El Lema de Nakayama y algunas consecuencias

Índice

1 El Lema de Nakayama

El siguiente resultado es el *Lema de Nakayama* en una de sus versiones.

Teorema 1.1. *Sea k un anillo conmutativo (con 1). Si M un k-módulo f.g. y $\mathfrak{a} \subset k$ es un ideal que verifican:*

$$d \in 1 + \mathfrak{a} \quad , \quad d\,M = 0 \quad \Rightarrow \quad M = 0 \ , \tag{1}$$

entonces $\mathfrak{a}\,M = M$ implica $M = 0$.

Demostración. Si $\mathfrak{a}$ y M verifican las hipótesis y $\mathfrak{a}\,M = M$, entonces, eligiendo generadores, $M = \langle m_1, \ldots, m_r \rangle$ y

$$m_i \ = \ a_i^j\, m_j$$

con $a_i^j \in \mathfrak{a}$. Si $A \in \mathsf{Mat}_{r\times r}(k)$ denota la matriz con coeficientes a_i^j e I la matriz identidad, en el anillo $\mathsf{Mat}_{r\times r}(k)$,

$$\mathsf{adj}(I - A)\,(I - A) \ = \ \mathsf{det}(I - A)\, I$$

y, entonces $\mathsf{det}(I - A)\, m_i = 0$, para cada i. Si $d = \mathsf{det}(I - A)$, entonces $d \in 1 + \mathfrak{a}$ y cumple que $d\,M = 0$. Así, debe ser $M = 0$. □

2 Algunos corolarios

El Teorema 1.1 tiene varias consecuencias importantes. En primer lugar, en una extensión finita de anillos $k \subset B$ (es decir, B es f.g. en tanto k-módulo), el ideal (en B) que se obtiene por extensión a partir de un ideal *propio* de k, también debe ser propio.

Corolario 2.1. *Sea $k \subset B$ una extensión finita de anillos conmutativos (con 1). Si $\mathfrak{a} \subset k$ es un ideal tal que $\mathfrak{a} \neq k$, entonces $\mathfrak{a}^e := \mathfrak{a}\, B \neq B$.*

Demostración. Si $B = 0$, $k = 0$ y no hay nada que probar. Supongamos, entonces, que $1 \neq 0$ $(1 = 1_B = 1_k)$; en particular, $B \neq 0$ como k-módulo. Si $\mathfrak{a} \neq k$, $1 \notin \mathfrak{a}$. Si $d \in k$ y $d\,B = 0$, con lo cual, $d\,1 = 0$ y, así, $d = 0$. En particular, dado que $1 \notin \mathfrak{a}$, $d - 1 \notin \mathfrak{a}$, tampoco. En definitiva, para todo $d \in k$,

$$d \notin 1 + \mathfrak{a} \quad \vee \quad d\,B \neq 0 \quad \vee \quad B = 0\ ,$$

que equivale a (1). Como $B \neq 0$ (mejor dicho, *asumiendo* $B \neq 0$), $\mathfrak{a}\, B \neq B$. □

Corolario 2.2. *Si todo elemento de $1 + \mathfrak{a}$ es invertible y M es un k-módulo f.g., $M' + \mathfrak{a}\, M = M$ implica $M' = M$.*

Observación 2.3. Si M está dado y las operaciones de multiplicación por elementos de $1 + \mathfrak{a}$ son inyectivas, entonces $\mathfrak{a}\, M = M$ implica $M = 0$, por el Teorema 1.1.

Demostración. Veamos, primero el caso $M' = 0$. En este caso, se asume que $\mathfrak{a}\, M = M$ y se debe probar que $M = 0$. Pero, si todo elemento de $1 + \mathfrak{a}$ es invertible, la condición (1) se verifica y $\mathfrak{a}\, M = M$ implica $M = 0$. En general, se aplica el mismo razonamiento al cociente M/M'. □

Corolario 2.4. *Sea $\mathfrak{a} \subset k$ un ideal tal que todo elemento de $1 + \mathfrak{a}$ es invertible. Dado un k-módulo M, un subconjunto $\{m_1, \ldots, m_r\}$ genera M, si y sólo si genera $M/\mathfrak{a}\, M$.*

Demostración. Si $\{m_1, \ldots, m_r\}$ genera M, genera el cociente. Recíprocamente, si el conjunto de clases de los elementos $m_1, \ldots, m_r$ genera $M/\mathfrak{a}\, M$ y si $M' = \langle m_1, \ldots, m_r \rangle \subset M$, entonces $M' + \mathfrak{a}\, M = M$, con lo que, por el Corolario 2.2, $M' = M$. □

Corolario 2.5 (Teorema de intersección de Krull)**.** *Si k es un anillo conmutativo noetheriano y $\mathfrak{a} \subset k$ es un ideal tal que todos los elementos de $1 + \mathfrak{a}$ son invertibles, entonces*

$$\bigcap_{n \geq 1} \big(\mathfrak{a}^n + \mathfrak{b}\big) \ = \ \mathfrak{b}\ , \tag{2}$$

para todo ideal $\mathfrak{b} \subset k$.

Demostración. Supongamos, primero, que $\mathfrak{b} = 0$. Sea $M := \bigcap_{n \geq 1} \mathfrak{a}^n$. Por el Teorema 1.1, o bien, por el Corolario 2.2, será suficiente probar que $\mathfrak{a}\, M = M$. La inclusión $\mathfrak{a}\, M \subset M$ es consecuencia de que M es ideal (módulo). En cuanto a la otra inclusión, todo elemento $x \in M$ se puede escribir de la siguiente manera: fijado un conjunto finito de generadores de $\mathfrak{a}$, $\{a_1, \ldots, a_r\}$, para cada $x \in M$ y cada $n \geq 1$, existe un polinomio homogéneo $f \in k[T_1, \ldots, T_r]$ de grado n, tal que

$$x = f(a_1, \ldots, a_r) .$$

Sea $I \subset k[T_1, \ldots, T_r]$ el ideal generado por los polinomios homogéneos f tales que $f(a_1, \ldots, a_r) \in M$. Como k es noetheriano, $k[T_1, \ldots, T_r]$ también lo es (Teorema de la base de Hilbert) e I está generado por un conjunto finito de polinomios homogéneos, por ejemplo, $\{f_1, \ldots, f_s\}$. Sean $d_i := \mathsf{gr}(f_i)$ y sea $d \geq \max\{d_1, \ldots, d_s\}$. Dado $x \in M$, en particular, $x \in \mathfrak{a}^{d+1}$ y $x = f(a_1, \ldots, a_r)$ para cierto f homogéneo de grado $d+1$. Si

$$f = \sum_i g_i\, f_i \ , \tag{3}$$

con $g_i \in k[T_1, \ldots, T_r]$, separando por grados, los términos de grado distinto de $d+1$ se deben cancelar ($k[T_1, \ldots, T_r]$ es k-libre), con lo que, en la igualdad (3), se puede asumir, sin pérdida de generalidad, que cada g_i es homogéneo de grado $d+1-d_i$. Entonces,

$$x = \sum_{i=1}^{s} g_i(a_1, \ldots, a_r)\, f_i(a_1, \ldots, a_r) .$$

Como $f_i \in I$, $f_i(a_1, \ldots, a_r) \in M$ y, como $d+1-d_i > 0$, $g_i(a_1, \ldots, a_r) \in \mathfrak{a}$. En definitiva, $x \in \mathfrak{a}\, M$.

En general, si $\mathfrak{a} \subset k$ y $M := \bigcap_{n\geq 1} \big(\mathfrak{a}^n + \mathfrak{b}\big)$,

$$\Big(\frac{\mathfrak{a}+\mathfrak{b}}{\mathfrak{b}}\Big)^n = \frac{\mathfrak{a}^n+\mathfrak{b}}{\mathfrak{b}} \ ,$$

en $k/\mathfrak{b}$. Entonces,

$$\frac{M+\mathfrak{b}}{\mathfrak{b}} = \bigcap_{n\geq 1} \frac{\mathfrak{a}^n+\mathfrak{b}}{\mathfrak{b}} = \bigcap_{n\geq 1} \Big(\frac{\mathfrak{a}+\mathfrak{b}}{\mathfrak{b}}\Big)^n .$$

La primera igualdad es consecuencia de que $k \to k/\mathfrak{b}$ es sobre y $\mathfrak{a}^n + \mathfrak{b} \supset \mathfrak{b}$, mientras que la segunda se debe a que $c\,(1+a) \in \mathfrak{b}$ implica $c \in \mathfrak{b}$, siempre que $a \in \mathfrak{a}$ y $c \in k$. $\square$

Observación 2.6. Se puede ver de la demostración que la condición de que todos los elementos de $1+\mathfrak{a}$ sean invertibles se puede debilitar un poco: la conclusión sigue siendo válida, si se asume que

$$\big(\forall c \in k\big)\ \big(\forall a \in \mathfrak{a}\big)\ \big(c\,(1+a) \in \mathfrak{b} \Rightarrow c \in \mathfrak{b}\big) \tag{4}$$

En el caso en que $\mathfrak{b} = 0$, esto quiere decir que $1+\mathfrak{a}$ no contiene divisores de cero.

3 Subvariedades de codimensión 1

Sea X una variedad y sea $C \subset X$ una subvariedad de codimensión 1. Supongamos que X es no singular en codimensión 1. Entonces C está dada por una ecuación local $\mathcal{I}_C(U) = \langle h \rangle \subset \mathcal{O}_X(U)$, en algún abierto $U \subset X$. Como X es irreducible, U también lo es y el anillo $\mathcal{O}_X(U)$ es un dominio íntegro. En particular, si $I := \mathcal{I}_C(U)$, $1 + I$ no contiene divisores de cero y, por el Corolario 2.5,

$$\bigcap_{n \geq 1} I^n = 0 \ .$$

En particular, si $f \in \mathcal{O}_X(U)$ no es cero, o bien $f \notin I$, o bien existe $n \geq 1$ tal que $f \in I^n \smallsetminus I^{n+1}$. Dicho de otra manera, el conjunto

$$\big\{ n \geq 1 \ : \ f \notin I^n \big\}$$

no es vacío y, por buena ordenación, contiene un primer elemento.

---x---

Referencias

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969). 1969.

[2] I. R. Shafarevich. *Basic Algebraic Geometry 1. Varieties in Projective Space. Translated from the Russian by Miles Reid.* 3rd ed. Berlin: Springer, 2013.