PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
FACULTAD DE MATEMÁTICAS
DEPARTAMENTO DE MATEMÁTICA

Primer Semestre de 2019

Tarea 2

Introducción a la Geometría Algebraica — MAT 2335

Fecha de Entrega: 2019/04/11

Nicholas Mc-Donnell

Índice

Notas

En esta tarea se usará la notación $\overline{a} = (a_1, ..., a_n)$

Problema 1.25:

(a) Muestre que $V(y - x^2) \subset \mathbb{A}^2_{\mathbb{C}}$ es irreducible; en efecto, $I(V(y - x^2)) = I(y - x^2)$

(b) Separe $V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subset \mathbb{A}^2_{\mathbb{C}}$ en componentes irreducibles.

Solución problema 1.25:

(a) Se puede notar que si $(y - x^2)$ es un ideal primo entonces $V(y - x^2)$ es irreducible, y si $p(x, y) = y - x^2$ es un polinomio irreducible el ideal generado es primo. Usando criterio de Eisenstein (con y sobre $\mathbb{C}[y][x]$) esto se tiene que p es irreducible, por lo que el ideal es primo y $V(p)$ es irreducible.

(b) Se factoriza cada polinomio

$$y^4 - x^2 = (y^2 - x)(y^2 + x)$$
$$y^4 - x^2y^2 + xy^2 - x^3 = -(x - y)(x + y)(x + y^2)$$

Con lo que se puede notar que ambos tienen el polinomio $x + y^2$ en común, por lo que $V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) = V(y^2 + x) \cup V(y^2 - x, (x - y)(x + y))$. Se puede notar que $V(y^2 - x, (x - y)(x + y))$ son tres puntos $(0, 0), (1, 1), (1, -1)$, y $(0, 0) \in V(y^2 + x)$, luego $V(x - 1, y - 1) = \{(1, 1)\}, V(x - 1, y + 1) = \{(1, -1)\}$, por lo que se puede separar el conjunto algebraico en los conjuntos mostrados.

■

Problema 1.29:

Muestre que $\mathbb{A}^n_k$ es irreducible si k es infinito.

Solución problema 1.29: Sea $\mathbb{A}^n_k$ reducible, luego existen V_i tal que $\mathbb{A}^n_k = \bigcup_{i=1}^n V_i$, donde cada V_i es de la forma $V(f_{i,1}, ..., f_{i,n_i})$ con los $f_{i,j}$ no cero, notamos que $V_i \subseteq V(f_{i,1})$, por lo que $\mathbb{A}^n_k \subseteq \bigcup_{i=1}^n V(f_{i,1})$, pero se sabe que $\bigcup_{i=1}^n V(f_{i,1}) = V(\prod_{i=1}^n f_{i,1})$, con lo cual se ve que $V(\prod_{i=1}^n f_{i,1}) = \mathbb{A}^n_k$, pero se sabe[1] que si k es infinito el único polinomio que es cero para todos los valores es el cero, por lo que k tiene que ser finito.

■

[1] Por tarea anterior

Problema 1.30:

Sea $k = \mathbb{R}$

(a) Muestre que $I(V(x^2 + y^2 + 1)) = (1)$

(b) Demuestre que todo subconjunto algebraico de $\mathbb{A}^2_{\mathbb{R}}$ es igual a $V(F)$ para algún $F \in \mathbb{R}[x, y]$

Solución problema 1.30:

(a) Ya que $\mathbb{R}$ es un cuerpo ordenado se sabe que $x^2 \geq 0 \quad \forall x \in \mathbb{R}$, dado esto se nota que $x^2 + y^2 + 1 \geq 1 > 0 \quad \forall x, y \in \mathbb{R}$, por lo que $V(x^2 + y^2 + 1) = \emptyset$. Con esto se puede concluir lo que queríamos.

(b) Sea A un subconjunto algebraico en $\mathbb{A}^2_{\mathbb{R}}$, luego A puede ser una de cuatro cosas, un conjunto finito de puntos, una curva, el plano o la unión de las anteriores, se nota que el último caso se reduce a los otros, ya que si la unión se puede ver como los ceros de la multiplicación de los polinomios correspondientes. En el primer caso, donde $S = \{(a_1, b_1), ..., (a_n, b_n)\}$, el polinomio $\prod_{i=1}^{n}((x - a_i)^2 + (y - a_i)^2)$ cumple lo pedido. El segundo caso, por definición una curva es un polinomio, por lo que cumple lo pedido. Y el último caso, el polinomio 0 cumple lo que se quiere.

■

Problema 1.31:

(a) Encuentre los componentes irreducibles de $V(y^2 - xy - x^2y + x^3)$ en $\mathbb{A}^2_{\mathbb{R}}$ y también en $\mathbb{A}^2_{\mathbb{C}}$

(b) Haga lo mismo para $V(y^2 - x(x^2 - 1))$, y para $V(x^3 + x - x^2y - y)$

Solución problema 1.31:

(a) La siguiente factorización se puede ver $y^2 - xy - x^2y + x^3 = (x - y)(x^2 - y)$, por lo que $V(y^2 - xy - x^2y + x^3) = V(x - y) \cup V(x^2 - y)$, ambos son irreducibles por criterio de Eisenstein (usando y en $k[y][x]$), por lo que es la factorización en conjuntos irreducibles. Esto es independiente de k, por lo que es la misma factorización para $\mathbb{C}$ y para $\mathbb{R}$.

(b) Se nota que $y^2 - x(x^2 - 1)$ es irreducible por criterio de Eisenstein (usando x en $k[x][y]$), por lo que $V(y^2 - x(x^2 - 1))$ es irreducible. Para el otro conjunto algebraico, se ve que $x^3 + x - x^2y - y = (x^2 + 1)(x - y)$, luego en $\mathbb{C}$ $x^2 + 1 = (x - i)(x + i)$, con lo que se tiene que $V(x^3 + x - x^2y - y)$ se separa en $V(x - y)$ y $V(x^2 + 1)$ en $\mathbb{A}^2_{\mathbb{R}}$, y en $V(x - y)$, $V(x - i)$ y $V(x + i)$ en $\mathbb{A}^2_{\mathbb{C}}$.

$\blacksquare$

Problema 1.33:

(a) Separe $V(x^2+y^2-1, x^2-z^2-1) \subset \mathbb{A}^3_{\mathbb{C}}$ en componentes irreducibles.

(b) Sea $V = \{(t, t^2, t^3) \in \mathbb{A}^3_{\mathbb{C}} : t \in \mathbb{C}\}$. Encuentre $I(V)$, y demuestre que es irreducible.

Solución problema 1.33:

(a) Sea $V = V(x^2+y^2-1, x^2-z^2-1)$, notamos que $V = V(x^2-z^2-1, y^2+z^2) = V(x^2-z^2-1, z-iy) \cup V(x^2-z^2-1, z+iy)$, los cuales se denominan V_1, V_2 correspondientemente. Se sabe que si $C[x,y,z]/I(V_i)$ es dominio, $I(V_i)$ es primo, y V_i es irreducible. Notamos que $(\mathbb{C}[x,y,z]/(z+iy))/(x^2-y^2-1) \simeq \mathbb{C}[x,y,z]/I(V_2)$, por lo que cocientando en orden, claramente $\mathbb{C}[x,y,z]/(z+iy) \simeq \mathbb{C}[x,y]$. Ahora, se cocienta $\mathbb{C}[x,y]/(x^2-y^2-1)$, se nota que si x^2-y^2-1 es irreducible, $\mathbb{C}[x,y]/(x^2-y^2-1)$ es dominio. Se asume que existen p, q de grado 1 tal que $x^2-y^2-1 = p \cdot q$:

$$p(x,y) = ax + by + c$$
$$q(x,y) = dx + ey + f$$

Se ven las siguientes relaciones:

$$\begin{aligned} ad &= 1 & (ea+bd) &= 0 \\ be &= -1 & (cd+af) &= 0 \\ cf &= -1 & (bf+ec) &= 0 \end{aligned}$$

Con lo que se nota que ninguno es cero, luego se trabajan un poco las expresiones y se consigue:

$$\begin{aligned} a &= d^{-1} \\ b &= -e^{-1} \\ e^2 &= d^2 \end{aligned}$$

Lo que nos da dos casos

Caso $e = d$: Se nota que entonces $e(a+b) = 0$, por lo que $a = -b$, se suma $cd + af = 0$ con $bf + ec = 0$ y se consigue $cd + ce = 0$, pero eso es $2cd = 0$, una contradicción.

Caso $e = -d$: Se nota que entonces $e(a-b) = 0$, siguiendo la demostración anterior, pero restando, se llega a lo mismo, otra contradicción.

Por lo que se tiene lo pedido.

(b) Se nota que $V(y - x^2, z - x^3) = V$, luego $I(V) = (y - x^2, z - x^3)$, se sabe que si $C[x,y,z]/I(V)$ es un dominio, entonces $I(V)$ es primo. Sea φ morfismo natural, luego claramente $\operatorname{Im}\varphi = \mathbb{C}[x]$ y $I(V) \subseteq \ker\varphi$, sea $p \in \ker\varphi$, luego $p(x, x^2, x^3) = 0$, pero eso significaría que $p \in I(V)$, por lo que $I(V) = \ker\varphi$. Luego se sabe que $\mathbb{C}[x]$ es euclidiano, por lo que particularmente es un dominio. Entonces $I(V)$ es primo y V es irreducible.

■

Problema 1.37:

Sea k un cuerpo cualquiera, $F \in k[x]$ un polinomio de grado $n > 0$. Muestre que los residuos $\overline{1}, \overline{x}, ..., \overline{x}^{n-1}$ forman una base de $k[x]/(F)$ sobre k.

Solución problema 1.37: Sea $F(x) = \sum_{i=0}^{n} a_i x^i$ y φ es morfismo natural de $k[x]$ a $k[x]/(F)$, luego se quiere que $k[x]/(F)$ sea un espacio vectorial sobre k tal que $\dim k[x]/(F) = n$. Viendo F en $k[x]/(F)$ se puede notar que $\overline{x}^n = -\varphi(a_n)^{-1}\sum_{i=0}^{n-1}\varphi(a_i)\overline{x}^i$, por lo que $\overline{x}^n$ se puede escribir en la base propuesta. Claramente $\overline{x}^{n+k} = -\varphi(a_n)^{-1}\sum_{i=0}^{n-1}\varphi(a_i)\overline{x}^{i+k}$, por lo que para $j \geq n$ $\overline{x}^j$ se puede escribir en base a los $\overline{x}^i$ donde $n - j \leq i < j$, dado esto se ve que como $\overline{x}^n$ se puede escribir en la base propuesta, si $j \geq n$ $\overline{x}^j$ se puede escribir en la base propuesta. Con esto se tiene que para todo $G \in k[x]$ $\overline{G}$ se puede escribir en la base propuesta, como φ es sobreyectivo, todo elemento en $k[x]/(F)$ se puede escribir en la base propuesta, cumpliendo lo pedido.

■

Problema 1.45:

Sea R un subanillo de S, S un subanillo de T.

(a) Si $S = \sum Rv_i, T = \sum Sw_j$, muestre que $T = \sum Rv_i w_j$.

(b) Si $S = R[v_1, ..., v_n], T = S[w_1, ..., w_m]$, muestre que $T = R[v_1, ..., v_n, w_1, ..., w_m]$.

(c) Si R, S, T son cuerpos, y $S = R(v_1, ..., v_n), T = S(w_1, ..., w_m)$, demuestre que $T = R(v_1, ..., v_n, w_1, ..., w_m)$.

Solución problema 1.45:

(a) Sea $u \in T$, luego $u = \sum_{j=1}^{n} \alpha_j w_j$ donde los $\alpha_j \in S$, como están en S, se pueden escribir de la siguiente forma $\alpha_j = \sum_{i=1}^{m} \beta_{i,j} v_i$, juntando ambas cosas: $u = \sum_{j=1}^{n} \sum_{i=1}^{m} \beta_{i,j} w_j v_i$ donde $\beta_{i,j} \in R$, por ende $T = \sum R v_i w_j$.

(b) Asumamos que $T \subsetneq R[v_1, ..., v_n, w_1, ..., w_m]$, eso implica que existe $a \in T$ tal que $a \notin R[v_1, ..., v_n, w_1, ..., w_m]$. Como $a \in T$, a se puede escribir en base a los w_i y elementos en S, pero cada elemento en S se puede escribir en base a los v_j y elementos en R, por lo que a se puede escribir en base a los w_i, los v_j y elementos en R, pero eso significaría que $a \in R[v_1, ..., v_n, w_1, ..., w_m]$, una contradicción.

(c) Es análogo a la (b), usando la definición de extensión de cuerpo en vez de la de anillo.

■

Problema 1.49:

Sea k un cuerpo, $L = k(x)$ el cuerpo de funciones racionales en una variable sobre k.

(a) Muestre que todo elemento de L que es integral sobre $k[x]$ ya esta en $k[x]$. (Hint: Si $z^n + a_1 z^{n-1} + ... = 0$, tome $z = F/G$, con F, G coprimos. Entonces $F^n + a_1 F^{n-1} + ... = 0$, por lo que G divide a F.)

(b) Muestre que no hay un elemento no cero $F \in k[x]$ tal que para todo $z \in L$, $F^n z$ es integral sobre $k[x]$ para algún $n > 0$.

Solución problema 1.49:

(a) Sea $a \in k(x)$ tal que $a \notin k[x]$ y a es integral sobre $k[x]$, luego sea $p(y)$ el polinomio mónico en $k[x][y]$ tal que $p(a) = 0$. Se puede escribir $a = F/G$ donde $F, G \in k[x]$ y son coprimos. Luego $p(F/G) = (F/G)^n + \sum_{i=0}^{n-1} \alpha_i \left(\frac{F}{G}\right)^i = 0$, se toma $G^n \cdot p(F/G) = F^n + \sum_{i=0}^{n-1} \alpha_i F^i G^{n-i} = 0$, se puede escribir $F^n = -\sum_{i=0}^{n-1} \alpha_i F^i G^{n-i}$, y se nota que $G \mid F^n$ por lo que $G \mid F$, pero G, F son coprimos, una contradicción, con eso tenemos que no existe $a \in k(x) \setminus k[x]$ que sea integral.

(b) Por (a), se sabe que si $a \in L$ integral sobre $k[x]$ entonces esta $a \in k[x]$. Ahora, se asume que existe F y $n > 0$ tal que para todo $z \in L$ $F^n z$ es integral, específicamente entonces cumple para $1/F^{n+1}$, entonces $F^n / F^{n+1} = 1/F$ es integral, pero entonces $1/F \in k[x]$, lo que claramente es una contradicción.

■

Problema 1.51:

Sea k un cuerpo, $F \in k[x]$ un polinomio irreducible mónico de grado $n > 0$.

(a) Muestre que $L = k[x]/(F)$ es un cuerpo, y si a es el residuo de x en L, entonces $F(a) = 0$.

(b) Suponga que L' es una extensión de cuerpo de k, $y \in L'$ tal que $F(y) = 0$. Demuestre que el homorfismo de $k[x]$ a L' que toma x a y, induce un isomorfismo de L con $k(y)$.

(c) Con L', y como en (b), suponga que $G \in k[x]$ y $G(y) = 0$. Muestre que F divide a G.

(d) Muestre que $F = (x - a)F_1, F_1 \in L[x]$

Solución problema 1.51:

(a) Como F es irreducible, entonces (F) es maximal, y se sabe que un anillo cocientado por un ideal maximal es un cuerpo. Sea $a = \overline{x}$, luego $\overline{F(x)} = 0$, se puede operar $\overline{F(x)}$ de la siguiente forma

$$\begin{aligned}\overline{F(x)} &= \overline{\sum_{i=0}^{n} b_i x^i} \\ &= \sum_{i=0}^{n} \overline{b_i x^i} \\ &= \sum_{i=0}^{n} \overline{b_i}\overline{x^i} \\ &= \sum_{i=0}^{n} \overline{b_i} \cdot \overline{x}^i\end{aligned}$$

Ya que $b_i \in k$, entonces $\overline{b_i} = b_i$, por lo que $\overline{F(x)} = \sum_{i=0}^{n} b_i a^i = 0$, con lo que a es una raíz.

(b) Se denota φ el homorfismo, de $k[x]$ a L' tal que $x \mapsto y$, por primer teorema de isomorfismo $\operatorname{Im}\varphi \simeq k[x]/\ker\varphi$, se nota que si $\operatorname{Im}\varphi = k(y)$ y $\ker\varphi = (F)$ tenemos lo pedido. Trivialmente $\operatorname{Im}\varphi \subseteq k(y)$, luego se sabe por una parte del 1.37 que la base de $k(y)$ sobre k tiene a lo más el grado de F elementos que la generan, y más específicamente, todo elemento α de $k(y)$ se puede escribir de la siguiente forma:

$$\alpha = \sum_{i=0}^{n} \alpha_i y^i$$

Donde $n = \dim k(y)$, luego sea $P(x) = \sum_{i=0}^{n} \alpha_i x^i$, claramente $\varphi(P) = \alpha$, por lo que $\alpha \in \operatorname{Im}\varphi$, por lo que $\operatorname{Im}\varphi = k(y)$. Se puede ver que $\ker\varphi \subseteq (F)$, sea $P \in (F)$, luego $P = \alpha \cdot F$ donde $\alpha \in k[x]$, entonces $\varphi(P) = \varphi(\alpha)\cdot\varphi(F) = \varphi(\alpha)\cdot 0 = 0$, por lo que $\ker\varphi = (F)$. Con esto se tiene lo que se quería.

(c) Ya que $G(y) = 0$, $G \in \ker\varphi = (F)$, por lo que $F \mid G$.

(d) Como $a \in L$, $F(a) = 0$ y $F \in k[x] \subset L[x]$, entonces $(x-a) \mid F$, más aún existe $F_1 \in L[x]$ tal que $F_1(x)\cdot(x-a) = F(x)$.

■

Problema 1.54:

Sea R un dominio con K su cuerpo cociente, y sea L una extensión finita y algebraica de K

(a) Para todo $v \in L$, demuestre que existe $a \in R$ distinto a cero tal que av es integral sobre R

(b) Muestre que hay una base $v_1, ..., v_n$ para L sobre K (como un espacio vectorial) tal que cada v_i es integral sobre R.

Solución problema 1.54:

(a) Notemos que como L es una extensión finita, por lo que existen $x_1, ..., x_n$ tal que $K(x_1, ..., x_n) = L$. Se nota que si todos los x_i cumplen la propiedad pedida y además la suma y la multiplicación de elementos que cumplen la propiedad, tambien la cumplen, tenemos lo pedido. Se observa $L = K(x_i)$, sea $1, x_i, x_i^2, ..., x_i^k$ tal que sean l.i. y que si se añade x_i^{k+1} son l.d., esto se logra ya que L es una extensión finita sobre K. Luego x_i^{k+1} se puede escribir en la base:

$$x_i^{k+1} = -\sum_{j=0}^{k} a_j x_i ji \tag{1}$$

Con esto se nota que hay un polinomio mónico $p(x) = x^{k+1} + \sum_{j=0}^{k} a_j x^j$, tal que x_i es raíz. Por el problema 1.51, p es irreducible (si no lo fuera existiría un cuerpo estrictamente entre L y K). Se nota que los $a_j \in K$, por lo que cada $a_j = \frac{b_j}{c_j}$ con los $b_j, c_j \in R$, sea $c = \prod_{j=0}^{k} c_j$, luego $c \cdot p \in R[x]$ y esto claramente nos lleva a concluir que cx_i es integral. Por lo que todos para todo x_i existe $a \in R$ tal que ax_i es integral. Sean $x, y \in L$ tal que cumplen que $\exists b, c \in R$ tal que bx, cy son integrales sobre R. Se recuerda el coralario de la proposición 3[2], con lo que como bx, cy son integrales, $bcxy$ es integral y $bc(x+y) = cbx + bcy$ es integral, por lo que tenemos lo que queríamos.

(b) Por lo visto en (a), se puede notar que las bases de $K(x_i)$ se pueden extender con elementos de las otras bases, como los x_i son integrales, las bases también lo son (son potencias de los x_i)

■

[2]Los elementos integrales forman un subanillo