f_b = c(X - a_1)^{r_1}(X - a_2)^{r_2}...(X - a_l)^{r_l}$$

Con $c, a_i \in K$ y $r_i \geq 0 \, \forall i \in \{1, ..., l\}$, y además $\sum_{i=1}^{l} r_i = n$.
Recordemos ahora que K puede ser 'visto´ dentro de B, con lo que en particular, puede mirarse a las a_i dentro de B.

¿Puede suceder que f_b tenga raíces en B, diferentes a las que se identifican con las a_i?
Por el absurdo supongamos que $\exists u \in B : f_b(u) = 0 \wedge u$'$\neq$´$a_i$´s
Luego, $(X - a_1)^{r_1}...(X - a_l)^{r_l}(X - u)$ '$\in$´$B[X]$, y divide a f_b.
Pero entonces, $\text{Gr}(f_b) \geq n + 1$ ABS! (recordar que el grado de f_b es n)

Luego, $\forall b \in B, \exists a \in K : b$ se identifica con a vía σ. Observar que esto nos dice que B '$\subseteq$´K.

Concluímos de todo esto, que K'$=$´B, en el sentido de que $B \subseteq \sigma(K)$ y B contiene una copia de K vía el mapeo dado por σ.
Luego, $\forall X_i + I \in B, \exists a_i \in K : X_i + I = \sigma(a_i) = a_i + I$,
entonces $(X_i - a_i) + I = 0 + I$, con lo cual resulta que $X_i - a_i \in I$.
Notar que esto sucede para todo $i = 1, ..., n$, por lo que $\langle X_1 - a_1, ..., X_n - a_n \rangle \subseteq I$.
Pero por lema 4.1 $\langle X_1 - a_1, ..., X_n - a_n \rangle$ es maximal!!,
Afirmamos finalmente que $\langle X_1 - a_1, ..., X_n - a_n \rangle = I$ ■

Corolario 6.2. Si los ideales I y J definen la misma variedad, y un polinomio g pertenece a uno de los ideales, entonces alguna potencia de g pertenece al otro ideal.

Demostración.
Por hipótesis $V(I) = V(J) \Rightarrow IV(I) = IV(J) \Rightarrow$, por teorema de los ceros $\sqrt{I} = \sqrt{J}$.
Sea $g \in I$, luego $g \in \sqrt{I}$, pues $\exists 1 \in N : g^1 \in I$. Pero entonces $g \in \sqrt{J}$, es decir, $\exists r \in \mathbb{N} : g^r \in J$, como queríamos ver. ♣

Corolario 6.3. Todo ideal radical, es el ideal de alguna variedad.
i.e $\forall J$ ideal, tal que $J = \sqrt{J}, \exists V$, variedad, tal que $J = I(V)$.

Demostración. .

- Antes que nada..., dada una variedad V, veamos que efectivamente $I(V)$ es un ideal radical (i.e $I(V) = \sqrt{I(V)}$)

  ($\subseteq$) Sea $f \in I(V)$, luego, existe $1 \in \mathbb{N} : f^1 \in I(V)$, entonces $f \in \sqrt{I(V)}$.

  ($\supseteq$) Sea $f \in \sqrt{I(V)}$, luego, $\exists r \in \mathbb{N} : f^r \in I(V)$, con lo cual, $f^r(x) = 0 \; \forall x \in V$, pero entonces $f(x) = 0 \; \forall x \in V$, resultando así, $f \in I(V)$.

- Veamos ahora la existencia de una variedad V, tal que el ideal radical J sea $J = I(V)$.

  Se tiene J ideal, tal que $J = \sqrt{J}$.
  Por Teorema de los ceros, sabemos que $IV(J) = \sqrt{J}$ que por hipótesis resulta ser igual a J.
  Luego, para todo ideal radical J, existe la variedad $V(J)$, cumpliendo que $I(V(J)) = J$ ♣

Corolario 6.4. Sean $f_1, ..., f_r, g \in K[X_1, ..., X_n]$, y asumamos que g se anula en donde se anulan todas las f_i.
Luego existen polinomios $h_1, ..., h_r \in K[X_1, ..., X_n]$ y un entero positivo s tal que $g^s = h_1 f_1 + ... + h_r f_r$.

Demostración.

Sea $I = \langle f_1, f_2, ..., f_r \rangle$.
Luego, $V(I) = V(\{f_1, ..., f_r\}) = \{x \in A^n : f_i(x) = 0 \ \forall i = 1, ..., r\}$ y por ende,
$IV(I) = \{g : g(x) = 0, \forall x \in V(I)\}$ resulta ser el conjunto de polinomios que se anulan en donde se anulan todas las f_i. Además, por el teorema de los ceros $IV(I) = \sqrt{I}$.
Luego, si g pertenece al conjunto de polinomios que se anulan en donde se anulan las f_i, entonces $g \in IV(I) = \sqrt{I}$; con lo cual, $\exists s \in \mathbb{N} : g^s \in I$, y siendo $I = \langle f_1, ..., f_r \rangle$, deberán existir $h_1, ..., h_r \in K[X_1, ..., X_n] : g^s = h_1 f_1 + ... + h_r f_r$ como queríamos ver. ♣

6.1. Problemas propuestos

Problema 6.1. Sea $f \in K[X_1, ..., X_n]$ y asumamos que la factorización de f en polinomios irreducibles es $f = f_1^{n_1}...f_r^{n_r}$.
Muestra que la descomposición de $V(f)$ en subvariedades irreducibles (sección 2, problemas 5 y 6), está dada por $V(f) = \bigcup_{i=1}^{r} V(f_i)$.

- Veamos que $V(f) = \bigcup_{i=1}^{r} V(f_i)$
  ($\subseteq$) Sea $x \in V(f) \Rightarrow f(x) = f_1^{n_1}(x)...f_r^{n_r}(x) = 0 \Rightarrow \exists i \in \{1, ..., r\} : f_i^{n_i}(x) = 0 \Rightarrow f_i(x) = 0$.
  Luego, $x \in V(f_i) \Rightarrow x \in \bigcup_{i=1}^{r} V(f_i)$

  ($\supseteq$) Sea $x \in \bigcup_{i=1}^{r} V(f_i) \Rightarrow \exists i \in \{1, ..., r\} : x \in V(f_i) \Rightarrow f_i(x) = 0 \Rightarrow f_i^{n_i}(x) = 0$
  $\Rightarrow f_1^{n_1}(x)...f_i^{n_i}(x)...f_r^{n_r}(x) = 0 \Rightarrow f(x) = 0 \Rightarrow x \in V(f)$

- Veamos ahora, que $V(f_i), i = 1, ..., r$, son variedades irreducibles.

  Por ejercicios 1-4 sección 2, sabemos que $V(\langle f_i \rangle)$ es irreducible, sii $IV(\langle f_i \rangle)$ es un ideal primo. Veremos entonces, este hecho equivalente.
  Siendo $K[X_1, ..., X_n]$ un DFU, por lema 1.10 resulta que f_i es un elemento primo y luego, por definición $\langle f_i \rangle$ es un ideal primo.
  Por otro lado, por teorema de los ceros, se sabe que $IV(\langle f_i \rangle) = \sqrt{\langle f_i \rangle}$;
  y por ejercicio 2 de la sección 4, $\sqrt{\langle f_i \rangle} = \bigcap_{P_i \in A} P_i$, siendo $A = \{P_i : P_i$ es un ideal primo que contiene a $\langle f_i \rangle$ $\}$.
  Finalmente observemos que siendo $\langle f_i \rangle$ el menor ideal primo que se contiene a si mismo, $\bigcap_{P_i \in A} P_i = \langle f_i \rangle$. Con lo cual, $\sqrt{\langle f_i \rangle} = \langle f_i \rangle$, y por ende $IV(\langle f_i \rangle) = \langle f_i \rangle$.
  Queda así, totalmente en evidencia que $IV(\langle f_i \rangle)$ es un ideal primo.
  Concluímos entonces que $V(f_i)$ es irreducible $\forall i \in \{1, ..., r\}$ □

Problema 6.2. Bajo las hipótesis del problema 1, muestra que $IV(f) = \langle f_1...f_r \rangle$.

Recordemos entonces que $f = f_1^{n_1}....f_r^{n_r}$.
Bien, por teorema de los ceros, sabemos que $IV(\langle f \rangle) = \sqrt{\langle f \rangle}$.
Afirmamos que $\sqrt{\langle f \rangle} = \langle \prod_{i=1}^{r} f_i \rangle$; veámoslo:
($\supseteq$) Sea $g \in \langle \prod_{i=1}^{r} f_i \rangle \Rightarrow \exists h_1 \in K[X_1, ..., X_n] : g = h_1 f_1...f_r$
Llamemos $n :=$ máx $\{n_1, ..., n_r\}$, luego:

$$\begin{aligned} g^n &= h_1^n f_1^n ... f_r^n \\ &= h_1^n f_1^{n_1} f_1^{n-n_1} ... f_r^{n_r} f_r^{n-n_r} \\ &= q \prod_{i=1}^{r} f_i^{n_i}, q \in K[X_1, ..., X_n] \\ &= qf. \end{aligned}$$

Con lo cual $g \in \sqrt{\langle f \rangle}$.

($\subseteq$) Sea $g \in \sqrt{\langle f \rangle}$, entonces $\exists n \in \mathbb{N} : g^n \in \langle f \rangle$, y por ende resulta $g^n = h_1 f_1^{n_1} .... f_r^{n_r}$, para algún $h_1 \in K[X_1, ..., X_n]$.
Observemos que esto en particular nos dice que $f_i | g^n \, \forall i \in \{1, ..., r\}$, pero entonces, siendo los f_i primos, afirmamos que $f_i | g \, \forall i \in \{1, ..., r\}$. Luego $f_1 f_2 ... f_r | g$ pues:
$f_1 | g \Rightarrow g = f_1 h_1$ (para algún $h_1 \in K[X_1, ..., X_n]$)
$f_2 | g \Rightarrow f_2 | f_1 h_1 \wedge f_2$ no divide a f_1, por lo que f_2 debe dividir a h_1...
$\vdots$
Siguiendo el procedimiento se prueba que $f_1 f_2 ... f_r | g$.
Con esto, $g \in \langle \prod_{i=1}^{r} f_i \rangle$, quedando así demostrada la igualdad $IV(f) = \sqrt{\langle f \rangle} = \langle \prod_{i=1}^{r} f_i \rangle$ □

Problema 6.3. Sea una colección de subconjuntos X_i de A^n, cualquiera.
Muestra que $I(\bigcup_i X_i) = \bigcap_i I(X_i)$.

($\subseteq$) Sea $f \in I(\bigcup_i X_i)$ $\Rightarrow$ f se anula sobre todos los $x \in \bigcup_i X_i$
$\Rightarrow$ f se anula sobre cada X_i
$\Rightarrow$ $f \in I(X_i) \forall i$
$\Rightarrow$ $f \in \bigcap_i I(X_i)$

($\supseteq$) $f \in \bigcap_i I(X_i)$ $\Rightarrow$ $\forall i, f \in I(X_i)$ con lo cual f se anula sobre $X_i, \forall i$
$\Rightarrow$ f se anula sobre $\bigcup_{i=1}^{r} X_i$
$\Rightarrow$ $f \in I(\bigcup_{i=1}^{r} X_i)$.

Resulta así que: $I(\bigcup_i X_i) = \bigcap_i I(X_i)$. □

Problema 6.4. Muestre que todo ideal radical I de $K[X_1, ..., X_n]$ es la intersección de finitos ideales primos.

Por corolario 5.3, sabemos que todo ideal radical es igual al ideal de alguna variedad. Más formalmente, si J es un ideal tal que $J = \sqrt{J}$, entonces $\exists V$, variedad, tal que $J = I(V)$
Luego, siendo I ideal radical ($I = \sqrt{I}$), deberá existir un variedad V, cumpliendo que $I = I(V)$.
Por ejercicio 5 de la sección 2, sabemos que V, puede expresarse como: $V = \bigcup_{i=1}^{r} V_i$ para ciertas subvariedades propias e irreducibles V_i; más aún, por ejercicio anterior resulta que

$I(V) = I(\bigcup_{i=1}^{r} V_i) = \bigcap_{i=1}^{r} I(V_i)$.
Notemos además, que siendo las variedades V_i irreducible, los ideales $I(V_i)$ resultan ser primos (por ejercicios 1-4, sección 2).
Con esto ha resultado, $I = I(V) = \bigcap_{i=1}^{r} I(V_i)$, intersección finita de ideales primos. □

Problema 6.5. Supongamos que X es una variedad en A^2, definida por las ecuaciones $f_1(x,y) = ... = f_m(x,y) = 0, m \geq 2$ y sea g el máximo común divisor de las f_i.
Si g es constante, muestra que X es un conjunto finito (posiblemente vacío).

Notación: Nos referiremos al conjunto $\{x \in A^2 : f(x) = 0\}$ como $\{f = 0\}$.

- Si algún f_i es un polinomio constante no nulo, entonces la ecuación $f_i(x,y) = 0$, no tiene solución. Luego la variedad definida por las ecuaciones $f_1(x,y) = ... = f_i(x,y) = ... = f_m(x,y) = 0$, resulta ser vacía.
  Digamos $X = \emptyset$.

- Si ningún f_i es constante no nulo
  Sea f un factor irreducible de algún f_i; de la definición de irreducible, sale que f es en particular no constante.
  Luego f no divide a g (pues g es constante, por hipótesis).
  entonces, debe $\exists f_j, j \neq i \in \{1, ..., m\} : f$ no divide a f_j, pues si $f \mid f_l \forall l \in \{1, ..., m\}$, entonces f sería un divisor común que no divide a g. Abs!! (Se contradice la definición de $m.c.d$)
  Luego, el conjunto $\{x \in A^2 : f(x) = f_j(x) = 0\}$ es de cardinal finito, pues:

  Si g es un polinomio irreducible y g es un polinomio arbitrario en $k[X,Y]$, vale que si f no divide a $g \Rightarrow$ el sistema de ecuaciones dado por $f(X,Y) = g(X,Y) = 0$ tiene finitas soluciones. Este es un hecho válido que no demostraremos.

  Consideremos ahora la factorización de f_1 en polinomios irreducibles, digamos $f_1 = f_{1_1} f_{1_2} ... f_{1_l}$.
  Por lo dicho anteriormente, para cada factor f_{1_i} de la factorización, $\exists f_{j_i}, j_i \neq 1_i \in \{1, ..., m\}$ tal que la ecuación $f_{1_i}(x) = f_{j_i}(x) = 0$ tiene finitas soluciones.
  Afirmamos luego que $f_1 = f_{1_1} f_{1_2} ... f_{1_l} = f_{j_1} = f_{j_2} = ... = f_{j_l} = 0$ tiene finitas soluciones (1)
  Con esto:

  - si las f_{j_i} ¨barren¨ todas las f_n, con $n \in \{2, 3, ..., m\}$, en el sentido de que $\{f_{j_1}; f_{j_2}; ...; f_{j_l}\} = \{f_2; ...; f_m\}$, resulta directo que X es un conjunto finito.
  - Si no, observemos que:
    $\{f_1 = f_2 = ... = f_m = 0\} \subset \{f_1 = f_{j_1} = f_{j_2} = ... = f_{j_l} = 0\}$,
    con lo cual resulta ser de cardinal finito, por serlo el conjunto más grande.

Veamos (1) : Esto es, si $f_{1_i} = f_{j_i} = 0$ tiene finitas soluciones para $i = 1, ..., l$,
entonces $f_1 = f_{1_1} f_{1_2} ... f_{1_l} = f_{j_1} = f_{j_2} = ... = f_{j_l} = 0$ tiene también finitas soluciones.

$$\begin{aligned} \{f_{1_1} f_{1_2} ... f_{1_l} = f_{j_1} = f_{j_2} = ... = f_{j_l} = 0\} &= (\bigcup_{i=1}^{l} \{f_{1_i} = 0\}) \cap \{f_{j_1} = f_{j_2} = ... = f_{j_l} = 0\} \\ &= \bigcup_{i=1}^{l} (\{f_{1_i} = 0\} \cap \{f_{j_1} = f_{j_2} = ... = f_{j_l} = 0\}). \end{aligned}$$

Ahora notemos que $\{f_{1_i} = 0\} \cap \{f_{j_1} = f_{j_2} = ... = f_{j_l} = 0\} \subseteq \{f_{1_i} = 0\} \cap \{f_{j_i} = 0\}$,
siendo f_{j_i} el que cumplía que la ecuación $f_{1_i}(x) = fj_i(x) = 0$ tenga finitas soluciones.
Con esto, el conjunto $A_i = \{f_{1_i} = 0\} \cap \{f_{j_1} = f_{j_2} = ... = f_{j_l} = 0\}$,
resulta ser de cardinal finito $\forall i = 1, ..., l$.
Luego, $X = \bigcup_{i=1}^{l} A_i$ tiene cardinal finito, pues es unión finita de conjuntos de cardinal finito. □

Problema 6.6. Muestra que toda variedad de A^2 (excepto la misma A^2), es la unión de un conjunto finito y una curva algebraica.

Sea $V \subsetneq A^2$ una variedad,
Por corolario 3.2, $\exists f_1, ..., f_r \in K[X, Y] : V = \bigcap_{i=1}^{r} V(f_i)$.
Llamemos $g = \text{m.c.d}\{f_i i = 1, ..., r\}$.
Luego, $\forall i = 1, ..., r$, f_i puede expresarse como $f_i = gh_i$, con $h_i \in K[X, Y]$.
Observemos que el m.c.d de las h_i´s debe ser una constante, pues:
Sea $m = m.c.d\{h_i\text{´s }\}$; luego, $m|h_i \forall i$, pero entonces, desde que $f_i = gh_i$, se tendrá que $gm|f_i \forall i$.
Ahora, como el $m.c.d\{f_i\text{´s }\}$ es g, se tiene que $gm|g$; es decir $\exists p \in K[X, Y] : g = gmp \Rightarrow g - gmp = 0$ o dicho de otro modo $g(1 - mp) = 0$. Y siendo $g \neq 0$, valdrá que $mp = 1$. Luego, tanto m como p son escalares, más aún, son uno el inverso multiplicativo del otro.

Veremos que $V = V(g) \cup (\bigcap_{i=1}^{r} V(h_i))$. Si esto fuera ciero, Listo!, pues $V(g)$ es una curva algebraica y $\bigcap_{i=1}^{r} V(h_i))$ es, por ejercicio anterior, un conjunto finito.

$$
\begin{aligned}
(\subseteq) \text{Sea } x \in V \quad &\Rightarrow \quad x \in \bigcap_{i=1}^{r} V(gh_i) \\
&\Rightarrow \quad (gh_i)(x) = 0 \, \forall i = 1, ..., r \\
&\Rightarrow \quad g(x) = 0 \vee h_i = 0 \, \forall i = 1, ..., r \\
&\Rightarrow \quad x \in V(g) \vee x \in \bigcap_{i=1}^{r} V(h_i) \\
&\Rightarrow \quad x \in (V(g) \cup \bigcap_{i=1}^{r} V(h_i)) \\
(\supseteq) \text{Sea } x \in V(g) \cup (\bigcap_{i=1}^{r} V(h_i)) \quad &\Rightarrow \quad g(x) = 0 \vee h_i = 0 \, \forall i = 1, ..., r \\
&\Rightarrow \quad gh_i(x) = 0 \, \forall i = 1, ..., r \\
&\Rightarrow \quad f_i(x) = 0 \, \forall i = 1, ..., r \\
&\Rightarrow \quad x \in \bigcap_{i=1}^{r} V(f_i) \\
&\Rightarrow \quad x \in V
\end{aligned}
$$

Con esto concluímos que V es la unión de una curva algebraica con un conjunto finito. □

Problema 6.7. De un ejemplo de dos polinomios irreducibles distintos en $K[X, Y]$ con el mismo conjunto nulo, y explique por qué esto no puede suceder si K es un cuerpo algebraicamente cerrado.

Consideremos los polinomions $p(x, y) = x^2 + y^2 \wedge q(x, y) = 2x^2 + y^2 \in \mathbb{R}[X, Y]$
Ambos polinomios son irreducibles, y el conjunto de puntos donde se anulan es $\{(0, 0)\}$.

Luego, $V(\langle f\rangle) = V(\langle g\rangle)$.
Si el cuerpo fuera algebraicamente cerrado, por el teorema de los ceros valdría que alguna potencia de f pertenecería a $\langle g\rangle$, i.e, existiría $m \in \mathbb{N} \wedge q \in \mathbb{R}[X,Y] : f^m = qg$.
Esto dice que $g|f^m$, pero siendo f primo por teo. 1.9, el que g divida a un producto , implica que divide a unos de sus factores. Pero entonces, $g|f$ ABS! (pues f y g son coprimos). □

Problema 6.8. Si K no es un cuerpo algebraicamente cerrado, de un ejemplo explícito de falla de alguna versión del teorema de los ceros.

Es sabido que el cuerpo $\mathbb{R}$ no es algebraicamente cerrado. Consideremos entonces, el anillo de polinomios en una variable $\mathbb{R}[X]$, y en él el ideal I generado por $p(x) = x^2 + 1$.
Notemos que $V(I) = V(\langle p\rangle) = \{x \in \mathbb{R} : p(x) = 0\} = \emptyset$.
No obstante, $I \neq \mathbb{R}$, lo que contradice el teorema débil de los ceros (si $V(I) = \emptyset \Rightarrow I = \mathbb{R}$).
Queda en evidencia, que el teorema de los ceros falla si el cuerpo no es algebraicamente cerrado. □

7. Localización

Supongamos que se tiene un polinomio $g \in I(V)$ para cierta variedad irreducible V, (observar que esto en particular implica que $I(V)$ es un ideal primo), y supongamos que demás que estamos interesados en estudiar funciones racionales del tipo $\frac{f}{g}$, en una vecindad un punto $x \in V$.
Necesitaríamos entonces que $g(x) \neq 0$, por lo que nos convendría tratar con polinomios g que no pertenecieran a $I(V)$, aunque esto permita que g se anule en algunos, no todos, los puntos de V.
El instrumento técnico que hace esto posible, es la construcción del *Anillo de fracciones* $S^{-1}R$, que siendo $R = K[X_1, ..., X_n]$ y $S = R - I(V)$, también recibe el nombre de *Localización de R según S*.
Estudiaremos ahora, el proceso de construcción del anillo de fracciones en general.

Sea S un subconjunto multiplicativo del anillo R; Definimos sobre $R \times S$ la siguiente relación de equivalencia:

$$(a, b) \sim (c, d) \text{ sii } \exists s \in S : s(ad - bc) = 0$$

Observemos que si no hubiera divisores de cero en R, $s(ad - bc) = 0 \Leftrightarrow ad - bc = 0$ *(Recordar que* $0 \notin S$*)*, con lo cual la relación de equivalencia podría escribirse como:

$$(a, b) \sim (c, d) \text{ sii } a/b = c/d$$

Si $a \in R$ y $b \in S$, nos referiremos a la clase de equivalencia del par (a, b), como la fracción $\frac{a}{b}$.
El conjunto de todas las clases de equivalencias, según la relación recién definida, será anotado por medio de $S^{-1}R$, y será llamado *Anillo de fracciones de R según S o Localización de R según S.*
Como es de esperarse por el nombre sugerente que hemos dado al conjunto cociente, este adquiere estructura de anillo, con las operaciones de ¨suma¨ y ¨producto¨ definidas como sigue:

$$\textit{Suma: } \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\textit{Producto: } \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Verificándose así que:

$$\text{El elemento neutro para la suma, resulta ser } \frac{0}{1} \left(= \frac{0}{s} \forall s \in S\right)$$

$$\text{El inverso aditivo de } \frac{a}{b} \text{ es } -\left(\frac{a}{b}\right) = \frac{-a}{b}$$

$$\text{La identidad del producto es } \frac{1}{1} \left(= \frac{s}{s} \forall s \in S\right)$$

Teorema 7.1. Sea S un subconjunto multiplicativo de un anillo conmutativo R, con las definiciones previas $S^{-1}R$ es un anillo conmutativo con unidad.
Si R fuera Dominio Íntegro, $S^{-1}R$ también lo sería.
Si R es un Dominio íntegro y $S = R - \{0\}$, entonces $S^{-1}R$ es un cuerpo, y se lo llama *Cuerpo cociente de R*

Así como los números racionales (cocientes de enteros), contienen una copia de $\mathbb{Z}$ (pues cada entero a puede identificarse con el racional $a/1$, cabe preguntarnos si $S^{-1}R$ contendrá una copia de R...

Proposición 7.2. Sea $h : R \to S^{-1}R$, dada por $h(a) = a/1$, afirmamos que h es un homomorfismo de anillos, más aún, si en S no hay divisores de cero, entonces h resulta ser un monomorfismo y diremos que S puede ser 'sumergido´ dentro de $S^{-1}R$, en particular:

(i) Un anillo conmutativo R puede sumergirse en su *Anillo de fracciones completo*, esto es $S^{-1}R$, siendo S el conjunto de todos los no divisores de cero de R.

(ii) Un Dominio Íntegro R puede sumergirse en su cuerpo de cocientes

Corolario 7.3. El Cuerpo de Cocientes F de un dominio íntegro R, es el menor cuerpo que contiene a R.

Si X es cualquier subconjunto del anillo R, definimos $S^{-1}X = \{\frac{x}{s} : x \in X, s \in S\}$.
Ya con algunas nociones generales, nos interesaremos especialmente en el conjunto $S^{-1}I$, siendo I un ideal de R.

Lema 7.4. .

(1) Si I es un ideal de R, entonces $S^{-1}I$ es un ideal de $S^{-1}R$;

(2) Si J es otro ideal de R, entonces:

(I) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$
(II) $S^{-1}IJ = (S^{-1}I)(S^{-1}J)$
(III) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$
(IV) $S^{-1}I$ es un ideal propio sii $S \cap I = \emptyset$

Demostración. .

(1) Veamos entonces que siendo I ideal de R, resulta que $S^{-1}I$ es un ideal de $S^{-1}R$

- ($\subseteq$) Sea $\frac{x}{s} \in S^{-1}I \Rightarrow x \in I \wedge s \in S \Rightarrow x \in R \wedge s \in S$ *(pues $I \subseteq R$)* $\Rightarrow \frac{x}{s} \in S^{-1}R$
- ($\neq \emptyset$) $1 \in S$, por ser S multiplicativo, y $0 \in J$ por ser este ideal de R. Luego $\frac{0}{1} \in S^{-1}I$
- (Suma cerrada en $S^{-1}I$)
  Sean $\frac{x}{s}, \frac{y}{t} \in S^{-1}I$. Por definición de suma, resulta que $\frac{x}{s} + \frac{y}{t} = \frac{xt+sy}{st}$.
  Ahora, siendo I ideal, tanto xt como $sy \in I$, más aún, su suma lo está.
  Por otro lado, siendo la multiplicación cerrada en S, se tiene que $st \in S$.
  Luego, $\frac{x}{s} + \frac{y}{t} = \frac{xt+sy}{st} \in S^{-1}I$.
- (Existencia de opuesto en $S^{-1}I$)
  Sea $\frac{x}{s} \in S^{-1}I$, luego $x \in I \wedge s \in S$.
  Siendo I ideal, se tiene que para el elemento $x \in I$, su opuesto $-x$ también $\in I$, con lo que $\frac{-x}{s} \in S^{-1}I$.
  De la definición de suma se desprende rápidamente que $\frac{-x}{s}$ es el opuesto del elemento dado.

- (Absorvencia)
  Sean $\frac{x}{s} \in S^{-1}I$ y $\frac{a}{t} \in S^{-1}R$.
  Consideremos $\frac{x}{s}\frac{a}{t}$, esto es, por definición de producto, $\frac{xa}{st}$, que claramente pertenece a $S^{-1}I$.

Ha resultado asi, $S^{-1}I$ ideal de $S^{-1}R$

(2) (I) ($\subseteq$) Sea $\frac{i+j}{s} \in S^{-1}(I+J)$, luego, por definición de suma, esto es $\frac{i}{s} + \frac{j}{s}$, que claramente pertenece a $S^{-1}I + S^{-1}J$.

($\supseteq$) Sea $\frac{i}{s} + \frac{j}{t} \in S^{-1}I + S^{-1}J$, por definición de suma, esto es $\frac{it+sj}{st}$.
Ahora, como $i \in I, j \in J$, siendo ambos I, J ideales, por definición de suma de ideales, se tiene que $it + sj \in I + J$. Además $st \in S$ por ser este un conjunto multiplicativo.
Luego, es claro que $\frac{it+sj}{st} \in S^{-1}(I+J)$
Valiendo así la igualdad dada.

(II) ($\subseteq$) Sea $\frac{\sum_{l=1}^{n} i_l j_l}{s} \in S^{-1}(IJ)$. Dicha suma finita puede verse como:

$$\frac{i_1 j_1}{s} + \frac{i_2 j_2}{s} + ... + \frac{i_n j_n}{s} = \frac{i_1}{s}\frac{j_1}{1} + ... + \frac{i_n}{s}\frac{j_n}{1}$$

Siendo evidente entonces que cada sumando es producto de un elemento de $S^{-1}I$ por otro de $S^{-1}J$, resulta claro que la suma total, corresponde a un elemento de $(S^{-1}I)(S^{-1}J)$.
($\supseteq$) Sea $\sum_{l=1}^{n} \frac{i_l}{s_l}\frac{j_l}{t_l} \in (S^{-1}I)(S^{-1}J)$; por definición de suma, esto resulta ser $\sum_{l=1}^{n} \frac{i_l j_l}{s_l t_l}$.
Ahora, cada sumando pertenece a $S^{-1}(IJ)$, y siendo este un ideal (pues IJ lo es), se tendrá, que la sumatoria entera representa un elemento de $S^{-1}(IJ)$, como queríamos ver.

(III)
$$\begin{aligned} \tfrac{x}{s} \in S^{-1}(I \cap J) &\Leftrightarrow x \in I \cap J \wedge s \in S \\ &\Leftrightarrow x \in I \wedge s \in S \wedge x \in J \wedge s \in S \\ &\Leftrightarrow \tfrac{x}{s} \in S^{-1}I \wedge \tfrac{x}{s} \in S^{-1}J \\ &\Leftrightarrow \tfrac{x}{s} \in S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J \end{aligned}$$

(IV) ($\Rightarrow$) Por el contrarecíproco, supongamos que $S \cap I \neq \emptyset$.
Luego $\exists s \in S \cap I$. Pero entonces $\frac{s}{s} = 1 \in S^{-1}I$!!.
Siendo $S^{-1}I$ un ideal de $S^{-1}R$, resulta entonces $S^{-1}I = S^{-1}R$, i.e, $S^{-1}I$ no es un ideal propio.

($\Leftarrow$) Por el contrarecíproco, supongamos que $S^{-1}I$ no es un ideal propio, es decir, supondremos que $S^{-1}I = S^{-1}R$.
Luego, dado $\frac{1}{1} \in S^{-1}R$, deben existir $s \in S, a \in I : \frac{1}{1} = \frac{a}{s}$, pero entonces por definición de igualdad de clases, resulta que deberá existir $t \in S : t(s-a) = 0$, o dicho de otro modo $ts = ta$. Luego, el elemento $ts \in S \cap I$, con lo que dicha intersección resulta ser no vacía.

Recordemos que $S^{-1}R$ tiene estructura de anillo.
Veremos que los ideales de $S^{-1}R$ tienen una forma especial; para ello recordemos la aplicación $h : R \to S^{-1}R$ definida en proposición 6.2, como $h(a) = \frac{a}{1}$ $\surd$

Lema 7.5. Sea J un ideal de $S^{-1}R$, y definamos $I = h^{-1}(J)$ (preimagen por h de J).
Afirmamos que:

(a) I es un ideal de R;

(b) $S^{-1}I = J$

Demostración. .

(a) Veamos que I es un ideal de R.

- *($I \subseteq R$)*
  Recordemos que $h : R \to S^{-1}R$, y que por definición $I = h^{-1}(J)$, siendo J ideal de $S^{-1}R$. Luego, es claro que la preimagen de J por h cae en R. i.e, $I \subseteq R$.
- *($I \neq \emptyset$)*
  Siendo J ideal de $S^{-1}R$, se tiene que $\frac{0}{1} \in J$. Pero $\frac{0}{1} = h(0)$, con lo cual $0 \in h^{-1}(J)$. Luego $0 \in I$, y por ende I es no vacío.
- *(Suma cerrada en I)*
  Sean $x, y \in I$. Queremos ver que $x + y \in I$, para ello deberá existir un elemento en J, del cual $x + y$ sea preimagen.
  Como $x, y \in I$, $\exists \frac{r_1}{s}, \frac{r_2}{t} \in J : x = h^{-1}(\frac{r_1}{s})$, $y = h^{-1}(\frac{r_2}{t})$.
  Observemos que siendo J ideal, la suma $\frac{r_1}{s} + \frac{r_2}{t} = \frac{r_1 t + r_2 s}{st} \in J$.
  ¿Será que $x + y = h^{-1}(\frac{r_1 t + r_2 s}{st})$?. Esto sucedería sii $h(x + y) = (\frac{r_1 t + r_2 s}{st})$, veámoslo:
  $h(x + y) = h(x) + h(y)$, por ser h homomorfismo de anillos; Pero $h(x) = \frac{r_1}{s}, h(y) = \frac{r_2}{t}$, con lo cual dicha suma resulta igual a $\frac{r_1 t + r_2 s}{st}$ como queríamos ver.
- *(Existencia de opuesto en I)*
- *(Absorvencia)*
  Sean $x \in I, r \in R$. ¿Será que $xr \in I$?
  $h(xr) = h(x)h(r)$ ahora, $h(x) \in J$ ideal, con lo cual el producto también.
  Luego, xr es preimagen de alguien de J por h, a saber, $xr = h^{-1}(h(x)h(r))$. Con esto, $xr \in I$. Análogamente, si consideramos rx.
  Resulta así, I ideal de R.

(b) Veremos ahora que $S^{-1}I = J$

($\subseteq$) Sea $\frac{i}{s} \in S^{-1}I \Rightarrow i \in I, s \in S$
Como $i \in I, h(i) = \frac{i}{1} \in J$. Luego, $\frac{i}{s} = \frac{i}{1}\frac{1}{s} \in J$, pues $\frac{i}{1}$ lo hace, y J tiene la propiedad de la absorvencia.

($\supseteq$) Sea $\frac{a}{s} \in J \Rightarrow a \in R$, $s \in S$. Veamos que $a \in I$, con lo que $\frac{a}{s}$ pertenecería a $S^{-1}I$
$h(a) = \frac{a}{1} = \frac{a}{s}\frac{s}{1}$. Ahora, como $\frac{a}{s} \in J$ ideal, se tiene que el producto recién mencionado también lo hace; luego $h(a)$ pertenece a J, o dicho de otro modo, $a \in h^{-1}(J) = I$.
Finalmente afirmamos que $\frac{a}{s} \in S^{-1}I$. $\surd$

Estudiaremos ahora un poco más de cerca, propiedades que adquiere el conjunto $S^{-1}I$, en donde I es un ideal primo del anillo R.

Lema 7.6. .

(a) Si I es un ideal de $R \Rightarrow I \subseteq h^{-1}(S^{-1}I)$;

(b) Si I es además primo y disjunto con S, entonces vale la igualdad $(I = h^{-1}(S^{-1}I))$.

Demostración. .

(a) Sea $a \in I$.
Queremos ver que a es preimagen por h, de alguien que viva en $S^{-1}I$.
Bueno, $h(a) = \frac{a}{1}$ por definición de h; además por hipótesis $a \in I$, con lo que $\frac{a}{1} \in S^{-1}I$.
Luego, $a = h^{-1}(\frac{a}{1})$ y por ende $a \in h^{-1}(S^{-1}I)$ como queríamos ver.

(b) $(\subseteq)$ Vale por inciso anterior;

$(\supseteq)$Supongamos que I es un ideal primo de R disjunto con S. Queremos ver que $h^{-1}(S^{-1}I) \subseteq I$.

$$\begin{aligned}
\text{Sea } a \in h^{-1}(S^{-1}I) &\Rightarrow h(a) = \tfrac{a}{1} \in S^{-1}I \\
&\Rightarrow \exists i \in I,\ s \in S : \tfrac{a}{1} = \tfrac{i}{s} \\
&\Rightarrow \exists t \in S : (as - i)t = 0 \textit{ (por def. de igualdad de clases)} \\
&\Rightarrow ast = it \in I \\
&\Rightarrow ast \in I \wedge st \in S (st \notin I) \\
&\Rightarrow a \text{ debe pertenecer a } I, \text{ pues recordemos que I es primo.}
\end{aligned}$$

√

Lema 7.7. Si I es un ideal primo de R disjunto con S, entonces $S^{-1}I$ es un ideal primo de $S^{-1}R$.

Demostración.
Ya hemos visto en el lema 6.4 inciso 1, que siendo I ideal de R, resulta que $S^{-1}I$ es un ideal de $S^{-1}R$. Resta entonces ver, que bajo las hipótesis dadas, $S^{-1}I$ es además primo.
Sea $\frac{a}{s}\frac{b}{c} \in S^{-1}I$. Queremos ver que uno u otro factor pertenece a $S^{-1}I$.
A priori sabemos con certeza, que $a, b \in R$ y $s, t \in S$. pero como $\frac{ab}{st} \in S^{-1}I$, deberá existir $\frac{i}{u} \in S^{-1}I : \frac{ab}{st} = \frac{i}{u}$. Luego, por definición de igualdad de clases, $\exists v \in S : (abu - ist)v = 0$, o dicho de otro modo, $abuv = istv$. Ahora, como I es primo y $i \in I$ se tiene que $istv \in I \Rightarrow abuv \in I$, pero $uv \notin I$ pues $uv \in S$, que es disjunto con I.
Luego $ab \in I$ y otra vez por ser I primo, se tendrá que $a \in I \vee b \in I \Rightarrow \frac{a}{s} \in S^{-1}I \vee \frac{b}{c} \in S^{-1}I$, como queríamos ver.
Ha resultado así, $S^{-1}I$ ideal primo de $S^{-1}R$. √

Teorema 7.8. Existe una correspondencia uno a uno entre los ideales primos de R que son disjuntos con S, y los ideales primos de $S^{-1}R$.
Más formalmente, sean $A = \{\text{ideales primos de } R \text{ disjuntos con } S\}$, y $B = \{\text{ideales primos de } S^{-1}R\}$. Luego existe una correspondencia $H : A \to B$ dada por $H(P) = S^{-1}P$, con inversa $H^{-1} : B \to A$ dada por $H^{-1}(Q) = h^{-1}(Q)$

Demostración. .

- Sea P un ideal primo de R disjunto con S.

  Hemos visto en lema 6.7, que $S^{-1}P$ resulta ser un ideal primo de $S^{-1}R$, con lo cual H, va realmente de A en B.

- Sea ahora Q ideal primo de $S^{-1}R$

  - $h^{-1}(Q)$ resulta ser un ideal primo de R;
  - Veamos que es además disjunto con S
    Por el absurdo supongamos que $h^{-1}Q \cap S \neq \emptyset$.
    Luego por lema 6.4 item 2 inciso iv, resulta que $S^{-1}(h^{-1}(Q)) = S^{-1}R$; pero siendo por lema 6.5 inciso b, $S^{-1}(h^{-1}(Q)) = Q$, resulta que $Q = S^{-1}R$ Abs!!, pues por definición de ideal primo, $Q \neq$ espacio total.
    Luego $Q \cap S = \emptyset$

- Veamos que los mapeos que sugerentemente hemos llamado H y H^{-1}, son efectivamente uno el inverso del otro.
  $H \circ H^{-1}(Q) = H(h^{-1}(Q)) = Q$ (*Por lema 6.5 inciso b*)
  $H^{-1} \circ H(P) = H^{-1}(S^{-1}P) = h^{-1}(S^{-1}P) = P$ (*Por lema 6.6 inciso b*) ■

Lema 7.9. Si P es un ideal primo de R, entonces $S = R - P$, es un conjunto multiplicativo.

Demostración. .

- $0 \in P$, pues P es un ideal, luego, $0 \notin S$.

- $1 \notin P$, pues siendo primo, es en particular propio, con lo cual 1 no puede estar...
  Luego $1 \in R - P = S$.

- Sen $a, b \in S = R - P$. Veamos que $ab \in R - P$.
  Supongamos que $ab \notin R - P$, entonces $ab \in P$, pero siendo P primo, $a \in P \vee b \in P$. Luego, $a \notin S \vee b \notin S$. Abs!!!.
  Afirmamos entonces que S es multiplicativamente cerrado, y finalmente, multiplicativo. $\surd$

Observación 7.10. En el caso en que el conjunto multiplicativo S, tenga la forma mencionada en el lema anterior, es frecuente anotar $R(P) = S^{-1}R$, y referirse a tal conjunto, como la *localización de R en P*.
Por otro lado, si I es un ideal de R, suele anotarse $I(P) = S^{-1}I$.

Mostraremos ahora que $R(P)$ es un Anillo Local, esto es, un anillo con un único ideal maximal. Pero daremos antes, algunas condiciones equivalentes a la de ser anillo local.

Proposición 7.11. Son equivalentes:

(a) R es anillo local *(Hay un único ideal maximal, digamos M)*;

(b) Hay un ideal propio de R, digamos I, que contiene a todas las no unidades de R;

(c) El conjunto de las no unidades de R es un ideal.

Demostración.

$(a) \Rightarrow (b)$ Sea a un elemento no inversible de R (o no unidad).
Observemos que $\langle a \rangle$ resulta ser un ideal propio, pues es claramente $\neq \emptyset$ y $\neq R$ (pues $1 \notin \langle a \rangle$); luego por teorema 1.4 de las preliminares, dicho ideal está contenido en un ideal maximal; pero siendo M por hip. el único ideal con esta característica, afirmamos que $\langle a \rangle \subset M$.
Como esto sucede para todo $\langle b \rangle$ con b no unidad..., concluimos que todos los elementos no inversibles de R están contenidos en M.
Obs: M es un ideal propio, como consecuencia de la definición de ideal maximal.

$(b) \Rightarrow (c)$ Veamos que el conjunto de todas las no unidades de R, tiene estructura de ideal.

- El conjunto de unidades de R está obviamente contenido en R;
- 0 (neutro respecto a la operación $+$), es no inversible. *($\neq \emptyset$)*
- Sean a, b no inversibles. Luego, por hip, $a, b \in I$, pero entonces $a + b \in I$.
  Si $a + b$ fuera inversible, el 1 pertenecería a I, con lo que resultaría $I = R$. Esto no puede suceder, puesto a que I es un ideal propio.
  Luego $a + b$ es no inversible. *(Suma cerrada)*
- Sea a no unidad. Luego $a \in I$, y por ende también está $-a$.
  Si $-a$ fuera una unidad, se tendría que $1 \in I$ resultando así $I = R$,lo que es abs!
  Luego, $-a$ es no unidad. *(Existencia opuesto)*
- Sean a no inversible, $r \in R$.
  Por hipótesis se tiene que $ar \in I$.
  Como antes, si ar fuera inversible, entonces resultaría $I = R$, y esto no puede suceder.
  Luego ar es no inversible. *(Absorvencia)*

Luego queda demostrado que el conjunto de elementos no inversibles, tiene estructura de ideal.

$(c) \Rightarrow (a)$ Sea $A = \{a \in R : \nexists a^{-1} \in R$ cumpliendo que $aa^{-1} = a^{-1}a = 1\}$.
Por hipótesis A es un ideal, afirmamos que:

- A es maximal.
  Supongamos que $\exists I$ ideal de R tal que $A \subseteq I \subseteq R$.
  - Si $A = I$ Listo!
  - Si $A \subsetneq I \Rightarrow \exists$ alguna unidad en $I \Rightarrow 1 \in I \Rightarrow I = R$
- A es el único ideal maximal
  Sea H un ideal propio, (candidato a ser ideal maximal), luego H no puede contener una unidad, pues de lo contrario $1 \in H$ y por ende $H = R$ y no sería propio...
  Con esto, $\forall H$ ideal propio de R, $H \subseteq A$, luego A es el único ideal maximal de R. ▲

Teorema 7.12. Sean P ideal primo de R y $S = R - P$, un conjunto multiplicativo.
Afirmamos que $R(P) = R^{-1}S$ es un anillo local.

Demostración.

Queremos ver que en $R(P)$ existe un único ideal maximal.
Sea Q un ideal maximal cualquiera de $R(P)$, este existe por corolario 1.5;
notemos que Q resulta ser un ideal primo, por lo que, por teorema 6.8, deberá existir un ideal primo I de R disjunto con S, tal que $Q = I(P)$.
Observar que: I disjunto con $S = R - P \Rightarrow I \subseteq P \Rightarrow Q = S^{-1}I \subseteq S^{-1}P$.
Ahora, siendo Q maximal, se tendrá que $P(P) = Q \vee P(P) = R(P)$.
Si $P(P) = R(P) \Rightarrow P(P)$ no sería propio, con lo que por la aplicación del lema 6.4, item 2, inciso iv , resulta $S \cap P \neq \emptyset$ Abs!!, pues $S = R - P$;
Luego, $P(P) = Q$. Esto dice que todo ideal maximal es igual a $P(P)$, con lo que este resulta ser el único ideal maximal de $R(P)$.
Afirmamos así, que $R(P)$ es un anillo local. ■

Localización de módulos

Si M es un R-Módulo y S es un subconjunto multiplicativo de R, la construcción empleada para construir la localización de M en S ($S^{-1}M$), puede ser escencialmente repetida y así dividir elementos de M por elementos de S.
Si $x, y \in M$ y $s, t \in S$, diremos que (x, s) está relacionado con (y, t) sii $\exists u \in S : u(tx - sy) = 0$.
La clase de equivalencia del elemento (x, s) según la relación dada se anotará $\frac{x}{s}$;
La suma de clases estará dada por: $\frac{x}{s} + \frac{y}{t} = \frac{tx+sy}{st}$;
Si $\frac{s}{s} \in S^{-1}R$ y $\frac{x}{t} \in S^{-1}M$, definimos el producto como: $\frac{a}{s}\frac{x}{t} = \frac{ax}{st}$.
De esta forma, $S^{-1}M$ se convierte en un $S^{-1}R$-módulo.

7.1. Problemas propuestos

Problema 7.1. Sea M un ideal maximal de R, asumamos que para cada $x \in M, 1+x$ es una unidad.
Muestra que R es un anillo local con ideal maximal M.
Sugerencia: Muestra que si $x \notin M \Rightarrow x$ es una unidad

Supongamos que $x \notin M$.
Observemos que $\langle M, x\rangle$ es un ideal cumpliendo que: $M \subset \langle M, x\rangle \wedge M \neq \langle M, x\rangle$
(pues $x \in \langle M, x\rangle$ y $x \notin M$). Luego, siendo M maximal, se tiene que $\langle M, x\rangle = R$, y por ende resulta que $1 \in \langle M, x\rangle$, i.e $\exists m \in M, r \in R : 1 = m + rx$.
Ahora, por hipótesis $\forall y \in M, 1+y$ es una unidad; por lo que $(-m)+1 = rx$ es inversible, y por tanto x es una unidad. Pues notemos que:

$$\begin{aligned} rx \text{ inversible} &\Rightarrow \exists a \in R : a(rx) = (rx)a = 1 \\ &\Rightarrow \text{ en virtud de la conmutatividad y asociatividad del producto en R resulta,} \\ &\quad (ar)x = x(ra) = 1, ar = ra \in R \\ &\Rightarrow x \text{ inversible} \end{aligned}$$

Hemos visto así, que si $x \notin M \Rightarrow x$ es una unidad. De lo que se deduce que si x no es una unidad, entonces $x \in M$.
Luego M es un ideal propio que contiene a todas las no unidades de R, resultando así R, por teorema 6.11, un anillo local con único ideal maximal M. □

Problema 7.2. Sea R el anillo de todas las matrices de $n \times n$ con coeficientes en un cuerpo K.
Si A es un elemento no nulo de R y si 1 es la matriz identidad, ¿Es siempre $\{1, A, A^2, ...\}$ multiplicativo?

Recordemos que una de las condiciones que deben cumplirse para que un conjunto L sea multiplicativo, es que $0 \notin L$.
Observemos ahora que si la matriz A fuera nilpotente, entonces dicha condición no se verificaría y $\{1, A, A^2, ...\}$ no sería multiplicativo. □

Sea S un subconjunto multiplicativo de el anillo R.
Definiremos dos mapeos, uno de R-módulos en $S^{-1}R$-módulos, y otro de los homomorfismos de R-módulos a los homomorfismos de $S^{-1}R$- módulos como sigue:

- $\varphi_1 : \{R - \text{Módulos}\} \longrightarrow \{S^{-1}R - \text{Módulos}\}$, dada por $\varphi_1(M) = S^{-1}M$; y
- $\varphi_2 : \{$ Homomorfismos de R-Módulos$\} \longrightarrow \{$Homomorfismos de $S^{-1}R$-Módulos$\}$ dada por: $\varphi_2(f) = S^{-1}f$, siendo f homomorfismo de M en N (R-Módulos) y $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ definida como $S^{-1}f(\frac{x}{s}) = \frac{f(x)}{s}$
  (Observar que siendo f homomorfismo, también lo es $S^{-1}f$).

Problema 7.3. Si $g : N \to L, f : M \to N$, y escribimos la composición de R-Módulos como un producto, muestra que $S^{-1}(gf) = S^{-1}gS^{-1}f$ y que si 1_M es el mapeo identidad sobre M, entonces $S^{-1}(1_M) = 1_{S^{-1}M}$

Siendo la composición de homomorfismos de R-Módulos cerrada, resulta que $gf : M \to L$, es un homomorfismo de R-Módulos.
Luego, $S^{-1}(gf) : S^{-1}M \longrightarrow S^{-1}L$, y está dada por: $S^{-1}(gf)(\frac{x}{s}) = \frac{g(f(x))}{s}$, ahora:

$$\begin{array}{rcl} \frac{g(f(x))}{s} & = & S^{-1}g(\frac{f(x)}{s}) \\ & = & S^{-1}g(S^{-1}f(\frac{x}{s})) \\ & = & S^{-1}gS^{-1}f(\frac{x}{s}) \end{array}$$

Siendo esta igualdad válida $\forall \frac{x}{s} \in S^{-1}M$, concluímos que $S^{-1}(gf) = S^{-1}gS^{-1}f$.
Por otro lado, $S^{-1}(1_M) : S^{-1}M \to S^{-1}M$, y está dada por $S^{-1}(1_M)(\frac{x}{s}) = \frac{1_M(x)}{s} = \frac{x}{s}$.
Luego $\forall \frac{x}{s} \in S^{-1}M, S^{-1}1_M(\frac{x}{s}) = \frac{x}{s}$. Con lo cual $S^{-1}1_M = 1_{S^{-1}M}$ □

Problema 7.4. Si $M \xrightarrow{f} N \xrightarrow{g} L$, es una sucesión exacta, entonces $S^{-1}M \overset{S^{-1}f}{\to} S^{-1}N \overset{S^{-1}g}{\to}$, también lo es.

Nos preguntamos entonces, si Imag($S^{-1}f$)= Nu($S^{-1}g$).

($\subseteq$) Sea $\frac{x}{s} \in$ Imag($S^{-1}f$) (contenida en $S^{-1}N$), $\Rightarrow \exists \frac{m}{s_2} \in S^{-1}M : \frac{x}{s} = S^{-1}f(\frac{m}{s_2}) = \frac{f(m)}{s_2}$.
Consideremos ahora $S^{-1}g(\frac{x}{s})$; esto es $S^{-1}g(\frac{f(m)}{s_2}) = \frac{g(f(m))}{s_2} = \frac{0_L}{s_2}$ (pues $f(m) \in$ Nu(g) por hipótesis). Luego, $\frac{x}{s} \in \mathrm{Nu}\, S^{-1}g$, y con esto, Imag($S^{-1}f$) $\subseteq$ Nu($S^{-1}f$).

($\supseteq$) Sea ahora $\frac{n}{s} \in$ Nu($S^{-1}g$) $\Rightarrow S^{-1}g(\frac{n}{s}) = \frac{g(n)}{s} = \frac{0_L}{1}$. Esto dice que $(0_L, 1) \sim (g(n), s)$.
$\Rightarrow \exists t \in S : t(g(n)) = 0$, y siendo g morfismo resulta $g(tn) = 0$.
$\Rightarrow tn \in$ Nu(g) = Imag(f) (por hip.), con lo cual deberá existir $y \in M : tn = f(y)$.
Luego $\frac{tn}{s} = \frac{f(y)}{s} \Rightarrow \exists l \in S : l(f(y)s - tns) = 0$
$\Rightarrow \exists l \in S : l(n(ts) - f(y)s) = 0. \Rightarrow \frac{n}{s} = \frac{f(y)}{ts}$.
Luego, $\frac{n}{s} = S^{-1}f(\frac{y}{ts})$, y por ende $\in$ Imag($S^{-1}f$). Concluimos así, que Imag($S^{-1}f$)= Nu($S^{-1}g$), y la sucesión resulta exacta. □

8. Descomposición primaria

Hemos visto que todo ideal radical de $K[X_1, ..., X_n]$ puede expresarse como intersección finita de ideales primos (sección 5, problema 5).
Una planteo natural de hacerse, es si existe algún resultado similar para ideales arbitrarios.
Veremos que la respuesta es afirmativa, si generalizamos de ideales primos a ideales primarios.

Definición. Un ideal Q en un anillo R se dirá *Primario* si:
Q es un ideal propio y si $ab \in Q \Rightarrow a \in Q \vee b^n \in Q$ para agún entero positivo n.

Observación 8.1. .

1. La condición sobre b, equivale a decir $b \in \sqrt{Q}$).
   Una definición equivalente a la dada para ideal primario es que $R/Q \neq 0$ y que si $(a+Q)(b+Q) = 0$ en R/Q, entonces $a+Q = 0$ o $(b+Q)^n = 0$ para algún entero positivo n.
   Esto en particular nos dice que si $b+Q$ es un divisor de cero en R/Q, entonces es nilpotente, i.e alguna potencia de él es nula.

2. Se sigue de la definición que todo ideal primo es primario. (Pues, si $ab \in Q$ (Ideal Primo) $\Rightarrow a \in Q \vee b^1 \in Q$, con lo cual Q primario.)

3. Además, si Q es primario, entonces $\sqrt{Q}$ es el menor ideal primo que contiene a Q, (recordar que hemos visto en sección 4, problema 2, que $\sqrt{Q}$ es la intersección de todos los ideales primos que contienen a Q).

Definición. Si Q es un ideal primario y $P = \sqrt{Q}$, diremos que Q es P- primario.

Lema 8.2. Si P es un ideal primo, entonces para todo entero positivo n vale que $\sqrt{P^n} = P$

Demostración.
($\supseteq$) Sea $x \in P \Rightarrow x^n \in P^n \Rightarrow x \in \sqrt{P^n}$.
($\subseteq$) Recordemos que $\sqrt{P^n}$ es la intersección de todos los ideales primos que contienen a P^n, por lo que sucede en particular, que si M es un ideal primo que contiene a P^n, entonces $\sqrt{P^n} \subseteq M$.
Observemos ahora que P es un ideal primo que contiene a P^n, luego vale lo anteriormente dicho, resultando así $\sqrt{P^n} \subseteq P$ $\surd$

Definición. Definimos el *Nilradical de un anillo* R, como el conjunto de todos los elementos nilpotentes de R y anotamos $\mathcal{N}(R)$, esto es:

$$\mathcal{N}(R) = \{x \in R : \exists n \in \mathbb{N}, x^n = 0\}$$

Observar que esto nos dice que $\mathcal{N}(R)$ no es más que la raíz del ideal nulo, que coincide además, con la intersección de todos los ideales primos del anillo.

Proposición 8.3. Sea Q un ideal de R. Si $\sqrt{Q}$ es maximal, entonces Q es un ideal primario.

Demostración.

Como consecuencia del problema 2 de la sección 4, sabemos que $\sqrt{Q}$ es la intersección de todos los ideales primos que contienen a Q; con lo que en particular resulta ser el menor ideal primo que contiene a Q.Pero además, es el mayor ideal primo que contiene a Q, pues
supongamos que $\exists I$ ideal primo de $R : Q \subseteq \sqrt{Q} \subseteq I$, luego siendo $\sqrt{Q}$ maximal, se tendrá que $\sqrt{Q} = I \vee I = R$, pero I no puede ser R por def. de ideal primo. Luego $\sqrt{Q} = I$.
Resulta así, que $\sqrt{Q}$ es el ideal primo más grande que contiene a Q, y a su vez el más chico!!. Afirmamos entonces que es el único ideal primo que contiene a Q.
Ahora, por teorema de correspondencia (1.8 de las preliminares), sabemos que la función
$\pi : A = \{\text{ideales} J \,\text{de}\, R : Q \subseteq J\} \to R/Q$, dada por $\pi(J) = R/J$ es biyectiva. Más aún, puede verse que los ideales primos de R/Q provienen de ideales primos de A. Uniendo estos dos hechos, deducimos que en R/Q hay un único ideal primo.
Recordemos ahora que el nilradical de R/Q, es la intersección de todos los ideales primos de R/Q, por lo que, habiendo un único ideal primo en R/Q, se sigue que este coincide con $\mathcal{N}(R/Q)$.
Por otro lado, todo elemento de R/Q que no sea inversible genera un ideal propio, que por teorema 1.4 de las preliminares, estará contenido en un ideal maximal, y por ende primo de R/Q; luego, estará contenido en $\mathcal{N}(R/Q)$.
De aquí, que si $a + Q \in R/Q \Rightarrow a + Q$ inversible $\vee$ $a + Q$ nilpotente.
Consideremos el producto $(x + Q)(y + Q) = 0$ en R/Q.
Como los factores son divisores de cero, no puede ser unidades, luego deben ser nilpotentes.
Se concluye entonces, que Q es primario. ▲

Corolario 8.4. Si M es un ideal maximal, entonces M^n es M-Primario $\forall n \in \mathbb{N}$.

Demostración.

Debemos ver que $M = \sqrt{M^n}$ y que M^n es primario.
M maximal implica M primo, luego por lema 7.1 $\forall n \in \mathbb{N}, \sqrt{M^n} = M$. No sólo esto, observar que en particular implica que $\sqrt{M^n}$ es maximal, por lo que por proposición anterior resulta M^n primario.
Finalmente afirmamos que M^n es M-Primario. ♣

Proposición 8.5. Sean $Q_i, i = 1, ..., n$ ideales P-Primarios.
Si $Q = \bigcap_{i=1}^{n} Q_i \Rightarrow Q$ es P-primario.

Demostración.

Debemos ver que: Q es primario y que $P = \sqrt{Q}$.

- Veamos que $P = \sqrt{Q}$.

$$\begin{aligned} Q = \bigcap_{i=1}^{n} Q_i \Rightarrow \sqrt{Q} &= \sqrt{\bigcap_{i=1}^{n} Q_i} \\ &= \bigcap_{i=1}^{n} \sqrt{Q_i} \,(\text{por problema 1 de esta sección}) \\ &= \bigcap_{i=1}^{n} P \,(\text{por hip.}) \\ &= P \end{aligned}$$

Luego $\sqrt{Q} = P$.

- Veamos ahora, Q primario.
  Sea $ab \in Q$ y supongamos que $a \notin Q$. (Debería suceder que $b^n \in Q$ para algún $n \in \mathbb{N}$).
  Como $a \notin \bigcap_{i=1}^{n} Q_i$, deberá existir $i \in \{1, ..., n\} : a \notin Q_i$. Pero ab si $\in Q_i$, con lo cual, $b^l \in Q_i$ para algún $l \in \mathbb{N}$; esto dice que $b \in \sqrt{Q_i}$, pero entonces $b \in P$, y por item anterior, $b \in \sqrt{Q}$, con lo cual podemos afirmar que existe $s \in \mathbb{N} : b^s \in Q$.
  Finalmente, Q es primario, con lo cual ha resultado ser P-Primario. ■

Veremos luego, que en un anillo Noetheriano todo ideal propio I admite una descomposición primaria, esto es, I puede expresarse como intersección finita de ideales primarios.

Definición. Diremos que un ideal I es irreducible, si $\forall J, K$ ideales, se verifica que, si $I = J \cap K \Rightarrow I = J \vee I = K$

Lema 8.6. Si R es Noetheriano, entonces todo ideal de R puede expresarse como intersección finita de ideales irreducibles.

Demostración.

Sea $S = \{$ideales de R que no pueden expresarse como intersección finita de ideales irreducibles $\}$
Por el absurdo, supongamos que S es no vacío, y veamos a S como la familia de ideales $(I_\alpha)_\alpha$
Siendo R Noetheriano, deberá existir I perteneciente a la familia, maximal entre los elementos de la misma respecto de la inclusión.
Notar que I es reducible, pues si fuera irreducible, el sería intersección de finitos, a saber él mismo, ideales irreducibles, por lo que no estaría en la familia, ABS!.
Siendo I reducible, deberán existir J, K ideales, tales que $I = J \cap K \operatorname{con} I \neq J \wedge I \neq K$. Esto nos dice que $I \subsetneq K \wedge I \subsetneq J$.
Ahora, como I es maximal en S, se tiene que ni K ni J pueden pertenecer a S, con lo cual ambos resultan expresables como intersección finita de ideales irreducibles. Pero entonces, también lo es I! ABS!! (pues entonces I no pertenecería a S).
Luego $S = \emptyset$, lo que implica que todo ideal de R puede expresarse como intersección finita de ideales irreducibles. √

Si pudiéramos mostrar que todo ideal irreducible y propio es primario, tendríamos la descomposición primaria deseada.
La cadena de razonamientos que seguiremos es la siguiente:
Si I es un ideal irreducible y propio de R, entonces por el teorema de correspondencia, 0 es un ideal irreducible del anillo Noetheriano R/I.
Luego, si pudiéramos mostrar que 0 es primario en R/I, otra vez por el teorema de correspondencia, resultaría que I es primario en R.
Se tendría así, que todo ideal irreducible y propio de R, es primario.

Teorema 8.7. *Teorema de descomposición primaria*: Todo ideal propio en un anillo Noetheriano admite una descomposición primaria

Demostración.

Por lo dicho anteriormente, basta ver que si 0 es un ideal irreducible de R, entonces es primario.
Sea $ab = 0$, y supongamos que $a \neq 0$. Queremos ver que $\exists m \in \mathbb{N} : b^m = 0$.
Consideremos la siguiente cadena de ideales, formada por anuladores:

$$An(b) \subseteq An(b^2) \subseteq An(b^3) \subseteq ...$$

Siendo R Noetheriano, dicha cadena se estabiliza. i.e $\exists n \in \mathbb{N} : An(b^n) = An(b^i) \forall i \geq n$.
Si pudiéramos ver que $\langle a \rangle \cap \langle b^n \rangle = 0$, entonces siendo 0 irreducible, se tendría que $\langle a \rangle = 0 \vee \langle b^n \rangle = 0$.
Ahora $\langle a \rangle \neq 0$ (pues $a \neq 0$ por hip). Luego $\langle b^n \rangle = 0$ como queríamos ver.
Veamos entonces tal intersección!.
La inclusión $\subseteq$ es trivial, pues 0 pertence a todo ideal. Veamos entonces la otra inclusión.
Sea $x \in \langle a \rangle \cap \langle b^n \rangle \Rightarrow \exists r, s \in R : x = ra \wedge x = sb^n$.
Multiplicando por b se llega a que $bx = rab = sb^{n+1}$ (recordar que R es conmutativo!).
Ahora, $ab = 0$ por hip., con lo cual $sb^{n+1} = 0 \Rightarrow s \in An(b^{n+1}) = An(b^n)$ (por la estabilización).
Finalmente recordemos que $x = sb^n$, por lo que como $s \in An(b^n)$, resulta $x = 0$ como queríamos ver.
Se concluye así, 0 ideal primario. ■

8.1. Problemas propuestos

Problema 8.1. Si $I_1, ..., I_n$ so ideales arbitrarios, muestra que:

$$\sqrt{\bigcap_{i=1}^{n} I_i} = \bigcap_{i=1}^{n} \sqrt{I_i}$$

$(\subseteq)$

$$\begin{aligned}
\text{Sea } x \in \sqrt{\bigcap_{i=1}^{n} I_i} &\Rightarrow \exists m \in \mathbb{N} : x^m \in \bigcap_{i=1}^{n} I_i \\
&\Rightarrow \exists m \in \mathbb{N} : x^m \in I_i \forall i = 1, ...n \\
&\Rightarrow x \in \sqrt{I_i} \forall i = 1, ...n \\
&\Rightarrow x \in \bigcap_{i=1}^{n} \sqrt{I_i}
\end{aligned}$$

$(\supseteq)$

$$\begin{aligned}
\text{Sea } x \in \bigcap_{i=1}^{n} \sqrt{I_i} &\Rightarrow x \in \sqrt{I_i} \forall i = 1, ..., n \\
&\Rightarrow \exists m_i \text{ Para cada } i = 1, ..., n : x^{m_i} \in I_i \\
&\quad \text{Sea } m = \text{máx}_{i=1,...,n}\{m_i\} \\
&\Rightarrow x^m \in I_i \forall i = 1, ..., n \\
&\Rightarrow x^m \in \bigcap_{i=1}^{n} I_i \\
&\Rightarrow x \in \sqrt{\bigcap_{i=1}^{n} I_i}
\end{aligned}$$

□

Problema 8.2. Sea $I = \langle XY - Z^2 \rangle$ en $K[X, Y, Z]$, con K cuerpo; y sea $R = K[X, Y, Z]/I$. Muestra que si $P = \langle X + I, Z + I \rangle$ entonces P es primo.

Nota: Nos referiremos a la clase de equivalencia del elemento f según la relación $f \sim g$ sii $f - g \in I$, como $\overline{f}$ o $f + I$, en forma idistinta.
Notaremos a la clase de $\overline{f}$ en el cociente R/P, como $\overline{\overline{f}}$.

Recordemos que por teorema 1.9, un ideal P en un anillo R es primo sii R/P es Dominio Íntegro. Veamos entonces, este hecho equivalente; i.e, veamos que R/P es un D.I.
Para ello, demostraremos previamente, el siguiente resultado:

Sea $f : A \to B$ un isomorfismo. Se afirma que A es Dominio Ìntegro sii B también lo es.

$(\Rightarrow)$ Sean $b_1, b_2 \in B : b_1 b_2 = 0$
Siendo f suryectiva, $\exists a_1, a_2 \in A : b_1 = f(a_1), b_2 = f(a_2)$
Luego $f(a_1)f(a_2) = 0$, pero siendo f morfismo, esto es $f(a_1 a_2) = 0$; y siendo f inyectiva, esto dice que $a_1 a_2 = 0$
Finalmente siendo A un Dominio Íntegro, aseguramos que $a_1 = 0 \vee a_2 = 0$.
Se tiene así, que en virtud de la linealidad, $f(a_1) = 0 \vee f(a_2) = 0$. Esto es, $b_1 = 0 \vee b_2 = 0$.
Concluímos entonces, que B es Dominio Íntegro.

($\Leftarrow$) Sean $a_1, a_2 \in A : a_1 a_2 = 0$
Siendo f lineal, se tendrá que $f(a_1 a_2) = 0$, y por ser f morfismo, esto es $f(a_1)f(a_2) = 0$
Pero $f(a_i) \in B$ para $i = 1, 2$ por lo que, por ser B Dominio Integro, resulta $f(a_1) = 0 \vee f(a_2) = 0$.
Se tiene entonces, en virtud de la inyectividad, que $a_1 = 0 \vee a_2 = 0$, resultando así, A Dominio Íntegro.

Ahora si, bajo esta consideración previa, veamos que $R/P \cong K[Y]$, ya que siendo $K[Y]$ Dominio Íntegro, se tendría lo deseado.

La idea será, a grosso modo, ver que lo único que sobrevive en el cociente R/P son las clases de polinomios en la variable Y.

Desde que la clase de la suma es la suma de clases, a la hora de ver qué sucede en el cociente con un polinomio arbitrario, bastará considerar el caso particular, en el que tal polinomio es en realidad, un monomio.
Consideremos entonces $aX^pY^qZ^r \in K[X, Y, Z]$.
Obsevemos que, $\overline{XY - Z^2} = \overline{0}$ en R, (pues $XY - Z^2 \in I$), con lo cual $\overline{XY} = \overline{Z^2}$ en R.
Luego, recordando que la clase de un producto coincide con el producto de las clases, se tiene que:

$$\overline{aX^pY^qZ^r} = \overline{aX^{p_1}Y^{q_1}Z^i}, \text{ con } p_1 > p,\ q_1 > q,\ i = 0, 1$$

Mirando ahora, a dónde va esto en el cociente R/P, obtenemos que:

- Si $i = 0 \vee p_1 \geq 1 \Rightarrow \overline{\overline{aX^{p_1}Y^{q_1}Z^i}} = \overline{\overline{0}}$, pues $\overline{Z}$ y $\overline{X} \in P \Rightarrow \overline{\overline{Z}} = \overline{\overline{X}} = \overline{\overline{0}}$

- Si $i = 0 \wedge p_1 = 0 \Rightarrow \overline{\overline{aX^{p_1}Y^{q_1}Z^i}} = \overline{\overline{aY^{q_1}}}$

Queda en evidencia así, que lo único que sobrevive en R/P son las clases de polinomios en la variable Y únicamente.
Afirmamos entonces $R/P \cong K[Y]$.
Luego, R/P Dominio Íntegro, y consecuentemente P ideal primo. □

Problema 8.3. Continuando con el problema anterior, muestra que P^2 no es primario.

Observemos primero que $XY - Z^2 \in I$, por lo que dicho polinomio se relaciona con 0.
Es decir, que si anotamos como $a + I$ a la clase de equivalencia de a en el cociente R, lo dicho anteriormente se traduce en que $(XY - Z^2) + I = 0 + I$; y recordando que la suma y el producto de clases, son las clases de la suma / producto respectivamente, obtenedremos que
$(X + I)(Y + I) = Z^2 + I$.
Ahora, $Z + I \in P$, por lo que $Z^2 + I \in P^2$.
Sin embargo $X + I \notin P^2$ y $(Y + I)^n$ tampoco para ningún $n \in \mathbb{N}$. Pues de lo contrario $Y + I$ pertenecería a $\sqrt{P^2}$, que siendo P primo resulta igual a P *(por lema 7.2)*, y claro está, que $Y + I \notin P$.
Luego, no hay chance de que P^2 sea un ideal primario. □

Problema 8.4. Sea $R = K[X, Y]$, y sean $P_1 = \langle X \rangle$, $P_2 = \langle X, Y \rangle, Q = \langle X^2, Y \rangle$.
Muestra que P_1 es primo, y que P_2^2 y Q son P_2-Primarios.

- Veamos que P_1 es primo.
  Puede verse que $R/P_1 \cong K[Y]$, pues los únicos polinomios que no van a parar a la clase del cero en el cociente, son aquellos de la forma $\sum_{i=1}^{n} a_i Y^i$. (polinomios constantes o en la variable Y unicamente).
  Luego, siendo $K[Y]$ dominio íntegro, concluímos R/P_1 dominio íntegro, y por ende, P_1 ideal primo.

- Veamos que P_2^2 es P_2- Primario.
  Observemos que P_2 resulta maximal por la aplicación del lema 4,1, pues $\exists (0,0) \in K^2 : P_2 = \langle X, Y \rangle$, luego por corolario 7,4, P_2^n es P_2-Primario $\forall n \in \mathbb{N}$,con lo cual para $n = 2$ se tendrá en paricular $P_2^2 P_2-$Primario.

- Veamos ahora que Q es P_2-Primario, (Q primario y $\sqrt{Q} = P_2$)
  Bastará ver que $\sqrt{Q} = P_2$, pues siendo P_2 maximal, concluiríamos por proposición 7.3,Q primario. Veámoslo,
  ($\subseteq$) Sea $p \in \sqrt{Q} \Rightarrow \exists n \in \mathbb{N} : p^n \in Q \Rightarrow \exists q, r \in R : p^n = qX^2 + rY \Rightarrow p^n \in P_2 \Rightarrow p \in \sqrt{P_2}$
  Pero observemos ahora, que siendo P_2 maximal *(lema 4.1)*, resulta $P_2 = \sqrt{P_2}$, pues:
  Si $l \in P_2 \Rightarrow l^1 \in P_2 \Rightarrow l \in \sqrt{P_2}$, con lo cual $P_2 \subseteq \sqrt{P_2}$, entonces por maximalidad, $P_2 = \sqrt{P_2} \vee P_2 = R$. Claramente $P_2 \neq R$. Concluímos así, $P_2 = \sqrt{P_2}$.
  Se sigue entonces, que $p \in P_2$.

  ($\supseteq$) Sea $p \in P_2 \Rightarrow \exists q, r \in R : p = qX + rY \Rightarrow p^2 = q^2X^2 + 2qXrY + r^2Y^2 \Rightarrow p^2 = q^2X^2 + Y(2qrX + rY) \Rightarrow p^2 \in \langle X^2, Y \rangle = Q \Rightarrow p \in \sqrt{Q}$.

  Concluímos finalmente que Q es P_2- Primario. □

Problema 8.5. Continuando con el problema 4, sea $I = \langle X^2, XY \rangle$.
Muestra que $P_1 \cap P_2^2$ y $P_1 \cap Q$ son ambas descomposiciones primarias de I.

Hemos visto en ejercicio anterior que P_2^2, P_1 y Q son ideales primarios.
Resta ver entonces, para afirmar que las descomposiciones propuestas son efectivamente descomposiciones primarias de I, las siguientes dos igualdades:

1. $I = P_1 \cap P_2^2$;
2. $I = P_1 \cap Q$.

Veamos 1.
¿$\langle X^2, XY \rangle = \langle X, Y \rangle^2 \cap \langle X \rangle$?
Observemos que $\langle X, Y \rangle^2 = \langle X^2, XY, Y^2 \rangle$; pues:
($\subseteq$) Sea $p_1 \in \langle X, Y \rangle^2 \Rightarrow \exists p \in \langle X, Y \rangle : p^2 = p_1$
Ahora, $p \in \langle X, Y \rangle \Rightarrow \exists q, r \in R : p = qX + rY$, con lo que $p^2 = q^2X^2 + 2qXrY + r^2Y^2 = q^2X^2 + mXY + r^2X^2, m \in R$, quedando claro así que $p^2 = p_1 \in \langle X^2, XY, Y^2 \rangle$.

($\supseteq$) Sea $p \in \langle X^2, XY, Y^2\rangle \Rightarrow \exists m_1, m_2, m_3 \in R : p = m_1X^2 + m_2XY + m_3Y^2$

----------FALTA----------

Ahora si!, veamos que efectivamente $\langle X^2, XY\rangle = \langle X^2, XY, Y^2\rangle \cap \langle X\rangle$

($\subseteq$) Sea $p = a(X,Y)X^2 + b(X,Y)XY \in I$. Es claro que $p \in \langle X^2, XY, Y^2\rangle$, y además siendo $p = X(a(X,Y)X + b(X,Y))$, resulta evidente también que $p \in \langle X\rangle$. Se tiene así que p pertenece a la intersección.

($\supseteq$) Sea $p \in P_2^2 \cap P_1$. Luego $p = a(X,Y)X \wedge p = f(X,Y)X^2 + g(X,Y)XY + h(X,Y)Y^2$, para ciertos a, f, g y $h \in K[X,Y]$.

Notemos que esto implica, que cada monomio en la segunda expresión deberá ser de la forma $t(X,Y)X$, para algún $t \in K[X,Y]$. En particular, deberá existir $h_2 \in K[X,Y]$:

$h(X,Y)Y^2 = h_2XY^2$. Resultando claro así que $p \in \langle X^2, XY\rangle$, pues cada sumando de la segunda expresión lo hace.

Ha quedado así demostrado 1.

Veamos 2.

($\subseteq$) Sea $p = aX^2 + bXY \in I \Rightarrow p = X(aX + bY) \wedge p = aX^2 + (bX)Y$
$\Rightarrow p \in \langle X\rangle \cap \langle X^2, Y\rangle$
$\Rightarrow p \in P_1 \cap Q$

($\supseteq$) Sea $p \in P_1 \cap Q \Rightarrow p = aX \wedge p = bX^2 + cY$
$\Rightarrow$ Deberá existir $c_2 \in K[X,Y] : cY = c_2YX$
$\Rightarrow p = bX^2 + c_2XY$
$\Rightarrow p \in I$

Luego las dos descomposiciones propuestas, son efectivamente descomposiciones primarias de I. □

Problema 8.6. Hemos visto en problema 5 de la sección 5, que todo ideal radical en $K[X_1, ..., X_n]$, es intersección de finitos ideales primos.
Muestra que el resultado sigue siendo válido en cualquier anillo noetheriano R.

Sea I un ideal radical del anillo R.

Por teorema de la descomposición primaria (7.7), I puede escribirse como intersección finita de ideales primarios, i.e:

$$I = \bigcap_{i=1}^{n} J_i,\ J_i \text{ primarios.}$$

Por ejercicio 1 de esta misma sección, resulta que:

$$\sqrt{I} = \bigcap_{i=1}^{n} \sqrt{J_i}$$

Ahora, llamemos $P_i = \sqrt{J_i}$, y notemos que por observación 7.1 inciso 3, estos ideales son primos.
Luego, siendo I un ideal radical ($I = \sqrt{I}$), resulta que

$$I = \bigcap_{i=1}^{n} P_i, \text{ con } P_i \text{ ideales primos.}$$

Y se tiene así, que todo ideal radical en un anillo Noetheriano R, puede expresarse como intersección finita de ideales primos. □

Problema 8.7. Sea $R = K[X, Y]$, y sea $I_n = \langle X^3, XY, Y^n \rangle$.
Muestra que para todo entero positivo n, I_n es un ideal primario de R.

Para esto, haremos uso de la proposición 7.3, que enuncia que si $\sqrt{I_n}$ es maximal, entonces I_n es primario; y para la maximalidad, veremos que los ideales $\sqrt{I_n}$, resultan ser iguales a un ideal al que sabemos maximal.
Ahora si, trabajemos!

- $X^3 \in I_n \Rightarrow X \in \sqrt{I_n} \Rightarrow \langle X \rangle \subseteq \sqrt{I_n}$;
- $Y^n \in I_n \Rightarrow Y \in \sqrt{I_n} \forall n \in \mathbb{N} \Rightarrow \langle Y \rangle \subseteq \sqrt{I_n}$;

De estos dos hechos se deduce que $\langle X, Y \rangle \subseteq \sqrt{I_n}$.
Ahora, por lema 4.1, sabemos que $\langle X, Y \rangle$ es un ideal maximal, con lo cual deberá suceder que $\sqrt{I_n} = R \vee \sqrt{I_n} = \langle X, Y \rangle$.
Es claro que $1 \notin \sqrt{I_n} \Rightarrow \sqrt{I_n} = \langle X, Y \rangle$.
Resulta así, $\sqrt{I_n}$ maximal y finalmente primario. □

Bibliografía

[1] *Abstract Algebra: 1st Graduate year course*;
Ash R.; 2000.

[2] *Algebra: An Approach via Module Theory*;
Adkins W.A, Weintraub S.H;
Springer-Verlag, New York, 1992.

[3] *Algebra*. Graduate Texts in Mathematics 73;
Hungerford;
Springer-Verlag, New York, 1974.

[4] *Geometría Algebraica*;
Carlos Ivorra del Castillo