Lecturas Matemáticas
Volumen **18** *(1997), páginas 153-160*

Una nota sobre automorfismos polinómicos

Carlos R. Videla

CINVESTAV-IPN, MÉXICO

1. En el Congreso de la Sociedad Matemática Mexicana del año pasado (1996) dicté un cursillo sobre teoría de Modelos basado en mis notas [7]. Uno de los resultados que se discutieron es la hermosa demostración de J. Ax de la parte (a) del siguiente Teorema:

Teorema 1. Si $F : \mathbb{C}^n \to \mathbb{C}^n$ es una aplicación polinómica inyectiva entonces:

(a) $F(\mathbb{C}^n) = \mathbb{C}^n$
(b) $F^{-1} : \mathbb{C}^n \to \mathbb{C}^n$ es polinómico

Aquí n es un entero positivo y $\mathbb{C}$ es el conjunto de todos los $z = (z_1, \ldots, z_n)$ con cada z_i un número en el campo de los complejos $\mathbb{C}$.

Una aplicación $F = (f_1, \ldots, f_n)$ es polinómica si cada componente es un polinomio. En el caso del teorema, cada componente es un polinomio de n variables con coeficientes en $\mathbb{C}$. Ax prueba el resultado (a) para cualquier campo algebraicamente cerrado en [1]. La demostración de Ax y la demostración en [3] son de carácter algebraico, (es decir no transfieren el resultado al caso general del caso complejo).

Posteriormente, en [2], Ax generaliza el teorema y demuestra que si $F : V \to V$ es un morfismo inyectivo de la variedad V en si misma sobre un campo algebraicamente cerrado entonces F es sobreyectivo.

La segunda parte del teorema aparece en [8]. La demostración usa un criterio para variedades algebraicas en $\mathbb{C}^n$ debido a W. Rudin y el teorema de Liouville.Aun en el caso en que $V = \mathbb{C}^n$ y el morfismo F es polinómico, Ax no discute la posibilidad de que el inverso sea polinómico. En mi cursillo intenté dar una demostración de la parte (b) para cualquier campo algebraicamente cerrado de característica cero usando la completez de la teoría de dichos campos.

El resultado se podría transferir si fuese posible expresar el resultado de (b) por medio de una sentencia en el lenguaje $\mathcal{L} = \{+, \cdot, -, 0, 1\}$. Vimos en clase que esto se podría hacer si, por ejemplo, existiese una cota en el grado del inverso en función del grado de F en el caso complejo. Tanto yo como los alumnos pensamos que esto era improbable. Estábamos equivocados pues de hecho si existe tal acotación (vea [9, pag. 292]).

En esta nota presentamos una demostración de (b) debida a K. McKenna que es poco conocida y hasta la fecha no se ha publicado, y una generalización de (b) reemplazando $\mathbb{C}$ por cualquier campo algebraicamente cerrado de característica cero, sin usar el hecho que hay una cota al grado del inverso. Sin embargo, en esta prueba si usamos el hecho que el teorema vale en el caso complejo. En la última sección damos una demostración esencialmente algebraica asumiendo el teorema 1 (a) para campos algebraicamente cerrados. Esta última prueba está inspirada en una demostración reciente del teorema 1 debida a W. Rudin [6].

2. Los siguientes resultados seran usados:

(A) Teorema de Tarski:
La clase de funciones semialgebraicas de $\mathbb{R}^n$ en $\mathbb{R}$ coincide con la clase de funciones de $\mathbb{R}^n$ en $\mathbb{R}$ definibles en la estructura $\widetilde{\mathbb{R}} = (\mathbb{R}, +, -, \cdot, <, \{c_r, : r \in \mathbb{R}\})$.

(B) Crecimiento de funciones semialgebraicas:
Si $F : \mathbb{R}^n \to \mathbb{R}$ es semialgebraica y continua entonces existe $c \in \mathbb{R}$ y $m \in \mathbb{N}$ tales que
$$|f(x)| \leq c(1 + ||x||^2)^m.$$

(C) Teorema de Robinson:
Si K y L son dos campos algebraicamente cerrados y $K \subset L$ entonces K es una subestructura elemental de L (notación: $K < L$) es decir si φ

es una sentencia en el lenguaje

$$\mathcal{L}_K = \{+, \cdot, -, \{c_k : k \in K\}\}$$

entonces φ es verdadera en K si y sólo si φ es verdadera en L.

En la notación usual de modelos esto se escribe como

$$K \models \varphi \Longleftrightarrow L \models \varphi$$

Demostraciones de (A) y (C) aparecen en [7] capítulo 1 y en [5]. Son resultados clásicos hoy en día. Para (B) el lector puede consultar [4] p. 38. Para conveniencia del lector en el apéndice explicamos brevemente las nociones de "definible", "fórmula", "sentencia" y "semialgebraico".

3. Comenzamos con la demostración del Teorema 1(b).

Considere la función real G definida como sigue:

$$G : \mathbb{R}^{2n} \longrightarrow \mathbb{R}$$
$$(x_1, y_1, \ldots, x_n, y_n) \longmapsto ||F^{-1}(x_1 + y_1 i, x_2 + y_2 i, \ldots, x_n + y_n i)||$$

Puesto que F es polinómico, G es definible en la estructura $\widetilde{\mathbb{R}}$. Por resultados de variable compleja F^{-1} es analítica.

En particular F^{-1} es continua y por (A) G es semialgebraica. Aplicando (B) obtenemos que $||F^{-1}||$ está acotada por un polinomio, luego por el teorema de Liouville F^{-1} es polinómico.

Dejamos como ejercicio para el lector demostrar que si K es el subcampo de $\mathbb{C}$ generado por los coeficientes de las componentes polinómicas de F entonces los coeficientes de las componentes de F^{-1} pertenecen a K.

4. Sea K un campo algebraicamente cerrado de característica cero y $F : K^n \to K^n$ una aplicación polinómica biyectiva. Entonces F^{-1} es polinómica.

Para demostrar esto considere el subcampo L de K generado por los coeficientes de las componentes de F. Sea L_1 una clausura algebraica de L dentro de K. El grado de transcendencia de L_1 es finito luego se puede inyectar en $\mathbb{C}$. Sea $\sigma : L_1 \to \mathbb{C}$ una inyección, y pongamos $L' = \sigma(L_1) \subset \mathbb{C}$.

La restricción $F|_{L_1}$ es una aplicación polinómica biyectiva de L_1^n en si mismo pues la afirmación que dice que F es biyectiva se puede escribir por medio de una sentencia en el lenguaje $\mathcal{L}_L$ y aplicamos el resultado (C) a $L_1 < K$.

Haciendo actuar a σ tenemos que

$$\sigma(F|_{L_1}) : L'^n \to L'^n$$

es una biyección polinómica. Aquí $\sigma(F) = (\sigma f_1, \ldots, \sigma f_n)$ y σ actúa sobre un polinomio de la manera obvia: actuando sobre los coeficientes. Aplicando (C) al par $L' < \mathbb{C}$ tenemos que $\sigma(F|_{L_1})$ se extiende una aplicación polinómica biyectiva de $\mathbb{C}^n$ en si mismo. Por el teorema 1(b), el inverso, llamémoslo G, es polinómico y por la observación al final de 3, tiene sus coeficientes en $\sigma(L) \subset L'$. Tenemos el siguiente diagrama:

$$\begin{array}{c} L \hookrightarrow L_1 < K \\ \Big\downarrow \sigma \\ \sigma(L_1) = L' < \mathbb{C} \end{array}$$

La restricción de G a L' es el inverso (polinómico!) de $\sigma(F|_{L'})$. Aplicando σ^{-1} tenemos que $\sigma^{-1}(G|_{L_1})$ es el inverso de $F|_{L_1}$. Claramente la aplicación $\sigma^{-1}(G|_{L'})$ es polinómica, llamémosla G'. Por (C) aplicado al par $L' < K$, G' se extiende a K y es el inverso polinómico de F. Con eso terminamos.

5. El teorema 1(b) es falso para campos algebraicamente cerrados de característica $p > 0$. La función $p(x) = x^p$ es un isomorfismo de $\widetilde{\mathbb{F}}_p$ (la clausura algebraica del campo de p elementos) en si mismo. Su inverso es $r(x) = x^{1/p}$ que no es un polinomio.

Puesto que el teorema 1(b) es cierto para cualquier campo algebraicamente cerrado de cartacterística cero, debería existir una demostración algebraica. En la siguiente sección presentamos una. El teorema 1(a) es cierto si se sustituye $\mathbb{C}$ por $\mathbb{R}$. Esto está demostrado en [3] y [4]. Ambas demostraciones usan ideas bastante elaboradas de topología algebraica. La busqueda de una demostración simple es algo que creo vale la pena. Por otro lado, no hemos podido encontrar otros campos distintos a los finitos, reales cerrados o algebraicamente cerrados donde valga el teorema 1(a). Sería interesante saber si hay más ejemplos.

Note que el teorema 1 dice que el conjunto de biyecciones polinómicas sobre $\mathbb{C}^n$ forma un grupo bajo composición, es decir es un subgrupo del grupo de automorfismos analíticos de $\mathbb{C}^n$.

6. Presentamos ahora una demostración de carácter esencialmente algebraico (usando el teorema 1(a) y 2(C)) del siguiente resultado:

Teorema 2. Sea K un campo algebraicamente cerrado de característica cero y $F : K^n \to K^n$ una aplicación polinómica inyectiva. Entonces F es sobreyectiva y su inverso F^{-1} es polinómico.

Demostración. Sean K y $F = (f_1, \ldots, f_n)$ dados como en las hipótesis del teorema. Por lo dicho en la sección 1, F es sobreyectiva. Sea K' un campo algebraicamente cerrado que extiende a K y que contiene n números $\lambda_1, \ldots, \lambda_n$ transcendentales sobre K y algebraicamente independientes sobre K. Sea F' la extensión de F a K'^n. Puesto que la afirmación que dice que F es biyectiva se puede escribir por medio de una sentencia en el vocabulario $\mathcal{L}_K = \{+, -, \cdot, \{c_k : k \in K\}\}$, se sigue de (C) que F' es biyectiva de K'^n en si mismo. Argumentamos ahora como Rudin [6].

Necesitamos el siguiente lema.

Lema. Sea M/L una extensión de campos de característica cero con $M = L(a_1, \ldots, a_n) \neq L$. Sea $\overline{M}$ una clausura algebraica de M. Entonces existe un monomorfismo $\sigma : M \to \overline{M}$ que fija L y que mueve al menos un a_i.

Demostración. Existe un subconjunto no vacío de $\{a_1, \ldots, a_n\}$, llamémoslo $\{a_1, \ldots, a_\ell\}$ (después de un reordenamiento), minimal con la propiedad que $M = L(a_1, \ldots, a_\ell)$. Sea $L' = L(a_1, \ldots, a_{\ell-1})$.

Si $\ell = 1$, entonces $L' = L$. Tenemos que $L \subset L' \subsetneqq M = L'(a_\ell)$. Definimos σ como sigue: si $x \in L'$ $\sigma(x) = x$.

Si $x = a_\ell$, entonces si a_ℓ es transcendental sobre L' ponemos $\sigma(a_\ell) = a_\ell + 1$; si a_ℓ es algebraico sobre L' con polinomio minimal $p(x)$, definimos $\sigma(a_\ell)$ como cualquier otra raíz de $p(x)$ en $\overline{M}$. Puesto que $p(x)$ es separable (aquí usamos que estamos en característica cero), $p(x)$ tiene raíces distintas entonces $\sigma(a_\ell)$ está bien definida. Finalmente extendemos σ a $L(a_\ell)$ de la manera obvia.

Continuamos con la demostración del teorema.

Sean $\vec{\eta} = (\eta_1, \ldots, \eta_n) = F'(\lambda_1, \ldots, \lambda_n) = F'(\vec{\lambda})$.

Afirmación: $K(\vec{\eta}, \vec{\lambda}) = K(\vec{\eta})$.

Demostración. De lo contrario, por el Lema, existe un monomorfismo σ de $K(\vec{\eta}, \vec{\lambda})$ en K' que fija $K(\vec{\eta})$ y mueve al menos un λ_i. Pongamos $\vec{w} = (\sigma(\lambda_1), \dots, \sigma(\lambda_n))$.

Entonces $\vec{w} \neq \vec{\lambda}$. Por otro lado,

$$f_j(\vec{\lambda}) = \sigma(f_j(\vec{\lambda}) = f_j(\sigma(\lambda_1), \dots, \sigma(\lambda_n)) = f_j(\vec{w}).$$

Luego $F'(\vec{\lambda}) = F'(\vec{w})$, lo cual es una contradicción. La afirmación implica que existen polinomios $r_j, S_j \in K[x_1, \dots, x_n]$ primos relativos en $K'[x_1, \dots, x_n]$ tales que $S_j(\vec{\eta}) \neq 0$ y $\lambda_j = \frac{r_j(\vec{\eta})}{S_j(\vec{\eta})}$.

Reescribiendo esto tenemos $\lambda_j S_j(F'(\vec{\lambda}) - r_j(F'(\vec{\lambda})) = 0$.

Puesto que el conjunto $\{\lambda_1, \dots, \lambda_n\}$ es algebraicamente independiente sobre K tenemos que

$$x_j S_j(F'(\vec{x})) - r_j(F'(\vec{x})) = 0 \quad \forall \vec{x} \in K^{'n}.$$

En otras palabras, puesto que F' es sobreyectiva,

$$V(S_j) := \{\vec{x} \in K^{'n} : S_j(\vec{x}) = 0\} \subset V(r_j) := \{\vec{x} \in K^{'n} : r_j(\vec{x}) = 0\}.$$

Suponga que $V(S_j) \neq \phi$. Sean $S_j = c g_1^{n_1} \dots g_\ell^{n_\ell}$ y $r_j = c' h_1^{m_1} \dots h_m^{m_m}$ factorizaciones de S_j y r_j en irreducibles en $K'[x_1, \dots, x_n]$. Los ideales que corresponden a las variedades $V(S_j)$ y $V(r_j)$ son $\left(\prod_{i=1}^{\ell} g_1\right)$ y $\left(\prod_{i=1}^{m} h_i\right)$. Tenemos que $\left(\prod_{i=1}^{m} h_i\right) \subset \left(\prod_{i=1}^{\ell} g_i\right)$. Luego existe $h \in K'[x_1, \dots, x_n]$ tal que $\prod_{i=1}^{m} h_i = h \prod_{i=1}^{\ell} g_i$.

Luego S_j y r_j no son primos relativos, lo cual es una contradicción.

Esto implica que $V(S_j) = \phi$ y por lo tanto $S_j \circ F' : K^{'n} \to K'$ es constante. Como F' es inyectiva, S_j es constante. Sin pérdida de generalidad $S_j = 1$.

Sea $G = (r_1, \dots, r_n)$. Entonces $G(F'(\vec{x})) = \vec{x} \ \ \forall \vec{x} \in K^{'n}$. Concluímos que $G = F^{-1}$.

Nota. Uno de los objetivos de esta nota era dar una demostración algebraica del teorema 1. Como hizo notar el revisor, la demostración del teorema 2 no es puramente algebraica pues depende de dos resultados de la Teoría de Modelos: la completez y modelo completez de la teoría de campos algebraicamente cerrados de característica cero. Sin embargo, en mi opinión, esta dependecia

es superficial. Los dos resultados usados son consecuencias de la eliminación de cuantificadores para la teoría en cuestion y este resultado es un ejercicio de división de polinomios en varias variables e inducción (de hecho esta fue la demostración que dió A. Tarski en los años veinte). Demostraciones posteriores (por ejemplo las que aparecen en [5] y [7]) usan resultados que son propios de la teoría de modelos como compacidad, saturación, etc. pero oscurecen el hecho de que en realidad no son necesarios.

Apéndice. Un lenjuage adecuado para estudiar propiedades de los números reales es $\mathcal{L}_{\mathbb{R}} = \{+, -, \cdot, <, \{c_r : r \in \mathbb{R}\}\}$. En este lenguaje las $\mathcal{L}_{\mathbb{R}}$–fórmulas básicas son: $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$, $p(x_1, \ldots, x_n) < q(x_1, \ldots, x_n)$ donde $p, q \in \mathbb{R}[x_1, \ldots, x_n]$ para algún $n \in \mathbb{N}$. El conjunto de $\mathcal{L}_{\mathbb{R}}$–fórmulas se obtiene al cerrar el conjunto de fórmulas básicas bajos las operaciones booleanas $\wedge, \vee, \neg$ y los cuantificadores $\exists, \forall$. Así, por ejemplo, las siguientes son $\mathcal{L}_{\mathbb{R}}$–fórmulas:

(a) $\exists x(yx^2 + x + w = 0)$
(b) $\forall x \exists y(y^2 + \sqrt{2y} - \pi = x)$

La fórmula (a) difiere de manera sustancial de (b). En (b) se afirma que para cualquier x hay una solución a cierta ecuación. Esta afirmación es verdadera o falsa. En (a) no se afirma nada pues las variables y, w estan "libres", es decir, no estan ligadas a un cuantificador. Fórmulas como (b)

se llaman sentencias.

Fórmulas con variables libres se suelen denotar por $\varphi(x_1, \ldots, x_n)$ donde se entiende que las variables libres estan en $\{x_1, \ldots, x_n\}$ pero no necesariamente cada x_i es libre. Así (a) se puede denotar por $\varphi(y, w)$ o $\varphi(y, z, v, w)$ pero no por $\varphi(y, z)$.

A cada fórmula $\varphi(x_1, x_2, \ldots, x_n)$ se le asocia un subconjunto S de $\mathbb{R}^n$ de manera natural: $S = \{(r_1, \ldots, r_n) \in \mathbb{R}^n : \varphi(r_1, \ldots, r_n)$ es verdadera$\}$.

Por ejemplo la fórmula en (a) define un subconjunto en $\mathbb{R}^2$, a saber $\{(r_1, r_2) : r_1 \neq 0$ y $1 - 4r_1, r_2 \geq 0\} \cup \{(0, r_2)\}$, aquí hemos ordenado las variables libres $\{y, w\}$ como $y = x_1$, $w = x_2$. Subconjuntos como los de arriba se llaman $\mathcal{L}_{\mathbb{R}}$–definibles o simplemente definibles. En el caso de campos, un lenguaje adecuado para formular propiedades intresantes es $\mathcal{L} = \{+, -, \cdot, 0, 1\}$. Las fórmulas básicas en este contexto son ecuaciones e inecuaciones polinómicas con coeficientes enteros. En el caso del teorema de Robinson ((C) arriba) las fórmulas básicas del lenguaje $\mathcal{L}_K$ son ecuaciones e inecuaciones polinómicas con coeficinetes en K.

Finalmente, recordamos la definición de conjunto semialgebraico. Sea $A \subseteq \mathbb{R}^n$. Decimos que A es semialgebraico si A es una combinación finita de uniones, intersecciones y completos de conjuntos de la forma $\{p(x_1, \ldots, x_n) > 0\}$ donde $p \in \mathbb{R}[x_1, \ldots, x_n]$. Una función $f : A \subset \mathbb{R}^n \to \mathbb{R}^m$ es semialgebraica si su gráfica $G(f) \subset \mathbb{R}^n \times \mathbb{R}^m$ es un subconjunto semialgebraico.

Bibliografía

[1] J. Ax, *The elementary theory of finite fields*,Ann. Math. 88 (1968), pp 239–271.

[2] J. Ax, *Injective endomorphisms of varieties and schemes*,Pacific Journal of Mathematics 31 (1969), pp 1–7.

[3] A. Bialynicki–Birula, M. Rosenlicht,*Injective morphisms of real algebraic varieties*,P.A.M.S., 13 (1962) pp. 200–203.

[4] J. Bochnak, M. Coste, M.F. Roy,*Géometrie Algébrique Réelle*,Springer–Verlag, N. York (1987).

[5] Chang, Keisler,*Model Theory*,North–Holland, Amsterdam (1973).

[6] W. Rudin,*Injective polynomial maps are automorphisms*,Amer. Math. Monthly, (1995) pp. 540–543.

[7] C. Videla,*Un Curso de Lógica Matemática*,Soc. Mat. Mexicana (1995).

[8] T. Winiarski, *Inverse of polynomial automorphism of* $\mathbb{C}^n$,Bull. L'Academie Polonaise Sciencias Vol. XXVII No. 9 (1979) pp. 673–674.

[9] Wright, Connell, Bass, *The Jacobian conjecture: reduction of degree and formal expansion of the inverse*, Bull. AMS 7 (1982) pp 287–330.

(Recibido en agosto de 1996; revisado en septiembre de 1997)

Departamento de Matematicas, CINVESTAV-IPN
Avenida IPN No. 2508,
07000 Mexico, D. F
e-mail: cvidela@@math.cinvestav.mx