UNA INTRODUCCIÓN A LA GEOMETRÍA ALGEBRAICA

JUAN MIGLIORE Y CHRIS PETERSON

1. introducción

Estas notas suplementan las lecciones del curso "Introducción a la geometría algebraica y aplicacions", que forma parte de la Escuela de Matemática de América Latina y el Caribe (EMALCA), durante el periodo 10-21 de octubre, 2011, en Asunción, Paraguay.

El libro principal del curso es el libro de Cox, Little y O'Shea [1]. Además vamos a usar las notas de Dickenstein [2]. Pero visto que [1] está escrito en inglés y es muy largo, y [2] es breve, quisimos escribir estas notas para dar algunos detalles de lo que vamos a hacer en el curso, por lo menos en parte. Pero son notas muy incompletas, y va a haber bastante en el curso que no se encuentra en estas notas!!

Es para nosotros un gran placer poder ofrecer este curso, y esperamos que tanto las charlas como estas notas sean útiles e interesantes para los estudiantes del curso.

2. Álgebra lineal

Recordamos muy brevemente algunas ideas de álgebra lineal. Sea K un cuerpo. Para nosotros, K casi siempre será el cuerpo de números reales, $K = \mathbb{R}$, o el cuerpo de números complejos, $K = \mathbb{C}$. Pero puede también ser cualquier otro cuerpo, por ejemplo los enteros modulo p, $K = \mathbb{Z}_p$.

Definición 2.1. Un *espacio vectorial* sobre K es un conjunto V, cuyos elementos se llaman *vectores*, con dos operaciones: adición y multiplicación escalar, que satisfacen ciertos axiomas que vamos a dar en las lecciones. Una *base* de un espacio vectorial es un conjunto de vectores $\{v_1, \ldots, v_n\}$ tal que cada $v \in V$ es combinación lineal de los v_i, y tal que no existe un conjunto $\{w_1, \ldots, w_{n-1}\}$ con la misma propriedad. Entonces los v_i son *linearmente independientes.* $\square$

Definición 2.2. Sean $x_1, \ldots, x_n$ variables. Un *monomio* en estas variables es un producto de variables. Por ejemplo, si las variables son x_1, x_2, x_3, x_4 entonces $x_1x_2^3x_3x_4^7$ es un monomio, pero también x_1^5 es un monomio. Un *polinomio* es una combinación lineal finita de monomios. Por ejemplo,

$$3x_1^4x_2 - 15x_1x_2x_3^5x_4$$

es un polinomio. El *grado* de un polinomio es la suma máxima de los exponentes de los monomios. Por ejemplo, el grado de $3x_1^4x_2 - 15x_1x_2x_3^5x_4$ es $1+1+5+1 = 8$ porque $4+1 = 5 < 8 = 1+1+5+1$. Un *polinomio omogeneo* es una combinación lineal finita de monomios del mismo grado d. $\square$

Ejemplo 2.3. Sea R_d el conjunto de polinomios omogeneos de grado d. Entonces R_d es un espacio vectorial.

El conjunto de polinomios no necesariamente omogeneos de grado d no es un espacio vectorial.

El conjunto de polinomios no necesariamente omogeneos de grado $\leq d$ es un espacio vectorial. $\square$

Ahora vamos a introducir K^n. Se lo puede estudiar en dos niveles: como nada más que un conjunto, o con una estructura adicional, la estructura de un espacio vectorial. Para nosotros, casi siempre va a ser como conjunto:

Definición 2.4. El *espacio afín de dimensión* n, que escribimos a veces $\mathbb{A}^n$ y a veces K^n, es el conjunto de n-tuplas $(p_1, \ldots, p_n)$ tal que $p_i \in K$.

Ejemplo 2.5. $(1, 2, 3, 4) \in \mathbb{R}^4$ y $\mathbb{C}^4$ y $\mathbb{Q}^4$.
$(\pi, 2\pi, 3\pi, 4\pi) \in \mathbb{R}^4$ y $\mathbb{C}^4$ pero no $\mathbb{Q}^4$.
$(1, 2, 3, 4) \notin \mathbb{R}^3$. □

Definición 2.6. El *espacio vectorial* K^n es el espacio afín junto con las reglas de adición de vectores y de multiplicación escalar. □

Pregunta 2.7. *Cuales son los subconjuntos "interesantes" de* K^n*?*

En cierto sentido, la respuesta a esta pregunta es el campo de geometría algebraica!!!!! Es una respuesta un poco larga – ya por siglos estamos tratando de entenderla. Pero el primer paso se encuentra con el álgebra lineal.

Consideremos un sistema de m ecuaciones lineales en n variables

$$\begin{array}{ccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \ldots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \ldots & + & a_{2,n}x_n & = & b_2 \\ & & & & \vdots & & & & \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \ldots & + & a_{m,n}x_n & = & b_m \end{array} \tag{2.1}$$

donde los x_j son los variables $(1 \le j \le n)$ y $a_{i,j}$ y b_i $(1 \le i \le m,\ 1 \le j \le n)$ son los constantes; es decir $a_{i,j}$ y b_j son elementos de K. Sabemos cómo encontrar la solución de este sistema. Es el *método de transformaciones elementales de filas* (o *eliminación Gausiana*). Con esto podemos ver si un sistema de ecuaciones tiene solución, cual es la dimensión del conjunto de soluciones, y podemos parametrizar este conjunto. La idea de la eliminación es de usar las transformaciones elementales de filas para obtener una matriz en *forma normal* – "Reduced row echelon form (RREF)" – o por lo menos *forma triangular* – "Row echelon form" (REF).

Ejemplo 2.8.

$$\begin{array}{ccccccccc} 3x_1 & + & 4x_2 & + & 5x_3 & + & 6x_4 & = & 7 \\ 6x_1 & + & 7x_2 & + & 8x_3 & + & 9x_4 & = & 10 \end{array} \rightsquigarrow \left[\begin{array}{cccc|c} 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 8 & 9 & 10 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc|c} 1 & 0 & -1 & -2 & -3 \\ 0 & 1 & 2 & 3 & 4 \end{array}\right]$$

(RREF) y luego la solución

$$\begin{array}{rcl} x_1 & = & -3 + s + 2t \\ x_2 & = & 4 - 2s - 3t \\ x_3 & = & s \\ x_4 & = & t \end{array}$$

donde s y t son elementos árbitros de K. Entonces la solución tiene dimensión 2, ya que hay dos parámetros para la solución. □

Observación 2.9. Todo esto funciona porque las transformaciones elementales de filas no cambian la solución. Vamos a ver algo parecido cuando pasamos a las variedades. □

Repetimos que un sistema puede no tener ninguna solución, como por ejemplo el sistema

$$\begin{array}{ccccc} x & + & y & = & 5 \\ x & + & y & = & 6. \end{array}$$

También puede tener un número finito, non-cero, de soluciones (entonces necesariamente una).

Ahora observamos que el sistema (2.1) se puede escribir como

$$\begin{array}{rcl} f_1(x_1,\ldots,x_n) & = & 0 \\ f_2(x_1,\ldots,x_n) & = & 0 \\ & \vdots & \\ f_m(x_1,\ldots,x_n) & = & 0 \end{array} \tag{2.2}$$

donde

$$\begin{array}{rcl} f_1(x_1,\ldots,x_n) & = & a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n - b_1 \\ & \vdots & \\ f_m(x_1,\ldots,x_n) & = & a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n - b_m. \end{array}$$

Los polinomios $f_1,\ldots,f_m$ son de grado 1, pero tienen términos de grado 1 y términos de grado 0 (los constantes b_i). La solución del sistema (2.1) es igual al conjunto de puntos $P = (p_1,\ldots,p_n)$ en K^n por los cuales

$$\begin{gathered} f_1(p_1,\ldots,p_n) = 0 \\ \vdots \\ f_m(p_1,\ldots,p_n) = 0 \end{gathered}$$

Definición 2.10. Vamos a denotar esta solución con

$$V(f_1,\ldots,f_m) = \{P \in K^n \mid f_i(P) = 0 \text{ por } i = 1,\ldots,m\}. \qquad \square$$

¿Qué ocurre cuando hacemos las transformaciones elementales? Estamos haciendo combinaciones lineales de las $f_i(x_1,\ldots,x_m)$ con el objeto de transformarlas en forma que se puede obtener información útil. Repetimos: la observación importante es que **haciendo estas combinaciones lineales no cambiamos la solución del sistema.** Observamos también que estas transformaciones elementales trabajan en el espacio de filas (row space) de la matriz, cambiando la basis pero dejando intacto el espacio mismo.

Un caso muy importante ocurre cuando los b_i son todos 0. En este caso el sistema (2.1) *siempre* tiene por lo menos una solución, es decir $x_j = 0$ por todos los j. Igual que antes, podemos encontrar la dimensión del conjunto de las soluciónes. Los polinomios $f_1,\ldots,f_m$ ahora son *polinomios homogéneos*.

Observen que cuando los polinomios son homogéneos, si $(r_1,\ldots,r_n)$ es una solución del sistema de ecuaciones y si λ es un número arbitrario, entonces $(\lambda r_1,\ldots,\lambda r_n)$ también es una solución. Podemos decir la misma cosa en otras palabras: si un punto $P = (r_1,\ldots,r_n)$ es parte del conjunto de soluciones entonces toda la recta que contiene P y el orígen $(0,\ldots,0)$ es parte del conjunto de soluciones. Es simplemente porque si

$$a_1r_1 + \cdots + a_nr_n = 0$$

entonces también

$$a_1 \cdot (\lambda r_1) + \cdots + a_n \cdot (\lambda r_n) = \lambda \cdot (a_1r_1 + \cdots + a_nr_n) = \lambda \cdot 0 = 0.$$

3. El espacio afín y variedades afinas

Ahora simplemente vamos a dejar que el sistema de ecuaciones (2.1) contenga polinomios de grado mayor de uno. En otras palabras, los polinomios $f_1,\ldots,f_m$ de (2.2) pueden ser de cualquier grado. Ahora la definición 2.10 queda igual, pero ahora hay más posibilidades para los f_i. Ponemos $R = K[x_1,\ldots,x_n]$; es decir, vamos a considerar polinomios en las variables $x_1, \dots, x_n$. Como vamos a ver, R tiene la estructura de un *anillo*.

Definición 3.1. Una *variedad algebraica afina* es un subconjunto V del espacio afín K^n tal que existen polinomios $f_1, \dots, f_m$ para los cuales

$$V = V(f_1, \dots, f_m) = \{P \in K^n \mid f_i(P) = 0 \text{ por } i = 1, \dots, m\}.$$

En otras palabras, V es el conjunto de soluciones del sistema (2.2), pero ahora los f_i tienen grado ≥ 0. □

Ejemplo 3.2.
1. Los polinomios que definen una variedad algebraica afina no son únicas. Por ejemplo, en K^3, usando las variables x, y, z, tenemos $V(x) = V(x^2) = \{(0, a, b) \mid a, b \in K\}$. Entonces V es un plano.
2. Si uno de los f_i tiene grado 0 pero no es el polinomio 0, es decir si es un constante, entonces $V(f_1, \dots, f_m) = \emptyset$, el conjunto vacío, que entonces también es una variedad. No importa cuales son los otros polinomios.
3. Si el cuerpo es $\mathbb{R}$ entonces también podemos obtener $\emptyset$ con otros polinomios. Por ejemplo, si las variables son x, y, z y $f(x, y, z) = x^2 + y^2 + z^2 + 1$ entonces $V(f) = \emptyset$. Si el cuerpo es $\mathbb{C}$, esto ya no es cierto.
4. Si hay solamente un polinomio, y es el polinomio $f = 0$, entonces $V(f) = K^n$. Entonces también K^n es una variedad.

Las notas de Dickenstein dan una lista larga de ejemplos y aplicaciones.

4. El espacio proyectivo y variedades proyectivas

Las notas de Dickenstein [2] hablan de variedades algebraicas *afines*; es decir, sus variedades "viven" en el espacio K^n. Sin embargo, una gran parte de la geometría algebraica estudia variedades *proyetivas*. En esta sección veremos lo que es el espacio proyectivo, y qué necesitamos para definir variedades proyectivas. Para poder visualizar

Para empezar, vamos a dar la definición del espacio proyectivo como un conjunto. Despus vamos a estudiar la estructura de este conjunto. Hay varios puntos de vista para estudiar el espacio proyectivo. Estos incluyen

- Empezando con los axiomas. (JM va a mencionar esto en la charla para la Sociedad Cientifica del Paraguay.)
- Empezando con el espacio afín K^n y añadiendo puntos del infinito, que tienen la estructura de un espacio proyectivo de dimensión $n - 1$.
- Punto de vista topológico.

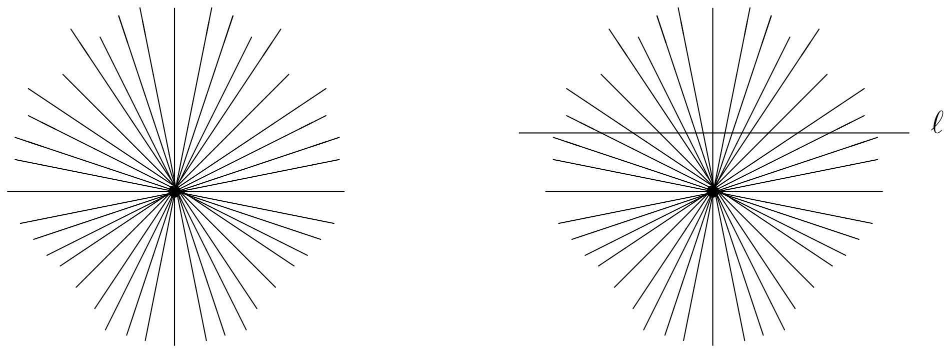
Vamos a dar algunos detalles en las lecciones.

Definición 4.1. El *espacio proyectivo de dimensión n*, denotado $\mathbb{P}^n$, es el conjunto de rectas en el espacio afina de dimensión $n + 1$ que pasan por el origen $(0, ..., 0)$. Es decir, $\mathbb{P}^n$ es el conjunto de subespacios lineales de dimensión 1 en el espacio vectorial $\mathbb{C}^{n+1}$.

Porqué decimos que $\mathbb{P}^n$ tiene dimensión n si se trata de $\mathbb{C}^{n+1}$? Empecemos con valores chicos de n.

Primero vamos a considerar $n = 0$. En este caso $\mathbb{A}^{n+1} = \mathbb{A}^1$ es una recta (es decir, es un espacio vectorial de dimensión 1). Hay solamente una recta dentro de $\mathbb{A}^1$ (es decir, hay un solo subespacio de dimensión 1), que es $\mathbb{A}^1$ mismo. Entonces $\mathbb{P}^0$ *es un solo punto*, igual que $\mathbb{A}^0$.

Ahora consideremos $n = 1$. En este caso $\mathbb{A}^{n+1} = \mathbb{A}^2$. Los subespacios de dimensión 1 dentro de $\mathbb{A}^2$ son las rectas que pasan por el origen:



Si consideramos la recta λ con ecuación $y = 1$, podemos representar a cada una de estas rectas en el dibujo *menos una* (cual???) con un punto de λ. Entonces podemos considerar el espacio $\mathbb{P}^1$ como la unión de ℓ con un punto más, que llamamos el punto del infinito de $\mathbb{P}^1$.

De la misma manera, $\mathbb{P}^2$ se puede ver como la unión de $\mathbb{A}^2$ con una recta proyectiva, $\mathbb{P}^1$, del infinito. Y siguiendo así, $\mathbb{P}^n$ es la unión de $\mathbb{A}^n$ y $\mathbb{P}^{n-1}$.

A los puntos del espacio proyectivo podemos dar coordinadas proyectivos, que es parecido a los de los puntos del espacio afín, pero no idéntico. Recordamos que $\mathbb{P}^n$ es el conjunto de rectas de $\mathbb{A}^{n+1}$ que pasan por el origen. Es decir, un punto de $\mathbb{P}^n$ tiene la forma

$$\{(\lambda a_0, \lambda a_1, \dots, \lambda a_n) \mid \lambda \in K\}$$

donde no todas las a_i son cero. Pero podemos cambiar $(a_0, \dots, a_n)$ con cualquier multiplo escalar non-cero, y tenemos la misma recta pasando por el origen en A^{n+1}, es decir tenemos el mismo punto de $\mathbb{P}^n$. Associamos a este punto las coordinadas $[a_0, \dots, a_n]$, entendiendo que

$$[a_0, \dots, a_n] = [\lambda a_0, \dots, \lambda a_n]$$

por cualquier $\lambda \neq 0$.

Ejemplo 4.2. En $\mathbb{P}^4$ tenemos el punto

$$[1, 2, 3, 4, 5] = [2, 4, 6, 8, 10] = [3\pi, 6\pi, 9\pi, 12\pi, 15\pi].$$

Observen que $[0, 0, 0, 0, 0]$ *no* es un punto de $\mathbb{P}^4$. □

Con estas coordinadas, ¿podemos hacer lo mismo que hicimos para el espacio afín y decir que si $f_1, \dots, f_m$ son polinomios con $n + 1$ variables entonces definen una variedad $V(f_1, \dots, f_m)$? La primera respuesta es **¡¡no!!**.

Ejemplo 4.3. Sea $f(w, x, y, z) = w - x^2 + y^3 - z^4$. Entonces $f(1, 1, 1, 1) = 0$, pero $f(2, 2, 2, 2) = -10 \neq 0$. Así que no es claro si f tiene el valor cero para el punto $[1, 1, 1, 1]$ de $\mathbb{P}^3$.

Por otro lado, si $g(w, x, y, z) = wz^3 - x^2z^2 + y^3z - z^4$ entonces

$$g(1, 1, 1, 1) = f(2, 2, 2, 2) = 0.$$

¿Cual es la diferencia entre f y g? □

La observación importante es que si f es omogeneo en las variables $x_0, \dots, x_n$ y $P = [a_0, \dots, a_n]$ es un punto de $\mathbb{P}^n$, entonces

$$f(P) = f(a_0, \dots, a_n) = 0 \textit{ si y solamente si } f(\lambda a_0, \dots, \lambda a_n) = 0 \textit{ por cada valor de } \lambda.$$

Definición 4.4. Una *variedad proyectiva* es un subconjunto V del espacio proyectivo $\mathbb{P}^n$ tal que existen polinomios *omogeneos* $f_1, \dots, f_m$ en $n+1$ variables para los cuales

$$V = V(f_1, \dots, f_m) = \{P \in \mathbb{P}^n \mid f_i(P) = 0 \text{ por } i = 1, \dots, m\}.$$

□

5. Grupos, anillos e ideales

Definición 5.1. Un *grupo* $(G, *)$ es un conjunto, G, con una operación $*$ tal que estos axiomas son válidos:

- Por cada $a, b, c \in G$ tenemos $(a * b) * c = a * (b * c)$ (*asociatividad*);
- Existe un *elemento de identidad* e tal que por cada $a \in G$ tenemos $a*e = e*a = a$;
- Por cada elemento $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a*a^{-1} = a^{-1} * a = e$.

El grupo es *abeliano* si $a * b = b * a$ por cada $a, b \in G$. □

Ejemplo 5.2. (1) Si V es un espacio vectorial entonces $(V, +)$ es un grupo abeliano.
(2) Si G es el conjunto de 2×2 matrices con determinante non-cero entonces $(G, \cdot)$ es un grupo pero no es abeliano.
(3) $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}_n, +)$ son grupos abelianos.
(4) $(\mathbb{R}, \cdot)$ no es un grupo pero $(\mathbb{R} - \{0\}, \cdot)$ y $(\mathbb{C} - \{0\}, \cdot)$ son grupos. En cambio, $(\mathbb{Z} - \{0\}, \cdot)$ no es un grupo.

Definición 5.3. Un *anillo* $(R, +, \cdot)$ es un conjunto junto con dos operaciones, $+$ y $\cdot$, que llamamos *adición* y *multiplicación*, tales que valen estos axiomas:

- $(R, +)$ es un grupo abeliano;
- La multiplicación es asociativa;
- Vale la distributividad $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ y $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Si la multipicación es conmutativa entonces R es un *anillo conmutativo*. Normalmente no se supone que haya un elemento 1 que es la identidad para la multiplicación, pero nosotros siempre vamos a suponer que existe. □

Ejemplo 5.4. (1) $\mathbb{Z}$ es un anillo conmutativo.
(2) Si M es el conjunto de 2×2 matrices entonces M es un anillo pero no es conmutativo.
(3) $R = K[x_1, \dots, x_n]$ es un anillo conmutativo. Para nosotros éste es el ejemplo más importante.

Definición 5.5. Sea $(R, +, \cdot)$ un anillo y sea $I \subset R$ un conjunto. Entonces I es un *ideal* si $(I, +)$ es un grupo y si $a \cdot I \subset I$ y $I \cdot b \subset I$ por cada $a, b \in R$.

Proposición 5.6. *Si $R = \mathbb{Z}$ entonces los ideales son todos de la forma*

$$n\mathbb{Z} = \{na \mid n \in \mathbb{Z}\}$$

Por ejemplo, $6\mathbb{Z} = \{\cdots - 18, -12, -6, 0, 6, 12, 18, \dots\}$ es un ideal en $\mathbb{Z}$.

(Verificar...)

Proposición 5.7. *Sea R un anillo y sean $f_1, \ldots, f_r \in R$. Pongamos*

$$I = \{c_1 f_1 + c_2 f_2 + \cdots + c_r f_r \mid c_i \in R \quad \text{por } i = 1, \ldots, r\}.$$

Entonces I es un ideal en R. Lo designamos con

$$I = \langle f_1, \ldots, f_r \rangle$$

y decimos que los f_i generan *I.*

(Verificar...)

El caso más importante para nosotros es el caso $R = K[x_1, \ldots, x_n]$.

Observación 5.8. Puede ser que no necesitamos todos los f_i. Por ejemplo, en el anillo $R = \mathbb{R}[x, y, z]$, tenemos

$$\langle x^2 + y^2, x^2 + z^2, y^2 - z^2 \rangle = \langle x^2 + y^2, x^2 + z^2 \rangle$$

Si no se puede quitar ninguno de los f_i entonces decimos que los f_i forman una *base* para I. Es muy parecido a la noción de base para un espacio vectorial. □

Ejemplo 5.9. El ejemplo principal para nosotros es este. Sea V una variedad en $\mathbb{A}^n$. Entonces

$$I(V) = \{f \in K[x_1, \ldots, x_n] \mid f(P) = 0 \text{ por cada } P \in V\}$$

es un ideal que llamamos *el ideal de V*. Si V es una variedad en $\mathbb{P}^n$ entonces $I(V)$ es el ideal *generado por*

$$\{f \in K[x_0, \ldots, x_n] \mid f \text{ es omogeneo y } f(P) = 0 \text{ por cada } P \in V\}.$$

En ambos casos, un teorema de Hilbert (Hilbert Basis Theorem) asegura que hay un número *finito* de polinomios que generan $I(V)$.

Bibliografía

[1] D. Cox, J. Little y D. O'Shea, "Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. Third edition." Undergraduate Texts in Mathematics. Springer, New York, 2007.

[2] A. Dickenstein, *Sistemas de ecuaciones polinomiales*, minicurso UMA (1995).