FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Dimensión en álxebra e xeometría

Pablo Montaña Fernández

Xullo, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Dimensión en álxebra e xeometría

Pablo Montaña Fernández

Xullo, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Dimensión en álxebra e xeometría
Breve descrición do contido
As variedades alxébricas son os subconxuntos do espazo afín definidos por un sistema de ecuacións polinómicas. A falta dun análogo do teorema da función inversa provoca que a noción de dimensión neste tipo de conxuntos requira a introdución de nocións de dimensión no contexto dos aneis conmutativos. O traballo abordará o estudo das posibles nocións de dimensión en aneis conmutativos. Tamén se abordará a conexión entre dimensión e grao de trascendencia mediante o teorema de normalización de Noether. Explorarase a conexión entre a álxebra e a xeometría: ecuacións fronte a proxeccións lineares.
Recomendacións
Ter un bo coñecemento das materias Estruturas e Ecuacións Alxébricas.
Outras observacións

Índice

Resumo

As variedades alxébricas son os subconxuntos do espazo afín determinados por un sistema de ecuacións polinómicas. A falta dun análogo do teorema da función inversa provoca que a noción de dimensión neste tipo de conxuntos requira a introdución de nocións de dimensión no contexto dos aneis conmutativos.

O obxectivo deste traballo é analizar as propiedades que debe verificar unha definición de dimensión neste ámbito e estudar a dimensión de Krull como definición apropiada. Veremos varios resultados que nos brinda, como se aplica ao caso das variedades alxébricas e distintas caracterizacións que a relacionan con outros aspectos xeométricos.

Abstract

Algebraic varieties are defined as the set of points satisfying a system of polynomial equations. The lack of a result akin to the inverse function theorem implies that the notion of dimension concerning this kind of sets demands the introduction of notions of dimension within the context of commutative rings.

The aim of this dissertation is to analyze the conditions that a dimension definition must satisfy in this field and to study the Krull dimension as an appropriate definition. We will see several results about it, how we may apply it to algebraic varieties and some characterizations that connect it with other geometric aspects.

Introdución

Un concepto fundamental en xeometría é o de dimensión. En moitos casos, xorde de xeito intuitivo e así afirmamos que unha recta ten unha dimensión, un plano ten dúas dimensións e o mundo que nos rodea é (polo menos dende un punto de vista espacial) tridimensional.

Xeralizando a noción de puntos, rectas e planos, podemos considerar variedades lineares. Unha variedade linear é un subconxunto do espazo afín que é solución dun sistema de ecuacións lineares. Xeometricamente, é unha traslación dun subespazo vectorial, polo que é sinxelo definir a súa dimensión empregando esta natureza. Podemos xeralizar a construción e considerar un sistema de ecuacións polinómicas non necesariamente lineares. A solución dun sistema deste tipo é un subconxunto do espazo afín e recibe o nome de variedade alxébrica afín. Porén, non se pode estender a noción de dimensión como dimensión dun subespazo vectorial, polo que o camiño a seguir debe ser distinto.

A álxebra conmutativa é unha ferramenta moi útil para explicar moitas cuestións relativas á xeometría. En certo modo, pódese pensar que álxebra conmutativa e xeometría alxébrica son en moitos casos dúas caras da mesma moeda. É por isto que para estudar o concepto de dimensión de variedades alxébricas, podemos tratar de enmarcalo no ámbito dos aneis conmutativos, e chegar así a unha definición apropiada, de gran valor teórico, e que nos brinde a posibilidade de entender o seu significado xeométrico.

Ao longo da historia das matemáticas, o concepto de dimensión empregouse fundamentalmente de xeito intuitivo. Así, na Antiga Grecia entendían unha curva como algo limitado por puntos, unha superficie como algo limitado por curvas e un volume como algo limitado por superficies. Posteriormente, comezou a verse a dimensión dun obxecto como o número mínimo de parámetros necesarios para describilo dalgunha maneira. Porén, Cantor, en 1875, deu unha correspondencia bixectiva entre os puntos dunha curva e un plano, facendo evidente a necesidade de especificar que se entende por dimensión.

No eido topolóxico, a comezos do século XX deuse unha primeira definición concisa: a dimensión dun espazo nun punto defínese de xeito inductivo como o menor número n tal que toda veciñanza do punto arbitrariamente pequena ten fronteira de dimensión menor que n. Esta definición implicaba que a dimensión debía ser unha propiedade local.

En canto ao caso alxébrico, unha das primeiras definicións de dimensión chegou no século XIX a raíz do traballo coas superficies de Riemann e a esixencia de que o n-espazo afín debía ter dimensión n. Así, falábase da dimensión dunha variedade alxébrica sobre o corpo K como o grao de trascendencia sobre K do corpo de funcións racionais na variedade. Esta definición foi de feito aceptada ata ben entrado o século XX, pero deixou de ser funcional para novas construcións xurdidas neses anos (hai aneis que non conteñen corpos, polo que a definición carecía de utilidade neses casos). De feito, xa se tiña a idea de que a dimensión debía ser unha propiedade local dun punto, polo que esa definición non parecía ser a apropiada. Foi entón cando Krull propuxo o que hoxe coñecemos como dimensión dun anel: o supremo das lonxitudes de cadeas de ideais primos distintos.

Ao longo deste traballo, estudaremos esta definición e veremos resultados interesantes que verifica. Así mesmo, intentaremos xustificar por que se considera que é unha definición apropiada. No Capítulo 1 introducimos ferramentas necesarias de álxebra conmutativa que precisaremos máis adiante; son resultados elementais de teoría de aneis conmutativos e módulos. No Capítulo 2 presentamos as variedades alxébricas e vemos as súas propiedades. O Teorema dos Ceros de Hilbert permitiranos pasar ao eido alxébrico para traballar con estes obxectos xeométricos. No Capítulo 3, facemos un análise dende un punto de vista xeométrico das propiedades que debería verificar unha definición "correcta" de dimensión. Estas propiedades, como veremos despois, son verificadas pola definición de Krull. No Capítulo 4 entramos de cheo nesta definición e vemos as súas propiedades, así como resultados interesantes entre os que se atopan algúns dos axiomas do capítulo previo. No Capítulo 5, estudamos a relación existente entre a dimensión dunha variedade e o número de ecuacións necesario para describila, introducindo para iso o Teorema do Ideal Principal de Krull. Por último, vemos dúas caracterizacións: no Capítulo 6, vemos que a definición coincide precisamente co grao de trascendencia no caso de dominios afíns empregando o célebre Teorema de Normalización de Noether; no Capítulo 7, damos unha caracterización mediante as funcións de Hilbert-Samuel cuxo principal interese reside en que permite o cálculo explícito da dimensión de moitos aneis.

Todos os aneis considerados serán aneis conmutativos e unitarios.

Capítulo 1

Preliminares

Ao longo deste capítulo veremos diversas definicións e resultados de álxebra conmutativa que nos serán útiles e necesarios para o resto do traballo. Salvo mención expresa, A designará un anel conmutativo unitario, M un A-módulo e K un corpo. As demostracións que non se aportan poden consultarse nos libros de Atiyah e Macdonald [3], Eisenbud [6] ou Fulton [7].

1.1. Aneis noetherianos

O contexto do noso estudo será maiormente o dos aneis noetherianos, os cales cumpren propiedades moi interesantes como a dada polo coñecido Teorema da base de Hilbert.

Proposición 1.1. *Dado un anel A, son equivalentes as seguintes condicións:*

1. *Todo ideal en A é finitamente xerado.*
2. *Toda cadea ascendente de xeito estrito de ideais en A é estacionaria.*
3. *Cada conxunto non vacío de ideais en A ten un elemento maximal.*

Definición 1.2. Un anel que cumpre unha das condicións equivalentes anteriores dise *noetheriano.*

Observación 1.3. Os únicos ideais dun corpo son 0 e o propio corpo polo que todo corpo é noetheriano.

Proposición 1.4. *Se A é noetheriano e I é un ideal en A, A/I é noetheriano.*

Demostración. Dado un ideal J en A/I, a súa preimaxe é un ideal finitamente xerado, e as imaxes dos seus xeradores xeran J. □

Proposición 1.5. *Sexa A noetheriano e I un ideal en A. Entón o conxunto de ideais primos de A minimais sobre I é finito.*

Teorema 1.6 (Teorema da base de Hilbert)**.** *Se A é noetheriano, entón o anel de polinomios $A[x]$ é noetheriano.*

Corolario 1.7. *Se A é noetheriano, tamén o é $A[x_1, \dots, x_n]$.*

Demostración. Inmediato por indución en n usando o isomorfismo de aneis $A[x_1, \dots, x_{n+1}] \cong A[x_1, \dots, x_n][x_{n+1}]$. □

O resultado é tamén certo para álxebras finitamente xeradas sobre un anel noetheriano.

Corolario 1.8. *Se B é unha álxebra finitamente xerada sobre un anel noetheriano A, entón B é noetheriano.*

Demostración. Por ser B finitamente xerada sobre A, $B \cong A[x_1, \dots, x_n]/I$ para algún ideal I en A. Por 1.4 e 1.7 B é noetheriano. □

1.2. Localización

O seguinte proceso de localización recibe o seu nome pola posibilidade que nos brinda de estudar as variedades alxébricas "preto" dun punto, como veremos no seguinte capítulo.

Definición 1.9. Sexan A un anel, M un A-módulo e $U \subset A$ un conxunto mulitplicativamente pechado. Definimos a *localización de M en U*, denotado $U^{-1}M$ ou $M[U^{-1}]$, como o conxunto de clases de equivalencia $(m, u) \in M \times U/\sim$ dado pola relación $(m, u) \sim (m', u')$ se existe $v \in U$ tal que $v(u'm - um') = 0$. A clase de equivalencia (m, u) denótase m/u.

É inmediato dotar a $M[U^{-1}]$ de estrutura de A-módulo coa suma e produto por escalar análogos ao caso de fraccións habituais.

Da definición de ideal primo dedúcese que se $P \subset A$ é primo, $A - P$ é un conxunto multiplicativamente pechado (se $f, g \notin P$ entón fg non pode estar en P). A localización de A sobre tal conxunto denótase por A_P. O conxunto de elementos $I = \{a/u \in A_P \mid a \in P\}$ forman un ideal maximal de A_P, e este é o único ideal maximal de A_P, é dicir, A_P é un *anel local.*

A seguinte proposición descríbenos como son os ideais da localización $A[U^{-1}]$ con respecto ao anel A. Isto daranos unha ferramenta útil para traballar máis adiante no eido xeométrico. A aplicación $i : A \to A[U^{-1}]$ denota a inclusión natural $a \mapsto a/1$.

Proposición 1.10. *1. Todo ideal $I \subset A[U^{-1}]$ verifica $I = i^{-1}(I)A[U^{-1}]$. Polo tanto, a aplicación $I \mapsto i^{-1}(I)$ do conxunto de ideais de $A[U^{-1}]$ no conxunto de ideais de A é inxectiva. Preserva as inclusións, interseccións e a primalidade.*

2. Un ideal $J \subset A$ é da forma $i^{-1}(I)$ para algún ideal I de $A[U^{-1}]$ se e só se $J = i^{-1}(JA[U^{-1}])$, caso que se dá se e só se cada elemento $u \in U$ é un non-divisor de cero módulo J. En particular, $I \mapsto i^{-1}(I)$ é unha bixección entre os primos de $A[U^{-1}]$ e os primos de A con $A \cap U = \emptyset$.

Observación 1.11. No caso da localización de A sobre un ideal primo P, o segundo apartado da proposición anterior danos unha correspondencia bixectiva entre os primos de A_P e os primos Q de A tales que $Q \cap (A - P) = \emptyset$, é dicir, os primos de A contidos en P. Dado un ideal $Q \subset P$, denotaremos por $Q_P := QA_P$ ao ideal primo de A_P correspondente. En xeral, dado un ideal $I \subset P$ non necesariamente primo, é inmediato que $I_P := IA_P$ é un ideal en A_P e empregaremos a mesma notación.

Dado un anel $A \neq 0$, sexa $S \subset A$ o subconxunto (multiplicativamente pechado) de elementos non-divisores de cero de A. A localización de A sobre S, $A[S^{-1}]$, recibe o nome de *anel total de fraccións* de A e denotarémolo por $Q(A)$.

1.3. Aneis artinianos

Existe unha condición dual á de ser noetheriano: que toda cadea descendente de ideais sexa estacionaria. Isto dá lugar aos aneis artinianos:

Definición 1.12. Un anel A dise *artiniano* se toda cadea descendente de ideais en A é estacionaria.

Os aneis artinianos, pese a ter unha definición análoga aos noetherianos, non verifican as mesmas propiedades. De feito, son un tipo moi particular de aneis noetherianos. Pero antes de enunciar o teorema que o amosa cómpre introducir varias definicións sobre módulos.

Definición 1.13. Dado un módulo M, chámase *cadea* de submódulos de M a unha sucesión de submódulos

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r.$$

Unha cadea deste tipo dise que ten lonxitude r.

Definición 1.14. Unha cadea de submódulos de M dise que é unha *serie de composición de M* se é unha cadea maximal, no sentido de que non se pode insertar de xeito estrito outro submódulo na cadea.

O seguinte resultado afírmanos que toda serie de composición ten a mesma lonxitude.

Teorema 1.15 (Jordan-Hölder). *Se un módulo M ten unha serie de composición de lonxitude r, entón toda serie de composición de M ten lonxitude r.*

Definición 1.16. Defínese a *lonxitude* dun módulo M como a lonxitude dunha serie de composición de M. Se non ten ningunha serie de composición dise que M ten lonxitude ∞.

A lonxitude dun módulo é unha xeralización da dimensión dun espazo vectorial. Estamos agora en condicións de enunciar o seguinte teorema. A demostración pode verse en [1, pp. 32-34].

Teorema 1.17. *Sexa A un anel. As seguintes condicións son equivalentes:*

1. *A é noetheriano e todo ideal primo en A é maximal.*
2. *A é de lonxitude finita como R-módulo.*
3. *A é artiniano.*

Se se verifican estas condicións, entón A ten un número finito de ideais maximais.

Os aneis artinianos, como veremos no Capítulo 3, xogarán un papel fundamental nas condicións de finitude de variedades alxébricas. Rematamos esta sección con dúas consecuencias do anterior teorema que nos serán útiles na demostración do Teorema do Ideal Principal de Krull.

Corolario 1.18. *Sexa A un anel noetheriano e M un A-módulo finitamente xerado. As seguintes condicións son equivalentes:*

1. *M é de lonxitude finita.*
2. *Existen $P_1, \dots, P_r$ ideais maximais en A tales que $\prod_{i=1}^{r} P_i$ aniquila M.*
3. *Todos os ideais primos que conteñen a $\operatorname{ann}(M)$ son maximais.*
4. *$A/\operatorname{ann}(M)$ é un anel artiniano.*

Corolario 1.19. *Sexa I un ideal dun anel noetheriano A. Se P é un ideal primo que contén a I, son equivalentes:*

1. *P é minimal entre os ideais primos que conteñen a I.*
2. *R_P/I_P é artiniano.*
3. *Na localización R_P verifícase $P_P^r \subset I_P$ para r suficientemente grande.*

1.4. Elementos nilpotentes

Un elemento a dun anel A dise *nilpotente* se existe $r > 0$ tal que $a^r = 0$.

Proposición 1.20. *O conxunto N de elementos nilpotentes dun anel A é un ideal, e A/N non ten elementos nilpotentes distintos de* 0.

O ideal N recibe o nome de *nilradical* de A. Un anel dise *reducido* se non ten elementos nilpotentes distintos de 0, polo que $A_{\mathrm{red}} := A/N$ é un anel reducido para calquera anel A.

Proposición 1.21. *O nilradical de A é a intersección de todos os ideais primos de A.*

Corolario 1.22. *Sexa $A \neq 0$ un anel cun número finito de ideais primos minimais, $P_1, \ldots, P_s$. Entón o nilradical de A é $\bigcap_{i=1}^s P_i$. Ademais, $\bigcup_{i=1}^s P_i$ só contén divisores de cero e se A é reducido, $\bigcup_{i=1}^s P_i$ é o conxunto de todos os divisores de cero de A.*

Sexa agora I un ideal de A. Defínese o *radical* de I como

$$\operatorname{rad} I = \{a \in A \mid a^r \in I \text{ para algún } r > 0\}.$$

Se $\pi : A \to A/I$ é o homomorfismo canónico, temos que $\operatorname{rad} I = \pi^{-1}(N)$, onde N é o nilradical de A/I, e polo tanto $\operatorname{rad} I$ é un ideal.

Proposición 1.23. *O radical dun ideal $I \subset A$ é a intersección de todos os ideais primos de A que conteñen a I.*

Demostración. Aplicar a proposición anterior a A/I. □

Proposición 1.24. *Se M é un A-módulo finitamente xerado e I é un ideal de A, entón*

$$\operatorname{rad}(\operatorname{ann}(M/IM)) = \operatorname{rad}(I + \operatorname{ann} M).$$

En particular, se A é un anel local con ideal maximal $\mathfrak{m}$, entón M/IM ten lonxitude finita se e só se $(I + \operatorname{ann} M) \supset \mathfrak{m}^n$ para un n suficientemente grande.

1.5. Dependencia enteira

Lembremos que se B é unha A-álxebra, un elemento $b \in B$ dise *enteiro* sobre A se é raíz dun polinomio mónico con coeficientes en A.

Proposición 1.25. *Sexan $A \subset B$ aneis. Son equivalentes:*

1. *$b \in B$ é enteiro sobre A.*

2. *$A[b]$ é un A-módulo finitamente xerado.*

3. *$A[b]$ está contido nun subanel C de B tal que C é un A-módulo finitamente xerado.*

Demostración. Véxase [3, p. 66]. □

Proposición 1.26. *Sexa A un anel e J un ideal do anel de polinomios $A[x]$. Sexa $B := A[x]/J$. Entón B é un A-módulo finitamente xerado se e só se J contén un polinomio mónico.*

Definición 1.27. O *radical de Jacobson* dun anel A, denotado $J(A)$, é a intersección de todos os ideais maximais de A.

Proposición 1.28 (Lema de Nakayama)**.** *Sexa A un anel, $I \subset J(A)$ un ideal contido no radical de Jacobson e M un A-módulo finitamente xerado. Verifícase:*

1. *Se $IM = M$, entón $M = 0$.*

2. *Se as imaxes de $m_1, \ldots, m_r \in M$ en M/IM xeran M/IM como A-módulo, entón $m_1, \ldots, m_r$ xeran M como A-módulo.*

Os seguintes dous resultados son esencialmente consecuencia do lema de Nakayama.

Proposición 1.29 (Teorema do ascenso)**.** *Supoñamos que $A \subset B$ é unha extensión enteira de aneis $-$é dicir, todos os elementos de B son enteiros sobre $A-$. Entón, dado un ideal primo P en A, existe un primo Q en B tal que $P = Q \cap A$. Ademais, se I é un ideal en B verificando $I \cap A \subset P$, o anterior ideal Q pode tomarse de xeito que conteña a I.*

Proposición 1.30 (Incomparabilidade)**.** *Se $A \subset B$ é unha extensión enteira de aneis, calquera dous ideais primos de B distintos coa mesma intersección con A son incomparables.*

Capítulo 2

Variedades alxébricas

Neste capítulo introducimos o obxecto xeométrico central do noso estudo: as variedades alxébricas. Veremos a súa definición, algunhas propiedades, e a relación que teñen con certos ideais do anel de polinomios. Esta relación entre variedades e ideais, dada polo Teorema dos Ceros de Hilbert (*Nullstellensatz*, polo seu nome en alemán) permitiranos traballar no marco da álxebra conmutativa para acadar resultados con aplicacións xeométricas. Ademais, construiremos o anel de coordenadas dunha variedade, o cal garda unha íntima relación coa variedade en si.

Dado un polinomio $f \in K[x_1, \dots, x_n]$ podemos considerar unha función $f : K^n \to K$ do n-espazo afín K^n no corpo K; a imaxe de cada punto $(a_1, \dots, a_n)$ vén dada substituíndo en f os x_i polos a_i. As funcións deste tipo reciben o nome de *funcións polinómicas* e se K é infinito, polinomios distintos definen funcións distintas (só o polinomio identicamente nulo se pode anular para todo K^n). Polo tanto, podemos ver o anel de polinomios $K[x_1, \dots, x_n]$ como o anel de funcións polinómicas en K^n. As variedades alxébricas serán subconxuntos do espazo afín que anulan un certo conxunto de funcións polinómicas.

Definición 2.1. Dado un subconxunto $S \subset K[x_1, \dots, x_n]$ de funcións polinómicas, podemos asociarlle un subconxunto do espazo afín

$$V(S) := \{(a_1, \dots, a_n) \in K^n \mid f(a_1, \dots, a_n) = 0 \quad \forall f \in S\},$$

que recibe o nome de *variedade alxébrica (afín).*

Observación 2.2. Dise afín para diferencialo do caso proxectivo. Ao longo deste traballo, se non se especifica o contrario, referirémonos sempre a variedades alxébricas afíns.

Observación 2.3. Se I é o ideal xerado por S en $K[x_1, \dots, x_n]$, tense que $V(S) = V(I)$. En efecto, os polinomios de I son da forma $\sum g_i f_i$ con $g_i \in K[x_1, \dots, x_n]$ e $f_i \in S$, polo que os puntos que anulan os polinomios de S anulan os polinomios de I. A inclusión recíproca é trivial. Polo tanto na definición de $V(S)$ podemos intercambiar S polo ideal que xera. Como $K[x_1, \dots, x_n]$ é noetheriano, o ideal I é finitamente xerado, é dicir, existen polinomios $f_1, \dots, f_m$ tales que $I = (f_1, \dots, f_m)$ e así podemos ver $V(I)$ como o conxunto de solucións do sistema de ecuacións polinómicas

$$f_i(x_1, \dots, x_n) = 0 \quad (i = 1, \dots, m)$$

Exemplos 2.4. Se $K = \mathbb{R}$:

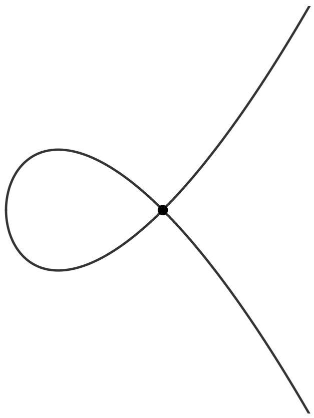


Figura 2.1: Cúbica nodal, $V(y^2 - x^3 - x^2) \subset \mathbb{R}^2$

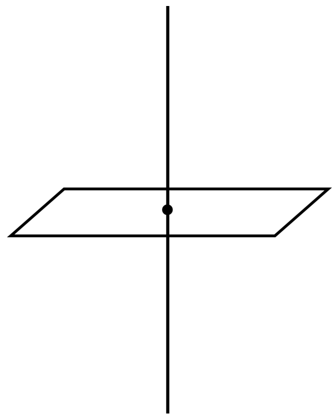


Figura 2.2: $V(xz, yz) \subset \mathbb{R}^3$

As variedades alxébricas cumpren as seguintes propiedades inmediatas:

1. $V(0) = K^n$ e $V(K[x_1, \dots, x_n]) = \emptyset$, polo que $\emptyset$ e K^n son variedades alxébricas.

2. Se $\{I_\alpha\}$ é unha familia arbitraria de ideais tense que $\bigcap_\alpha V(I_\alpha) = V\left(\bigcup_\alpha I_\alpha\right)$, e así a intersección arbitraria de variedades é unha variedade.

3. Se $\{I_i\}_{i=1}^n$ é unha familia finita de ideais e $\prod_{i=1}^n I_i$ é o seu produto, tense que $\bigcup_{i=1}^n V(I_i) = V\left(\prod_{i=1}^n I_i\right)$, polo que a unión finita de variedades é unha variedade.

Polo tanto, as variedades alxébricas son os pechados dunha topoloxía sobre K^n, a cal recibe o nome de *topoloxía de Zariski*. Nos casos $K = \mathbb{R}$ ou $\mathbb{C}$ tense que esta topoloxía é moito menos fina que a topoloxía usual.

Definición 2.5. Se V é unha variedade alxébrica, unha *subvariedade* de V é unha variedade alxébrica contida en V. Se V non se pode expresar como unión de subvariedades non vacías e contidas estritamente en V, dise que V é unha variedade alxébrica *irreducible*.

Observación 2.6. Algúns autores reservan o termo variedade para o caso irreducible e denominan conxunto alxébrico ao que nós definimos como variedade alxébrica.

Unha subvariedade de V dise *compoñente irreducible* de V se é maximal entre as subvariedades irreducibles. Empregando o lema de Zorn e o Teorema da Base de Hilbert é inmediato probar o seguinte feito:

Proposición 2.7. *Toda variedade alxébrica é unión finita de compoñentes irreducibles. Se ademais esiximos que ningunha compoñente esté contida noutra, esta descomposición é única.*

Do xeito "recíproco" ao feito previamente, a cada subconxunto do espazo afín podemos asociarlle un ideal do anel de polinomios: dado $X \subset K^n$, definimos

$$I(X) := \{f \in K[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in X\},$$

que certamente é un ideal en $K[x_1, \dots, x_n]$. Podemos así construír para cada $X \subset K^n$ a K-álxebra finitamente xerada

$$A(X) := K[x_1, \dots, x_n]/I(X),$$

que recibe o nome de *anel de coordenadas* de X. Pode identificarse co anel de funcións polinomicas en X, pois dous polinomios $f, g \in K[x_1, \dots, x_n]$ definen a mesma función en X se toman o mesmo valor para cada punto de X, é dicir, se $f - g \in I(X)$.

O teorema fundamental da álxebra vincula álxebra e xeometría ao afirmar que todo polinomio nunha variable sobre $\mathbb{C}$ (un obxecto alxébrico) está univocamente determinado, salvo produto por unha constante, polo conxunto das súas raíces (un obxecto xeométrico). O seguinte teorema, debido a Hilbert, xeraliza esta idea a ideais radicais de polinomios en varias variables.

Teorema 2.8 (Teorema dos Ceros de Hilbert)**.** *Sexa K un corpo alxebricamente pechado. Se $I \subset K[x_1, \dots, x_n]$ é un ideal, entón*

$$I(V(I)) = \operatorname{rad} I.$$

Como consecuencia, existe unha correspondencia biunívoca entre as variedades alxébricas do n-espazo afín e os ideais radicais de $K[x_1, \dots, x_n]$.

Demostración.

1. Forma débil: se $V(I) = \emptyset$ entón $I = (1)$.

   Supoñamos que $I \neq (1)$ e tomemos $\mathfrak{m}$ un ideal maximal contendo a I. Temos entón que $\mathcal{K} := K[x_1, \dots, x_n]/\mathfrak{m}$ é un corpo e polo tanto (lema de Zariski, [3]) $\mathcal{K}$ é unha extensión alxébrica de K. Por ser K alxebricamente pechado, $\mathcal{K} = K$. Entón, para cada x_i existe un $a_i \in K$ tal que $x_i - a_i \in \mathfrak{m}$, logo $(x_1 - a_1, \dots, x_n - a_n) \subset \mathfrak{m}$ e por ser $(x_1 - a_1, \dots, x_n - a_n)$ maximal (como veremos máis adiante) tense $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ e así $(a_1, \dots, a_n) \in V(\mathfrak{m}) \subset V(I)$ polo que $V(I) \neq \emptyset$.

2. Teorema dos Ceros.

Supoñamos $g \in IV(I)$ e tomemos $J := I + (x_{n+1}g - 1) \subset K[x_1, \dots, x_n, x_{n+1}]$. Dado $P \in V(J) = V(I) \cap V(x_{n+1}g - 1)$, temos por un lado que $P \in V(I)$ polo que $g(P) = 0$ e así $x_{n+1}g - 1$ evaluado en P é -1. Por outro lado, $P \in V(x_{n+1}g - 1)$ e polo tanto $x_{n+1}g - 1$ evaluado en P é 0, chegando así a unha contradición. Temos entón que $V(J)$ ten que ser vacío e aplicando a forma débil sabemos que $J = (1)$. Tomemos $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ xeradores de I. Entón, como $1 \in J = (f_1, \dots, f_r) + (x_{n+1}g - 1)$, temos que $1 = \sum_{i=1}^r a_i(x_1, \dots, x_{n+1})f_i + b(x_1, \dots, x_{n+1})(x_{n+1}g - 1)$, onde os a_i e b son polinomios en $K[x_1, \dots, x_{n+1}]$. Facendo o cambio de variable $y = 1/x_{n+1}$ e multiplicando por unha potencia o suficientementa grande de y para quitar denominadores obtemos

$$y^N = \sum_{i=1}^{r} c_i(x_1, \dots, x_n, y)f_i + d(x_1, \dots, x_n, y)(g - y)$$

e substituíndo g por y temos que $g^N = \sum_{i=1}^r c_i(x_1, \dots, x_n, g)f_i \in I$ polo que $g \in \operatorname{rad} I$.

Reciprocamente, se $0 \neq g \in \operatorname{rad} I$ entón existe N tal que $g^N \in I$. Dado $P \in V(I)$, temos que $g^N(P) = 0$ polo que $g(P) = 0$ e así $g \in I(V(I))$.

□

Podemos ir máis aló nesta correspondencia: os ideais primos correspóndense con variedades irreducibles. Este feito é consecuencia directa do teorema anterior e do seguinte resultado:

Proposición 2.9. *Unha variedade alxébrica V é irreducible se e só se $I(V)$ é un ideal primo.*

Demostración. Procederemos en ambas implicacións por redución ao absurdo. Supoñamos que existen polinomios $f_1, f_2 \notin I(V)$ tales que $f_1 f_2 \in I(V)$. Entón $V \subset V(f_1, f_2) = V(f_1) \cup V(f_2)$, polo que $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ e como $f_i \notin I(V)$, $V \cap V(f_i) \subsetneq V$ e V non sería irreducible.

Reciprocamente, supoñamos que $V = V_1 \cup V_2$ con $V_i \subsetneq V$. Entón $I(V) \subsetneq I(V_i)$ e se tomamos $f_i \in I(V_i) - I(V)$ temos que $f_1 f_2 \in I(V)$, polo que $I(V)$ non sería primo. □

En particular, se K é alxebricamente pechado, temos unha correspondencia biunívoca entre os ideais primos (en particular radicais) de $K[x_1, \dots, x_n]$ e as variedades irreducibles do n-espazo afín. Ademais podemos determinar cales son os ideais maximais. Notemos primeiro que dado un punto $p = (a_1, \dots, a_n) \in K^n$ temos que $I(p) = \mathfrak{m}_p := (x_1 - a_1, \dots, x_n - a_n)$. En efecto, é obvio que $\mathfrak{m}_p \subset I(p)$, e como pasar ao cociente $K[x_1, \dots, x_n]/\mathfrak{m}_p$ consiste en identificar as variables x_i cos escalares a_i temos $K[x_1, \dots, x_n]/\mathfrak{m}_p \cong K$ e así $\mathfrak{m}_p$ é maximal, de onde $\mathfrak{m}_p = I(p)$. Só nos falta ver que todos os ideais maximais son desta forma. Tomemos entón un ideal maximal $\mathfrak{m}$ en $K[x_1, \dots, x_n]$. En particular é un ideal radical, e polo teorema 2.8 temos $I(V(\mathfrak{m})) = \mathfrak{m}$. Pero se

$p \in V(\mathfrak{m})$, entón

$$\mathfrak{m} = I(V(\mathfrak{m})) \subset I(p) = \mathfrak{m}_p$$

e pola maximalidade de $\mathfrak{m}$ temos que $\mathfrak{m} = \mathfrak{m}_p$. Rematamos de demostrar entón o seguinte resultado:

Proposición 2.10. *Se K é alxebricamente pechado, existe unha correspondencia biunívoca entre as variedades alxébricas do n-espazo afín e os ideais radicais de $K[x_1, \dots, x_n]$ na que as variedades irreducibles se corresponden con ideais primos e os puntos con ideais maximais.*

Esta correspondencia tamén se pode particularizar para corresponder as subvariedades dunha variedade dada V cos ideais radicais do seu anel de coordenadas $A(V) = K[x_1, \dots, x_n]/I(V)$. Unha vez máis, as subvariedades irreducibles de V correspóndense con ideais primos de $A(V)$ e os puntos con ideais maximais.

Ao longo deste traballo, aínda que moitos dos resultados se poden xeralizar para corpos arbitrarios, K fará referencia a un corpo alxebricamente pechado salvo mención expresa.

2.1. Anel local

Un dos obxectos fundamentais da topoloxía son as veciñanzas locais dun punto. Moitos resultados que atinxen a espazos topolóxicos poden reducirse ao caso local para facilitar a súa resolución. No eido alxébrico, haberá certos casos nos que nos interesará averiguar as propiedades dunha variedade alxébrica V "preto" dun punto $p \in V$.

Se consideramos a topoloxía de Zariski, as veciñanzas abertas de p en V serán conxuntos da forma $V - W$, sendo W unha subvariedade de V que non contén ao punto p. Como nos interesan veciñanzas arbitrariamente "pequenas", precisamos que W sexa "grande", polo que podemos supoñer que W está formado polos puntos que anulan unha única función polinómica f que non se anula en p, é dicir, que $W = V(f)$ con $f(p) \neq 0$.

A cuestión radica en que $V - W$ pode verse como unha variedade alxébrica de K^{n+1} contida en V por proxección (ver [6], pp. 58,59), e o seu anel de coordenadas $A(V - W)$ obtense engadindo a $A(X)$ unha inversa multiplicativa de f. Polo tanto, se a $A(X)$ lle engadimos inversos multiplicativos de todas as funcións polinómicas que non se anulan en p, obtemos un novo obxecto alxébrico que reúne en certo modo as características locais de V en p. É o que se denomina *anel local* da variedade V en p.

Este feito xeométrico motiva a definición do proceso de localización que víamos no capítulo anterior. De feito, podemos xustificar a definición dada de anel local dunha variedade nun punto: se $A(V)$ é o anel de coordenadas de V e $P \subset A(V)$ é o ideal de funcións polinómicas que se anulan nun punto $p \in V$, o anel local da variedade V en p coincide coa localización de $A(V)$ en $A(V) - P$, é dicir, con $A(V)_P$.

2.2. Morfismos entre variedades

Rematamos este capítulo estudando unha cuestión presente na maioría de áreas das matemáticas. Tras construír un obxecto matemático −por exemplo, un espazo vectorial− aparece de xeito inmediato a necesidade de construír aplicacións entre estes obxectos que conserven a súa estrutura −nese caso serían as aplicacións lineares, que preservan a suma e o produto por escalar−. Nesta sección construiremos os morfismos entre variedades alxébricas −os cales son aplicacións continuas na topoloxía de Zariski− e veremos cando podemos dicir que dúas variedades son esencialmente a mesma, é dicir, son "isomorfas".

Definición 2.11. Sexan $V \subset K^n, W \subset K^m$ variedades alxébricas. Unha aplicación $\varphi : V \to W$ dise *morfismo* entre as variedades V e W se existen polinomios $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ tales que

$$\varphi(a_1, \dots, a_n) = (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n))$$

para todo $(a_1, \dots, a_n) \in V$. Nese caso, as funcións polinómicas $f_i : V \to K$ determinadas por cada polinomio f_i denomínanse *compoñentes* de φ.

Definición 2.12. Dúas variedades alxébricas $V \subset K^n$ e $W \subset K^m$ dinse *isomorfas* se existen morfismos entre variedades $\varphi : V \to W$ e $\psi : W \to V$ tales que $\varphi \circ \psi = \mathrm{id}_W$ e $\psi \circ \varphi = \mathrm{id}_V$.

Seguindo coa filosofía de comparar o camiño xeométrico co alxébrico, vexamos que ocorre cos aneis de coordenadas. Sexa $\varphi : V \to W$ un morfismo de variedades. Lembremos que se W é unha variedade alxébrica, $A(W)$ é o anel de funcións polinómicas en W. Dado un elemento $g : W \to K$ de $A(W)$, podemos compoñer co morfismo φ para obter unha aplicación $g \circ \varphi : V \to K$. A seguinte proposición dinos que $g \circ \varphi$ é unha función polinómica (e polo tanto un elemento de $A(V)$) e que a aplicación $g \longmapsto f \circ \varphi$ é un morfismo de K-álxebras.

Proposición 2.13. *Sexan $V \subset K^n, W \subset K^m$ variedades alxébricas e $\varphi : V \to W$ un morfismo de variedades. Entón para toda función polinómica $g \in A(W)$ tense que $g \circ \varphi \in A(V)$ e a aplicación $\widehat{\varphi} : A(W) \to A(V)$ inducida por φ é un homomorfismo de aneis que deixa fixo $K \subset A(W)$.*

Demostración. Para non causar ambigüidade denotaremos os polinomios con letras maiúsculas e as funcións polinómicas por letras minúsculas. Sexa $G(y_1, \dots, y_m) \in K[y_1, \dots, y_m]$ un polinomio que determina a función polinómica $g : W \to K$. Como φ é un morfismo de variedades, está determinado por polinomios $H_i(x_1, \dots, x_n), \quad i = 1, \dots, m$. Compoñendo, temos o polinomio

$$G(H_1(x_1, \dots, x_n), \dots, H_m(x_1, \dots, x_n)) \in K[x_1, \dots, x_n]$$

o cal determina trivialmente a $g \circ \varphi$ polo que esta última é unha función polinómica en V. Para a segunda parte, que $\widehat{\varphi} : A(W) \to A(V)$ é un homomorfismo de aneis dedúcese directamente como consecuencia da suma e produto de polinomios. Consideremos entón $k \in K \subset A(W)$ unha función constante con valor k. Tense entón que $\widehat{\varphi}(k) = k \circ \varphi$ volve ser unha función constante con valor k polo que $\widehat{\varphi}$ deixa fixo K. $\square$

O seguinte resultado dinos que o recíproco tamén é certo, establecendo entón a correspondencia (con frechas opostas) entre morfismos de variedades e morfismos (como K-álxebras) de aneis de coordenadas.

Proposición 2.14. *Sexan $V \subset K^n, W \subset K^m$ variedades alxébricas e $\phi : A(W) \to A(V)$ un morfismo de K-álxebras. Entón existe un único morfismo de variedades $\varphi : V \to W$ que induce ϕ.*

Demostración. Para cada función coordenada $y_i \in A(W) = K[y_1, \dots, y_m]/I(W)$, tense $\phi(y_i) \in A(V)$, polo que existe un polinomio $F_i \in K[x_1, \dots, x_n]$ que determina a función polinómica $\phi(y_i)$. Podemos construír entón o morfismo de variedades

$$\varphi = (F_1(x_1, \dots, x_n), \dots, F_m(x_1, \dots, x_n)).$$

Pola suma e produto definidos en $A(V)$ e a hipótese de que ϕ é un morfismo de K-álxebras, dedúcese directamente que dado calquera polinomio $G \in K[y_1, \dots, y_m]$, a función polinómica que determina, $g \in A(W)$, verifica:

$$g \circ \varphi = \phi(g) \tag{2.1}$$

Vexamos agora que φ leva V en W. Sexa $(a_1, \dots, a_n) \in V$. Dado un polinomio $G \in I(W)$, tense que determina a función identicamente nula $g \in A(W)$, logo $\phi(g) = 0$ e por (2.1) $g \circ \alpha \in A(V)$ é a función identicamente nula, polo tanto

$$G(\varphi(a_1, \dots, a_n)) = g \circ \varphi(a_1, \dots, a_n) = 0.$$

Temos entón que todo polinomio de $I(W)$ se anula en $\varphi(a_1, \dots, a_n)$, e así $\varphi(a_1, \dots, a_n) \in W$. Que φ induce ϕ é inmediato por (2.1). Fáltanos ver que φ está univocamente determinado. Sexa $\psi : V \to W$ outro morfismo de variedades tal que $\widehat{\psi} = \phi$. Tense que $\widehat{\psi}$ leva cada función coordenada $y_i \in A(W)$ na i-ésima compoñente de ψ. Analogamente, $\widehat{\varphi}$ leva cada función coordenada $y_i \in A(W)$ na i-ésima compoñente de φ. Como $\widehat{\psi} = \phi = \widehat{\varphi}$, tense que ψ e φ teñen as mesmas compoñentes e polo tanto son o mesmo morfismo de variedades. $\square$

Lema 2.15. *Sexan V,W e Z variedades alxébricas e $\varphi : V \to W$ e $\psi : W \to Z$ morfismos de variedades. Verifícase:*

1. $\widehat{\mathrm{id}_V} = \mathrm{id}_{A(V)}$.
2. $\widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi}$.

Demostración. 1. Dada $f \in A(V)$, tense $\widehat{\mathrm{id}_V}(f) = f \circ \mathrm{id}_V = f$.

2. Dada $f \in A(Z)$, entón $\widehat{\psi \circ \varphi}(f) = f \circ (\psi \circ \varphi) = (f \circ \psi) \circ \varphi = \widehat{\psi}(f) \circ \varphi = \widehat{\varphi}(\widehat{\psi}(f)) = \widehat{\varphi} \circ \widehat{\psi}(f)$. □

O seguinte é o resultado central desta sección, xa que nos permite afirmar que a condición de que dúas variedades sexan isomorfas é equivalente ao isomorfismo (como K-álxebras) dos seus aneis de coordenadas.

Teorema 2.16. *Dúas variedades alxébricas V e W son isomorfas se e só se existe un isomorfismo de K-álxebras $A(V) \cong A(W)$.*

Demostración. Sexan $\varphi : V \to W$ e $\psi : W \to V$ morfismos de variedades de xeito que $\alpha \circ \beta = \mathrm{id}_W$ e $\beta \circ \alpha = \mathrm{id}_V$. Entón, pola proposición 2.13, $\widehat{\varphi} : A(W) \to A(V)$ e $\widehat{\psi} : A(V) \to A(W)$ son morfismos de K-álxebras. Ademais polo lema anterior, $\widehat{\varphi} \circ \widehat{\psi} = \mathrm{id}_{A(V)}$ e $\widehat{\psi} \circ \widehat{\varphi} = \mathrm{id}_{A(W)}$.

Reciprocamente, supoñamos que $\phi : A(W) \to A(V)$ é un isomorfismo de K-álxebras. Por 2.14, existen morfismos de variedades $\varphi : V \to W$ e $\psi : W \to V$ tales que $\widehat{\varphi} = \phi$ e $\widehat{\psi} = \phi^{-1}$. Polo lema anterior temos

$$\widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi} = \phi \circ \phi^{-1} = \mathrm{id}_{A(V)}$$

e pola unicidade vista en 2.14 e o primeiro apartado do lema anterior temos que $\psi \circ \varphi = \mathrm{id}_V$. Analogamente veise que $\varphi \circ \psi = \mathrm{id}_W$. □

Capítulo 3

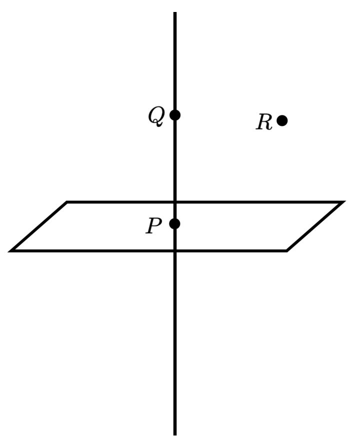
Unha “boa” definición de dimensión

O obxectivo deste traballo é desenvolver o concepto de dimensión no ámbito dos aneis conmutativos. Este marco é tan abstracto, que a noción de dimensión non é tan intuitiva como noutros casos e poden xurdir distintas posibles definicións. Porén, non podemos olvidarnos de que partimos do eido xeométrico das variedades alxébricas, polo que parece razonable esixir que a definición dada verifique certas propiedades xeométricas que a priori sabemos que se deberían cumprir.

Neste capítulo presentamos catro tales propiedades en forma de axiomas, explicando o seu contido xeométrico e por que se deberían verificar. Esta versión é unha adaptación do sistema completo de axiomas presentado por Eisenbud [6], a cal vai ser suficiente para xustificar que a dimensión de Krull é en efecto unha “boa” definición de dimensión.

Nos próximos capítulos, probaremos que esta definición verifica os catro axiomas.

Primeiro axioma



Como se pode observar na figura, a cal representa unha variedade alxébrica reducible, a dimensión en P, Q e R parece, intuitivamente, que non debería ser a mesma. Veise así que a dimensión debería ser un concepto local. Como vimos no capítulo anterior, o anel local dunha variedade nun punto, que recolle a información da variedade "preto" do punto, coincide coa localización do seu anel de coordenadas no ideal asociado ao punto. Xeralizando a un anel calquera, obtemos o primeiro axioma.

Axioma 1. $\dim A = \sup_{P \in \mathrm{Spec}(A)} \dim A_P$.

Segundo axioma

Lembremos que dada unha variedade alxébrica V, o seu anel de coordenadas $A(V)$ é o anel de funcións polinómicas en V. Se $f : V \to K$ é unha función de $A(V)$ e existe n tal que f^n é a función identicamente nula, tense entón que f é a función identicamente nula. Vemos así que as funcións nilpotentes non teñen relevancia dende un punto de vista xeométrico, polo que parece razonable esixir que as nilpotencias non afecten á dimensión.

Axioma 2. Se $I \subset A$ é un ideal nilpotente, entón $\dim A = \dim A/I$.

Terceiro axioma

Polo teorema do valor regular, sabemos que dadas dúas variedades diferenciables M e N e unha aplicación regular sobrexectiva $f : M \to N$, a fibra de calquera punto $q \in N$ é unha variedade diferenciable de dimensión $\dim M - \dim N$. No noso caso, dado un morfismo entre variedades $\varphi : V \to W$ e o correspondente homomorfismo de aneis $\psi : A(W) \to A(V)$, tense que $\varphi(X)$ é denso en Y se e só se ψ é un homomorfismo inxectivo. Se considermos $A(V)$ como $A(W)$-módulo mediante o monomorfismo ψ, veremos máis adiante neste traballo que se tal módulo é finitamente xerado entón as fibras de φ son finitas, e polo tanto 0-dimensionais, polo que se conseguimos que se verifique un resultado análogo ao das variedades diferenciables, teriamos $\dim V = \dim W$. Xeralizando a calquera anel, postulamos o terceiro axioma.

Axioma 3. Se $A \subset B$ son aneis tales que B é un A-módulo finitamente xerado, entón $\dim A = \dim B$.

Cuarto axioma

Vexamos por último un caso particular de variedade alxébrica da cal coñecemos cal debería ser a súa dimensión. O n-espazo afín, pensado como variedade K-linear, ten dimensión n. Como $K[x_1, \ldots, x_n]$ é o anel de coordenadas de K^n, a súa dimensión debería ser tamén n. Polo tanto, temos o cuarto e último axioma.

Axioma 4. Se K é un corpo, dim $K[x_1, \dots, x_n] = n$.

Capítulo 4

Dimensión de Krull

Neste capítulo presentamos a definición moderna de dimensión dun anel: a dimensión de Krull, proposta polo matemático alemán Wolfgang Krull coa motivación xeométrica de definir a dimensión dunha variedade alxébrica. Desenvolveremos varios resultados que nos brinda esta definición e xustificaremos a súa correcta elección como definición de dimensión probando xa algúns dos axiomas enunciados no capítulo anterior.

Definición 4.1. A *dimensión de Krull* dun anel A é o supremo das lonxitudes r de cadeas de ideais primos

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_r$$

en A. Denotarase por $\dim A$.

Definición 4.2. Se I é un ideal en A, defínese a *dimensión de I* como a dimensión de A/I.

Observación 4.3. Definir deste xeito a dimensión dun ideal ten a seguinte explicación xeométrica: o análogo da dimensión de Krull para variedades alxébricas sería definila como o supremo das lonxitudes de cadeas de subvariedades (non baleiras) irreducibles. De feito, isto xa nos é familiar no caso dos espazos vectoriais, os cales teñen como dimensión (vectorial) a lonxitude da cadea máis longa posible de subespazos propios. Como ademais, no caso de traballar sobre un corpo alxebraicamente pechado, as subvariedades irreducibles dunha variedade V se corresponden cos ideais primos do seu anel de coordenadas $A(V)$, tense que a dimensión (como variedade) de V é igual á dimensión (como anel) de $A(V)$. Polo tanto, se $I(V) \subset K[x_1, \ldots, x_n]$ é o ideal correspondente a V parece natural definir a súa dimensión como a dimensión de V, é dicir, a dimensión como anel de $A(V) = K[x_1, \ldots, x_n]/I(V)$.

A anterior observación lévanos á seguinte definición.

Definición 4.4. Se V é unha variedade alxébrica afín, defínese a *dimensión de V* como

$$\dim V := \dim A(V)$$

Exemplos 4.5. 1. Os únicos ideais dun corpo K son 0 e K, polo que dim $K = 0$.

2. Se $A \neq 0$ é un dominio de ideais principais que non é corpo entón dim $A = 1$. En efecto, existe un elemento irreducible $a \in A$ logo $0 \subset (a) \neq A$ é unha cadea de ideais primos de lonxitude 1. Ademais, se $(q) \subset (p)$ son ideais primos non nulos, tense que q é irreducible e que p divide a q, logo p e q son asociados e $(p) = (q)$. É dicir, non hai cadeas máis longas de ideais primos ca as de lonxitude 1.

3. $K[x]$ e $\mathbb{Z}$ son dominios de ideais principais e non son corpos, polo que dim $K[x] = 1 =$ dim $\mathbb{Z}$.

Definición 4.6. Dado un ideal primo I en A, defínese a *codimensión de I* (ou *altura* ou *rango*) como a dimensión do anel local A_I. Denotarase como codim I.

Observación 4.7. Se I non é primo, defínese codim I como o mínimo das codimensións dos ideais primos que conteñen a I.

Proposición 4.8. *Se I é un ideal primo en A,* codim I *coincide co supremo das lonxitudes das cadeas de ideais primos descendendo dende I.*

Demostración. Por 1.10 sabemos que as cadeas de ideais primos de A_I se corresponden con cadeas de ideais primos de A que non intersecan a $A - I$, é dicir, que están contidos en I. □

Este feito permítenos probar xa que a dimensión de Krull satisface o Axioma 1.

Corolario 4.9 (Axioma 1)**.** *Dado un anel A,* dim $A = \sup_{I \in \mathrm{Spec}(A)} \dim A_I$.

Demostración. Pola proposición anterior sabemos que dim A_I é o supremo das lonxitudes das cadeas de ideais primos en A descendendo dende I, logo dim $A \geq$ dim A_I para todo ideal primo I. Se dim $A = \infty$ existen cadeas de lonxitude arbitraria. Polo tanto, calquera que sexa $k \in \mathbb{N}$ existe un ideal primo J e unha cadea de ideais primos

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_s = J$$

con $k < s \leq \dim A_J$, e así $\sup_{I \in \mathrm{Spec}(A)} \dim A_I = \infty$. Se dim $A = r$ é finito, tense que existe unha cadea de ideais primos

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_r$$

polo que dim $A = r \leq \dim A_{I_r}$ e así dim $A = \max_{I \in \mathrm{Spec}(A)} \dim A_I$. □

Aproveitamos este momento para demostrar tamén o segundo dos axiomas, o cal é consecuencia inmediata da definición.

Proposición 4.10 (Axioma 2). *Se I é un ideal nilpotente dun anel A, entón* $\dim A = \dim A/I$.

Demostración. Como I é un ideal nilpotente, en particular cada elemento de I é nilpotente. Sexa P un ideal primo de A. Se $f \in I$, existe n tal que $f^n = 0 \in P$ e por ser P primo temos que $f \in P$. Polo tanto, todo ideal primo de A contén a I e así temos unha correspondencia bixectiva que conserva a orde entre os ideais primos de A e os ideais primos de A/I, obtendo o resultado. □

Existe unha relación moi próxima entre os aneis artinianos e os aneis de dimensión nula. De feito, os aneis noetherianos de dimensión cero son precisamente aqueles que son artinianos (xa viramos que todo anel artiniano é noetheriano). Isto ten unha aplicación xeométrica directa pois vainos permitir caracterizar as variedades alxébricas finitas. Os seguintes dous resultados son consecuencia do teorema 1.17:

Corolario 4.11. *Sexa V unha variedade alxébrica sobre K. Son equivalentes:*

1. *V é un conxunto finito.*
2. *$A(V)$ é un espazo vectorial sobre K de dimensión (vectorial) o número de puntos de V.*
3. *$A(V)$ é artiniano.*

Demostración. $1 \Rightarrow 2$: Sexa $V = \{v_1, \dots, v_s\}$. Como $A(V)$ é o anel de funcións polinómicas en V, temos que $A(V) \cong A(v_1) \times \cdots \times A(v_s)$. Agora ben, cada función polinómica con dominio unitario correspóndese cun único elemento de K e viceversa, polo que $A(v_i) \cong K$ e así $A(V) \cong K^s$ é un espazo vectorial sobre K de dimensión s, o número de puntos de V.

$2 \Rightarrow 3$: Un ideal de $A(V)$ é en particular un K-subespazo vectorial de $A(V)$. Como $A(V)$ ten dimensión finita como K-espazo vectorial, toda cadea descendente de subespazos estaciona, polo que toda cadea descendente de ideais tamén estaciona.

$3 \Rightarrow 1$: Se $A(V)$ é artiniano, o teorema 1.17 asegúranos que ten un número finito de ideais maximais. Como os maximais de $A(V)$ se corresponden cos puntos de V, temos que V é finito. □

Corolario 4.12. *Se A é noetheriano,* $\dim A = 0$ *se e só se A é artiniano.*

Demostración. Un anel de dimensión 0 é un anel no que toda cadea de ideais primos ten lonxitude 0, é dicir, un anel no que todo ideal primo é maximal. Neste caso, como A é noetheriano, o teorema 1.17 asegúranos que esa condición é equivalente a ser artiniano. □

Polo tanto, como o anel de coordenadas dunha variedade é noetheriano (é unha álxebra finitamente xerada sobre un corpo) estes dous últimos resultados permítennos caracterizar as variedades alxébricas finitas:

Proposición 4.13. *Unha variedade alxébrica é finita se e só se ten dimensión* 0.

Rematamos este capítulo probando o Axioma 3 presentado no capítulo anterior.

Proposición 4.14. *Sexa $\psi : A \to B$ un homomorfismo de aneis que fai de B unha extensión enteira sobre A. Entón calquera ideal primo de A contendo ao núcleo de ψ é a imaxe recíproca dun ideal primo de B. Ademais, se I é un ideal de B, entón*

$$\dim I = \dim \psi^{-1}(I)$$

Demostración. Sexa P un ideal primo en A contendo a $\ker \psi$. Pola correspondencia natural entre ideais de A contendo a $\ker \psi$ e ideais de $A/\ker \psi$, e polo isomorfismo $A/\ker \psi \cong \psi(A)$, podemos facer abuso de linguaxe e denotar por A a súa imaxe por ψ en B. Como $A \subset B$ é unha extensión enteira, podemos aplicar a proposición 1.29 para deducir que existe un ideal primo Q en B tal que $P = Q \cap A$ de onde $P = Q \cap A$, é dicir, $P = \psi^{-1}(A)$. Para ver a igualdade das dimensións, dado un ideal I en B, supoñamos que temos unha cadea de ideais primos en A ascendendo dende $\psi^{-1}I$. Polo argumento anterior e a segunda parte da proposición 1.29, podemos construír unha cadea de ideais primos en B ascendendo dende I de xeito que cada un deles teña como imaxe recíproca un dos ideais da cadea en A. Polo tanto $\dim\,(I) \geq \dim \psi^{-1}(I)$. Por outro lado, dada unha cadea de ideais primos distintos en B contendo a I, as súas imaxes recíprocas dan unha cadea de ideais primos en A contendo a $\psi^{-1}(A)$ que tamén son distintos por 1.30 (se $\psi^{-1}(J_1) = \psi^{-1}(J_2)$ por incomparabilidade temos que $J_1 \not\subseteq J_2$ e $J_2 \not\subseteq J_1$, o cal é unha contradición). Polo tanto, $\dim\,(I) \leq \dim \psi^{-1}(I)$. □

Corolario 4.15 (Axioma 3)**.** *Se $A \subset B$ son aneis tales que B é un A-módulo finitamente xerado, entón dim $A =$ dim B.*

Demostración. Por ser B un A-módulo finitamente xerado é en particular unha extensión enteira sobre A. Basta tomar $C = B$ en 1.25, apartado 3, para ver que todo elemento de B é enteiro. Tomando na proposición anterior $I = 0$ e tendo en conta que $A \subset B$ (polo que ψ é a inclusión e o núcleo é nulo) tense o resultado. □

A versión xeométrica da proposición anterior vai na liña da explicación que dabamos no capítulo anterior sobre o Axioma 3:

Corolario 4.16. *Se $\varphi : V \to W$ é un morfismo de variedades alxébricas tal que $A(V)$ é un $A(W)$-módulo finitamente xerado, entón:*

1. *As fibras de φ son finitas.*

2. *Dada unha subvariedade* V_1 *de* V*, entón* $\varphi(V_1)$ *é unha subvariedade de* W *con* $\dim V_1 = \dim \varphi(V_1)$. *En particular, se* $A(W) \subset A(V)$*, entón* φ *é sobrexectiva.*

Demostración. O primeiro apartado é consecuencia do segundo. En efecto, dado $q \in W$, como φ é Zariski-continua tense que $\varphi^{-1}(q)$ é unha subvariedade de V. Polo apartado 2 e se $\varphi^{-1}(q) \neq \emptyset$, entón

$$\dim \varphi^{-1}(q) = \dim \varphi(\varphi^{-1}(q)) = \dim q = 0$$

e pola proposición 4.13 $\varphi^{-1}(q)$ é finito.

Para o apartado 2, podemos substituír V por V_1 e W pola Zariski-clausura de $\varphi(V_1)$ e asumir $A(W) \subset A(V)$. A proba redúcese así a ver que V e W teñen a mesma dimensión e que φ é sobrexectiva, pois nese caso $\varphi(V) = \overline{\varphi(V)}$ sería unha subvariedade. Pero ambos resultados son consecuencia inmediata dos dous resultados anteriores. $\square$

Capítulo 5

Número de ecuacións e dimensión

É ben coñecido o feito de que o número mínimo necesario de ecuacións para describir unha variedade linear m-dimensional do n-espazo afín é $n - m$. Reciprocamente, un sistema de ecuacións lineares con n incógnitas e r ecuacións independentes determina unha variedade linear de dimensión $n - r$. Porén, no caso das variedades alxébricas a situación non é tan simple e só podemos conseguir certas acotacións destos valores. Ao longo deste capítulo encargarémonos de estudar estas acotacións, para o cal introduciremos o Teorema do Ideal Principal de Krull; un resultado fundamental en xeometría alxébrica cuxas consecuencias non só nos serán útiles neste capítulo, senón tamén para establecer caracterizacións da dimensión de Krull nos posteriores.

Neste traballo xa existe de xeito implícito unha acotación superior do número de ecuacións necesarias para describir unha variedade alxébrica, e é que este número é finito. En efecto, o Teorema da Base de Hilbert demostra que o anel de polinomios é noetheriano, e así todo ideal é finitamente xerado e toda variedade é a solución dun sistema cun número finito de ecuacións. Isto quere dicir que toda variedade é a intersección dun número finito de hipersuperficies. En 1882 Kronecker precisou esta información ao darse conta de que toda variedade de K^n é a intersección de $n + 1$ superficies. De feito tras esta publicación, algúns matemáticos chegaron a afirmar que este número era mínimo ao atopar algún exemplo de variedade que, ao parecer, non era posible expresala como intersección de n hipersuperficies. Porén, estaban errados, e non foi ata finais do século pasado que se puido probar que toda variedade de K^n é a intersección de n hipersuperficies.

Damos aquí o seguinte teorema demostrado por Eisenbud e Evans:

Teorema 5.1 ([5]). *Se A é un anel noetheriano de dimensión $d < \infty$ e $I \subset A[x]$ é un ideal, existen elementos $f_1, \dots, f_{d+1} \in I$ tales que*

$$\text{rad } I = \text{rad } (f_1, \dots, f_{d+1}).$$

Como veremos máis adiante neste capítulo, o Teorema do Ideal Principal de Krull permítenos probar a natural igualdade $\dim K[x_1, \dots, x_n] = n$. Temos así unha cota superior para o número de ecuacións necesarias para describir unha variedade alxébrica.

Corolario 5.2. *Se V é unha variedade alxébrica do n-espazo afín, precísanse como moito n ecuacións para describila.*

Demostración. Tomemos $A = K[x_1, \dots, x_{n-1}]$, de xeito que $\dim A = n-1$ e $A[x] \cong K[x_1, \dots, x_n]$. Polo teorema anterior, existen $f_1, \dots, f_n \in I(V) \subset A[x]$ tales que $\text{rad } I(V) = \text{rad } (f_1, \dots, f_d)$ e como $\text{rad } I(V) = I(V)$ temos

$$V = V(I(V)) = V(\text{rad } (f_1, \dots, f_n)) = V(f_1, \dots, f_n).$$

□

5.1. Teorema do Ideal Principal de Krull

O Teorema do Ideal Principal (TIP) de Krull permítenos dar un número mínimo de ecuacións necesarias para describir unha variedade alxébrica. Ao longo desta sección todos os aneis fan referencia a aneis noetherianos.

Comezamos presentando a versión orixinal do teorema. Para demostralo precisamos introducir un concepto relativo a descomposición primaria: se Q é un ideal primo de A, a *n-ésima potencia simbólica* $Q^{(n)}$ é a imaxe recíproca pola inclusión natural $i : A \to A_Q$ de $(Q_Q)^n$. Polo visto en 1.11, $(Q_Q)^n = Q^n A_Q$, polo que $Q^{(n)} = i^{-1}(Q^n A_Q) = \{a \in A \mid ab \in Q^n \text{ para algún } b \in A - Q\}$. Polo tanto, os elementos que non pertencen a Q son non-divisores de cero módulo $Q^{(n)}$, e por 1.10 temos que $(Q^{(n)})_Q = (Q_Q)^n$.

Teorema 5.3 (Teorema do Ideal Principal)**.** *Se $x \in A$ e P é un ideal minimal entre os ideais primos de A que conteñen a x, entón* $\text{codim } P \leq 1$.

Demostración. Sexa $Q \subsetneq P$ un ideal primo. Intercambiando A pola localización A_P podemos supoñer que P é maximal. Tomemos a cadea descendente

$$A \supset Q \supset Q^{(2)} \supset Q^{(3)} \supset \cdots$$

a cal induce unha cadea descendente $Q^{(n)} + (x)$ en $A/(x)$. Como P é minimal sobre (x), temos por 1.19 que $A/(x)$ é artiniano, polo que tal cadea se estabiliza e existe n tal que $Q^{(n)} + (x) = Q^{(n+1)} + (x)$. Polo tanto, dado $f \in Q^{(n)}$, podemos poñer

$$f = g + ax$$

con $a \in A$ e $g \in Q^{(n+1)}$, de onde $ax \in Q^{(n)}$. Como P é minimal sobre (x) temos que $x \notin Q$ e pola definición de $Q^{(n)}$ tense que $a \in Q^{(n)}$, e así deducimos que

$$Q^{(n)} = (x)Q^{(n)} + Q^{(n+1)}$$

e cocientando obtemos $Q^{(n)}/Q^{(n+1)} = (x)Q^{(n)}/Q^{(n+1)}$. Como $(x) \subset P$ e P é maximal podemos aplicar o lema de Nakayama (1.28) e así $Q^{(n)}/Q^{(n+1)} = 0$, de onde obtemos $Q^{(n)} = Q^{(n+1)}$. Localizando esta vez en Q, e tendo en conta que $(Q^{(r)})_Q = (Q_Q)^r$, a anterior igualdade convértese en

$$(Q_Q)^n = (Q_Q)^{n+1} = Q_Q(Q_Q)^n$$

e aplicando unha vez máis o lema de Nakayama obtemos $(Q_Q)^n = 0$ e por 1.19 A_Q é artiniano. O corolario 4.12 permítenos concluír que dim $A_Q = 0$, polo que codim $Q = 0$ e así codim $P \leq 1$, como queríamos demostrar. $\square$

Podemos pensar que o TIP é un primeiro paso nun proceso inductivo e podemos xeralizalo a un número finito de xeradores:

Teorema 5.4 (Teorema do Ideal Principal xeralizado)**.** *Sexan $x_1, \dots, x_c \in A$ e P minimal entre os ideais primos que conteñen a $x_1, \dots, x_c$. Entón* codim $P \leq c$.

Demostración. O caso $c = 1$ é o TIP e xa está probado. Supoñamos o resultado certo para $c - 1$ xeradores. De xeito análogo ao TIP, podemos localizar en P e considerar que P é o único ideal maximal de A. Polo corolario 1.19, existe r tal que $P^r \subset (x_1, \dots, x_c)$ −é dicir, P é nilpotente módulo $(x_1, \dots, x_c)$−. Sexa P_1 un ideal primo tal que $P \supsetneq P_1$ sen ideais primos entre ambos. Como P é minimal sobre $(x_1, \dots, x_c)$, P_1 non pode conter a todos os x_i. Supoñamos sen perda de xeralidade que $x_1 \notin P_1$. Temos entón que P é minimal sobre $P_1 + (x_1)$ e outra vez como consecuencia do corolario 1.19 temos que P é nilpotente módulo $P_1 + (x_1)$ e en particular existen $a_i \in A$ e $y_i \in P_1$ tales que, para un n suficientemente grande,

$$x_i^n = y_i + a_i x_i \quad i = 2, \dots, c.$$

Consideremos agora $\bar{A} := A/(y_2, \dots, y_c)$ e denotemos tamén cunha barra encima as imaxes en $\bar{A}$ dos elementos e ideais de A. Como P é nilpotente módulo $(x_1, \dots, x_c)$, pola ecuación anterior dos x_i temos que tamén é nilpotente módulo $(x_1, y_2, \dots, y_c)$, e así P é minimal sobre $(x_1, y_2, \dots, y_c)$ e así $\bar{P}$ é un primo minimal sobre $\bar{x_1}$. Polo TIP, temos que codim $\bar{P} \leq 1$ e como $\bar{P_1} \subsetneq \bar{P}$ deducimos que $\bar{P_1}$ é un primo minimal en $\bar{A}$. Volvendo a A, temos que P_1 é un primo minimal sobre $(y_2, \dots, y_c)$. Pola hipótese de indución, temos que codim $P_1 \leq c - 1$ e así codim $P \leq c$.

$\square$

O teorema que acabamos de probar constitúe un pilar fundamental en xeometría alxébrica e ten moitas consecuencias. A primeira que imos ver é a que nos proporciona unha cota inferior para o número de ecuacións necesario para describir unha variedade alxébrica. Para tal obxectivo precisaremos supoñer certo que neste caso, dado un ideal $I \subset A$, se verifica a fórmula dim $A =$ dim $I +$ codim I. Tal identidade, pese a parecer natural, non se verifica en xeral pero si no contexto que nos ocupa, como probaremos máis adiante empregando o Teorema de Normalización de Noether.

Cabe mencionar que polo Axioma 1 a dimensión dunha variedade é o máximo das dimensións das súas compoñentes irreducibles.

Corolario 5.5. *Sexa $V := V(I)$ unha variedade alxébrica non vacía dada por un ideal $I = (f_1, \dots, f_m)$. Entón, se W é unha compoñente irreducible de V, tense*

$$\dim W \geq n - m.$$

Demostración. Supoñamos que $W \subset V$ é unha compoñente irreducible de V. Entón $I(W)$ é un ideal primo minimal sobre $(f_1, \dots, f_m)$. Polo TIP xeralizado temos que codim $I(W) \leq m$ e así

$$\dim W = n/I(W) = n - \operatorname{codim} I(W) \geq n - m.$$

□

Corolario 5.6. *Para describir unha variedades alxébrica V do n-espazo afín precísanse como mínimo $n - m(V)$ ecuacións, onde $m(V)$ denota o mínimo das dimensións das compoñentes irreducibles de V.*

Demostración. Polo corolario anterior, m polinomios definen unha variedade ou ben vacía ou ben cuxas compoñentes irreducibles teñen dimensión $\geq n - m$. Entón, $m < n - m(V)$ ecuacións só poden determinar unha variedade cuxas compoñentes irreducibles teñan dimensión $\geq n - m > n - (n - m(V)) = m(V)$ polo que non poden determinar V e teriamos o resultado. □

5.2. Aplicacións do TIP

Para rematar este capítulo veremos algunhas consecuencias que ten o Teorema do Ideal Principal. Comezamos vendo que o recíproco tamén se verifica, pero primeiro precisamos un resultado previo, coñecido como de lema de evitación de primos. Recibe o seu nome do feito de que como consecuencia tense que se un ideal J non está contido en ningún dun número finito de primos P_j, entón existe un elemento en J que "evita" a todos os P_j no sentido de que non está contido en ningún deles.

Lema 5.7 (Lema de evitación de primos). *Sexan $I_1, \dots, I_r, J$ ideais en A tales que $J \subset \bigcup_{j=1}^r I_j$. Se os I_j son todos primos agás ao sumo 2, entón J está contido nalgún dos I_j.*

Demostración. Procederemos por indución en r. O caso $r = 1$ é obvio. Supoñamos $r > 1$ e, por redución ao absurdo, que J non está contido en ningún dos I_j. Pola hipótese de indución, J non está contido en unións máis pequenas dos I_j. Polo tanto, para cada $i \in \{1, \dots, r\}$, podemos tomar $x_i \in J$ tal que $x_i \notin \bigcup_{j \neq i} I_j$. Como $J \subset \bigcup_{j=1}^r I_j$, temos que $x_i \in I_i$. Se $r = 2$, entón $x_1 + x_2$ non está en I_1 nin en I_2, contradicindo a hipótese de que $J \subset I_1 \cup I_2$. Se $r > 2$, podemos supoñer pola hipótese que I_1 é primo, e temos que $x_1 + x_2 x_3 \cdots x_r$ non pertence a ningún dos I_j, volvendo contradicir a hipótese. En efecto, se $x_1 + x_2 x_3 \cdots x_r \in I_1$, entón $x_2 x_3 \cdots x_r \in I_1$ e por ser primo algún dos x_i, con $i > 1$ pertencería a I_1, o cal non pode ser. Pola outra banda, se $x_1 + x_2 x_3 \cdots x_r \in I_j$, con $j > 1$, teriamos que $x_1 \in I_j$. □

Estamos en condicións xa de demostrar o recíproco do TIP.

Corolario 5.8. *Se P é un ideal de A de codimensión c, entón é un primo minimal sobre un ideal xerado por c elementos.*

Demostración. O caso $c = 0$ é inmediato. Por indución, supoñamos o resultado certo para $c - 1$. Como P ten codimensión c, existe un ideal primo $P_1 \subset P$ de codimensión $c - 1$. Pola hipótese de indución, existen $x_1, \dots, x_{c-1} \in P$ tales que P_1 é minimal sobre $(x_1, \dots, x_{c-1})$. Supoñamos entón que codim $(x_1, \dots, x_{c-1}) = c - 1$. P non está contido en ningún dos primos minimais sobre $(x_1, \dots, x_{c-1})$ (os cales son un número finito por ser A noetheriano) xa que estes teñen, polo TIP xeralizado, codimensión $\leq c - 1$. Polo tanto, polo lema de evitación de primos, existe $x_c \in P$ que non pertence a ningún dos primos minimais sobre $(x_1, \dots, x_{c-1})$. Entón, P é minimal sobre $(x_1, \dots, x_{c-1}, x_c)$. En efecto, supoñamos que existe un primo $Q \subset P$ minimal sobre $(x_1, \dots, x_c)$. Teriamos entón polo TIP que codim $Q \leq c$. Pero ademais Q contén a algún dos primos minimais sobre $(x_1, \dots, x_{c-1})$, sen ser ningún deles xa que $x_c \in Q$ e x_c non pertencía a ningún dos minimais. Polo tanto, codim $Q > c - 1$ e así codim $Q = c$, de onde deducimos que $Q = P$ xa que $Q \subset P$ e codim $P = c$. □

Outra aplicación do TIP é a seguinte caracterización da dimensión dun anel local. Lembremos que un anel é local se só ten un ideal maximal. Escribiremos $(A, \mathfrak{m})$ para referirnos a un anel local A cuxo único ideal maximal é $\mathfrak{m}$.

Corolario 5.9. *Sexa $(A, \mathfrak{m})$ un anel local. Entón a dimensión de A é o mínimo número d tal que existen d elementos $x_1, \dots, x_d \in \mathfrak{m}$ tales que $\mathfrak{m}^n \subset (x_1, \dots, x_d)$ para n suficientemente grande.*

Demostración. Por ser A local, temos que dim $A = \text{codim } \mathfrak{m} =: d$. Polo corolario anterior, existen $x_1, \dots, x_d \in \mathfrak{m}$ tales que $\mathfrak{m}$ é minimal sobre $(x_1, \dots, x_d)$, e por 1.23 tense que rad $(x_1, \dots, x_c) = \mathfrak{m}$ e así $\mathfrak{m}^n \subset (x_1, \dots, x_d)$ para un n suficientemente grande por 1.18.

Vexamos que este número é mínimo. En efecto, supoñamos que existen $r < d$ elementos $x_1, \dots, x_r$ tales que $\mathfrak{m}^n \subset (x_1, \dots, x_r)$ para un n suficientemente grande. Tense entón que $\mathfrak{m}$ é minimal entre os primos sobre $(x_1, \dots, x_r)$ e polo TIP temos que codim $\mathfrak{m} \leq r < d = \text{codim } \mathfrak{m}$, o cal é unha contradición. $\square$

Este último corolario vainos permitir probar un teorema moi útil, do cal deduciremos o Axioma 4, é dicir, que o n-espazo afín ten dimensión n como variedade alxébrica.

Teorema 5.10. *Se $\varphi : (A, \mathfrak{m}) \to (B, \mathfrak{n})$ é un homomorfismo de aneis que leva $\mathfrak{m}$ en $\mathfrak{n}$, entón*

$$\dim B \leq \dim A + \dim B/\mathfrak{m}B.$$

Demostración. Sexan $d := \dim A$ e $e := \dim B/\mathfrak{m}B$. Polo corolario 5.9, existen d elementos $x_1, \dots, x_d \in \mathfrak{m}$ tales que $\mathfrak{m}^s \subset (x_1, \dots, x_d)$ para s suficientemente grande. Como φ leva $\mathfrak{m}$ en $\mathfrak{n}$, temos que $\mathfrak{m}B \subset \mathfrak{n}$ e polo tanto $B/\mathfrak{m}B$ é un anel local con ideal maximal $\mathfrak{n}$. Volvendo aplicar 5.9 temos que existen e elementos $y_1, \dots, y_e \in B/\mathfrak{m}B$ tales que $\mathfrak{n}^t \subset (y_1, \dots, y_e)$ para t suficientemente grande. Tomando representantes, podemos supoñer que existen $y_1, \dots, y_e \in B$ tales que $\mathfrak{n}^t \subset \mathfrak{m}B + (y_1, \dots, y_e)$ para t suficientemente grande. Xuntando ambas condicións temos

$$\mathfrak{n}^{st} \subset (\mathfrak{m}B + (y_1 \dots, y_e))^s \subset \mathfrak{m}^s B + (y_1 \dots, y_e) \subset (x_1, \dots, x_d, y_1, \dots, y_e)B.$$

Polo tanto, $\mathfrak{n}$ é un primo minimal sobre un ideal xerado por $d + e$ elementos, e polo teorema do ideal principal podemos concluír que $\dim B = \text{codim } \mathfrak{n} \leq d + e = \dim A + \dim B/\mathfrak{m}B$. $\square$

Corolario 5.11. *Se P é un ideal primo dun anel A, entón existen ideais primos Q en $A[x]$ que se contraen a P, e para un ideal maximal dese tipo tense que*

$$\dim A[x]_Q = 1 + \dim A_P.$$

Demostración. Vexamos primeiro o resultado no caso no que A é un corpo, e polo tanto $P = (0)$. Como a contración dun ideal primo segue sendo primo, neste caso temos que todo ideal Q de $A[x]$ se contrae ao (0). Ademais, se tomamos Q maximal, $Q \neq (0)$ e polo tanto codim $Q > 0$ por ser $A[x]$ un dominio (o cal implica que (0) é primo e temos a cadea $(0) \subsetneq Q$). Ademais, por ser A corpo temos que $A[x]$ é un dominio de ideais principais, polo que Q é principal e polo TIP temos que codim $Q \leq 1$, deducindo entón que codim $Q = 1$. Localizando, obtemos que $\dim A[x]_Q = \text{codim } Q = 1 = 1 + \dim A_P$ xa que $\dim A_{(0)} = 0$.

No caso xeral, temos que $PA[x]$ é un ideal primo de $A[x]$ ($A[x]/PA[x] \cong (A/P)[x]$ que por ser P primo é un dominio) e $PA[x] \cap A = P$, probando así a primeira parte do enunciado. Reemplacemos A pola localización A_P e supoñamos entón que A é un anel local con ideal maximal P. Sexa Q un ideal maximal de $A[x]$ contendo a P, de xeito que $P \subset Q \cap A$ e por ser P maximal $Q \cap A = P$. O obxectivo é demostrar que codim $Q = 1 +$ codim P.

Dada $P_0 \subsetneq \cdots \subsetneq P_d = P$ unha cadea de primos en A, temos que $P_0A[x] \subsetneq \cdots \subsetneq P_dA[x] = PA[x]$ é unha cadea de primos en $A[x]$ da mesma lonxitude. Como $A[x]/PA[x] \cong (A/P)[x]$ e A/P é un corpo, e Q é un ideal maximal en $A[x]/PA[x]$, tense que Q (visto en $A[x]/PA[x]$) ten codimensión 1 e polo tanto Q (visto en $A[x]$) ten codimensión $\geq 1+$codim P. Ademais, podemos aplicar o teorema anterior aos aneis locais A e $A[x]_Q$ para obter

$$\dim A[x]_Q \leq \dim A + \dim A[x]_Q/PA[x]_Q \leq \dim A + \dim (A/P)[x] \leq \dim A + 1,$$

polo que codim $Q = \dim A[x]_Q \leq \dim A + 1 =$ codim $P + 1$. □

Chegamos así a un resultado básico na teoría da dimensión de aneis noetherianos:

Corolario 5.12. $\dim A[x] = 1 + \dim A$.

Demostración. Dada $P_0 \subsetneq \cdots \subsetneq P_d$ unha cadea de primos en A, temos que $P_0A[x] \subsetneq \cdots \subsetneq P_dA[x] \subsetneq P_dA[x]+(x)$ é unha cadea de primos en $A[x]$ de maior lonxitude, polo tanto $\dim A[x] \geq \dim A + 1$. Reciprocamente, sexa Q un ideal maximal de $A[x]$ e $P := Q \cap A$. En particular, Q é maximal entre os primos Q' tales que $Q' \cap A = P$, polo que podemos aplicar o corolario anterior para obter

$$\text{codim } Q = \dim A[x]_Q = 1 + \dim A_P \leq 1 + \dim A.$$

Como Q é un ideal maximal arbitrario de $A[X]$, $\dim A[x] \leq 1 + \dim A$. □

Este resultado ten unha explicación xeométrica clara: se A e un anel de funcións nunha variedade, entón $A[x]$ é o anel de funcións no produto desa variedade e unha recta afín, polo que a fórmula dada parece natural. Porén, no caso non noetheriano non sempre se verifica.

Por indución no número de variables, e dado que $\dim K = 0$, o anterior corolario danos o Axioma 4:

Corolario 5.13 (Axioma 4)**.** *Se K é un corpo,*

$$\dim K[x_1, \ldots, x_n] = n.$$

En particular, toda variedade alxébrica ten dimensión finita.

Capítulo 6

Primeira caracterización. Normalización de Noether

O obxectivo deste capítulo e do seguinte será ver dúas caracterizacións da dimensión de Krull, para outorgarlle aínda máis validez como definición apropiada de dimensión e obter novas propiedades que verifica. Neste primeiro, veremos unha caracterización nun caso particular: a dos dominios afíns.

Un anel afín é unha K-álxebra finitamente xerada. Esta denominación vén do seguinte feito: está claro que se V é unha variedade alxébrica, $A(V) = K[x_1, \dots, x_n]/I(V)$ é unha K-álxebra finitamente xerada por $x_1, \dots, x_n$ (e reducida por ser $I(V)$ un ideal radical). Reciprocamente, se B é unha K-álxebra finitamente xerada temos que é a imaxe dun homomorfismo avaliación polo que $B \cong K[x_1, \dots, x_n]/I$ para algún ideal I. Se ademais esiximos que sexa reducida, temos que I é radical e polo Teorema dos Ceros de Hilbert temos que $I(V(I)) = I$ e así $B = A(V(I))$. Temos demostrado entón o seguinte resultado que explica o nome dos aneis afíns:

Proposición 6.1. *Se K é alxebricamente pechado e B é unha K-álxebra, entón $B = A(V)$ para algunha variedade alxébrica V se e só se B é reducida e finitamente xerada como K-álxebra.*

Propoñémonos entón probar neste capítulo o seguinte teorema:

Teorema 6.2. *Se A é un dominio afín sobre K, entón*

$$\dim A = \text{tr. deg.}_K A,$$

e este número é a lonxitude de calquera cadea maximal de ideais primos en A.

Con tr. deg.$_K A$ facemos referencia ao grao de transcendencia de corpo de fraccións $Q(A)$ sobre K. Para demostralo precisaremos un dos resultados fundamentais da teoría de aneis afíns:

o Teorema de Normalización de Noether. Pero antes, imos ver unha aplicación directa do anterior teorema: dimensión e codimensión son complementarios en aneis afíns.

Dado un ideal primo I dun dominio afín A, temos polo teorema anterior que a dimensión de A coincide coa lonxitude de calquera cadea maximal de ideais primos de A. Tomando cadeas maximais que conteñan a I temos o seguinte resultado, o cal xeralizamos a aneis afíns pola finitude dos ideais primos minimais dun anel noetheriano:

Corolario 6.3. *Dado un ideal I dun anel afín A, temos que*

$$\dim I + \operatorname{codim} I = \dim A.$$

Pasemos entón á demostración do teorema, para o cal, empregaremos o célebre Teorema de Normalización de Noether. A versión que damos aquí deste último é un refinamento debido a Nagata que adaptamos ao noso contexto (aínda que orixinalmente o formulou cun só ideal, nós expoñémolo para unha cadea de ideais). Basicamente describe a estrutura dun anel afín: dada unha cadea de ideais, existe un anel de polinomios sobre o cal o anel afín é un módulo finitamente xerado, e os ideais da cadea contráense a ideais xerados por segmentos das variables.

Lema 6.4. *Sexa $f \in A = K[x_1, \dots, x_r]$ un polinomio non constante. Entón existen elementos $x'_1, \dots, x'_{r-1} \in A$ tales que A é un módulo finitamente xerado sobre a K-subálxebra xerada por $x'_1, \dots, x'_{r-1}$ e f.*

Demostración. Basta probar que f se pode escribir en función de variables $x'_1, \dots, x'_{r-1}$ e x_r de xeito que sexa mónico en x_r. Nese caso, por 1.26, teriamos que A é un módulo finitamente xerado sobre $K[x'_1, \dots, x'_{r-1}, f]$. Sexa entón d o grao de f e denotemos por f_d a suma de todos os termos de f de grao d. Facendo os cambios de variable $x'_i = x_i - a_i x_r$, sendo os a_i elementos de K, temos que o termo contendo x_r^d é $f_d(a_1, \dots, a_{r-1}, 1)x_r^d$. Como podemos conseguir $a_1, \dots, a_{r-1} \in K$ tales que $f_d(a_1, \dots, a_{r-1}, 1) \neq 0$, dividindo temos que f é mónico en x_r en función das variables $x'_1, \dots, x'_{r-1}, x_r$.

□

Teorema 6.5 (Teorema de Normalización de Noether)**.** *Sexa A un anel afín de dimensión d sobre un corpo K. Entón A contén un anel de polinomios $B = K[x_1, \dots, x_d]$ tal que A é un B-módulo finitamente xerado. Ademais, se $I_1 \subset \cdots \subset I_m$ é unha cadea de ideais de A con* $\dim I_j = d_j$ *e $d_1 > d_2 > \cdots > d_m \geq 0$, entón B pódese escoller de xeito que*

$$I_j \cap B = (x_{d_j+1}, \dots, x_d) \quad \textit{para } j = 1, \dots, m.$$

Demostración. Por ser A unha K-álxebra finitamente xerada é da forma T/I con $T = K[y_1, \dots, y_r]$ un anel de polinomios. Pola correspondencia entre os ideais de T e os ideais de T/I, tomando as imaxes recíprocas dos I_j en T e engadindo á cadea o ideal $I_0 = I$, é suficiente con demostrar o resultado para o caso no que A é un anel de polinomios d-dimensional $A = K[y_1, \dots, y_d]$. Faremos a demostración en distintas etapas:

- Paso 1. Para demostrar o resultado, basta atopar $x_1, \dots, x_d \in A$ verificando

  (i) A é un módulo finitamente xerado sobre a k-subálxebra B xerada por $x_1, \dots, x_d$.

  (ii) $I_j \cap B \supset (x_{d_j+1}, \dots, x_d)$ para cada $j = 1, \dots, m$.

  En efecto, vexamos primeiramente que nese caso B é un anel de polinomios, é dicir, que os x_i son alxebricamente independentes sobre K. Supoñamos pola contra que son dependentes; entón, por (i), o grao de trascendencia de A sobre K sería o mesmo que o de B sobre K, que por ser os x_i dependentes é estritamente menor que d. Pero isto contradice a hipótese de que os $y_1, \dots, y_d$ son alxebricamente independentes.

  Por outra banda, vexamos que nese caso o contido en (ii) se converte en igualdade. En efecto, por 4.14 temos que dim $I_j \cap B =$ dim $I_j = d_j$, e polo Axioma 4, dim $(x_{d_j+1}, \dots, x_d) =$ dim $B/(x_{d_j+1}, \dots, x_d) =$ dim $K[x_1, \dots, x_{d_j}] = d_j$. Como o segundo ideal é primo, ambos os dous son o mesmo e temos a igualdade.

  Polo tanto, para probar o teorema é suficiente con atopar $x_1, \dots, x_d$ cumprindo (i) e (ii).

- Paso 2. Construiremos os x_i a partir dos y_i. Tomemos $x'_i = y_i$ para $i = 1, \dots, d$. Supoñamos agora que nalgún momento xa temos escollidos elementos $x_{e+1}, \dots, x_d$ e elementos auxiliares $x'_1, \dots, x'_e$ de xeito que verifiquen:

  (i') A é un módulo finitamente xerado sobre $B_e := K[x'1, \dots, x'_e, x_{e+1}, \dots, x_d]$.

  (ii') $I_j \cap B_e \supset (x_h, \dots, x_d)$ para $j = 1, \dots, m$ sendo $h = \text{máx}(d_j + 1, e + 1)$.

  Se conseguimos atopar un novo elemento x_e (o cal veremos no seguinte paso) e substituír os $x'_1, \dots, x'_{e-1}$ por novos elementos de xeito que (i') e (ii') aínda se verifiquen cambiando e por $e - 1$, podemos repetir o proceso ata chegar a $e = d_m$, momento no cal podemos tomar $x_i = x'_i$ para $i = 1, \dots, d_m$ e ter o resultado.

- Paso 3. Supoñamos entón que $x'_1, \dots, x'_e, x_{e+1}, \dots, x_d$ con $d_m < e \leq d$ verifican (i') e (ii'). Sexa j o menor índice tal que $e > d_j$. Asumamos (e probarémolo no seguinte e último paso) que $I_j \cap K[x'1, \dots, x'_e] \neq 0$ e escollamos x_e calquera polinomio non nulo de $I_j \cap K[x'1, \dots, x'_e]$. Polo lema anterior, existen elementos $x''_1, \dots, x''_{e-1} \in K[x'_1, \dots x'_e]$ tales que $K[x'_1, \dots x'_e]$ é un módulo finitamente xerado sobre $K[x''_1, \dots x''_{e-1}, x_e]$. Concluímos entón que os elementos $x''_1, \dots, x''_{e-1}, x_e, x_{e+1}, \dots, x_d$ verifican (i') e (ii') cambiando e por $e - 1$.

- Paso 4. Para rematar a proba, demostremos o que nos faltaba no paso anterior: $I_j \cap K[x'_1, \ldots, x'_e] \neq 0$. Noutro caso, como por (ii') temos que

$$(x_{e+1}, \ldots, x_d) \subset I_j \cap K[x'_1, \ldots, x'_e, x_{e+1}, \ldots, x_d],$$

entón $I_j \cap B_e = (x_{e+1}, \ldots, x_d)$, pero polo mesmo argumento empregado no paso 1, o ideal da esquerda ten dimensión d_j e o da dereita e, pero isto contradice $e > d_j$.

□

Este teorema ten por sí mesmo significado xeométrico: dada unha variedade afín V d-dimensional e unha cadea de subvariedades de V, existe un morfismo de variedades finito −o cal quere dicir que verifica as hipóteses de 4.16− entre V e un d-espazo afín, que leva a cadea de subvariedades de V nunha cadea de variedades coordenadas.

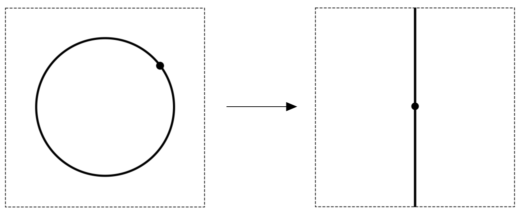


Figura 6.1: Morfismo de variedades que leva a circunferencia nunha recta coordenada e o punto na orixe.

Veremos agora un último resultado necesario para demostrar o teorema 6.2. Non incluímos a súa demostración porque fai uso de teoría de Galois demasiado avanzada para este traballo. Pode verse en [6, pp. 294-295] Lembremos que un *dominio normal* é un dominio que coincide coa súa normalización, é dicir, un dominio cuxa clausura enteira no seu corpo de fraccións é todo o corpo de fraccións.

Teorema 6.6 (Teorema do descenso para extensións enteiras de dominios normais)**.** *Sexa B un dominio normal e A un dominio contendo B. Se A é enteiro sobre B, entón, dados ideais primos $Q \subset Q_1$ de B e un primo P_1 de A tal que $Q_1 = P_1 \cap B$, entón existe un primo P de A tal que $P \subset P_1$ e $P \cap B = Q$.*

Estamos xa preparados para demostrar o teorema 6.2, o cal volvemos enunciar:

Teorema. *Se A é un dominio afín sobre K, entón*

$$\dim A = \text{tr. deg.}_K A,$$

e este número é a lonxitude de calquera cadea maximal de ideais primos en A.

Demostración. Sexa $B = K[x_1, \dots, x_d]$ o anel de polinomios sobre o que A é un módulo finitamente xerado que nos proporciona o Teorema de Normalización. Entón,

$$\text{tr.deg}_K B = \text{tr.deg}_K K(x_1, \dots, x_d) = d.$$

Como A é finitamente xerado sobre B, a extensión $Q(A) \mid Q(B)$ é finita, polo tanto alxébrica e así $\text{tr.deg}_{Q(B)} Q(A) = 0$, polo que $\text{tr.deg}_K A = d + 0 = d$.

Sexa agora $P_0 \subsetneq \cdots \subsetneq P_m$ unha cadea de ideais primos de A. Temos entón que $m \leq d$. Vexamos que se $m < d$, entón podemos engadir un primo distinto á cadea. Tomemos de novo B como no Teorema de Normalización, agora con $I_j = P_j$. Como $m < d$, haberá dous primos da cadea entre os que o salto de dimensión sexa 2, é dicir, existe un j tal que $\dim\, P_{j-1} - 1 > \dim\, P_j$. Poñamos $d_{j-1} := \dim\, P_{j-1}$ e $d_j := \dim\, P_j$. Entón, tomando $Q := (x_{d_{j-1}}, \dots, x_d)$, o cal é un ideal primo en B, temos a seguinte cadea estrita de primos

$$P_{j-1} \cap B = (x_{d_{j-1}+1}, \dots, x_d) \subsetneq Q \subsetneq (x_{d_j+1}, \dots, x_d) = P_j \cap B.$$

Vexamos que isto implica que existe un primo P de A contido de xeito estrito entre P_{j-1} e P_j. Reemplazando A por A/P_{j-1} e B por $B/(P_{j-1} \cap B)$ ($= K[x_1, \dots, x_d]/(x_{d_{j-1}+1}, \dots, x_d)$ o cal segue sendo un anel de polinomios) podemos supoñer que tanto P_{j-1} coma $P_{j-1} \cap B$ son o ideal nulo. Basta entón con probar que existe un ideal P en A contido en P_j de xeito que $P \cap B = Q_j$. Pero como B é un dominio de factorización única, en particular é normal e polo tanto polo teorema do descenso temos o resultado. $\square$

Capítulo 7

Segunda caracterización. Polinomio de Hilbert

Neste último capítulo imos ver unha segunda caracterización da dimensión dun anel, neste caso no ámbito dos aneis locais. De feito, traballaremos no eido máis xeral dos módulos finitamente xerados sobre un anel local. O obxectivo principal será ver que a dimensión dun anel local se pode expresar en función do grao dun polinomio: o polinomio de Hilbert-Samuel. Esta última caracterización ten unha aplicación computacional moi importante, xa que mediante o uso das bases de Gröbner e grazas ao seu recente desenvolvemento podemos calcular de xeito explícito as dimensións de moitos aneis.

Comezamos o capítulo cunha sección adicada principalmente a probar o lema de Artin-Rees, o cal precisaremos para demostrar o resultado que buscamos.

Ao longo deste capítulo, todos os aneis serán noetherianos e os módulos finitamente xerados.

7.1. Aneis graduados e filtracións

. Un *anel graduado* é un anel A acompañado dunha familia de subgrupos aditivos $\{A_n\}_{n\in\mathbb{N}}$ de A tales que

$$A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$$

como grupos abelianos, verificando $A_iA_j \subset A_{i+j}$ para todo $i, j \in \mathbb{N}$. Notemos que entón $A_0A_0 \subset A_0$, polo que A_0 é un subanel de A, e que $A_0A_i \subset A_i$, polo que A_i é un A_0-módulo para calquera $i \in \mathbb{N}$.

Exemplo 7.1. O primeiro exemplo de anel graduado é o anel de polinomios $K[x_1, \ldots, x_n]$, graduado polo propio grao dos polinomios: cada A_i é o subgrupo das formas (polinomios homoxéneos) de grao i.

Un elemento de A que pertence a un dos A_i dise *homoxéneo*, mentres que un ideal dise *ideal homoxéneo* se está xerado por elementos homoxéneos.

En xeral, dado un anel graduado $A = A_0 \oplus A_1 \oplus \cdots$, un *módulo graduado sobre* A é un A-módulo xunto cunha descomposición como grupos abelianos

$$M = \bigoplus_{-\infty}^{\infty} M_i,$$

de xeito que $A_i M_j \subset M_{i+j}$ para cada i, j.

Pasemos agora ao concepto de filtración. Dado un A-módulo M, unha *filtración* de M é unha cadea de submódulos

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots$$

e dado un ideal I de A, a anterior filtración dise unha *I-filtración* se $IM_i \subset M_{i+1}$ para todo $i \in \mathbb{N}$. Neste caso, unha I-filtración de M dise *I-estable* se $IM_i = M_{i+1}$ para i suficientemente grande.

Exemplo 7.2. A I-filtración estable de M dada por

$$M \supset IM \supset I^2 M \supset \cdots$$

recibe o nome de filtración I-ádica de M.

Podemos construír aneis e módulos graduados para calquera anel e calquera módulo. Sexa I un ideal de A, entón podemos considerar o anel graduado

$$\text{gr } A := A/I \oplus I/I^2 \oplus \cdots .$$

Para definir a multiplicación, basta facelo para elementos homoxéneos. Así, definimos a multiplicación entre $a + I^{n+1} \in I^n/I^{n+1}$ e $b + I^{m+1} \in I^m/I^{m+1}$ como

$$(a + I^{n+1})(b + I^{m+1}) := (ab) + I^{n+m+1} \in I^{n+m}/I^{n+m+1}$$

e é inmediato ver que está ben definida. Polo tanto, $(I^n/I^{n+1})(I^m/I^{m+1}) \subset I^{n+m}/I^{n+m+1}$ e vemos que en efecto é un anel graduado. Podemos xeralizar a construción e considerar un A-módulo M cunha I-filtración $M = M_0 \supset M_1 \supset \cdots$, para construír

$$\text{gr } M := M/M_1 \oplus M_1/M_2 \oplus \cdots ,$$

o cal é un (gr I)-módulo graduado considerando outra vez a operación natural $(a + I^{n+1})(b + M_{m+1}) := (ab) + M_{n+m+1}$, a cal volve estar ben definida por ser $M \supset M_1 \supset \cdots$ unha I-filtración.

Proposición 7.3. *Sexa I un ideal dun anel A e M un A-módulo finitamente xerado. Se $M = M_0 \supset M_1 \supset \cdots$ é unha I-filtración estable na que os submódulos son finitamente xerados, entón* $\mathrm{gr}\ M$ *é un módulo finitamente xerado sobre* $\mathrm{gr}\ A$.

Demostración. Por ser a filtración I-estable, temos que existe n tal que $IM_i = M_{i+1}$ para $i \geq n$. Entón

$$(I/I^2)(M_i/M_{i+1}) = M_{i+1}/M_{i+2} \text{ para } i \geq n.$$

En efecto, a inclusión "$\subset$" é inmediata pola definición da operación, e dado $b \in M_{i+1}/M_{i+2}$ podemos tomar un representante $b' \in M_{i+1} = IM_i$, polo que $b' = ac$ para algúns $a \in I$ e $c \in M_i$ e tomando o produto das imaxes nos cocientes vemos que coincide con b. Polo tanto, tomando unha unión de xeradores dos M_j/M_{j+1} con $0 \leq j \leq n$ podemos xerar todos os demais. Como cada M_i é finitamente xerado, tamén o é cada M_i/M_{i+1} e esa unión pódese tomar finita. $\square$

O obxectivo final desta sección será probar o lema de Artin-Rees. Pero antes, precisamos facer unha nova construción: se A é un anel e I un ideal de A, denotaremos por A^* ao anel graduado $A \oplus I \oplus I^2 \oplus \cdots$. Ademais, se M é un A-módulo e $M = M_0 \supset M_1 \supset \cdots$ é unha I-filtración de M, denotaremos por M^* á suma directa $M \oplus M_1 \oplus \cdots$, o cal é un A^*-módulo graduado de forma natural.

Podemos ver agora un resultado análogo á proposición anterior pero que neste caso se converte en equivalencia:

Proposición 7.4. *Sexa I un ideal dun anel A e M un A-módulo finitamente xerado. Se $M = M_0 \supset M_1 \supset \cdots$ é unha I-filtración na que os submódulos son finitamente xerados, entón a filtración é estable se e só se M^* é finitamente xerado como módulo sobre A^*.*

Demostración. Se a filtración é estable, temos que $IM_i = M_i$ para i suficientemente grande polo que bastará con tomar xeradores dun número finito de submódulos M_j para xerar todo M^*. Como cada un dos M_j é finitamente xerado, concluímos que M^* é finitamente xerado.

Reciprocamente, se M^* é finitamente xerado, entón podemos tomar un conxunto finito de xeradores de M^* de xeito que estén contidos en $\bigoplus_{i=0}^{n} M_i$. Ademais, expresando cada elemento como suma de compoñentes homoxéneas, podemos supoñer que ese conxunto finito de xeradores está formado por elementos homoxéneos. Polo tanto, cada xerador pertence a un M_i con $i \leq n$. Como estamos ante unha I-filtración, $\bigoplus_{k \geq 0} M_{n+k}$ está xerado como A^* módulo por M_n, polo que $M_{n+k} = I^k M_n$ e a filtración é estable. $\square$

Temos xa as ferramentas suficientes para demostrar o lema de Artin-Rees.

Proposición 7.5 (Lema de Artin-Rees). *Sexa A un anel noetheriano, I un ideal de A e $M' \subset M$ módulos finitamente xerados sobre A. Dada unha I-filtración estable $M = M_0 \supset M_1 \supset \cdots$, entón a filtración inducida $M' = M' \cap M_0 \supset M' \cap M_1 \supset \cdots$ é unha I-filtración estable de M'.*

Demostración. Como estamos ante unha I-filtración de M, temos que $I(M' \cap M_i) \subset IM' \cap IM_i \subset M' \cap M_{i+1}$ polo que a filtración de M' tamén é unha I-filtración. Por ser M' un A-submódulo de M, tense que $(M')^*$ é naturalmente un A^*-submódulo graduado de M^*. Agora, como A é noetheriano, o ideal I é finitamente xerado e polo tanto $A^* = A \oplus I \oplus I^2 \oplus \cdots$ é unha álxebra sobre A finitamente xerada, o cal implica por 1.8 que A^* é noetheriano. Pola proposición anterior, como a filtración de M é estable temos que M^* é un módulo finitamente xerado sobre A^* e polo tanto noetheriano, concluíndo así que o submódulo $(M')^*$ é finitamente xerado e de novo pola proposición anterior a filtración de M' é estable. $\square$

7.2. Funcións de Hilbert-Samuel

O noso obxectivo vai ser dar unha nova caracterización de dimensión no caso dos aneis locais. A partir de agora, A denotará un anel local con ideal maximal $\mathfrak{m}$. Por cuestións técnicas é apropiado traballar no contexto máis xeral dos módulos finitamente xerados. Por iso, precisamos introducir algunhas novas definicións.

Dado un A-módulo M finitamente xerado, definimos a súa *dimensión* como a dimensión (como ideal) de $\operatorname{ann} M$, é dicir, a dimensión (como anel) de $A/\operatorname{ann} M$.

Por outra banda, se $\mathfrak{q} \subset \mathfrak{m}$ é un ideal de A, dicimos que $\mathfrak{q}$ ten *colonxitude* finita en M se $M/\mathfrak{q}M$ ten lonxitude finita. Equivalentemente por 1.18, se $\mathfrak{m}^n$ aniquila $M/\mathfrak{q}M$ para algún n.

Introducimos agora as funcións de Hilbert-Samuel:

Definición 7.6. Sexa M un A-módulo finitamente xerado e $\mathfrak{q} \subset \mathfrak{m}$ un ideal de colonxitude finita en M. Entón a función

$$H_{\mathfrak{q},M}(n) := \operatorname{lonx} \mathfrak{q}^n M/\mathfrak{q}^{n+1}M$$

recibe o nome de *función de Hilbert-Samuel* de M respecto de $\mathfrak{q}$.

Unha das interesantes propiedades que verifica esta función é que para valores suficientemente grandes de n coincide cun polinomio con coeficientes racionais, e ese polinomio será clave á hora de ver a dimensión de M. No seguinte resultado empregamos a ben sabida propiedade seguinte: se unha función f sobre os naturais verifica que $f(n+1) - f(n)$ define un polinomio de grao d, entón $f(n)$ é un polinomio de grao $d+1$.

Proposición 7.7. *Sexa A un anel noetheriano, M un A-módulo finitamente xerado e $\mathfrak{q}$ un ideal de colonxitude finita en M. Entón, para n suficientemente grande, $H_{\mathfrak{q},M}(n)$ coincide cun polinomio $P_{\mathfrak{q},M}(n)$ de grao estritamente menor que o número de xeradores de $\mathfrak{q}$.*

Antes de levar a cabo a demostración, introducimos unha notación: se M é un módulo graduado, denotamos por $M(s)$ ao módulo graduado isomorfo a M resultante de "desprazar o grao" d veces. É dicir, $M(s)$ está graduado por $M(s)_n = M_{s+n}$.

Demostración. Reemplazando A por $A/\mathrm{ann}\ M$ e tomando $\mathrm{gr}\ A$ e $\mathrm{gr}\ M$ (respecto de $\mathfrak{q}$), podemos supoñer que A é un anel graduado. Procederemos por indución no número r de xeradores de $\mathfrak{q}$. Se $r = 0$ é inmediato; supoñamos entón que $\mathfrak{q}$ está xerado por $x_1, \ldots, x_r \in R_1$. Podemos construír a sucesión exacta de homomorfismos de grao 0

$$0 \to \{m \in M \mid x_1 m = 0\} \to M \xrightarrow{x_1} M(1) \to (M/x_1M)(1) \to 0$$

de onde obtemos

$$H_{\mathfrak{q},M}(n+1) - H_{\mathfrak{q},M}(n) = H_{\mathfrak{q},M/x_1M}(n+1) - H_{\mathfrak{q},\{m\in M|x_1m=0\}}(n).$$

Tanto M/x_1M como $\{m \in M \mid x_1m = 0\}$ se poden ver como módulos sobre $A/(x_1)$, de xeito que o ideal $\mathfrak{q}$ ten $r-1$ xeradores. Así, o membro da dereita na anterior igualdade é a diferencia de dúas funcións de Hilbert-Samuel que, pola hipótese de indución, coinciden para n suficientemente grande cun polinomio de grao $< r-1$. Polo tanto, pola observación previa á proposición, a función $H_{\mathfrak{q},M}(n)$ coincide para n suficientemente grande cun polinomio de grao $< r$. □

Denotando $L_{\mathfrak{q},M}(n) := \mathrm{lonx}\ M/\mathfrak{q}^n M$, temos a seguinte consecuencia:

Corolario 7.8. *Nas mesmas condicións que a proposición anterior, $L_{\mathfrak{q},M}(n)$ coincide para n suficientemente grande cun polinomio de grao $1 + \deg P_{\mathfrak{q},M}$.*

Demostración. Da sucesión exacta

$$0 \to \mathfrak{q}^n M/\mathfrak{q}^{n+1}M \to M/\mathfrak{q}^{n+1}M \to M/\mathfrak{q}^n M \to 0$$

obtemos que $L_{\mathfrak{q},M}(n+1) - L_{\mathfrak{q},M}(n) = H_{\mathfrak{q},M}(n)$. Polo mesmo argumento empregado na proposición anterior temos o resultado. □

Lema 7.9. *Se $0 \to M' \to M \to M'' \to 0$ é unha sucesión exacta de A-módulos finitamente xerados, e se $\mathfrak{q}$ é un ideal de colonxitude finita en M, entón o polinomio*

$$P_{\mathfrak{q},M'} + P_{\mathfrak{q},M''} - P_{\mathfrak{q},M}$$

ten coeficiente principal positivo e grao $< \deg P_{\mathfrak{q},M'}$.

Demostración. Polo corolario anterior basta probar o resultado para a función L. Unha vez máis, a sucesión exacta

$$0 \to (M' \cap \mathfrak{q}^n M)/\mathfrak{q}^n M' \to M'/\mathfrak{q}^n M' \to M/\mathfrak{q}^n M \to M''/\mathfrak{q}^n M'' \to 0$$

obtemos

$$L_{\mathfrak{q},M'}(n) + L_{\mathfrak{q},M''}(n) - L_{\mathfrak{q},M}(n) = \text{lonx } (M' \cap \mathfrak{q}^n M)/\mathfrak{q}^n M'.$$

O lema de Artin-Rees danos información sobre este polinomio. En efecto, como a $\mathfrak{q}$-filtración $M \supset \mathfrak{q}M \supset \mathfrak{q}^2 M \supset \cdots$ é estable, o lema dinos que a filtración inducida sobre M' tamén será estable, polo que existe un m tal que para todo $n \geq m$ se ten

$$M' \cap \mathfrak{q}^n M = \mathfrak{q}^{n-m}(M' \cap \mathfrak{q}^m M) \subset \mathfrak{q}^{n-m} M',$$

de onde obtemos

$$\text{lonx}(M' \cap \mathfrak{q}^n M)/\mathfrak{q}^n M' \leq L_{\mathfrak{q},M'}(n) - L_{\mathfrak{q},M'}(n-m)$$

obtendo o resultado. □

Xa estamos case en condicións de demostrar o teorema central deste capítulo. Porén, é necesario un último resultado previo, consecuencia do Teorema do Ideal Principal.

Proposición 7.10. *Sexan A un anel local con ideal maximal $\mathfrak{m}$ e M un A-módulo finitamente xerado. Entón, para cada $x \in \mathfrak{m}$ temos que*

$$\dim M/xM \geq \dim M - 1.$$

Demostración. Sexa $d := \dim M/xM = \dim A/\text{ann } (M/xM)$. Polo corolario 5.9 e a proposición 1.24, existe un ideal $(x_1, \dots, x_d)$ de colonxitude finita en M/xM, polo que $(M/xM)/(x_1, \dots, x_d)$ ten lonxitude finita, é dicir, $M/(x, x_1, \dots, x_d)M$ ten lonxitude finita, e así $(x, x_1, \dots, x_d)$ ten colonxitude finita en M. Volvendo aplicar 1.24, $\mathfrak{m}^n \subset (x, x_1, \dots, x_d) + \text{ann } M$ para un n suficientemente grande, e polo corolario 5.9 temos

$$\dim M = \dim A/\text{ann } M \leq d + 1 = \dim M/xM + 1.$$

□

Podemos xa probar o resultado buscado.

Teorema 7.11. *Se $(A, \mathfrak{m})$ é un anel local, M un A-módulo finitamente xerado e $\mathfrak{q}$ un ideal de colonxitude finita en M, entón*

$$\dim M = 1 + \deg P_{\mathfrak{q},M}.$$

Demostración. Vexamos primeiro que o grao do polinomio non depende de $\mathfrak{q}$. Podemos reemplazar A por $A/\text{ann } M$ e supoñer que ann $M = 0$. Por ser $\mathfrak{q}$ de colonxitude finita en M, existe unha potencia de $\mathfrak{m}$ que aniquila $M/\mathfrak{q}M$; polo tanto, existe un d tal que $\mathfrak{m}^d \subset \mathfrak{q} \subset \mathfrak{m}$. Así, para calquera n temos que $\mathfrak{m}^{dn} \subset \mathfrak{q}^n \subset \mathfrak{m}^n$, o cal induce

$$L_{\mathfrak{m},M}(n) \leq L_{\mathfrak{q},M}(n) \leq L_{\mathfrak{m},M}(dn).$$

de xeito que $L_{\mathfrak{q},M}(n)$ está acotado por polinomios que teñen o mesmo grao en n, polo que ten ese mesmo grao.

Agora, polo recíproco do Teorema do Ideal Principal (5.8), podemos atopar un ideal $\mathfrak{q}'$ de colonxitude finita en M xerado por dim M elementos. Pola proposición 7.7, $P_{\mathfrak{q}',M}$ ten grao estritamente menor que dim M e como o grao do polinomio é independente do ideal, temos que dim $M \geq \deg P_{\mathfrak{q},M} + 1$.

Para ver a outra desigualdade, farémolo por indución na dimensión de M. O caso de dimensión nula é trivial. Sexa entón dim $M > 0$ e P un ideal primo asociado a $M-$é dicir, un ideal primo que é o aniquilador dun elemento de $M-$ de dimensión dim M. Neste caso, A/P é isomorfo a un submódulo de M, e polo lema 7.9 é suficiente ver o resultado para $M = A/P$. Como a dimensión de M non é nula, temos que M non é un corpo e polo tanto P non é o ideal maximal de A e $\mathfrak{q} \nsubseteq P$. Por ser P primo é obvio que todo $x \in \mathfrak{q}$ que non esté en P é un non-divisor de cero. Así, dim $M/xM <$ dim M, e como $x \in \mathfrak{q} \subset \mathfrak{m}$ temos pola proposición anterior 7.10 que dim $M/xM =$ dim $M - 1$. Aplicando a hipótese de indución, temos que dim $M/xM = 1 + \deg P_{\mathfrak{q},M/xM}$. Por último, aplicando o lema 7.9 á sucesión exacta

$$0 \to M \xrightarrow{x} M \to M/xM \to 0$$

obtemos que o polinomio

$$P_{\mathfrak{q},M} + P_{\mathfrak{q},M/xM} - P_{\mathfrak{q},M} = P_{\mathfrak{q},M/xM}$$

ten grao estritamente menor que deg $P_{\mathfrak{q},M}$. Concluímos entón que

$$\dim M - 1 = \dim M/xM = 1 + \deg P_{\mathfrak{q},M/xM} < 1 + \deg P_{\mathfrak{q},M},$$

polo que dim $M \leq 1 + \deg P_{\mathfrak{q},M}$, rematando a demostración. □

Notemos que se no anterior teorema tomamos $M = A$ temos o caso particular dun anel local que mencionabamos ao comezo do capítulo:

Corolario 7.12. *Se A é un anel local, entón* dim $A = 1 + \deg P_A$.

Bibliografía

[1] A. Altman e S. Kleiman. *Introduction to Grothendieck Duality Theory*. Springer-Verlag, 1970.

[2] A. Altman e S. Kleiman. *A term of commutative algebra*. Worldwide Center of Mathematics, 2013.

[3] M. F. Atiyah e I. G. Macdonald. *Introducción al álgebra conmutativa.* Editorial Reverté, 1980.

[4] D. A. Cox, J. Little e D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2015.

[5] D. Eisenbud e E.G. Evans. Every algebraic set in n-space is the intersection of n hypersurfaces. *Inventiones Mathematicae* 19, 107–112, 1973.

[6] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer-Verlag, 1995.

[7] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. 2008.

[8] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 1985.