Tema 1

Variedades algebraicas

1.1. Conjuntos algebraicos afines

Sea k un cuerpo. Para todo entero positivo n, se denota por $\mathbb{A}^n k$ al k–espacio afín n–dimensional.
Fijado un sistema de referencia afín en $\mathbb{A}^n k$, la aplicación que a cada punto le asigna sus coordenadas afines es una biyección entre $\mathbb{A}^n k$ y k^n, el conjunto de n–uplas de elementos de k. A lo largo de estas notas asumiremos que en $\mathbb{A}^n k$ hay un sistema de referencia afín fijado de partida y haremos uso constantemente de la identificación del espacio afín con k^n.

(1.1.1) Definición. Sea n un entero positivo. Si S es un subconjunto del anillo de polinomios $k[x_1, \ldots, x_n]$, se llama *conjunto algebraico afín* definido por S, y se denota $V(S)$, al subconjunto de $\mathbb{A}^n k$

$$\{(a_1, \ldots, a_n);\ f(a_1, \ldots, a_n) = 0,\ \forall f \in S\}.$$

Si S es un conjunto unitario, pongamos $S = \{f\}$, entonces se dice que $V(S)$ es una *hipersuperficie*. Más concretamente, si $n = 2$ se dice que $V(S)$ es una *curva plana* y si $n = 3$, que $V(S)$ es una *superficie*.

(1.1.2) Proposición. *Sea n un entero positivo.*

(1.1.2.1) *Si S y T son subconjuntos de $k[x_1, \ldots, x_n]$ y $S \subseteq T$, entonces $V(S) \supseteq V(T)$.*

(1.1.2.2) *Si $S \subseteq k[x_1, \ldots, x_n]$ e I es el ideal generado por S, entonces $V(I) = V(S)$.*

(1.1.2.3) *Si $\{I_\alpha\}_{\alpha\in A}$ es una familia de ideales de $k[x_1, \ldots, x_n]$, entonces*

$$\bigcap_{\alpha\in A} V(I_\alpha) = V(\bigcup_{\alpha\in A} I_\alpha) = V(\sum_{\alpha\in A} I_\alpha).$$

(1.1.2.4) *Si I y J son ideales de $k[x_1, \ldots, x_n]$, entonces*

$$V(I) \cup V(J) = V(IJ).$$

(1.1.2.5) $V(0) = \mathbb{A}^n k$, $V(k[x_1, \ldots, x_n]) = \emptyset$ *y*

$$V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$$

para todo $a_1, \ldots, a_n \in k$.

Demostración. (1) Si $S \subseteq T$ y $(a_1, \ldots, a_n)$ es un punto de $V(T)$, entonces $f(a_1, \ldots, a_n) = 0$ para todo $f \in T$, y en particular para todo $f \in S$, luego

$$(a_1, \ldots, a_n) \in V(S).$$

(2) Dado que el ideal generado por la familia de polinomios S contiene a S, en virtud de (1) se tiene la inclusión $V(I) \subseteq V(S)$.
Sea $(a_1, \ldots, a_n) \in V(S)$. Si f pertenece a I, entonces existen

$$f_1, \ldots, f_n \in S, \quad g_1, \ldots, g_n \in k[x_1, \ldots, x_n]$$

tales que $f = \sum_{i=1}^n g_i f_i$. Dado que $f_i(a_1, \ldots, a_n) = 0$ para $1 \leq i \leq n$, el punto $(a_1, \ldots, a_n)$ también es un cero de f y por lo tanto pertenece a $V(I)$.

(3) Por (1) se puede afirmar que $V(\bigcup_{\beta \in A} I_\beta) \subseteq V(I_\alpha)$ para cada $\alpha \in A$, porque la unión contiene a cada uno de los ideales de la familia $\{I_\alpha\}_{\alpha \in A}$. Luego

$$V(\bigcup_{\beta \in A} I_\beta) \subseteq \bigcap_{\alpha \in A} V(I_\alpha).$$

Recíprocamente, si

$$(a_1, \ldots, a_n) \in \bigcap_{\alpha \in A} V(I_\alpha)$$

y $f \in \bigcup_{\alpha \in A} I_\alpha$, entonces existe $\alpha \in A$ tal que $f \in I_\alpha$, y además

$$f(a_1, \ldots, a_n) = 0$$

puesto que $(a_1, \ldots, a_n) \in V(I_\alpha)$.
Por otra parte, como el ideal generado por la unión $\bigcup_{\alpha \in A} I_\alpha$ es la suma $\sum_{\alpha \in A} I_\alpha$, el apartado (2) permite asegurar que

$$V(\bigcup_{\alpha \in A} I_\alpha) = V(\sum_{\alpha \in A} I_\alpha).$$

(4) Tanto I como J contienen a IJ, así que $V(I)$ y $V(J)$, y por lo tanto también $V(I) \cup V(J)$, están contenidos en $V(IJ)$.
Recíprocamente, si

$$(a_1, \ldots, a_n) \in V(IJ), \ (a_1, \ldots, a_n) \notin V(I),$$

entonces existe un polinomio f en I tal que $f(a_1, \ldots, a_n)$ es un elemento no nulo de k. Para todo polinomio $g \in J$ tenemos que

$$f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = fg(a_1, \ldots, a_n) = 0$$

porque $fg \in IJ$. Dado que en k no hay divisores de cero, $g(a_1, \ldots, a_n) = 0$, y esto implica que

$$(a_1, \ldots, a_n) \in V(J).$$

(5) Cualquier punto $(a_1, \ldots, a_n) \in \mathbb{A}^n k$ es un cero del polinomo nulo, así que $V(0) = \mathbb{A}^n k$.
Dado que los polinomios de grado cero (los elementos de k) no tienen ceros, el conjunto algebraico afín definido por el conjunto $k[x_1, \ldots, x_n]$ es vacío.
Finalmente, el punto $(a_1, \ldots, a_n)$ pertenece a

$$V(x_1 - a_1, \ldots, x_n - a_n)$$

porque $x_i - a_i$ se anula en $(a_1, \ldots, a_n)$ para $1 \leq i \leq n$.
Además, este es el único punto de $V(x_1 - a_1, \ldots, x_n - a_n)$ ya que si

$$(b_1, \ldots, b_n) \in V(x_1 - a_1, \ldots, x_n - a_n),$$

entonces $b_i - a_i = 0$ para cada i. □

(1.1.3) Si $n = 1$, entonces todo conjunto algebraico afín o bien es finito, o bien coincide con $\mathbb{A}^1 k$.
En efecto, si V es un conjunto algebraico afín, pongamos definido por el conjunto de polinomios $S \subseteq k[x]$, e I es el ideal generado por S, entonces $V = V(I)$. Además, como $k[x]$ es un dominio de ideales principales, podemos encontrar un polinomio f que genere a I, y entonces $V = V(f)$.
Si f es cero, entonces $V = \mathbb{A}^1 k$.
Si por el contrario f es distinto de cero, entonces f tiene a lo sumo un número finito de raíces, con lo que V es finito.

(1.1.4) Proposición. *Sea k un cuerpo no finito y $f \in k[x_1, \ldots, x_n]$ un polinomio no nulo.*

(1.1.4.1) *$V(f) \neq \mathbb{A}^n k$ y además $\mathbb{A}^n k \backslash V(f)$ es un conjunto no finito.*

(1.1.4.2) *Si f es no constante, k es algebraicamente cerrado y $n \geq 2$ entonces $V(f)$ es no finito.*

Demostración. (1) Si f es una constante, entonces $V(f) = \emptyset$, y su complementario es $\mathbb{A}^n k$, que es no finito por hipótesis.

Para el caso en que f es no constante podemos razonar por inducción sobre n. Si $n = 1$ entonces $V(f)$ es el conjunto de raíces de f, y su cardinal es finito. Como k es no finito, el complementario de $V(f)$ es también no finito, y en particular no vacío.

Supongamos que para todo polinomio no nulo $g \in k[x_1, \ldots, x_n]$, el complementario de $V(g)$ en $\mathbb{A}^n k$ es no finito (y en particular no vacío). Dado que $f \in k[x_1, \ldots, x_{n+1}]$ es no constante, es de grado al menos uno en alguna de las variables, pongamos x_i. Luego

$$f = g_0 + g_1 x_i + \ldots + g_m x_i^m \ ,$$

donde

$$g_j \in k[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1}], \ 0 \leq j \leq m \text{ y } g_m \neq 0,$$

con $m > 0$. Aplicando la hipótesis de inducción sobre g_m podemos garantizar que existe un punto

$$(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n+1}) \in \mathbb{A}^n k$$

que no pertenece a $V(g_m)$, esto es, tal que

$$g_m(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n+1}) \neq 0.$$

Luego

$$p(x_i) = f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_{n+1})$$

es un polinomio no constante en una variable y, tal como hemos comprobado para $n = 1$, el complementario de $V(p)$ en $\mathbb{A}^1 k$ es no finito.

Por lo tanto, el conjunto

$$\{(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{n+1}); \ a_i \in \mathbb{A}^1 k \backslash V(p)\} \ ,$$

que está contenido en el complementario de $V(f)$, es no finito.

(2) Dado que f es no constante, el grado de f en alguna de las variables, pongamos en x_i, es positivo, esto es,

$$f = g_0 + g_1 x_i + \ldots + g_m x_i^m \ ,$$

donde

$$g_j \in k[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n], \ 0 \leq j \leq m \text{ y } g_m \neq 0,$$

con $m > 0$. En virtud de (1), $\mathbb{A}^{n-1}k \setminus V(g_m)$ es no finito, y como k es algebraicamente cerrado, para cada punto $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ del complementario de $V(g_m)$ existe $a_i \in k$ tal que

$$(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) \in V(f).$$

Luego $V(f)$ es no finito. $\square$

(1.1.5) Sea X un conjunto de puntos de $\mathbb{A}^n k$ y sea F el conjunto de los polinomios $f \in k[x_1, \ldots, x_n]$ que se anulan en todos los puntos de X simultáneamente, esto es, tales que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n)$ perteneciente a X.

Está claro que el polinomio cero se anula en todos los puntos de X, luego $0 \in F$.

Además, si $f, g \in F$ y $h \in k[x_1, \ldots, x_n]$, entonces

$$f + g(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0$$

y

$$fh(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) \cdot h(a_1, \ldots, a_n) = 0$$

para todo $(a_1, \ldots, a_n) \in X$, luego $f + g$ y fh son elementos de F, con lo que F es un ideal de $k[x_1, \ldots, x_n]$.

(1.1.6) Definición. Si X es un subconjunto de $\mathbb{A}^n k$, se llama *ideal del conjunto* X, y se denota por $I(X)$ al ideal de $k[x_1, \ldots, x_m]$ formado por los polinomios que se anulan en todos los puntos de X simultáneamente.

(1.1.7) Proposición. *Sea n un entero positivo.*

(1.1.7.1) *Si X e Y son subconjuntos de $\mathbb{A}^n k$ y $X \subseteq Y$, entonces*

$$I(X) \supseteq I(Y).$$

(1.1.7.2) *Para cada $(a_1, \ldots, a_n) \in \mathbb{A}^n k$,*

$$I(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n).$$

Además $I(\emptyset) = k[x_1, \ldots, x_n]$ y si k es infinito, $I(\mathbb{A}^n k) = 0$.

(1.1.7.3) *$S \subseteq I(V(S))$ para todo $S \subseteq k[x_1, \ldots, x_n]$.*

(1.1.7.4) *Para todo $S \subseteq k[x_1, \ldots, x_n]$,*

$$V(I(V(S))) = V(S),$$

y para todo $X \subseteq \mathbb{A}^n k$,

$$I(V(I(X))) = I(X).$$

(1.1.7.5) *Si* $V, V' \subseteq \mathbb{A}^n k$ *son conjuntos algebraicos afines, entonces*

$$I(V \cup V') = I(V) \cap I(V').$$

(1.1.7.6) *Si* V *y* V' *son conjuntos algebraicos afines en el espacio afín* $\mathbb{A}^n k$, *entonces*

$$V \cup V' = V(I(V) \cdot I(V')).$$

Si $\{V_a\}_{a \in A}$ *son conjuntos algebraicos afines en* $\mathbb{A}^n k$, *entonces*

$$\bigcap a \in AV_a = V(\sum_{a \in A} I(V_a)).$$

(1.1.7.7) $I(X)$ *es un ideal radical para todo* $X \subseteq \mathbb{A}^n k$.

(1.1.7.8) *Para todo ideal* I *del anillo de polinomios* $k[x_1, \ldots, x_n]$,

$$V(I) = V(\mathrm{Rad} I)$$

y

$$\mathrm{Rad} I \subseteq I(V(I)).$$

Demostración. (1) Si f es un polinomio que se anula en todos los puntos de Y e $Y \supseteq X$, entonces f se anula en todos los puntos de X.

(2) El polinomio $x_i - a_i$ se anula en $(a_1, \ldots, a_n)$, así que pertenece al ideal $I(\{(a_1, \ldots, a_n)\})$ para cada i.
Si $f \in k[x_1, \ldots, x_n]$, entonces

$$g = f(y_1 + a_1, \ldots, y_n + a_n) \in k[y_1, \ldots, y_n]$$

es un polinomio en las indeterminadas $y_1, \ldots, y_n$, pongamos

$$g = \sum_{i_1, \ldots, i_n = 0}^{m} \lambda_{i_1, \ldots, i_n} y_1^{i_1} \cdots y_n^{i_n},$$

y su término independiente es $\lambda_{0,\ldots,0} = f(a_1, \ldots, a_n) \in k$. Luego

$$f = g(x_1 - a_1, \ldots, x_n - a_n) = \sum_{i_1, \ldots, i_n = 0}^{m} \lambda_{i_1, \ldots, i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}.$$

Si f se anula en $(a_1, \dots, a_n)$, entonces $\lambda_{0,\dots,0} = 0$, y por lo tanto

$$f = \sum_{\substack{i_1,\dots,i_n=0 \\ (i_1,\dots,i_n)\neq(0,\dots,0)}}^{m} \lambda_{i_1,\dots,i_n}(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} \in (x_1 - a_1, \dots, x_n - a_n).$$

Finalmente, para probar que $I(\mathbb{A}^n k) = 0$ cuando k es infinito, podemos utilizar un argumento de inducción sobre n.
Para $n = 1$, si $f \in I(\mathbb{A}^1 k)$, entonces f tiene infinitas raíces, luego $f = 0$.
Suponiendo el enunciado cierto para n, si $f \in I(\mathbb{A}^{n+1} k)$ es no nulo, entonces f es de grado $d \geq 1$ en alguna de las variables, pongamos x_i, puesto que $f \notin k$, o sea,

$$f = \sum_{j=0}^{d} g_j(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}) x_i^j.$$

Para cada n–upla $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n+1}) \in \mathbb{A}^n k$, el polinomio

$$f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_{n+1}) = \sum_{j=0}^{d} g_j(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n+1}) x_i^j$$

tiene infinitas raíces, y por lo tanto sus coeficientes son cero. Aplicando la hipótesis de inducción a g_j, tenemos que g_j es el polinomio cero para $1 \leq j \leq d$, y por tanto $f = 0$.

(3) Sea $f \in S$. Para todo $(a_1, \dots, a_n) \in V(S)$,

$$f(a_1, \dots, a_n) = 0,$$

luego $f \in I(V(S))$.

(4) Como $S \subseteq I(V(S))$, tenemos que

$$V(I(V(S))) \subseteq V(S).$$

Recíprocamente, si $(a_1, \dots, a_n) \in V(S)$, entonces

$$f(a_1, \dots, a_n) = 0$$

para todo $f \in I(V(S))$, de donde

$$(a_1, \dots, a_n) \in V(I(V(S))).$$

Por (3),

$$I(X) \subseteq I(V(I(X))).$$

Además, si $(a_1, \ldots, a_n)$ pertenece a X entonces

$$f(a_1, \ldots, a_n) = 0$$

para todo $f \in I(X)$, con lo que

$$(a_1, \ldots, a_n) \in V(I(X)).$$

Luego $X \subseteq V(I(X))$, y por (1),

$$I(V(I(X))) \subseteq I(X).$$

(5) Dado que $V, V' \subseteq V \cup V'$, por (1) tenemos que $I(V \cup V') \subseteq I(V), I(V')$. Por otra parte, si $f \in I(V) \cap I(V')$, entonces $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in V \cup V'$, es decir, $f \in I(V \cup V')$, de donde se sigue la otra inclusión.

(6) Como consecuencia de (1.1.2.4), (1.1.2.3) y de (4) tenemos que

$$V(I(V) \cdot I(V')) = V(I(V)) \cup V(I(V')) = V \cup V',$$

$$V(\sum_{a \in A} I(V_a)) = \bigcap_{a \in A} V(I(V_a)) = \bigcap_{a \in A} V_a.$$

(7) Si $f \in \mathrm{Rad}I(X)$, entonces existe un entero positivo m tal que $f^m \in I(X)$. Esto implica que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n)$ perteneciente a X, ya que $(f(a_1, \ldots, a_n))^m = 0$, y por tanto $f \in I(X)$.
Luego $I(X) = \mathrm{Rad}I(X)$, puesto que $I(X)$ está contenido en $\mathrm{Rad}I(X)$.

(8) Como $I \subseteq \mathrm{Rad}I$, tenemos que

$$V(\mathrm{Rad}I) \subseteq V(I).$$

Por otra parte, si $(a_1, \ldots, a_n) \in V(I)$ y $f \in \mathrm{Rad}I$, entonces existe un entero positivo m tal que $f^m \in I$, y por lo tanto

$$(f(a_1, \ldots, a_n))^m = 0.$$

Luego $f(a_1, \ldots, a_n) = 0$. Como este razonamiento es válido para cualquier $f \in \mathrm{Rad}I$, tenemos que $(a_1, \ldots, a_n) \in V(\mathrm{Rad}I)$.
Por otra parte, dado que $I \subseteq I(V(I))$ y $I(V(I))$ es un ideal radical,

$$\mathrm{Rad}I \subseteq \mathrm{Rad}I(V(I)) = I(V(I)).$$

$\square$

(1.1.8) El ideal

$$I = (x_1 - a_1, \ldots, x_n - a_n),$$

con $a_1, \ldots, a_n \in k$, es un ideal maximal de $k[x_1, \ldots, x_n]$.
En efecto, el homomorfismo de anillos que a cada $f \in k[x_1, \ldots, x_n]$ le asigna el elemento $f(a_1, \ldots, a_n) \in k$, tiene como núcleo al conjunto de polinomios que se anulan en $(a_1, \ldots, a_n)$, esto es, a

$$I(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n).$$

Por el primer teorema de isomorfía,

$$k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)$$

es isomorfo a k, y por lo tanto es un cuerpo. Luego $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal maximal.

(1.1.9) Nota. La aplicación I del conjunto de conjuntos algebraicos afines en el conjunto de ideales radicales de $k[x_1, \ldots, x_n]$ que a cada V le asigna el ideal $I(V)$ es inyectiva.
En efecto, si $I(V) = I(V')$, entonces

$$V = V(I(V)) = V(I(V')) = V'.$$

Sin embargo, I no tiene por qué ser sobreyectiva, pues por ejemplo el ideal $I = (x^2 + y^2)$ es un ideal radical de $\mathbb{R}[x, y]$ que define el conjunto algebraico $V(I) = \{(0, 0)\}$ y sin embargo

$$I(\{(0, 0)\}) = (x, y).$$

En efecto, el polinomio $x^2 + y^2$ es irreducible en $\mathbb{R}[x]$, porque si $x^2 + y^2 = fg$, entonces o bien el grado de f en x es dos y el grado de g es cero, o bien los grados de f y de g en x son uno.
En el segundo caso tenemos que

$$f = f_1(y)x + f_0(y), \; g = g_1(y)x + g_0(y),$$

y como $fg = x^2 + y^2$, entonces $f_1 g_1 = 1$, esto es, tanto f_1 como g_1 son constantes, que podemos suponer iguales a la unidad. Esto implica que

$$x^2 + y^2 = fg = x^2 + (f_0 + g_0)x + f_0 g_0,$$

o sea,

$$g_0 = -f_0 \quad \text{y} \quad x^2 + y^2 = x^2 - (f_0)^2,$$

que no es posible porque ningún polinomio de $k[y]$ al cuadrado es igual a $-y^2$.
Luego debe darse el primer caso, esto es, $f = f_2(y)x^2 + f_1(y)x + f_0(y)$ y $g = g(y)$, de donde se obtiene que g es una constante porque

$$x^2 + y^2 = fg = f_2(y)g(y)x^2 + f_1(y)g(y)x + f_0(y)g(y).$$

Dado que x^2+y^2 es irreducible y $k[x, y]$ es un dominio de factorización única, el ideal $(x^2 + y^2)$ es primo, y por lo tanto radical.

(1.1.10) Nota. Por otra parte, la aplicación V del conjunto de ideales radicales del anillo de polinomios $k[x_1, \ldots, x_n]$ en el conjunto de conjuntos algebraicos afines que a cada ideal radical I le asigna $V(I)$ es sobreyectiva.
En efecto, si $V = V(I)$ es un conjunto algebraico afín, entonces

$$V = V(I) = V(\mathrm{Rad} I).$$

Tanto la inyectividad de I como la sobreyectividad de V son consecuencia del hecho de que la composición $V \circ I$ es la aplicación identidad en el conjunto de los subconjuntos algebraicos afines de $\mathbb{A}^n k$.