Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020

Capítulo 5

Variedades Irreducibles y Descomposición

5.1 Teorema de los ceros de Hilbert

Dado $a \in \mathbb{F}$ y $f \in \mathbb{F}[X]$, denotamos por $\bar{f} = f(x_1, \ldots, f_{n-1}, a) \in \mathbb{F}[x_1, \ldots, x_{n-1}]$. Si $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ es un ideal, denotamos también

$$I_{x_n = a} = \{\bar{f} \mid f \in I\}.$$

Lema 5.1. *Si* $\mathbb{F}$ *es algebraicamente cerrado y* $I \subsetneq \mathbb{F}[x_1, \ldots, x_n]$*, existe* $a \in \mathbb{F}$ *tal que* $I_{x_n = a} \subsetneq \mathbb{F}[x_1, \ldots, x_{n-1}]$.

Demostración. La demostración se divide en dos casos.

Caso 1. $I \cap \mathbb{F}[x_n] \neq \{0\}$. Sea $f \in I \cap \mathbb{F}[x_n]$ no nulo. f no puede ser constante porque $1 \notin I$, y no perdemos generalidad en suponer que es mónico. Como $\mathbb{F}$ es algebraicamente cerrado,

$$f = \prod_{i=1}^{r} (x_n - b_i)^{m_i},$$

con $b_1, \ldots, b_r \in \mathbb{F}$. Supongamos que para todo $1 \leq i \leq r$, $I_{x_n = b_1} = \mathbb{F}[x_1, \ldots, x_{n-1}]$. Existe entonces, para cada $1 \leq i \leq r$, un $g_i \in I$ tal que $g_i(x_1, \ldots, x_{n-1}, b_i) = 1$. Esto implica que

$$\begin{aligned} 1 &= g_i(x_1, \ldots, x_{n-1}, b_i) \\ &= g_i(x_1, \ldots, x_{n-1}, x_n - (x_n - b_i)) = g_i - h_i(x_n - b_i) \end{aligned}$$

para ciertos $h_i \in \mathbb{F}[x_1, \ldots, x_n]$. Tenemos, por consiguiente

$$1 = \prod_{i=1}^{r} (g_i - h_i(x_n - b_i))^{m_i} = h \prod_{i=1}^{r} (x_n - b_i)_i^m + g,$$

donde $h = \prod_{i=1}^{r} h_i^{m_i}$ y $g \in I$. Como $\prod_{i=1}^{r}(x_n - b_i)^{m_i} = f \in I$, concluimos que $1 \in I$, lo que es imposible porque I es un ideal propio. Debe, por tanto, existir una raíz b_i tal que $I_{x_n = b_i} \neq \mathbb{F}[x_1, \ldots, x_{n-1}]$, lo que demuestra el lema en el caso 1.

Caso 2. $I \cap \mathbb{F}[x_n] = \{0\}$. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I con respecto al orden LEX. Podemos expresar

$$g_i = c_i(x_n) X^{\alpha(i)} + \sum_{\beta < \alpha(i)} c_\beta X^\beta$$

donde $c_i(x_n) \in \mathbb{F}[x_n] \setminus \{0\}$ y $\alpha(i)_n = 0$. Como $\mathbb{F}$ es algebraicamente cerrado, es infinito, por lo que existe $a \in \mathbb{F}$ tal que $c_i(a) \neq 0$ para cada $1 \leq i \leq r$. Es fácil comprobar que

$$I_{x_n = a} = \langle \overline{g_1}, \ldots, \overline{g_t} \rangle$$

y que $\exp(\overline{g_i}) = \alpha(i)$. Además $\alpha(i) \neq 0$ ya que en caso contrario $g_i = c_i \in I \cap \mathbb{F}[x_n] = \{0\}$, lo que es imposible. Veamos que $\{\overline{g_1}, \ldots, \overline{g_t}\}$ es una base de Gröbner para $I_{x_n=a}$. Sean $g_i, g_j \in G$ y $\gamma = \operatorname{lcm}(\alpha(i), \alpha(j))$. Sea

$$S = c_j(x_n)X^{\gamma-\alpha(i)}g_i - c_i(x_n)X^{\gamma-\alpha(j)}g_j.$$

Tenemos que $\exp(S) < \gamma$. Como $S \in I$, $S = \sum_{l=1}^{t} h_l g_l$ con $\exp(h_l g_l) \leq \exp(S)$. Evaluando en $x_n = a$,

$$c_j(a)X^{\gamma-\alpha(i)}\overline{g_i} - c_i(a)X^{\gamma-\alpha(j)}\overline{g_j} = \sum_{l=1}^{t} \overline{h_l}\,\overline{g_l}.$$

Como $\exp(\overline{g_i}) = \alpha(i)$, tenemos que $\overline{S}$ es un múltiplo constante del S-polinomio $S(\overline{g_i}, \overline{g_j})$. Además,

$$\gamma > \exp(S) \geq \exp(h_l g_l), \quad 1 \leq l \leq t,$$

por lo que

$$\gamma > \exp(\overline{h_l}\,\overline{g_l}), \quad 1 \leq l \leq t.$$

Por el Teorema 3.4, $\operatorname{rem}(S(\overline{g_i}, \overline{g_j}), \{\overline{g_1}, \ldots, \overline{g_t}\}) = 0$, lo que implica que $\{\overline{g_1}, \ldots, \overline{g_t}\}$ es una base de Gröbner para $I_{x_n=a}$. Como $\alpha(i) \neq 0$ para cada $1 \leq i \leq t$, tenemos que $1 \notin I_{x_n=a}$, lo que demuestra el caso 2 y el lema. □

Teorema 5.2 (Nullstellensatz débil). *Sea $\mathbb{F}$ un cuerpo algebraicamente cerrado. Sea $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ un ideal tal que $\mathbf{V}(I) = \varnothing$. Entonces $I = \mathbb{F}[x_1, \ldots, x_n]$.*

Demostración. Es un sencillo argumento inductivo obtenido a partir del Lema 5.1. □

Teorema 5.3 (Nullstellensatz)**.** *Sea* $\mathbb{F}$ *un cuerpo algebraicamente cerrado. Sea* $I \subseteq \mathbb{F}[x_1, \dots, x_n]$ *un ideal. Entonces* $f \in \mathbf{I}(\mathbf{V}(I))$ *si y solo si* $f^m \in I$ *para algún* $m \in \mathbb{N}$.

Demostración. Es sencillo comprobar que si $f^m \in I$, entonces $f \in \mathbf{I}(\mathbf{V}(I))$. Supongamos por tanto que $f \in \mathbf{I}(\mathbf{V}(I))$. Sea

$$J = \langle I \rangle + \langle yf - 1 \rangle \subseteq \mathbb{F}[x_1, \dots, x_n, y]$$

y sea $(a_1, \dots, a_n, a_{n+1}) \in \mathbb{F}^{n+1}$. Si $(a_1, \dots, a_n) \in \mathbf{V}(I)$, tenemos que $f(a_1, \dots, a_n) = 0$, por lo que

$$1 - a_{n+1} f(a_1, \dots, a_n) = 1 \neq 0,$$

es decir, $(a_1, \dots, a_n, a_{n+1}) \notin \mathbf{V}(J)$. Por otra parte, si $(a_1, \dots, a_n) \notin \mathbf{V}(I)$, tenemos que $(a_1, \dots, a_n, a_{n+1}) \notin \mathbf{V}(I) \supseteq \mathbf{V}(J)$ viendo $I \subseteq \mathbb{F}[x_1, \dots, x_n, y]$. En cualquier caso $(a_1, \dots, a_n, a_{n+1}) \notin \mathbf{V}(J)$, por lo que $\mathbf{V}(J) = \varnothing$. Por el Teorem 5.2,

$$1 = \sum_{i=1}^{s} p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(1 - yf)$$

para ciertos $p_i, q \in \mathbb{F}[x_1, \dots, x_n, y]$ y $f_i \in I$ con $1 \leq i \leq s$. Sea $y = \frac{1}{f}$. Tenemos que

$$1 = \sum_{i=1}^{s} p_i \left(x_1, \dots, x_n, \tfrac{1}{f} \right) f_i.$$

Multiplicando ambos lados de la igualdad por f^m con m suficientemente grande para que se eliminen todos los denominadores, tenemos que

$$f^m = \sum_{i=1}^{s} h_i f_i$$

para ciertos $h_i \in \mathbb{F}[x_1, \dots, x_n]$ con $1 \leq i \leq s$. En conclusión $f^m \in I$, como queríamos. □

5.2 Radical de un ideal

Sea I un ideal de un anillo conmutativo R. Se define el radical de I como el conjunto

$$\sqrt{I} = \{f \in R \mid f^m \in I \text{para algún } m \in \mathbb{N}\}$$

.

Proposición 5.4. $\sqrt{I}$ *es un ideal de* R *que contiene a* I.

Demostración. Es inmediato que $I \subseteq \sqrt{I}$. Sean $f, g \in \sqrt{I}$ y sean m, l tales que $f^m, g^l \in I$. Dado que

$$\begin{aligned}(f+g)^{m+l} &= \textstyle\sum_{k=0}^{m} \binom{m+l}{k} f^k g^{m+l-k} + \sum_{k=m+1}^{m+l} \binom{m+l}{k} f^k g^{m+l-k} \\ &= g^l \textstyle\sum_{k=0}^{m} \binom{m+l}{k} f^k g^{m-k} \\ &\quad + f^m \textstyle\sum_{k=m+1}^{m+l} \binom{m+l}{k} f^{k-m} g^{m+l-k} \\ &\in I,\end{aligned}$$

tenemos que $f + g \in \sqrt{I}$. Por otra parte,

$$(hf)^m = h^m f^m \in I$$

para cualquier $h \in A$. Por tanto $\sqrt{I}$ es un ideal. $\square$

Decimos que un ideal es radical si $I = \sqrt{I}$. Observemos que I es radical si y solo si

$$f^m \in I \text{ para algún } m \in \mathbb{N} \Rightarrow f \in I.$$

Lema 5.5. *Sea $A \subseteq \mathbb{F}^n$. Entonces $\mathbf{I}(A)$ es un ideal radical.*

Demostración. Supongamos que $f^m \in \mathbf{I}(A)$. Entonces para cualquier $a \in A$, $f(a)^m = 0$, lo que implica que $f(a) = 0$ para cualquier $a \in A$. En consecuencia $f \in \mathbf{I}(A)$. $\square$

Teorema 5.6 (Nullstellensatz fuerte)**.** *Sea $\mathbb{F}$ algebraicamente cerrado. Si $I \subseteq \mathbb{F}[x_1, \dots, x_n]$ es un ideal,*

$$\sqrt{I} = \mathbf{I}(\mathbf{V}(I)).$$

Demostración. Si $f \in \sqrt{I}$, tenemos que $f^m \in I \subseteq \mathbf{I}(\mathbf{V}(I))$. Por el Lema 5.5, $f \in \mathbf{I}(\mathbf{V}(I))$.
Por otra parte, si $f \in \mathbf{I}(\mathbf{V}(I))$, por el Teorema 5.3 $f^m \in I$ para algún $m \in \mathbb{N}$, es decir, $f \in \sqrt{I}$. $\square$

Teorema 5.7. *Sea $\mathbb{F}$ un cuerpo.*

(A) Las aplicaciones

$$\textit{variedades afines} \xrightarrow{\mathbf{I}} \textit{ideales}$$

y

$$\textit{ideales} \xrightarrow{\mathbf{V}} \textit{variedades afines}$$

invierten la inclusión.

(B) Para cada variedad V, $\mathbf{V}(\mathbf{I}(V)) = V$, *por lo que* $\mathbf{I}$ *es inyectiva.*

(C) $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$ *para cualquier ideal* I.

(D) Si $\mathbb{F}$ *es algebraicamente cerrado, las aplicaciones*

$$\textit{variedades afines} \xrightarrow{\mathbf{I}} \textit{ideales radicales}$$

y

$$\textit{ideales radicales} \xrightarrow{\mathbf{V}} \textit{variedades afines}$$

son biyecciones inversa una de otra que invierten la inclusión.

Demostración. Ejercicio. □

Proposición 5.8. *Sea* $I \subseteq \mathbb{F}[x_1, \dots, x_n]$. *Sea* $f \in \mathbb{F}[x_1, \dots, x_n]$ *y sea* $J = \langle I \rangle + \langle 1 - fy \rangle \subseteq \mathbb{F}[x_1, \dots x_n, y]$. *Tenemos que* $f \in \sqrt{I}$ *si y solo si* $J = \mathbb{F}[x_1, \dots x_n, y]$.

Demostración. Un argumento análogo al empleado en la demostración del Teorema 5.3 demuestra que si $J = \mathbb{F}[x_1, \dots x_n, y]$, tenemos que $f^m \in I$ para algún $m \in \mathbb{N}$, por lo que $f \in \sqrt{I}$.
Para ver la implicación contraria, supongamos que $f^m \in I \subseteq J$. Como $1 - fy \in J$, tenemos que

$$\begin{aligned} 1 &= y^m f^m + (1 - (yf)^m) \\ &= y^m f^m + (1 + yf + \cdots + (yf)^{m-1})(1 - yf) \in J, \end{aligned}$$

por lo que $J = \mathbb{F}[x_1, \dots x_n, y]$. $\square$

Proposición 5.9. $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Demostración. Si $f \in \sqrt{I \cap J}$, $f^m \in I \cap J \subseteq I$, por lo que $f \in \sqrt{I}$. Análogamente $f \in \sqrt{J}$ y tenemos la inclusión $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Si $f \in \sqrt{I} \cap \sqrt{J}$, existen m, l tales que $f^m \in I$ y $f^l \in J$. En consecuencia $f^{m+l} = f^m f^l \in I \cap J$, por lo que $f \in \sqrt{I \cap J}$. $\square$

5.3 Cocientes de ideales y saturación

Sea I un ideal en un anillo conmutativo R y sea $F \subseteq R$ no vacío. Se define el cociente como

$$I : F = \{f \in R \mid fg \in I \; \forall g \in F\}$$

Proposición 5.10. $I : F$ *es un ideal que contiene a* I.

Demostración. Es inmediato observar que si $f \in I$, entonces $fg \in I$ para todo $g \in F$, por lo que $f \in I : J$. Sean $f_1, f_2 \in I : J$. Entonces para todo $g \in F$, $f_1 g, f_2 g \in I$, lo que implica que

$$(f_1 + f_2)g = f_1 g + f_2 g \in I,$$

para todo $g \in F$. Esto demuestra que $f_1 + f_2 \in I : F$. Por otra parte, sea $f \in I : F$, $h \in R$ y $g \in F$. Como $fg \in I$, tenemos que $hfg \in I$. Al ser $g \in F$ un elemento arbitrario, tenemos que $hf \in I : F$, lo que demuestra que $I : F$ es un ideal. $\square$

Proposición 5.11. $I : F = I : \langle F \rangle$.

Demostración. Como $F \subseteq \langle F \rangle$, tenemos que $I : F \supseteq I : \langle F \rangle$. Sea $f \in I : F$ y sea $g = \sum_{i=1}^{s} h_i f_i \in \langle F \rangle$ para ciertos $f_1, \ldots, f_s \in F$. Como $ff_i \in I$, para cada $1 \leq i \leq s$, tenemos que

$$fg = \sum_{i=1}^{s} h_i f f_i \in I,$$

lo que implica que $f \in I : \langle F \rangle$ al ser g un elemento arbitrario de $\langle F \rangle$. $\square$

La saturación se define de manera similar. Sea I un ideal en un anillo conmutativo R y sea $F \subseteq R$ no vacío. La saturación de I respecto de F se define como

$$I : F^{\infty} = \{f \in R \mid \forall g \in F, \exists n \in \mathbb{N}, fg^{n} \in I\}$$

Proposición 5.12. $I : F^{\infty} = I : \langle F \rangle^{\infty}$.

Demostración. Como $F \subseteq \langle F \rangle$, tenemos que $I : F^{\infty} \supseteq I : \langle F \rangle^{\infty}$. Sea $f \in I : F^{\infty}$ y sea $g = \sum_{i=1}^{s} h_i g_i \in \langle F \rangle$ para ciertos $g_1, \ldots, g_s \in F$. Existe $n \in \mathbb{N}$ tal que $fg_i^{n} \in I$ para todo $1 \leq i \leq s$. Por el Teorema multinomial

$$g^{sn} = \textstyle\sum_{k_1 + \cdots + k_s = sn} \binom{sn}{k_1, \ldots, k_s} \prod_{i=1}^{s} (h_i g_i)^{k_i},$$

por lo que

$$fg^{sn} = \textstyle\sum_{k_1 + \cdots + k_s = sn} \binom{sn}{k_1, \ldots, k_s} \prod_{i=1}^{s} h_i^{k_i} f g_i^{k_i} \in I,$$

ya que $k_1 + \cdots + k_s = sn$ implica que existe un $1 \leq i \leq s$ tal que $k_i \geq n$. Dado que g es un elemento arbitrario de $\langle F \rangle$, tenemos que $f \in I : \langle F \rangle^{\infty}$. $\square$

En vista de las Proposiciones 5.11 y 5.12 no perdemos generalidad si nos restringimos a calculas cocientes y saturaciones de ideales.

Proposición 5.13. *Sean* I, J *ideales de* R. *Se verifican las siguientes afirmaciones:*

(A) $I : J^\infty$ *es un ideal.*

(B) $I \subseteq I : J^m \subseteq I : J^\infty$ *para todo* $m \in \mathbb{N}$.

(C) Si R *es Noetheriano, existe* $N \in \mathbb{N}$ *tal que* $I : J^\infty = I : J^n$ *para todo* $n \geq N$.

(D) Si J *es finitamente generado,* $\sqrt{I : J^\infty} = \sqrt{I} : J$.

Demostración. El apartado (A) es análogo a la parte correspondiente de la Proposición 5.10, y se deja como ejercicio.
Si $f \in I : J^m$ y $g \in J$, tenemos que $g^m \in J^m$, por lo que $fg^m \in I$, lo que implica que $f \in I : J^\infty$, es decir $I : J^m \subseteq I : J^\infty$. Observemos que $J_1 \subseteq J_2$ implica que $I : J_1 \subseteq I : J_2$, por lo que $I : J^m \subseteq I : J^{m+1}$, y en particular $I : J \subseteq I : J^m$ para cualquier $m \geq 1$. El apartado (B) es, por tanto, consecuencia de la Proposición 5.10.
La cadena descendente

$$J \supseteq J^2 \supseteq \cdots \supseteq J^n \supseteq \cdots$$

produce una cadena ascendente

$$I : J \subseteq I : J^2 \subseteq \cdots \subseteq I : J^n \subseteq \cdots .$$

Si R es Noetheriano, la cadena anterior debe estabilizar, es decir, existe $N \in \mathbb{N}$ tal que $I : J^N = I : J^n$ para todo $n \geq N$. Para demostrar

(C) veamos que $I : J^N = I : J^\infty$. Sea $f \in I : J^N$ y $g \in J$. Ya hemos visto que $I : J^N \subseteq I : J^\infty$, por lo que nos queda comprobar la inclusión contraria. Como $J = \langle g_1, \dots, g_s \rangle$, por la Proposición 5.12 $I : J^\infty = I : \{g_1, \dots, g_s\}^\infty$. Sea $f \in I : \{g_1, \dots, g_s\}^\infty$, existe $M \geq N$ tal que $fg_i^M \in I$ para cualquier $1 \leq i \leq s$, por lo que $f \in I : \langle g_1^M, \dots, g_s^M \rangle$. Es un ejercicio demostrar que

$$J^{sM} \subseteq \langle g_1^M, \dots, g_s^M \rangle,$$

por lo que

$$I : \langle g_1^M, \dots, g_s^M \rangle \subseteq I : J^{sM} = I : J^N.$$

En consecuencia $f \in I : J^N$, lo que demuestra (C).
El apartado (D) también lo demostramos por doble inclusión. Supongamos que $f \in \sqrt{I : J^\infty}$. Existe $m \in \mathbb{N}$ tal que $f^m \in I : J^\infty$. Dado $g \in J$, existe $M \in \mathbb{N}$ tal que $f^m g^M \in I$, lo que implica que $(fg)^{\text{máx}\{m,M\}} \in I$, es decir, $fg \in \sqrt{I}$. Como g es un elemento arbitrario de J, tenemos que $f \in \sqrt{I} : J$, lo que demuestra que $\sqrt{I : J^\infty} \subseteq \sqrt{I} : J$. Recíprocamente, sea $f \in \sqrt{I} : J$ y sea $J = \langle g_1, \dots, g_s \rangle$. Existe $M \in \mathbb{N}$ tal que $f^M g_i^M = (fg_i)^M \in I$ para cada $1 \leq i \leq s$, lo que implica que

$$f^M \in I : \langle g_1^M, \dots, g_s^M \rangle \subseteq I : J^{sM}$$

de igual forma a la demostración del apartado (C). Como por (B)

$$I : J^{sM} \subseteq I : J^\infty,$$

tenemos que $f \in \sqrt{I : J^\infty}$, lo que demuestra la inclusión $\sqrt{I} : J \subseteq \sqrt{I : J^\infty}$ y el resultado. $\square$

Proposición 5.14. *Sean* $I, J_1, \ldots, J_r$ *ideales en un anillo conmutativo* R. *Entonces*

$$I : \left(\sum_{i=1}^r J_i\right) = \bigcap_{i=1}^r (I : J_i)$$

y

$$I : \left(\sum_{i=1}^r J_i\right)^\infty = \bigcap_{i=1}^r (I : J_i^\infty)$$

Demostración. Ejercicio □

Corolario 5.15. *Sea* I *un ideal de* R *y* $g_1, \ldots, g_s \in R$. *Entonces*

$$I : \{g_1, \ldots, g_s\} = \bigcap_{i=1}^r (I : g_i)$$

y

$$I : \{g_1, \ldots, g_s\}^\infty = \bigcap_{i=1}^r (I : g_i^\infty) .$$

Teorema 5.16. *Sea* I *un ideal de* $\mathbb{F}[x_1, \ldots, x_n]$ *y sea* $g \in \mathbb{F}[x_1, \ldots, x_n]$.

(A) Si $I \cap \langle g \rangle = \langle h_1, \ldots, h_s \rangle$, *entonces* $I : g = \langle h_1/g, \ldots, h_s/g \rangle$.

(B) Sea $\tilde{I} = \langle I \rangle + \langle 1 - yg \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n, y]$. *Entonces*

$$I : g^\infty = \tilde{I} \cap \mathbb{F}[x_1, \ldots, x_n].$$

Demostración. Si $f \in \langle h_1/g, \ldots, h_s/g \rangle$, tenemos que $f = \sum_{i=1}^s a_i(h_i/g)$, por lo que

$$fg = \sum_{i=1}^s a_i h_i \in I \cap \langle g \rangle \subseteq I,$$

por lo que $f \in I : g$. Recíprocamente, si $fg \in I$, dado que $fg \in \langle g \rangle$, tenemos que $fg = \sum_{i=1}^r a_i h_i$, por lo que $f = \sum_{i=1}^r a_i(h_i/g)$, por lo que $I : g \subseteq \langle h_1/g, \ldots, h_s/g \rangle$. Con esto tenemos (A).
El apartado (B) se deja como ejercicio. □

5.4

Variedades irreducibles

Definición 5.17. Una variedad afín $V \subseteq \mathbb{F}^n$ se dice irreducible si $V = V_1 \cup V_2$ con V_1, V_2 variedades afines implica que $V = V_1$ o $V = V_2$.

Definición 5.18. Un ideal $I \subseteq R$ en un anillo conmutativo se dice primo si $fg \in I$ implica $f \in I$ o $g \in I$.

Proposición 5.19. *Un ideal $I \subseteq R$ es primo si y solo si R/I es un dominio.*

Demostración. Ejercicio. □

Proposición 5.20. *Una variedad afín $V \subseteq \mathbb{F}^n$ es irreducible si y solo si $\mathbf{I}(V)$ es un ideal primo.*

Demostración. Supongamos que V es irreducible y sean f, g tales que $fg \in \mathbf{I}(V)$. Sean $V_1 = V \cap \mathbf{V}(f)$ y $V_2 = V \cap \mathbf{V}(g)$. Dado $a \in V$, como $(fg)(a) = 0$ tenemos que $a \in \mathbf{V}(f)$ o $a \in \mathbf{V}(g)$, por lo que deducimos que $V = V_1 \cup V_2$. Dado que V es irreducible, tenemos que $V = V_1$ o $V = V_2$. Si $V = V_1 = V \cap \mathbf{V}(f)$, tenemos que $V \subseteq \mathbf{V}(f)$, lo que implica que $f \in \mathbf{I}(V)$. Si $V = V_2$ concluimos que $g \in \mathbf{I}(V)$, lo que implica que $\mathbf{I}(V)$ es primo.
Recíprocamente, supongamos que $\mathbf{I}(V)$ es primo y supongamos que $V = V_1 \cup V_2$. Supongamos que $V \neq V_1$. Como $V_2 \subseteq V$, tenemos que $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$. Sea $f \in \mathbf{I}(V_2)$. Dado que $V_1 \subsetneq V$, tenemos que $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$, por lo que existe $g \in \mathbf{I}(V_1) \setminus \mathbf{I}(V)$. Dado $a \in V = V_1 \cup V_2$, si $a \in V_1$ tenemos que $g(a) = 0$, y si $a \in V_2$ concluimos que $f(a) = 0$. En ambos casos $(fg)(a) = f(a)g(a) = 0$,

por lo que $fg \in \mathbf{I}(V)$. Como $\mathbf{I}(V)$ es primo y $g \notin \mathbf{I}(V)$ tenemos que $f \in \mathbf{I}(V)$, lo que implica que $\mathbf{I}(V) = \mathbf{I}(V_2)$. En consecuencia $V = V_2$ y V es irreducible. □

Corolario 5.21. *Si $\mathbb{F}$ es algebraicamente cerrado, $\mathbf{I}()$ y $\mathbf{V}()$ proporcionan biyecciones entre variedades irreducibles e ideales primos.*

Proposición 5.22. *Si $\mathbb{F}$ es un cuerpo infinito, toda variedad definida por parametrizaciones racionales es irreducible.*

Demostración. Sea V la menor variedad conteniendo a la imagen de la aplicación

$$\begin{aligned} \phi : \mathbb{F}^r \setminus W &\to \mathbb{F}^n \\ (a_1, \ldots, a_r) &\mapsto \left(\frac{f_1(a_1,\ldots,a_r)}{q_1(a_1,\ldots,a_r)}, \ldots, \frac{f_n(a_1,\ldots,a_r)}{q_n(a_1,\ldots,a_r)} \right), \end{aligned}$$

donde $f_1, \ldots, f_n, q_1, \ldots, q_n \in \mathbb{F}[t_1, \ldots, t_r]$ y $W = \mathbf{V}(q_1 \cdots q_n)$. Dado que $\mathbf{I}(V) = \mathbf{I}(\mathrm{im}(\phi))$, tenemos que

$$\mathbf{I}(V) = \{h \in \mathbb{F}[X] \mid (h \circ \phi)(a) = 0 \; \forall a \in \mathbb{F}^r \setminus W\}.$$

Si $a \in \mathbb{F}^r \setminus W$, tenemos que

$$(h \circ \phi)(a) = 0 \iff ((q_1 \cdots q_n)^N (h \circ \phi))(a) = 0.$$

Sea N el grado total de h. Es un ejercicio comprobar que

$$(q_1 \cdots q_n)^N (h \circ \phi) \in \mathbb{F}[t_1, \ldots, t_r].$$

Como $\mathbb{F}$ es infinito, concluimos que

$$h \in \mathbf{I}(V) \iff (q_1 \cdots q_n)^N (h \circ \phi) = 0 \in \mathbb{F}[t_1, \ldots, t_r].$$

Supongamos que $fg \in \mathbf{I}(V)$, y sean M y N los grados totales de f y g respectivamente. Como el grado total de fg es $M+N$, tenemos que

$$(q_1 \cdots q_n)^M (f \circ \phi)(q_1 \cdots q_n)^N (g \circ \phi) = \\ (q_1 \cdots q_n)^{M+N} (f \circ \phi)(g \circ \phi) = 0.$$

Como $\mathbb{F}[t_1, \dots, t_r]$ es un dominio y $(q_1 \cdots q_n)^M (f \circ \phi)$, $(q_1 \cdots q_n)^N (g \circ \phi)$ son polinomios, tenemos que uno de ellos debe ser cero, es decir, $f \in \mathbf{I}(V)$ o $g \in \mathbf{I}(V)$. Con esto demostramos que $\mathbf{I}(V)$ es un ideal primo, lo que implica por la Proposición 5.20 que V es irreducible. □

Definición 5.23. Un ideal $I \subseteq R$ se dice maximal si $I \neq R$, y para cualquier otro ideal J tal que $I \subseteq J \subseteq R$, se tiene que $J = I$ o $J = R$.

Proposición 5.24. $M \subseteq R$ *es maximal si y sólo si* R/M *es un cuerpo.*

Demostración. Ejercicio. □

Corolario 5.25. *Todo ideal maximal es primo.*

Demostración. Consecuencia inmediata del hecho de que todo cuerpo es un dominio. □

Proposición 5.26. *Dados* $a_1, \dots, a_n \in \mathbb{F}$, *el ideal*

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle \in \mathbb{F}[x_1, \dots, x_n]$$

es maximal.

Demostración. Ejercicio. □

Teorema 5.27. *Si $\mathbb{F}$ es algebraicamente cerrado,* $I \subseteq \mathbb{F}[X]$ *es maximal si y solo si*

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

para ciertos $a_1, \ldots, a_n \in \mathbb{F}$.

Demostración. Dado que $I \neq \mathbb{F}[X]$, $\mathbf{V}(I) \neq \varnothing$ por el Teorema 5.2, es decir, existe $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. Como para cualquier $f \in I$, tenemos que $f(a_1, \ldots, a_n) = 0$, tenemos que $f \in \mathbf{I}(\{(a_1, \ldots, a_n)\})$. Por tanto

$$I \subseteq \mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

donde la última igualdad es un ejercicio. Por la Proposición 5.26, tenemos que $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

Corolario 5.28. *Si $\mathbb{F}$ es algebraicamente cerrado, existe una biyección entre los puntos de $\mathbb{F}^n$ y los ideales maximales de $\mathbb{F}[x_1, \ldots, x_n]$.*

5.5 Descomposición de variedades

Proposición 5.29. *Las variedades afines satisfacen la condición de cadena descendente.*

Demostración. Supongamos que tenemos una cadena de variedades afines en $\mathbb{F}^n$

$$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_m \supseteq V_{m+1} \supseteq \cdots.$$

Esta cadena induce la cadena siguiente de ideales en $\mathbb{F}[x_1, \ldots, x_n]$

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \cdots \subseteq \mathbf{I}(V_m) \subseteq \mathbf{I}(V_{m+1}) \subseteq \cdots.$$

Como $\mathbb{F}[x_1, \ldots, x_n]$ es Noetheriano, existe m_0 tal que, $\mathbf{I}(V_{m_0}) = \mathbf{I}(V_m)$ para todo $m \geq m_0$, lo que implica que $V_{m_0} = V_m$ para todo $m \geq m_0$. □

Teorema 5.30. *Toda variedad* $V \subseteq \mathbb{F}^n$ *se descompone como una unión finita* $V = V_1 \cup \cdots \cup V_m$ *de variedades irreducibles.*

Demostración. Si V no puede ponerse como unión finita de variedades irreducibles tenemos $V = V_1 \cup V_1'$ con $V \supsetneq V_1$, $V \subsetneq V_1'$ y V_1 tampoco puede ponerse como unión finita de variedades irreducibles. Por el mismo argumento $V_1 = V_2 \cup V_2'$ con $V_1 \supsetneq V_2$, $V_1 \supsetneq V_2'$ y V_2 una variedad que no puede ponerse como unión finita de variedades irreducibles. Reiterando la construcción llegamos a una cadena infinita

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots$$

de variedades afines, lo que no puede existir por la Proposición 5.29. □

Definición 5.31. Sea $V \subseteq \mathbb{F}^n$ una variedad afín. Una descomposición

$$V = V_1 \cup \cdots \cup V_m$$

como unión de variedades irreducibles se dice minimal si $V_i \not\subseteq V_j$ cuando $i \neq j$.

Teorema 5.32. *Toda variedad afín* $V \subseteq \mathbb{F}^n$ *tiene una descomposición minimal, que es única salvo el orden.*

Demostración. El Teorema 5.30 garantiza una descomposición

$$V = V_1 \cup \cdots \cup V_m$$

como unión de variedades irreducibles. Si existen $i \neq j$ tales que $V_i \subseteq V_j$, tenemos que

$$V = V_1 \cup \cdots \cup V_{i-1} \cup V_{i+1} \cup \cdots \cup V_m$$

es también una descomposición en variedades irreducibles. Reiterando la operación llegamos a una descomposición minimal.
Para ver la unicidad, supongamos que tenemos otra descomposición minimal $V = V_1' \cup \cdots \cup V_l'$. Tenemos que

$$V_i = V_i \cap V = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_l').$$

Por la irreducibilidad de V_i, existe j tal que $V_i = V_i \cap V_j'$, es decir, $V_i \subseteq V_j'$. Argumentando de forma análoga, $V_j' \subseteq V_k$ para cierto k, por lo que

$$V_i \subseteq V_j' \subseteq V_k.$$

Por la minimalidad de la descomposición tenemos que $i = k$ y $V_i = V_j'$. Esto implica que $m \leq l$ y

$$\{V_1, \ldots, V_m\} \subseteq \{V_1', \ldots, V_l'\}.$$

Invistiendo los papeles de las descomposiciones tenemos que $l \leq m$ y

$$\{V_1', \ldots, V_l'\} \subseteq \{V_1, \ldots, V_m\}.$$

lo que da la unicidad de la descomposición minimal. □

5.6 Descomposición primaria de ideales

Definición 5.33. Un ideal $I \subseteq R$ se dice primario si $fg \in I$ implica que $f \in I$ o que $g^m \in I$ para cierto $m \geq 0$.

Lema 5.34. *Si* I *es primario,* $\sqrt{I}$ *es primo, en cuyo caso* $\sqrt{I}$ *es el menor ideal primo que contiene a* I.

Demostración. Ejercicio. $\square$

Si I es primario y $P = \sqrt{I}$, se dice que I es P-primario.
Digamos que $I \subseteq R$ es irreducible si $I = I_1 \cap I_2$ implica que $I = I_1$ o $I = I_2$.

Lema 5.35. *Todo ideal irreducible es primario.*

Demostración. Supongamos que I es irreducible y que $fg \in I$. Por la Proposición 5.13, existe N tal que $I : g^\infty = I : g^N$. Es un ejercicio comprobar que $I = (I + \langle g^N \rangle) \cap (I + \langle f \rangle)$. Como I es irreducible, tenemos que $I = (I + \langle g^N \rangle)$ o $I = (I + \langle f \rangle)$, lo que implica que $f \in I$ o $g^N \in I$. $\square$

Teorema 5.36. *Todo ideal de un anillo conmutativo Noetheriano* R *puede ponerse como intersección finita de ideales primarios.*

Demostración. Digamos que $I \subseteq R$ es irreducible si $I = I_1 \cap I_2$ implica que $I = I_1$ o $I = I_2$. De forma análoga al Teorema 5.30 pero empleando la condición de cadena ascendente, podemos demostrar que todo ideal puede escribirse como una intersección finita de ideales irreducibles. El Teorema es por tanto consecuencia del Lema 5.35. $\square$

Definición 5.37. Una descomposición primaria de un ideal I es una expresión $I = \bigcap_{i=1}^{m} Q_i$ donde Q_i es primario para todo $1 \leq i \leq m$. La descomposición se dice minimal si $\sqrt{Q_i} \neq \sqrt{Q_j}$ para $i \neq j$ y $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$.

Lema 5.38. *Si* I, J *son primarios tales que* $\sqrt{I} = \sqrt{J}$, *entonces* $I \cap J$ *es primario.*

Demostración. Ejercicio. □

Teorema 5.39 (Lasker-Noether)**.** *Todo ideal* $I \subseteq R$ *en un anillo conmutativo Noetheriano tiene una descomposición primaria minimal.*

Demostración. La existencia de la descomposición primaria $I = \bigcap_{i=1}^m Q_i$ es consecuencia del Teorema 5.36. Supongamos que existen $i \neq j$ tales que $\sqrt{Q_i} = \sqrt{Q_j}$. Por el Lema 5.38, $Q_{ij} = Q_i \cap Q_j$ es un ideal primario, por lo que podemos cambiar Q_i y Q_j por Q_{ij} en la descomposición primaria. Reiterando el procedimiento eventualmente llegamos a una descomposición primaria en la que cada radical es distinto. Llamamos nuevamente $I = \bigcap_{i=1}^m Q_i$ a dicha descomposición. Si existe i tal que $Q_i \supseteq \bigcap_{j \neq i} Q_j$, tenemos que $I = \bigcap_{j \neq i} Q_j$, una nueva descomposición primaria. Reiterando nuevamente la construcción, llegamos a una descomposición primaria minimal. □

Teorema 5.40 (Lasker-Noether)**.** *Sea* $I = \bigcap_{i=1}^m Q_i$ *una descomposición primaria minimal de un ideal propio* I *en un anillo conmutativo Noetheriano* R. *Sea* $P_i = \sqrt{Q_i}$ *para cada* $1 \leq i \leq m$. *Entonces* $\{P_i \mid 1 \leq i \leq m\}$ *son los ideales primos propios que aparecen en el conjunto* $\{\sqrt{I : f} \mid f \in R\}$.

Demostración. Como $I = \bigcap_{i=1}^m Q_i$, tenemos que $I : f = \bigcap_{i=1}^m (Q_i : f)$. Por tanto

$$\sqrt{I : f} = \bigcap_{i=1}^m \sqrt{Q_i : f} = \bigcap_{\substack{i=1 \\ Q_i \not\ni f}}^m \sqrt{Q_i : f} = \bigcap_{\substack{i=1 \\ Q_i \not\ni f}}^m P_i$$

(ver ejercicios). Si $\sqrt{I : f}$ es primo propio, entonces $\sqrt{I : f} = P_i$ para algún i por ser los primos irreducibles (ver ejercicios). Por otra parte, si $f \in \bigcap j \neq i Q_j \setminus Q_i$, tenemos que

$$\sqrt{I : f} = \bigcap_{\substack{j=1 \\ Q_j \not\ni f}}^{m} \sqrt{Q_j : f} = \sqrt{Q_i : f} = P_i,$$

lo que demuestra el teorema. □

Ejercicios sobre Variedades Irreducibles y Descomposición

Ejercicio 5.1. Encuentra $f \in \mathbf{I}(\mathbf{V}(I)) \setminus I$, donde $I = \langle x^2+y^2-1, y-1\rangle$.

Ejercicio 5.2. Demuestra que $\mathbf{V}(y-x^2, z-x^3) = \mathbf{V}((y-x^2)^2+(z-x^3)^2) \subseteq \mathbb{R}^3$.

Ejercicio 5.3. ¿Es posible encontrar dos ideales en $\mathbb{R}[x,y]$ que definan la misma variedad tales que ninguno esté incluido en el otro? Responde a la misma pregunta para $\mathbb{R}[x]$.

Ejercicio 5.4. Sea $\mathbb{F}$ un cuerpo.

1. Dado $g = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}[x]$ con $a_0 \neq 0$, se define la homogenización de g como

$$g^h = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n$$

   Demuestra que g tiene una raíz en $\mathbb{F}$ si y solo si existe $(a,b) \in \mathbb{F}^2 \setminus \{(0,0)\}$ tal que $g^h(a,b) = 0$.

2. Si $\mathbb{F}$ no es algebraicamente cerrado, demuestra que existe $f \in \mathbb{F}[x,y]$ tal que $\mathbf{V}(f) = \{(0,0)\}$.

3. Si $\mathbb{F}$ no es algebraicamente cerrado, demuestra que para cualquier $l > 0$ existe $f \in \mathbb{F}[x_1,\ldots,x_l]$ tal que $\mathbf{V}(f) = \{(0,\ldots,0)\}$.

4. Si $\mathbb{F}$ no es algebraicamente cerrado y $W = \mathbf{V}(g_1,\ldots,g_s)$ demuestra que existe $h \in \mathbb{F}[X]$ tal que $W = \mathbf{V}(h)$.

Ejercicio 5.5. Demuestra que $I : J^\infty$ es un ideal para cualesquiera ideales I, J en un anillo conmutativo R.

Ejercicio 5.6. Dado I ideal en un anillo conmutativo R,

1. Demuestra que $\sqrt{I}$ es un ideal radical.
2. Demuestra que I es radical si y solo si $\sqrt{I} = I$.
3. Demuestra que $\sqrt{\sqrt{I}} = \sqrt{I}$.

Ejercicio 5.7. Demuestra que un ideal es propio si y solo si su radical también es propio.

Ejercicio 5.8. Si $\sqrt{I} = \langle f_1, f_2 \rangle$ con $f_i^{m_i} \in I$, demuestra que $f^{m_1+m_2-1} \in I$ para cualquier $f \in \sqrt{I}$.

Ejercicio 5.9. Si I es un ideal en un anillo Noetheriano R, demuestra que existe $m \in \mathbb{N}$ tal que $f^m \in I$ para cualquier $f \in \sqrt{I}$.

Ejercicio 5.10. Determina si los siguientes polinomios pertenecen a los radicales indicados. En caso de respuesta afirmativa, encuentra la menor potencia que mete al polinomio en el ideal.

$$¿x + y \in \sqrt{\langle x^3, y^3, xy(x+y) \rangle}?,$$

$$¿x^2 + 3xz \in \sqrt{\langle x + z, x^2y, x - z^2 \rangle}?$$

Ejercicio 5.11. Sea R un DFU. Dados $f, g \in R$, se define (f, g) como el mayor (respecto de la divisibilidad) divisor común de f y g. Demuestra que existe (f, g). Demuestra que $h = (f, g)$ si y solo si $\langle h \rangle$ es el menor ideal principal que contiene a $\langle f, g \rangle$.

Ejercicio 5.12. Si $I = \langle f_1, \dots, f_s \rangle$, demuestra que $I^{sn} \subseteq \langle f_1^n, \dots, f_s^n \rangle$.

Ejercicio 5.13. Sean $I, J_1, \dots, J_r$ ideales en un anillo conmutativo R. Demuestra que

$$I : \left(\sum_{i=1}^r J_i\right) = \bigcap_{i=1}^r (I : J_i)$$

y

$$I : \left(\sum_{i=1}^r J_i\right)^\infty = \bigcap_{i=1}^r (I : J_i^\infty) \,.$$

Ejercicio 5.14. Demuestra que $\left(\bigcap_{i=1}^m I_i\right) : F = \bigcap_{i=1}^m (I_i : F)$.

Ejercicio 5.15. Sea I un ideal de $\mathbb{F}[x_1, \dots, x_n]$ y sea $g \in \mathbb{F}[x_1, \dots, x_n]$. Sea $\tilde{I} = \langle I \rangle + \langle 1 - yg \rangle \subseteq \mathbb{F}[x_1, \dots, x_n, y]$. Demuestra que

$$I : g^\infty = \tilde{I} \cap \mathbb{F}[x_1, \dots, x_n].$$

Ejercicio 5.16. Sean

$$f = (x+y)^2(x-y)(x+z^2)$$

y

$$g = (x+z^2)^3(x-y)(z+y).$$

Calcula $\langle f \rangle : \langle g \rangle$ considerando los polinomios con coeficientes en $\mathbb{Q}$ y en $\mathbb{Z}_2$.

Ejercicio 5.17. Sean I, J ideales de un anillo conmutativo R. Si I es radical, demuestra que $I : J$ es radical y $I : J = I : \sqrt{J} = I : J^\infty$.

Ejercicio 5.18. Sean $V, W \subseteq \mathbb{F}^n$ variedades afines. Demuestra que

$$\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V \setminus W).$$

Ejercicio 5.19. Demuestra que $I : J^{\infty} = I : J^{N}$ si y solo si $I : J^{N} = I : J^{N+1}$.

Ejercicio 5.20. Demuestra que

1. $IJ \subseteq K$ si y solo si $I \subseteq K : J$,
2. $(I : J) : K = I : (JK)$,

para cualesquiera ideales $I, J, K \subseteq R$.

Ejercicio 5.21. Demuestra que todo ideal primo es radical.

Ejercicio 5.22. Sean $f_1, \dots, f_n, q_1, \dots, q_n \in \mathbb{F}[t_1, \dots, t_r]$, $W = \mathbf{V}(q_1 \cdots q_n)$ y

$$\begin{aligned} \phi : \mathbb{F}^r \setminus W &\to \mathbb{F}^n \\ (a_1, \dots, a_r) &\mapsto \left(\frac{f_1(a_1, \dots, a_r)}{q_1(a_1, \dots, a_r)}, \dots, \frac{f_n(a_1, \dots, a_r)}{q_n(a_1, \dots, a_r)} \right). \end{aligned}$$

Dado $h \in \mathbb{F}[x_1, \dots, x_n]$, demuestra que

$$(q_1 \cdots q_n)^N (h \circ \phi) \in \mathbb{F}[t_1, \dots, t_r],$$

donde N es el grado total de h.

Ejercicio 5.23. Demuestra que

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle \in \mathbb{F}[x_1, \dots, x_n]$$

es un ideal maximal para cualesquiera $a_1, \dots, a_n \in \mathbb{F}$.

Ejercicio 5.24. Demuestra que $\mathbf{I}(\{(a_1, \dots, a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$.

Ejercicio 5.25. Demuestra que si I es primario, $\sqrt{I}$ es primo, en cuyo caso $\sqrt{I}$ es el menor ideal primo que contiene a I.

Ejercicio 5.26. Demuestra que en un anillo Noetheriano, todo ideal puede ser descrito como una intersección finita de ideales irreducibles.

Ejercicio 5.27. Demuestra que si $fg \in I$ e $I : g^\infty = I : g^N$, se tiene que $I = (I + \langle g^N \rangle) \cap (I + \langle f \rangle)$.

Ejercicio 5.28. Demuestra que si I, J son ideales primarios tales que $\sqrt{I} = \sqrt{J}$, entonces $I \cap J$ es primario.

Ejercicio 5.29. Si $P \subseteq R$ es primo, demuestra que $f \in P \iff P : f = P$, y $f \notin P \iff P : f = R$.

Ejercicio 5.30. Sea $I \subseteq R$ un ideal primario con $P = \sqrt{I}$, y sea $f \in R$. Demuestra que

1. si $f \in I$, entonces $I : f = R$,
2. si $f \notin I$, entonces $I : f$ es P-primario,
3. si $f \notin P$, entonces $I : f = I$.

Ejercicio 5.31. Si P es un ideal primo tal que $P \supseteq \bigcap_{i=1}^m I_i$, entonces existe i tal que $P \supseteq I_i$. Si $P = \bigcap_{i=1}^m I_i$, demuestra que $P = I_i$ para algún i.

Bibliografía

[1] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner Bases. A Computational Approach to Commutative Algebra.* Number 141 in Graduate Texts in Mathematics. Springer Science+Business Media, 1993.

[2] David A. Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Text in Mathematics. Springer, fourth edition, 2015.

[3] Ernst Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 1985.

[4] Serge Lang. *Undergraduate Algebra*. Undergraduate Text in Mathematics. Springer, second edition, 1990.