FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Descomposición primaria en aneis noetherianos

Marcos Parrado Freijo

2020/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Descomposición primaria en aneis noetherianos

Marcos Parrado Freijo

02/07/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Descomposición primaria en aneis noetherianos
Breve descrición do contido
Ideales primos. Cambio de anillo Módulos y su produto tensorial Anillos y módulos noetherianos Desomposición primaria Interpretación geométrica
Recomendacións
Outras observacións

Contidos

Resumo

A teoría de aneis e ideais é un obxecto de estudo dende mediados do século XIX e xoga un papel fundamental no desenvolvemento da álxebra e da xeometría moderna. Este traballo trata de achegar unha xeralización do teorema fundamental da aritmética dentro do contexto da teoría de ideais. Este será o teorema de Lasker-Noether e o fundamento a teoría de descomposición primaria para ideais. Con este fin introducimos todas as ferramentas necesarias para chegar ao noso propósito: un estudo da estrutura dos aneis e dos módulos enfatizando aqueles puntos non abordados ao longo do grao; resaltaremos a importancia dos aneis noetherianos e paralelamente estenderase un conxunto de conceptos topolóxicos.

Abstract

The theory of rings and ideals has been an object of study since the mid-nineteenth century and plays a key role in the development of modern algebra and geometry. This work seeks to provide a generalization of the fundamental theorem of arithmetic within the context of ideal theory. This will be the Lasker-Noether theorem and the foundation the primary decomposition theory for ideals. To this end we have introduced all the tools necessary to reach our purpose: an study of the structure of the rings and modules emphasizing those points not addressed throughout the degree; we will highlight the importance of the Noetherian rings and in parallel a set of topological concepts will be extended.

Introdución

Antes de dar comezo a unha breve indtorución histórica destacamos que as fontes desta fundaméntanse en [2] e [4]. O interés nas estruturas matemáticas ao longo do século XIX deu lugar a un afán pola xeralización no campo da aritmética e da teoría de números. O primer precendente son os traballos de Carl Friedrich Gauss (1777-1855) estendendo a idea de número enteiro cos seus números gaussianos, os da forma $a + bi$ con $a, b \in \mathbb{Z}$. Posteriormente Richard Dedekind (1831-1916) xeralizou esta idea na súa teoría de enteiros alxébricos, ou sexa, números que son raíces de ecuacións polinómicas con coeficientes enteiros.

Estes novos conxuntos, denominados dominios de integridade, non eran corpos, estrutura tan estudada dende os traballos de Évariste Galois (1811-1832), mais si tiñan propiedades compartidas con estes. Sen embargo, estas xeralizacións tiveron un prezo: a pérdida da factorización única. Recordemos que ser un dominio de factorización única implica, no ámbito da álxebra moderna, de forma natural ser un dominio de ideais principais. Por iso Dedekind e Ernst Kummer (1810-1893) introduciron na aritmética a noción de ideal.

Os defectos que os elementos tiñan por si mesmos eran suplidos por conxuntos multiplicativamente pechados. Así, no anel dos enteiros alxébricos, calquera ideal pode expresarse de forma única como produto de ideais primos. Ou sexa, a unicidade na factorización puido salvarse a través da teoría de ideais e aneis comezando, polo tanto, toda unha rama das matemáticas.

Esta iniciativa de xeralizar a teoría de números prosegue a comezos do século XX. Destacamos o traballo de Emanuel Lasker (1868-1941), discípulo de Max Noether (1844-1921), o cal en 1905 publica o artigo "Zur Theorie der Moduln und Ideale" no que dá unha versión, para aneis polinomiais, do teorema fundamental da aritmética. Para elo introduce a noción de ideais primarios e descomposición primaria que virán a substituir a idea de potencia de primo e fractorización dun número.

Dende mediados do século XIX foise desenvolvendo de forma paralela toda unha rama das matemáticas aparentemente non vinculante á anterior: a xeometría alxébrica. Non sería ata os traballos de David Hilbert (1862-1943) que se logra un vínculo entre a teoría de ideais en aneis de polinomios e as variedades alxébricas co seu famoso teorema dos ceros. Unha das matemáticas que seguiu de cerca as conferencias de Hilbert en Gotïnga foi Emmy Noether (1882-1935), filla de Max Noether. Esta interesouse pronto pola álxebra abstracta destacando entre outros feitos polo estudo das condicións de cadea e a xeralización do teorema de descomposición primaria de Lasker cara un conxunto máis amplo de aneis: os aneis noetherianos. Cabe destacar que é posible que Noether, a diferencia de Lasker, estivera altamente influenciada pola visión procedente da xeometría.

Por último, e cun afán de completitude, cabe mencionar que a comezos do século XX nace unha nova rama da man de Felix Hausdorff (1868-1942): a topoloxía conxuntista. Esta será estudada por continuístas dos estudos de Noether como Oscar Zariski (1899-1986) nos conceptos e ramas previamente mencionadas.

Así, o obxectivo final desta memoria é abordar a descomposición primaria en aneis noetherianos. Para elo incluiranse incialmente non só as ferramentas necesarias de aneis conmutativos e módulos, senon que, ademais, farase un estudo máis contextualizado destes co fin de desenvolver os coñecementos e as habilidades adquiridas no Grao.

Capítulo 1

Aneis e módulos

1.0.1. Introdución

O presente capítulo ten como obxectivo indagar naqueles aspectos da teoría de aneis e módulos que non foron abordados ao longo do grado. O obxectivo principal disto será establecer as ferramentas necesarias para a exposición dos obxectos do capítulo 2 e 3. En resumo, este capítulo consta de 3 seccións fundamentais: unha exposición inicial sobre os tipos de ideais dentro dun anel coa súa preservación por medio de operacións elementais. Unha segunda sección no que abordamos a búsqueda dunha topoloxía natural ao conxunto operacional: a topoloxía de Zariski; e por último, un terceiro bloque no que se introducirá unha revisión á teoría de módulos facendo énfase naqueles que manifesten unha finitude con respecto aos seus xeradores. Por último cabe recordar que todos os aneis cos que traballaremos neste traballo son conmutativos e, polo tanto, traballaremos no marco do que se coñece como álxebra conmutativa. Ao mesmo tempo asúmese coñecida as definicións, abordadas no Grao, sobre aneis, ideais e módulos.

1.0.2. Ideais primos, maximais e radicais

Unha vez que introducimos a noción de ideal, cabe preguntarse que tipos de ideais podemos atopar e, sobre todo, á hora de cocientar por esos ideais que propiedades interesantes lle dá ao cociente. Así imos inicialmente centrar a nosa atención en dous tipos destes:

Definición 1.1. Un ideal $\mathfrak{p}$ en A é *primo* se $\mathfrak{p} \neq (1)$ e se $xy \in \mathfrak{p}$ terase que $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$

A noción de ideal primo pretende xeralizar o concepto de número primo que tiñamos en $\mathbb{Z}$, ou sexa, a idea de ter un bloque básico dentro do noso conxunto operacional. Ao

longo deste traballo van ser de grande importancia, sobre todo, de cara á descomposición de ideais en certos tipos de aneis.

Definición 1.2. Un ideal $\mathfrak{m}$ en A é *maximal* se $\mathfrak{m} \neq (1)$ e $\nexists\ \mathfrak{a}$, ideal de A, tal que $\mathfrak{m} \subset \mathfrak{a} \subset (1)$.

Ambos son ideais por definición e polo tanto imos poder cocientar con eles. Son realmente importantes, polos cocientes que dan lugar:

Proposición 1.3. *Sexa A un anel entón verifícase:*

1. *Un ideal $\mathfrak{p}$ é primo se e só se $A/\mathfrak{p}$ é un dominio de integridade.*
2. *Un ideal $\mathfrak{m}$ é maximal se e só se $A/\mathfrak{m}$ é un corpo.*

Operar con este tipo de ideais vai ser interesante pola simplicación que dá traballar cos seus cocientes. É importante poder garantir a súa existencia para seguir traballando no marco máis xeral posible. Se asumimos o lema de Zorn (ou un caso particular de aneis como os noetherianos que non necesitarían do axioma de elección) pódese garantir que sempre se ten un número suficiente deles. Isto condénsase nos seguintes resultados:

Proposición 1.4. *Cada anel $A \neq \{0\}$ ten polo menos un ideal maximal.*

Corolario 1.5. *Se $\mathfrak{a} \neq (1)$ é un ideal de A entón existe un ideal maximal que contén a $\mathfrak{a}$.*

Corolario 1.6. *Cada elemento de A que non é unha unidade, ou sexa, que non ten inverso multipicativo, está contido nun ideal maximal.*

Polo tanto, a través destes resultados, podemos facernos unha idea de que os ideais maximais veñen a acoller a todos os elementos que van carecer de inverso e que van afastar ao anel A de ser, en definitiva, un corpo. Ao mesmo tempo imos poder disgregar o anel a partir deles tal e como o indica a seguinte proposición:

Proposición 1.7. *O anel A é unión disxunta do conxunto de unidades, denotado $\mathfrak{U}(A)$, e da unión de todos os ideais maximais. Ademais, se a unión de todos os maximais é un ideal entón tan só hai un ideal maximal e diremos que A é un anel local.*

É interesante preguntarse, ao estar falando de conxuntos operacionais, cales son as operacións que preservan a nosa estrutura para poder construír novos obxectos a partir dos xa coñecidos. Dado un anel A e dous ideais $\mathfrak{a}$ $\mathfrak{b}$ deste, destacamos as seguintes operacións:

1. A suma: $\mathfrak{a} + \mathfrak{b} = \{x + y |\ x \in \mathfrak{a}, y \in \mathfrak{b}\}$.

2. O produto: $\mathfrak{ab} = \{xy|\ x \in \mathfrak{a}, y \in \mathfrak{b}\}$.

3. A itersección entendida no sentido usual.

4. O cociente: $(\mathfrak{a} : \mathfrak{b}) = \{x \in A|\ x\mathfrak{b} \subseteq \mathfrak{a}\}$. No caso particular $(0 : \mathfrak{a})$ chamarémolo *anulador de* $\mathfrak{a}$ e denotarase por $Ann(\mathfrak{a})$.

Notemos que a suma e a intersección poden ser estendidas para o caso dun conxunto arbitrario de ideais. Ao mesmo tempo vannos permitir relacionar certas propiedades dos ideais en función da súa relación cos ideais primos:

Proposición 1.8. *Dado un anel A, sexan $\mathfrak{p}_1, ..., \mathfrak{p}_n$ os seus ideais primos e $\mathfrak{a}$ un ideal contido en $\cup_{i=1}^n \mathfrak{p}_i$ entón $\mathfrak{a} \subseteq \mathfrak{p}_i$ para algún i.*

Proposición 1.9. *Dado un anel A, sexan $\mathfrak{a}_1, ..., \mathfrak{a}_n$ e sexa $\mathfrak{p}$ un ideal primo tal que $\cap_{i=1}^n \mathfrak{a}_i \subset \mathfrak{p}$. Entón temos que $\mathfrak{a}_i \subset \mathfrak{p}$ para algún i. Se temos a igualdade $\cap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$ entón teremos que $\mathfrak{a}_i = \mathfrak{p}$ para algún i.*

Rematamos a sección introducindo un obxecto que xogará un papel fundamental á hora de xeralizar a noción de raíz dun número:

Definición 1.10. Sexa $\mathfrak{a}$ un ideal de A, definimos o seu *radical* como $r(\mathfrak{a}) = \{x \in A|\ x^n \in \mathfrak{a}$ para algún $n > 0\}$. Decimos que un ideal $\mathfrak{a}$ é un *ideal radical* se se verifica que $\mathfrak{a} = r(\mathfrak{a})$.

Nota 1.11. Os radicais e ideais radicais van gozar da seguinte interpretación interesante: van dar a noción dos elementos básicos que constitúen a un ideal. Pensémolo por exemplo en $\mathbb{Z}$ co ideal $(12) = (2^2 \cdot 3)$, os múltiplos de 12. Intuimos, de forma superficial, que se poidera entender a partir de dous fragmentos básicos o 2 e o 3. Esta é a información que nos dá o radical, pois $r(12) = (2 \cdot 3)$: danos unha base do nosos conxunto operacional.

Proposición 1.12. *O radical dun ideal $\mathfrak{a}$ é a intersección dos ideais primos que conteñen a $\mathfrak{a}$.*

Nota 1.13. Cabe mencionar que o radical da suma de ideais non sempre coincide coa suma dos radicais. Isto podemos observalo no seguinte exemplo: consideramos o anel de polinomios $\mathbb{Q}[x, y]$ e consideremos os ideais (x) e $(x - y^3)$. Vaise verificar o seguinte:

$$r((x) + (x - y^3)) = r(x, y^3) = (x, y) \neq (x, y^3) = (x) + (x - y^3) = r(x) + r(x - y^3)$$

A cuestión de fondo é que ao tomar antes a suma que o radical esta pode dar lugar a unha simplificación pola natureza destes ideais. Mentres que ao considerar antes os radicais non ten porque existir dita simplificación por cuestión de irreducibilidade. De feito sempre se ten que $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$ para dous ideais $\mathfrak{a}$ e $\mathfrak{b}$ de A.

Restrinximos, por último, a nosa mirada a un caso particular do radical. Os seguintes dous conceptos xunto co anterior permítenos observar a importancia dos ideais primos e maximais como ferramentas descriptivas dos obxectos definidos dentro dun anel.

Definición 1.14. Denominamos co nome de *nilradical* dun anel A e denotarémolo como $r(0)$ ao radical do ideal 0, ou sexa, ao conxunto de elementos nilpotentes. Defínese ao mesmo tempo o *anel reducido* de A como o anel sen os elemento nilpotentes, é dicir, $A/r(0)$.

Corolario 1.15 (da proposición (1.12))**.** *O nilradical de A é a intersección de todos os ideais primos de A.*

Como unha mera estensión e debido a que a noción de ideal primo non ten por que coincidir coa de ideal maximal, estendemos a caracterización do nilradical para ideais maximais:

Definición 1.16. Chamaremos *radical de Jacobson*, e denotarase como $\mathfrak{R}$, á intersección de todos os ideais maximais.

Os elementos do radical de Jacobson, ao igual que os elementos do nilradical, van ter unha caracterización individual, que materializamos nos seguintes resultados.

Proposición 1.17. *Se x é un elemento nilpotente entón $x+1$ é unha unidade.*

Proposición 1.18. *$x \in \mathfrak{R}$ se e só se $1-xy$ é unha unidade de A para todo $y \in A$.*

1.0.3. Estensión e contracción de ideais

Dado un homomorfismo de aneis $f : A \to B$ é interesante coñecer baixo que hipóteses se transmiten as subestruturas. Pódese demostrar que se $\mathfrak{a}$ é un ideal de A entón $f(\mathfrak{a})$ non ten que ser necesariamente un ideal de B. Isto podemos velo construíndo unha inxección entre $\mathbb{Z}$ e $\mathbb{Q}$. Así, e pola importancia que teñen os ideais, é interesante buscar un ideal próximo ao noso conxunto imaxe.

Definición 1.19. Defínese a *estensión* $\mathfrak{a}^e$ de $\mathfrak{a}$ como o ideal $Bf(\mathfrak{a})$.

Pese a que $f^{-1}(\mathfrak{b})$ sempre é un ideal cando $\mathfrak{b}$ é un ideal de B, por analoxía coa definición anterior, imos chamarlle a este *contracción* $\mathfrak{b}^c$ de $\mathfrak{b}$ en A.

Proposición 1.20. *Sexa A e B dous aneis, $f : A \to B$ un homomorfismo e $\mathfrak{a}$, $\mathfrak{b}$ dous ideais deles respectivamente. Entón verifícase:*

- $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ *e* $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$
- $\mathfrak{b}^c = \mathfrak{b}^{cec}$ *e* $\mathfrak{a}^e = \mathfrak{a}^{ece}$

1.0.4. Topoloxía [1][5]

Imos introducir unha topoloxía no noso anel A aproveitándonos da súa estrutura. É dicir, imos basearnos nos ideais que este teña para dar unha 'noción de proximidade'. Pese a que unha motivación da necesidade desta topoloxía sexa de carácter xeométrico imos centrarnos nunha visión puramente aritmética. Empregaremos, entón, o feito de que todo anel posúe ideais maximais, e polo tanto primos, para construír unha topoloxía a partir de como definimos as operacións. Así, sexa A un anel e X o conxunto de todos os ideais primos de A. Para cada subconxunto E de A indicaremos por $V(E)$ ao conxunto dos ideais primos que conteñen a E, ou sexa, temos que $V(E) = \{\mathfrak{p} \text{ tal que } E \subseteq \mathfrak{p}\}$. Imos ver que isto conforma unha topoloxía sobre A, para elo apoiarémonos nas propiedades de $V(E)$:

Proposición 1.21. *O conxunto $V(E)$ cumple as seguintes propiedades:*

1. $V(0) = X$ *e* $V((1)) = \emptyset$.
2. *Se* $\mathfrak{a}$ *é un ideal enxendrado por* E *entón* $V(\mathfrak{a}) = V(E) = V(r(\mathfrak{a}))$.
3. *Se* $(E_i)_{i\in I}$ *é unha familia de subconxuntos de* A *entón* $V(\cup_{i\in I}E_i) = \cap_{i\in I}V(E_i)$
4. $V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ *para calquera par de ideais* $\mathfrak{a}$ *e* $\mathfrak{b}$ *de* A.

Demostración.

1. Para calquera ideal primo $\mathfrak{p}$ temos que $0 \in \mathfrak{p}$ e entón $V(0) = X$. Como por definición de ser primo $1 \notin \mathfrak{p}$ temos que $V((1)) = \emptyset$.

2. Sexa $\mathfrak{p} \in X$. Por unha banda temos que $E \subseteq \mathfrak{a}$. Se $\mathfrak{a} \subseteq \mathfrak{p}$ para algún $\mathfrak{p}$ temos que $E \subseteq \mathfrak{p}$ e polo tanto $V(E) = V(\mathfrak{a})$. Así supoñamos que $E \subseteq \mathfrak{p}$, entón tense que $\mathfrak{a} = AE \subseteq A\mathfrak{p} = \mathfrak{p}$ e polo tanto tamén comparten ao primo, ou sexa, $V(E) = V(\mathfrak{a})$.

3. Dado un $\mathfrak{p} \in V(\cup_{i\in I}E_i)$ temos pola definición da aplicación V que $\cup_{i\in I}E_i \subset \mathfrak{p}$. Se está a unión necesariamente estará cada elemento, ou sexa, $E_i \subset \mathfrak{p}$ $\forall i \in I$. Tomando de novo a aplicación V obtemos que $\mathfrak{p} \in V(E_i)$ $\forall i \in I$, é dicir $\mathfrak{p} \in \cap_{i\in I}V(E_i)$. E polo tanto obtemos que $\mathfrak{p} \in \cap_{i\in I}V(E_i)$ se, e só se, $\mathfrak{p} \in V(\cup_{i\in I}E_i)$.

4. - Por un lado supoñamos que $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ pero $\mathfrak{b} \nsubseteq \mathfrak{p}$. Entón está claro que existe un $b \in \mathfrak{b} - \mathfrak{p}$ tal que $ab \in \mathfrak{p}$ para un $a \in \mathfrak{a}$. Pola primalidade de $\mathfrak{p}$ teremos que $a \in \mathfrak{p}$ e polo tanto $\mathfrak{a} \subseteq \mathfrak{p}$. Así se $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ acabamos de ver que $\mathfrak{a} \subseteq \mathfrak{p}$ ou $\mathfrak{b} \subseteq \mathfrak{p}$ entón $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$. Así $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$.

  Por outro lado temos que se $\mathfrak{p}$ contén a $\mathfrak{a}$ ou a $\mathfrak{b}$ necesariamente conterá a $\mathfrak{a}\mathfrak{b}$ e, polo tanto, $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq \mathfrak{p}$. Así $V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$.

- Por unha banda $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ se $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$ entón $V(\mathfrak{ab}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$.

  Por outra banda se $\mathfrak{ab} \subseteq \mathfrak{p}$ xa vimos antes que ou $\mathfrak{a} \subseteq \mathfrak{p}$ ou $\mathfrak{b} \subseteq \mathfrak{p}$ entón $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$ e así $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{ab})$.

□

Os conxuntos $V(E)$ satisfan os axiomas dos conxuntos pehados nun espazo topolóxico. Á topoloxía resultante chamarémoslle *topoloxía de Zariski* e ao espazo topolóxico X denotarémolo por $Spec(A)$ e será o *espectro primo de A*. Se nos fixamos, este espazo construíuse a partir dos seus pechados, entón podemos indagar sobre quen son os seus abertos. Pola definición de aberto como o complementario dun pechado nun espazo topolóxico arbitrario obtemos a seguinte definición para o caso dun ideal xerado por un elemento:

Definición 1.22. Dado un $f \in A$ definimos os *abertos básicos de* $Spec(A)$ e denotaranse como X_f, aos complementarios de $V((f))$ en $Spec(A)$. É fácil verificar que forman unha base da topoloxía de Zariski.

Unha vez que elaboramos os piares básicos do espazo topolóxico imos poder estudar as propiedades topolóxicas ou xerais deste, tal e como podemos observar no seguintes resultados. Antes introducimos unha definición ben coñecida da topoloxía.

Definición 1.23. Dado un espazo topolóxico X diremos que é *compacto* se para todo recubrimento de X por abertos da topoloxía existe un subrecubrimento finito.

Proposición 1.24. *Dado un $f \in A$ e o seu correspondente X_f, cúmprese:*

1. $X_f \cup X_g = X_{fg}$.
2. $X_f = \emptyset$ *se, e só se,* f *é nilpotente.*
3. $X_f = X$ *se, e só se,* f *é unha unidade.*
4. $X_f = X_g$ *se, e só se,* $r((f)) = r((g))$.
5. *Cada subconxunto* X_f *de* X *é compacto.*

Demostración. Vexamos cada un dos puntos:

1. Por (1.21) temos que $X_f \cap X_g = V(f)^c \cap V(g)^c = (V(f) \cup V(g))^c = V(fg)^c = X_{fg}$
2. $X_f = \emptyset$ se e só se $V(f) = X$. Así temos por definición que para todo $\mathfrak{p} \in X$ que $f \in \mathfrak{p}$. Ou sexa, pola caracterización do nilradical, $f \in r(0)$.

3. $X_f = X$ se, e só se, $V(f) = \emptyset$. Así temos por definición que para todo $\mathfrak{p} \in X$ que $f \notin \mathfrak{p}$. Ou sexa, ao non estar f en ningún maximal, $f \in \mathfrak{U}(X)$.

4. Imos probar algo mellor: $X_f = X_g \Leftrightarrow V(g) = V(f) \Leftrightarrow r((f)) = r((g))$. A primeira equivalencia tense debido a que a complementación invirte a orde dos contidos en ambas direccións. Pola proposicion (1.21) temos que $V(f) = V((f))$. Pola caracterización do radical temos que $r(f) = \cap\, V(f)$. Entón vexamos as dúas inclusións:

   - $r(f) \subseteq r(g) \Rightarrow V(g) = V(r(g)) \subseteq V(r(f))$.
   - $r(g) \subseteq r(f) \Rightarrow r(f) = \cap\, V(f) \subseteq \cap\, V(g) = r(g)$.

5. Sexa $\{X_f\}_{f \in E}$ un recubrimento aberto de X_f. Tomando complementarios vemos que $V(E) \subseteq V(f)$. Entón f está no ideal radical xerado por E. Isto implica que existen $\{g_1, ..., g_n\} \in E$, $\{a_1, ..., a_n\} \in A$ e un enteiro m tal que $f^m = \sum_{i=0}^{n} a_i g_i$. Polo tanto $V(g_1, ..., g_n) \subset V(f)$. Tomando de novo complementarios temos que $\{X_{g_i}\}_{i=1}^{n}$ é un subrecubrimento finito de abertos que cubre X_f. De feito se tomamos $f = 1$ obtemos que o noso conxunto X é en consecuencia compacto.

□

Rematamos esta sección e capítulo introducindo un concepto que será de grande importancia en xeometría alxébrica e que xa ten as súas raíces na teoría de ideais.

Definición 1.25. Un espazo topolóxico dise que é *irreducible* se $X \neq \emptyset$ e cada par de conxuntos abertos non baleiros se cortan en X, ou sexa, se cada conxunto non baleiro é denso en X.

Proposición 1.26. *Spec(A) é irreducible se, e só se, o nilradica de A é un ideal primo.*

Demostración.

⇒ Por un lado se *Spec(A)* é irreducible e fg son nilpotentes entón $X_f \cap X_g = X_{fg} = \emptyset$ por (1.24). Entón $X_f = \emptyset$ ou $X_g = \emptyset$, ao ser o espectro irreducible, e en consecuencia f ou g son nilpotentes dando lugar a que o nilradical sexa primo.

⇐ Supoñamos que o nilradical de A é primo. Sexan X_f e X_g dous abertos non baleiros. Entón f e g non son nilpotentes e polo tanto tampouco o será fg. Así $X_f \cap X_g = X_{fg}$ e non baleiro e polo tanto é irreducible.

□

Proposición 1.27. *Sexa X un espazo topolóxico, entón:*

1. *Se Y é un subespazo irreducible de X entón a súa clausura tamén o será.*

2. *Cada subespazo irreducible está nun subespazo maximal irreducible ou compoñente irreducible. O conxunto destes é pechado e recubren X.*

3. *Se A é un anel e $X = Spec(A)$ entón as compoñentes irreducibles de X son os conxuntos pechados $V(\mathfrak{p})$ onde $\mathfrak{p}$ é un ideal primo minimal de A.*

Demostración. Sexa X un espazo topolóxico, entón:

1. Consideremos dous abertos U e V de X tal que $U \cap \overline{Y}$ e $V \cap \overline{Y}$ sexan non baleiros. Pola definición de clausura, $U \cap Y$ e $V \cap Y$ son non baleiros. Como Y é irreducible temos que $(U \cap Y) \cap (V \cap Y)$ é un subespazo aberto non baleiro de $(U \cap \overline{Y}) \cap (V \cap \overline{Y})$. Entón $\overline{Y}$ é irreducible.

2. Se Y é un subespazo irreducible de X imos facer unha demostración clásica empregando o lema de Zorn. Entón sexa así Σ o conxunto dos subespazos irreducibles de X contendo a Y e ordeámolos coa inclusión. Sexa $\{Y_\alpha\}_{\alpha \in \Lambda}$ unha cadea de Σ e consideramos $Z = \cup_{\alpha \in \Lambda} Y_\alpha$ o candidato a cota da cadea ordeada. Vexamos que $Z \in \Sigma$. Sexa $U, V \subset Z$ abertos e non baleiros. Pola definición $U \cap Y_{\alpha_1} \neq \emptyset$ e $V \cap Y_{\alpha_2} \neq \emptyset$ para $\alpha_1, \alpha_2 \in \Lambda$. Sen pérdida de xeralidade asumamos que $\alpha_1 \leq \alpha_2$. Entón coa relación de orde do conxunto temos que $Y_{\alpha_1} \subseteq Y_{\alpha_2}$. Ademais temos que $U \cap Y_{\alpha_2} \neq \emptyset$ e $V \cap Y_{\alpha_2} \neq \emptyset$ e abertos en Y_{α_2}. Entón pola irreducibilidade deste temos que $U \cap V \cap Y_{\alpha_2} \neq \emptyset$. Polo tanto $U \cap V \cap \neq \emptyset$ tendo que Z é irreducible contendo a Y, ou sexa, $Z \in \Sigma$. Como Z é cota superior da cadea e pertence ao conxunto temos, polo lema de Zorn, que Z é irreducible maximal.

   Por último se Y é un subespazo maximal irreducible de X entón ten que ser igual a súa clausura por (1). Anteriormente comprobamos que son subespazos irreducibles de X. Por todo o anterior os subespazos maximais irreducibles cubren X.

3. Sexa $X = Spec(A)$ para algún anel A. Se Y é un espazo pechado irreducible de X entón hai un ideal radical $\mathfrak{a}$ tal que $Y = V(\mathfrak{a})$.Vexamos por contrarecíproco que $\mathfrak{a}$ é primo. Se $f, g \notin \mathfrak{a}$ temos que X_f e X_g intersecan Y, ao ser $\mathfrak{a}$ o seu propio radical. Como Y é irreducible temos que $X_f \cap X_g = X_{fg}$ interseca Y. Entón $fg \notin \mathfrak{a}$ e polo tanto $\mathfrak{a}$ é primo.

   Vexamos a outra implicación. Se $\mathfrak{p}$ é primo, sexa $Y = V(\mathfrak{p})$ e X_f, X_g intersecan a Y. Entón se $f, g \notin \mathfrak{p}$ implica que $fg \notin \mathfrak{p}$. Así $X_f \cap X_g = X_{fg}$ interseca Y e polo tanto é irreducible.

A condición de minimalidade ven da relación de inclusións coa aplicación V. Se $\mathfrak{p}, \mathfrak{q}$ son primos que cumplen $V(\mathfrak{p}) \subseteq V(\mathfrak{q})$ temos que $\mathfrak{q} \subseteq \mathfrak{p}$. Así as compoñentes irreducibles maximais de X son os primos minimais.

□

Se observamos acabamos de definir unha aplicación V entre dous conxuntos parcialmente ordeados: os ideales do anel A e os elementos do especto primo de A, $Spec(A)$. Debido ás propiedades con respecto á relación de orde vai ser natural ver unha conexión de Galois entre ambas estruturas. Así, baixo certas condicións, imos ter que a aplicación V terá unha inversa, I, tal e como observamos no seguinte resultado:

Proposición 1.28. *Sexa A un anel e $Spec(A)$ o seu espectro primo. Dada a relación $a \in \mathfrak{p}$ en $A \times Spec(A)$ vaise inducir as seguintes bixeccións monótonas:*

$$Rad(A) \underset{\mathrm{I}}{\overset{\mathrm{V}}{\rightleftarrows}} \mathcal{F}(Spec(A))$$

Sendo $Rad(A)$ o conxunto dos ideais radicais de A e $\mathcal{F}(Spec(A))$ o conxunto de pechados do espectro primo. Así, dado un $C \in \mathcal{F}(Spec(A))$, definimos $I(C) = \cap_{\mathfrak{p} \in C} \mathfrak{p}$.

1.0.5. Módulos de xeración finita [1][5]

Ao longo desta sección indagamos sobre unha clase particular de módulos xa presentados ao longo do grado. Ao igual que é natural falar de grupos libres e comprender a teoría de grupos en termos de cocientes destes; pódese facer un análogo á teoría de módulos e aneis. Así imos establecer a seguinte definición:

Definición 1.29. Diremos que un A-módulo M é *libre* se M é isomorfo a $\oplus_{i \in I} M_i$ onde cada M_i é isomorfo a A como A-módulo e, polo tanto, son módulos con base.

Estes módulos pódense carácterizar, tendo en conta a presentación de módulos e a noción de módulo libre, co seguinte resultado:

Proposición 1.30. *M é un módulo de xeración finita $\Leftrightarrow$ M é isomorfo a un cociente de A^n con $n \in \mathbb{N}$.*

Os seguintes resultados teñen como obxectivo dar un significado a noción de módulo finitamente xerado.

Proposición 1.31. *Sexa M un A-módulo con xeración finita, sexa $\mathfrak{a}$ un ideal de A e sexa ϕ un endomorfismo de A-módulos tal que $\phi(M) \subseteq \mathfrak{a}M$. Entón o endomorfismo satisfai a seguinte ecuación:*

$$\phi^n + a_1\phi^{n-1} + ... \ + a_n = 0, \quad a_i \in \mathfrak{a}$$

Demostración. Sexan $\{x_1, ..., x_n\}$ un conxunto de xeradores de M. Entón $\phi(x_i) \in \mathfrak{a}M$. Así temos pola pertenza que $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ con $a_{ij} \in \mathfrak{a}$. Como $\phi(x_i) = \sum_{j=1}^n \delta_{ij}\phi x_j = \sum_{j=1}^n a_{ij}x_j$ temos que $\sum_{j=1}^n(\delta_{ij}\phi - a_{ij})x_j = 0$.

Así denotamos como $\phi_{ij} = \delta_{ij}\phi - a_{ij}$ e a Φ_{ij} ao seu adxunto ou sexa $\Phi_{ij} = adj(\phi_{ij}) = (-1)^{i+j}det(\Delta\phi_{ij})$. Tendo en conta isto reescribimos a derradeira igualdade como segue $\sum_{j=1}^n(\delta_{ij}\phi - a_{ij})x_j = \sum_{j=1}^n \phi_{ij}x_j$. Así multiplicando polo adxunto obtemos $\sum_{j=1}^n \Phi_{ij}\phi_{ij}x_j = 0$. Se desenvolvemos esta suma obtemos o seguinte:

$$\begin{cases} \Phi_{11}\phi_{11}x_1 + ... + \Phi_{n1}\phi_{1n}x_n = 0 \\ \qquad\qquad\qquad ... \\ \Phi_{1n}\phi_{n1}x_1 + ... + \Phi_{nn}\phi_{nn}x_n = 0 \end{cases}$$

Aplicando a regla de Cramer temos que $\Phi_{ij}\phi_{ij} = det(\phi_{ij})I_n$. Obtendo no anterior que $\sum_{j=1}^n det(\phi_{ij})x_j = 0$. En consecuencia $det(\phi_{ij})$ anúlase en cada x_i tendo polo tanto que $det(\phi_{ij}) = 0$. Desenvolvendo o determinante obtemos que $\phi^n + a_1\phi^{n-1} + ... + a_n = 0, \quad a_i \in \mathfrak{a}$ demostrando o resultado. Por último cabe mencionar que o determinante está ben definido pois sempre nos podemos restrinxir a un subanel conmutativo. □

Teorema 1.32 (Lema de Nakayama)**.** *Sexa M un A-módulo con xeración finita e $\mathfrak{a}$ un ideal de A contido no radical de Jacobson $\mathfrak{R}$ de A. Entón se se cumple que $\mathfrak{a}M = M$ temos que $M = 0$.*

Demostración. Supoñamos que $M \neq 0$ e sexa $\{x_1, ..., x_n\}$ un conxunto mínimo de xeradores de M. Por hipótese temos que algún xerador verifica $x_i \in \mathfrak{a}M$. Supoñamos que é x_n e polo tanto pola mera pertenza imos poder escribir o xerador da seguinte forma $x_n = a_1x_1 + ...a_nx_n$ con $a_i \in \mathfrak{a}$. Despexando obtemos que $(1 - a_n)x_n = a_1x_1 + ...a_{n-1}x_{n-1}$. Como $a_n \in \mathfrak{N}$ temos por (1.18) que $1 - a_n$ é unha unidade de A. E polo tanto temos que $x_n = b_1x_1 + ... + b_{n-1}x_{n-1}$ sendo un absurdo co feito de que sexa un conxunto minimal de xeradores. □

Nota 1.33. O lema de Nakayama ven a dicirnos, dende unha perspectiva informal, que os módulos finitamente xerados sobre un anel conmutativo compórtanse, en certa medida, como espazos vectoriais sobre un corpo. De feito, e seguindo con esta interpretación, a proposición (1.31) é unha xeralización do teorema de Cayley-Hamilton de álxebra lineal.

Corolario 1.34. *Dado un A-módulo M con xeración finita, N un submódulo de M e $\mathfrak{a} \subseteq \mathfrak{R}$ un ideal. Entón se $M = \mathfrak{a}M + N$ entón $M = N$.*

Demostración. Aplicamos o lema de Nakayama ao módulo cociente M/N. Así $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N$ temos polo lema que $M = \mathfrak{a}M + N$ implica $0 = \mathfrak{a}M + N$ e polo tanto $M = N$. □

1.0.6. Sucesións exactas

Ata o de agora tan só traballamos con homomorfismos entre dous módulos. Un paso natural é estender esta noción a cadeas de homomorfismos entre un conxunto de módulos. Imos centranos nun tipo particular destas tranformacións en cadea que introducimos coa seguinte definición:

Definición 1.35. Dada unha sucesión de A-módulos e A-homomorfismos:

$$... \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to ...$$

diremos que é unha *sucesión exacta en M_i* se verifica que $Im(f_i) = Ker(f_{i+1})$. Diremos que a sucesión é *exacta* se o é para calquera M_i. Denominaremos unha sucesión exacta corta a unha sucesión da seguinte forma:

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

Nota 1.36. Realmente, podemos reducir o estudo das sucesións exactas ao estudo das sucesións exactas cortas pois cada unha das cadeas largas pode ser expresada como un conxunto de cadeas cortas. Para elo basta centrarse nun M_i e tomar os seguintes módulos intermedios na cadea $N_i = Im(f_i) = Ker(f_{i-1})$.

Como é natural ao introducir un obxecto novo, o seguinte resultado manifesta como se comporta este baixo as transformación propias da estrutura:

Proposición 1.37 (Propiedade de exactitude do Hom)**.** *Verificanse os seguintes resultados:*

- *Sexa*

  $$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

  unha sucesión de A-módulos e homomorfismos. Entón a sucesión é exacta se, e só se, para todos os A-módulos N é exacta a seguinte sucesión:

  $$0 \to Hom(M', N) \xrightarrow{\overline{f}} Hom(M, N) \xrightarrow{\overline{g}} Hom(M'', N)$$

- *Sexa*

$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$$

unha sucesión de A-módulos e homomorfismos. Entón a sucesión é exacta se, e só se, para todos os A-módulos M é exacta a seguinte sucesión:

$$0 \to Hom(M, N') \xrightarrow{\overline{f}} Hom(M, N) \xrightarrow{\overline{g}} Hom(M, N'')$$

1.0.7. Produto tensorial

O produto tensorial é o instrumento adecuado e natural que linealiza as aplicacións multilineais. Esta sentencia formalízase no seguinte resultado para o caso de dous módulos e polo tanto para aplicacións bilineais:

Proposición 1.38 (Propiedade universal do produto tensorial)**.** *Sexan M e N A-módulos. Entón existe un par (T, g) formado por un A-módulo T e un homomorfismo A-bilineal $g : M \times N \to T$ verificando a seguinte propiedade: para calquera A-módulo P e calquera aplicación A-bilineal $f : M \times N \to P$ existe unha única aplicación A-lineal $\overline{f} : T \to P$ tal que fai o seguinte diagrama conmutativo:*

$$\begin{array}{ccc} M \times N & & \\ {\scriptstyle g}\downarrow & \searrow^{f} & \\ T & \xrightarrow[\overline{f}]{} & P \end{array}$$

Ademais se existe outro par $(\overline{T}, \overline{g})$ verificando a propiedade anterior hai un único isomorfismo $j : T \to \overline{T}$ verificando que $j \circ g = \overline{g}$.

Demostración. A idea da demostración é a seguinte: Tomamos un módulo moi xenérico para cocientar polas propiedades que nos interesen que se manifesten. Así sexa $C = A^{M \times N}$ o conxunto de series formais $\sum_{i=1}^{n} a_i(x_i, y_i)$ de $M \times N$ ata A. Agora consideramos as propiedades desexadas representadas polo submódulo D xerado polos seguintes elementos:

$$\begin{cases} (x + w, y) - (x, y) - (w, y) \\ (x, w + y) - (x, w) - (x, y) \\ (ax, y) - a(x, y) \\ (x, ay) - a(x, y) \end{cases}$$

Tomamos así o módulo $T = C/D$. Dado un elemento $(x, y) \in C$ ten como imaxe no cociente un elemento $x \otimes y$. Polas condicións do cociente cumple a linealidade con respecto aos operandos facendo que a aplicación $g : M \times N \to T$ tal que $g(x, y) =: x \otimes y$ sexa A-bilineal. Vexamos que este é o módulo que nos permite factorizar ás aplicacións de $M \times N$ a P. Efectivamente cada homomorfismo de módulos $f : M \times N \to P$ esténdese a un homomorfismo de A-módulos $f : C \to P$. Se impoñemos a condición de A-bilinealidade a f observamos, pola construción do submódulo, que esta se anula en D. Así indúcese un homomorfismo $\overline{f} : T = C/D \to P$ tal que $\overline{f}(x \otimes y) = f(x, y)$. Esta aplicación está ben definida e o par (T, g) verifique as condicións da definición.

A unicidade tense de forma inmediata simplemente supoñendo a existencia doutra factorización e razoando cos homomorfismos obsérvase que efectivamente é a mesma factorización. □

Definición 1.39. Un módulo T que verifica a propiedade anterior recibirá o nome de *produto tensorial de M e N*. Notarémolo como $M \otimes_A N$ ou $M \otimes N$ cando se sobrentende o anel A sobre o que se asenta.

Exemplo 1.40. Ilustremos cun exemplo o uso desta nova construción. Para elo vexamos que $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$, se m e n son coprimos, ou sexa, se $(m, n) = 1$. Efectivamente pola identidade de Bezout, como m e n son coprimos, temos que $ma + nb = 1$ con $a, b \in \mathbb{Z}$. Sexa $x \otimes y \in (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$. Entón $x \otimes y = 1(x \otimes y) = (ma + nb)(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) = 0$.

Realmente esto que espuxemos para aplicacións A-bilineais poderíase estender ao caso xenérico, inicialmente comentado, das A-multilineais de forma análoga. Unha vez introducido o módulo produto tensorial cabe mencionar cal é o seu comportamento co resto de operacións dos módulos. Isto ven recollido no seguinte resultado:

Proposición 1.41. *Sexan M, N e P tres A-módulos. Entón verifícanse os seguintes isomorfismos:*

- $M \otimes N \cong N \otimes M$
- $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$
- $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$
- $A \otimes M \cong M$

O módulo produto tensorial depende do anel sobre o que se asentan as súas compoñentes. O certo é que ata o de agora tan só vimos módulos que dependen operacionalmente dun só anel, mais isto pode xeralizarse. Así introducimos a seguinte definición que nos permitirá relacionar produtos tensoriales asentados sobre distintos aneis:

Definición 1.42. Diremos que un módulo M é un (A, B)-*bimódulo* se é á vez A-módulo e B-módulo sendo ambas estruturas compatibles, ou sexa, $(ax)b = a(xb)$ $\forall a \in A$, $\forall b \in B$ e $\forall x \in N$. Para o caso dos aneis podemos enunciar unha definición semellante mais con entidade propia. Sexa un homomorfismo de aneis $A \to B$, entón diremos que B é unha A-*álxebra* se B é (A, B)-bimódulo.

Proposición 1.43. *Sexa M un A-módulo, P un B-módulo e N un (A, B)-bimódulo. Entón temos que $M \otimes_A N$ é un B-módulo, $N \otimes_A P$ é un A-módulo e ademais verifican o seguinte isomorfismo:*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$$

Demostración. A idea da demostración é considerar aplicacións dende produtos de módulos ata o módulo do noso interese co fin de definir aplicacións A-bilineais e B-bilineais para poder facer, co argumento da demostración da existencia do produto tensorial, un paso a un novo módulo no que substituamos o produto por produto tensorial. Para cada $z \in P$ temos que a aplicación $f_z : M \times N \to M \otimes_A (N \otimes_B P)$ que $f_z(x, y) = x \otimes (y \otimes z)$ é A-bilineal nas dúas primerias variables. Ademais cumple:

- $f_z(ax, y) = ax \otimes (y \otimes z) = a(x \otimes (y \otimes z)) = af_z(x, y)$
- $f_z(x, ay) = x \otimes (ay \otimes z) = x \otimes a(y \otimes z) = a(x \otimes (y \otimes z)) = af_z(x, y)$

Así f_z induce unha aplicación A-lineal $\overline{f_z} : M \otimes_A N \to M \otimes_A (N \otimes_B P)$ tal que $\overline{f_z}(x \otimes y) = x \otimes (y \otimes z)$. Podemos considerar así a seguinte aplicación bi-aditiva $g : (M \otimes N) \times P \to M \otimes_A (N \otimes_B P)$ tal que $g(x \otimes y, z) = \overline{f_z}(x \otimes y)$. Claramente g é A-lineal e B-lineal pois:

- $g((x \otimes y)b, z) = g(x \otimes yb, z) = x \otimes (yb \otimes z) = x \otimes (y \otimes z)b = (x \otimes (y \otimes z))b = g(x \otimes y, z)b$
- $g(x \otimes y, zb) = x \otimes (y \otimes zb) = x \otimes (y \otimes z)b = (x \otimes (y \otimes z))b = g(x \otimes y, z)b$

Pola propiedade universal g dá un (A, B)-homomorfismo lineal $\overline{g} : (M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$ tal que $\overline{g}((x \otimes y) \otimes z) = x \otimes (y \otimes z)$. Por un razoamento análogo podemos dar a aplicación inversa a $\overline{g}$ e demostrando así o isomorfismo. □

Ao mesmo tempo e como resulta obvio as características do módulo van a condicionar como será o seu produto tensorial. Por outra banda o produto tensorial vainos permitir reducir certos módulos máis complexo cara expresións máis depuradas. Neste aspecto imos centrar a nosa atención en dous casos particulares, de ambas casuísticas, dados polos seguintes dous resultados:

Proposición 1.44. *Sexa A un anel local, M e N dous A-módulos de xeración finita. Entón se $M \otimes N = 0$ implica que $M = 0$ ou $N = 0$.*

Demostración. Sexa $\mathfrak{m}$ o ideal maximal de A e consideramos o corpo residual $K = A/\mathfrak{m}$. Definimos os seguintes módulos $M_K = K \otimes_A M$ e $N_K = K \otimes_A N$ que son espazos vectoriais. Vai cumplirse entón que:

$$M_K \otimes N_K = (K \otimes M) \otimes (K \otimes N) = K \otimes (M \otimes N) = (M \otimes N)_K = 0$$

Como a dimensión dos espazo vectoriais é multiplicativa baixo un tensor temos que $M_K = 0$ ou $N_K = 0$. Supoñamos que $M_K = 0$, o outro caso é análogo. Temos que $M_K \cong M/\mathfrak{m}M$ entón $\mathfrak{m}M = M$ e polo lema de Nakayama temos que $M = 0$. Demostrando así a proposición. □

Definición 1.45. Sexa M un A-módulo. Definimos o $A[x]$-módulo de todos os polinomios en x con coeficientes en M, $M[x]$, como aquel módulo que contén expresións da forma $\sum_{i=0}^{r} m_i x^i$ con $m_i \in M$ para todo i.

Proposición 1.46. *Dado un anel A, un A-módulo M e un ideal I de A imos ter que se cumple os seguintes isomorfismos:*

1. $(M/IM) \cong M \otimes_A (A/I)$
2. $M[x] \cong A[x] \otimes_A M$.

Demostración.

1. A demostración deste isomorfismo é rutinario polo que nos restrinximos a demostración do segundo.

2. Definimos un homomorfismo de módulos $f : A[x] \times M \to M[x]$ de tal xeito que $f(\sum_{i=0}^{r} a_i x^i, m) = \sum_{i=0}^{r} (a_i m) x^i$. Claramente é bi-aditiva e A-bilinear e polo tanto induce un homomorfismo $\overline{f} : A[x] \otimes M \to M$ tal que $\overline{f}(\sum_{i=0}^{r} a_i x^i \otimes m) = \sum_{i=0}^{r} (a_i m) x^i$.

   Vexamos que ten un homomorfismo inverso. Consideremos a aplicación $g : M \to A[x] \otimes M$ de tal xeito que $g(\sum_{i=0}^{r} m_i x^i) = \sum_{i=0}^{r} (x^i \otimes m_i)$. É evidente que é $A[x]$-lineal e aditiva, vexamos esto, considerando $p(x) = \sum_{j=0} a_i x^j$:

$$g(p(x)\sum_{i=0}^{r} m_i x^i) = \sum_k \sum_{i+j=k} g(a_i m_j x^k) = \sum_i \sum_j (x^i x^j \otimes a_i m_j) = \sum_j ((\sum_i a_i x^i) x^j \otimes m_j)$$

$$= p(x) g(\sum_{i=0}^{r} m_i x^i)$$

Así a aplicación g está ben definida e é inversa da aplicación $\overline{f}$, demostrando así o resultado.

□

Nota 1.47. Se nos fixamos nas proposicións (1.46) e (1.43) teñen unha estrutura semellante. As dúas básanse en definir de forma interesada aplicacións dende un produto usual de módulos de tal xeito que cumplan a A-bilinealidade e bi-aditividade para posteriormente poder facer uso do teorema de existencia do produto tensorial obtendo unha nova aplicación en termos deste. Con este mesmo razoamento demóstranse as propiedades da proposición (1.41).

Unha vez que construímos o produto tensorial imos centrarnos, de forma breve, nas transformacións do propio obxecto: por unha banda e pola propia construción imos obter o que se denomina como a *propiedade de adxunción*, esta dá unha caracterización dos homomorfismos do produto tensorial en base aos homomorfismos dos módulos que o conforman. Por outra banda, imos adaptar as sucesións exactas a este ámbito. Así obtemos os seguintes resultados:

Proposición 1.48. *Sexa M un A-módulo, P un B-módulo e N un (A,B)-bimódulo. Entón verifícase o seguinte resultado:*

$$Hom_B(M \otimes_A N, P) \cong Hom_A(M, Hom_B(N, P))$$

Demostración. Unha vez comprobada a estrutura dos obxectos que se queren estudar o isomorfismo ven dado pola propia definición do produto tensorial. □

Proposición 1.49 (Propiedade de exactitude do produto tensorial)**.** *Sexa*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

unha sucesión de A-módulos e homomorfismos. Entón dado un A-módulo N calquera terase que a seguinte sucesión é exacta:

$$M' \otimes_A N \xrightarrow{f\otimes 1} M \otimes_A N \xrightarrow{g\otimes 1} M'' \otimes_A N \to 0$$

Demostración. A demostración é directa a partir dos resultados (1.48) e (1.37). □

Exemplo 1.50. Co anterior podemos xeralizar o exemplo de (1.40). Verifícase que $(\mathbb{Z}/m\mathbb{Z})\otimes_{\mathbb{Z}}$ $(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/(m,n)\mathbb{Z}$. Pra elo consideremos a seguinte sucesión exacta:

$$m\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

tensorizámola por $\mathbb{Z}/n\mathbb{Z}$, e por (1.49) temos que a seguinte sucesión é exacta :

$$m\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n \to (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \to 0$$

Polas propiedades de grupos cíclicos temos que $\mathbb{Z}/(m,n)\mathbb{Z} \cong m\mathbb{Z}/n$ e polas propiedades das sucesións exactas $m\mathbb{Z}/n \cong (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$.

Capítulo 2

Aneis e módulos noetherianos

2.0.1. Introdución

A partir deste capítulo imos restrinxir a nosa mirada a un conxunto de aneis e módulos que posúen propiedades de finitude: os aneis e módulos noetherianos. Estudaremos as súas propiedades e o seu bo comportamento con respecto a algunhas das operacións xa introducidas. Ademais, aquela condición vai ser decisiva para garantir certas descomposicións das estruturas, por exemplo, a existencia e unicidade de descomposicións primarias. Veremos ao mesmo tempo o teorema da base de Hilbert que permitirá traducir o anterior a unha linguaxe máis xeométrica, vendo así un canle entre a álxebra conmutativa e a xeometría alxébrica . Ao mesmo tempo, estenderemos esta noción a aspectos topolóxicos para completar así a nosa visión do visto no capítulo anterior.

2.0.2. Condicións de cadea. Aneis e módulos noetherianos

Así consideramos como Σ o conxunto de submódulos dun módulo M ordeados pola relación de orde "$\subseteq$".

Definición 2.1. Diremos que un A-módulo M é *noetheriano* se cumple a condición de cadea ascendente para o conxunto Σ. É dicir, cada secuencia crecente $N_1 \subset N_2 \subset ...$ en Σ é estacionaria. Ou sexa, $\exists\ k \in \mathbb{N}$ tal que a cadea se estabiliza, é dicir, $N_n = N_{n+1}\ \forall\ n > k$.

Definición 2.2. Diremos que un A-módulo M é *artiniano* se cumple a condición de cadea descendente para o conxunto Σ. É dicir, cada secuencia decrecente $N_1 \supset N_2 \supset ...$ en Σ é estacionaria. Ou sexa, $\exists\ k \in \mathbb{N}$ tal que a cadea se estabiliza, é dicir, $N_n = N_{n+1}\ \forall\ n > k$.

Ao mesmo tempo, e como indicamos no capítulo anterior, a condición de cadea ascendente (respectivamente descendente) pode enunciarse do seguinte xeito:

Proposición 2.3. *Sexa M un A-módulo e Σ o conxunto de submódulos deste. Entón equivalen:*

- *M é noetheriano (respectivamente artiniano).*
- *Cada subconxunto non baleiro de Σ ten un elemento maximal (respectivamente minimal).*

Nota 2.4. Está claro, por ser un caso particular, que esta construción se pode restrinxir a un anel A e aos seus subconxuntos de ideais.

Exemplo 2.5. Debido a súa importancia na xeometría alxébrica, o exemplo máis destacado de anel noetheriano, que demostraremos posteriormente, é o anel $k[x]$, sendo k un corpo. Sen embargo, o anel $k[x_1, x_2...]$ non cumple a condición de cadea ascendente. Isto toma sentido no feito de que estamos esixindo unha condición de finitude a un anel con infinitos xeradores.

Tal e como dictamos nun inicio, estas restriccións sobre os aneis agregan unha noción de finitude con respecto os seus subespazos que se materializa no seguinte resultado:

Proposición 2.6. *M é un A-módulo noetheriano se, e só se, cada submódulo de M é de xeración finita.*

Demostración.

$\Rightarrow$ Sexa N un submódulo de M e consideremos o conxunto de submódulos con xeración finita de N, Σ. Como $0 \in \Sigma$ temos que $\Sigma \neq \emptyset$ e polo tanto ten un elemento maximal V. Se $V = N$ temos que N é de xeración finita. Entón consideramos que $V \neq N$, vexamos que chegamos a unha contradición. Consideramos o submódulo $V + Ax$ con $x \in N$. Como $x \notin V$ temos que $V \subset V + Ax$ e ademais este último é de xeración finita o que contradí a maximalidade de V en Σ.

$\Leftarrow$ Consideremos unha cadea ascendente de submódulos $N_1 \subseteq N_2 \subset ...$ de M. Entón $N = \cup_{n=1}^{\infty} N_n$ é un submódulo de M e polo tanto, por hipótese temos que é de xeración finita. Consideremos un sitema de xeradores $\{x_1, ..., x_s\}$. Necesariamente algun xerador vai poder econtrarse nun dos sucesivos elos da cadea Entón se $x_i \in N_{n_i}$, para un submódulo selecionado da cadea, consideramos o maior desta selección $n = \text{máx}_{i=1}^{r} n_i$. Este conterá, por construción, a todos os xeradores polo que $N_n = M$ e a cadea e polo tanto estacionaria.

□

Como consecuencia deste resultado os aneis e módulos noetherianos van tomar un maior peso que os artinianos. Pese a que ambos den condicións de finitude, ser noetheriano dá unha información máis completa. De feito, no caso de aneis, a condición de cadea descendente implica a condición de cadea ascendente, ou sexa, ser un anel artiniano implica ser noetheriano. O recíproco non é certo e basta considerar $\mathbb{Z}$ como $\mathbb{Z}$-módulo para ter un contraexemplo sinxelo. Por iso, a partir de agora tan só nos referiremos ás propiedades dos noetherianos. Os seguintes resultados reflicten como se transmite esta finitude as sucesións exactas de módulos e a suma directa destes:

Proposición 2.7. *Sexa* $0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$ *unha sucesión exacta de* A*-módulos entón* N *é noetheriano se, e só se,* N' *e* N'' *son noetherianos.*

Demostración.

$\Rightarrow$ Tomamos unha cadea en N', para N'' é análogo. Pola construción da sucesión exacta inducimos coa aplicación f a cadea en N. Como este é noetheriano a cadea será estacionaria e polo tanto tamén a será a orixinal. É dicir, N' é noetheriano.

$\Leftarrow$ Consideramos unha cadea ascendente $\{U_n\}_{n\in\mathbb{N}}$ de submódulos de N. Facemos o seguinte razoamento para N' sendo o caso de N'' análogo. Temos que a cadea $\{f^-(U_n)\}_{n\in\mathbb{N}}$ é estacionaria para un certo $m \in \mathbb{N}$. Se tomamos de novo o homomorfismo obtemos que a cadea é estacionaria en N sendo, polo tanto, noetheriano.

□

Corolario 2.8. *Se* N_i*, con* $1 \leq i \leq n$ *son* A*-módulos noetherianos entón* $\oplus_{i=1}^n N_i$ *tamén é noetheriano.*

Pese a que comezamos construíndo os módulos noetherianos e definimos como un caso particular os aneis noetherianos. Tamén poderíamos construir os aneis noetherianos primeiro e posteriormente asentar sobre estes módulos con propiedades de finitude. Así o módulo herdará a condición noetheriana tal e como indica a seguinte proposición.

Proposición 2.9. *Sexa* A *un anel noetheriano e* M *un* A*-módulo de xeración finita entón* M *é noetheriano.*

Demostración. Ao ser M de xeración finita sabemos que este é un cociente de A^n. Como $A^n = \oplus_{i=1}^n A$ temos que é noetheriano ao ser A noetheriano. Ao ser $M \cong A^n/\mathfrak{a}$ para un certo ideal $\mathfrak{a}$ podemos construír unha sucesión exacta tendo por (2.7) que M é noetheriano. □

Corolario 2.10. *Sexa* A *un subanel de* B*, sendo* B *de xeración finita como* A*-módulo. Se* A *é noetheriano entón* B *é noetheriano.*

Como sempre, é importante saber cando certa propiedade pasa ao cociente. Neste caso temos o seguinte resultado que nos permitirá, como consecuencia, ver que a propiedade de ser noetheriano se transmite baixo homomorfismos:

Proposición 2.11. *Sexa A un anel noetheriano e $\mathfrak{a}$ un ideal de A entón $A/\mathfrak{a}$ é noetheriano.*

Demostración. Como en (2.9) tan só fai faia construír unha sucesión exacta para concluír con (2.7). Sexa entón $0 \to \mathfrak{a} \xrightarrow{f} A \xrightarrow{g} A/\mathfrak{a} \to 0$ como $\mathfrak{a}$ e A son noetherianos temos que $A/\mathfrak{a}$ tamén o será como A-módulo. Polo tanto tamén o será como $A/\mathfrak{a}$-módulo. □

Corolario 2.12. *Sexan A e B dous aneis e $f : A \to B$ un homomorfismo de aneis. Entón se A é noetheriano temos que $Im(f)$ é noetheriano.*

Cabe mencionar, por útimo, que se nos esiximos certas condicións de finitude sobre certos ideais básicos imos ter de forma inmediata a condición de ser noetheriano. É dicir, un anel no que cada ideal primo é de xeración finita vai implicar que este anel é necesariamente noetheriano. Isto obtense como consecuencia do seguinte resultado:

Proposición 2.13. *Sexa A un anel non noetheriano e sexa Σ o conxunto de ideais de A que non son de xeración finita. Imos ter que Σ ten elementos maximais e que estes son ideais primos.*

Demostración. Sabemos que Σ ten elementos maximais polo lema de Zorn. Imos proceder por reducción ao absurdo. Dado un maximal $\mathfrak{a}$ de Σ asumamos que existen $x, y \notin \mathfrak{a}$ pero que sen embargo $xy \in \mathfrak{a}$. Definimos o ideal $\mathfrak{b} = \mathfrak{a} + (x)$ que contén estritamente a $\mathfrak{a}$ e, debido a maximalidade deste, non pertence a Σ sendo, polo tanto, finitamente xerado. Sexa entón $\mathfrak{b} = \mathfrak{a}_0 + (x)$ onde $\mathfrak{a}_0$ é finitamente xerado. Imos ver que $\mathfrak{a}$ é finitamente xerado para obter así a contradición. Imos demostrar que $\mathfrak{a} = \mathfrak{a}_0 + x(\mathfrak{a} : x)$. Claramente $\mathfrak{a}_0 + x(\mathfrak{a} : x) \subset \mathfrak{a}$. Vexamos a outra inclusión. Dado un $a \in \mathfrak{a}$ temos que $a + xt \in \mathfrak{a}_0 + (x)$ para todo $t \in A$. Pero entón hai un $a_0 \in \mathfrak{a}_0$ e un $k \in A$ tal que $a = a_0 + x(k - t)$. Tendo que $x(k - t) \in \mathfrak{a}$ e así $k - t \in (\mathfrak{a} : x)$ e demostrando a igualdade. Como $(\mathfrak{a} : x)$ contén estritamente a $\mathfrak{a}$ temos, por un razoamento exposto antes, que é finitamente xerado. Como $\mathfrak{a}$ é suma de finitamente xerados debe ser necesariamente finitamente xerado obtendo unha contradición. Polo tanto dado $xy \in \mathfrak{a}$ necesariamente $x \in \mathfrak{a}$ ou $y \in \mathfrak{a}$ sendo polo tanto primo. □

Corolario 2.14. *Se A é un anel no que todo ideal primo $\mathfrak{p}$ é finitamente xerado entón A é noetheriano.*

2.0.3. Teorema da base de Hilbert

Unha das cararcterísticas máis interesantes dos aneis noetheriano é que conseguen transmitir a noción finitude cara conxuntos que aparentemente semellan máis complexos. Este é o caso do anel de polinomios sobre un conxunto. Así obtemos o seguinte resultado:

Teorema 2.15 (da base de Hilbert)**.** *Se M é un A-módulo noetheriano entón $M[x]$ é un $A[x]$-módulo noetheriano.*

Demostración. Estendemos a módulos a demostración de [5]. Sexa N un submódulo de $M[x]$ e supoñamos que non é finitamente xerado. Consideramos $f_1 \in N$ de grado mínimo. Procedemos por inducción e consideramos un $f_k \in N/ < f_1, ..., f_k >$. Sexa $f_k = m_k x^{n_k} + m_{k-1}x^{n_{k-1}} + ...$ con $m_k \neq 0$. Tense que $n_1 \leq n_2 \leq ...$. Ao ser M noetheriano como A-módulo terase que $< m_1, ..., m_k >=< m_1, ..., m_{k+1} >$ e temos que $m_{k+1} = \sum_{i=1}^{k} a_i m_i$, con $a_k \in A$. Basta considerar o polinomio $g := f_{k+1} - \sum_{i=1}^{k} a_i x^{n_{k+1}-n_i} f_i \in N/ < f_1, ..., f_k >$ para chegar a unha contradición ao ser de grado menor ou igual que f_{k+1}. □

Corolario 2.16.

1. *Se A é noetheriano entón $A[x_1, ..., x_n]$ é noetheriano. Ademais se B é unha A-álxebra de xeración finita entón B é un anel noetheriano.*

2. *Sexa M un A-módulo noetheriano e B unha A-álxebra de tipo finito entón terase que $M \otimes_A B$ é un B-módulo noetheriano.*

Demostración.

1. Inmediato de (2.15) e (2.11).

2. Como B é unha A-álxebra teremos que $B = A[x_1, ..., x_n]/I$. Así por (1.46) terase que: $M \otimes_A B = M \otimes_A A[x_1, ..., x_n]/I = (M \otimes_A A[x_1, ..., x_n])/I(M \otimes_A A[x_1, ..., x_n])$ é dicir que $M \otimes_A B = M[x_1, ..., x_n]/IM[x_1, ..., x_n]$. Polo tanto $M \otimes_A B$ é $A[x_1, ..., x_n]$-módulo noetheriano por (2.15) e así será B-módulo noetheriano.

□

Nota 2.17. Este resultado vai ser de gran importancia en xeometría alxébrica. Os ideais dos aneis de polinomios están en correspondencia coas variedades afíns dun espazo dadas por aqueles puntos que anulan aos polinomios que xeran devanditos ideais. Esta relación vai ser un caso particular de conexión de Galois ao igual que a observada en (1.28). Neste contexto, o teorema da base de Hilbert adquire un matiz máis comprensivo pois o que nos di é que toda variedade pode ser vista como a intersección dun número finito de ceros de polinomios.

2.0.4. Espazos topolóxicos noetherianos[1][5]

Ao longo desta sección imos continuar desenvolvendo conceptos topolóxicos con respecto ás estruturas e propiedades introducidas. Imos logo adaptar a noción de ser noetheriano aos espazos topolóxicos e ver que consecuencias ten con respecto ás propiedades topolóxicas do espazo.

Definición 2.18. Sexa X un espazo topolóxico, diremos que é *noetheriano* se cumple a condición de cadea ascendente para os subespazos abertos. Equivalentemente, se cumplen a condición maximal.

Como os espazos pechados son complementarios dos abertos podemos enunciar a definición da seguinte forma: un espazo topolóxico X dise *noetheriano* se cumple a condición de cadea descendente para os subespazos pechados, ou equivalentemente, se cumple a condición minimal. Vexamos agora que consecuencias ten esta condición sobre as propiedades topolóxicas do espazo:

Proposición 2.19. *Se X é noetheriano entón é compacto e cada subespazo del é noetheriano.*

Demostración. Vexamos que se X é noetheriano entón $Y \subseteq X$ é noetheriano. Sexa $Y \subseteq X$ un subespazo. En Y os abertos relativos son a intersección con este dos abertos de X. Así consideramos $\{U_n\}_{n\in\mathbb{N}}$ unha cadea ascendente de Y. Sexan agora en X os conxuntos V_n que verifican $U_n = V_n \cap Y$. Como X é noetheriano existe un N tal que $V_n = V_{n+1}$ para $n > N$. Por construción imos ter que $U_n = U_{n+1}$ para $n > N$ e polo tanto Y cumple a condición de cadea ascendente para os seus subespazos, ou sexa, $Y \subseteq X$ é noetheriano.

Vexamos agora que X é compacto. Sexa $\mathfrak{U}$ un recubrimento de X e Σ a coleción de unións finitas de elementos de $\mathfrak{U}$. Pola condición maximal, Σ ten un elemento maximal V. Vexamos que V cubre todo o espazo X. Supoñamos o contrario. Sexa $x \in X - V$ entón existe un $U \in \mathfrak{U}$ tal que $x \in U$. Pero como $\mathfrak{U}$ é un recubrimento aberto temos que $U \cup V \in \mathfrak{U}$ o que contradí a maximalidade de V. Así $V = X$ e temos que X é compacto. □

Proposición 2.20. *Sexa X un espazo topolóxico, entón equivale:*

1. *X é noetheriano.*
2. *Cada subespazo aberto de X é compacto.*
3. *Cada subespazo de X é compacto*

Demostración.

(1) $\Longrightarrow$ (3) Se X é noetheriano, temos que para un subespazo $Y \subseteq X$ tamén é noetheriano e compacto por (2.19).

(2) $\Longrightarrow$ (1) Sexa $U_1 \subseteq U_2 \subseteq ...$ unha cadea ascendente de subespazos abertos de X. Tomamos $U = \cup_{n\in\mathbb{N}} U_n$. U é un subespazo aberto e por hipótese é compacto. Logo U é unión finita de $\{U_{n_1}, ..., U_{n_m}\}$. Tomamos $n = \max_j n_j$ así, debido a que os U_j satsifan unha condición de cadea e recubren U, temos que $U = U_N$ para todo $N > n$, ou sexa, X é noetheriano.

□

A propiedade de ser noetheriano engade un concepto de finitude á estrutura da que falamos con respecto aos seus subespazos. De aí a que se cumpla a propiedade anterior. Ademais, esta finitude vai permitir unha descomposición deste en compoñentes irreducibles.

Proposición 2.21. *Se un espazo topolóxico X é noetheriano entón X é unión finita de subespazos pechados irreducibles.*

Demostración. Sabemos que os espazos maximais irreducibles $\{Y_i\}_i$ son pechados e cubren X por (1.27). Poden ocorrer dous casos:

1. $\cap_{i\in I} Y_i = \emptyset$. Entón o conxunto $\{X - Y_i\}_{i\in I}$ é un recubrimento aberto de X. Entón por (2.20) existe un subrecubrimento finito por ser o conxunto compacto. Así obtemos que X é unión de subespazos pechados maximais irreducibles.

2. $\cap_{i\in I} Y_i \neq \emptyset$. Entón existe un elemento de $x \in X$ que está na intersección. Terase que calquer entorno de calquera punto de X intersecará cun entorno de x. Obtendo que $X = \overline{\{x\}}$ e polo tanto X ten tan só un subespazo pechado irreducible.

   Así deducimos que o conxunto das compoñentes irreducibles dun espazo noetheriano son sempre finitas.

□

Nota 2.22. Como todo pechado irreducible está nun pechado maximal e como temos unha cantidade finita destes obtemos, de forma inmediata, que o número de compoñentes irreducibles é finita.

Por último tan só queda por observar que a noción de noetheriano no sentido topolóxico se traslada ao espectro primo. Xa vimos que este xoga un papel importante a hora de definir a topoloxía a partir das operacións propias de A, logo vai ser interesante que tamén posúa certas condicións de finitude. Así temos o seguinte resultado:

Proposición 2.23. *Se A é un anel noetheriano entón $Spec(A)$ é un espazo topolóxico noetheriano.*

Demostración. Todo subconxunto pechado de $Spec(A)$ é da forma $V(\mathfrak{a})$ para algún ideal radical $\mathfrak{a}$ de A. Sexa $\{V(\mathfrak{a}_j)\}_{j\in\mathbb{N}}$ unha cadea descendete de pechados de $Spec(A)$. Como $V(\mathfrak{a}_{j+1}) \subseteq V(\mathfrak{a}_j)$ temos que $\mathfrak{a}_j \subseteq \mathfrak{a}_{j+1}$. Como A é noetheriano para un certo N temos que $\mathfrak{a}_n = \mathfrak{a}_{n+1}$ con $n > N$ e polo tanto polas propiedades de V temos que $V(\mathfrak{a}_{n+1}) = V(\mathfrak{a}_n)$. É dicir, $Spec(A)$ é noetheriano. □

Nota 2.24. O recíproco da propoposición anterior non é certo. Sexa K un corpo e $A = K[x_1, x_2, ...]$ o anel de polinomios. Tomamos o ideal $\mathfrak{c} = (x_1, x_2^2, x_3^3, ...)$ para construír o anel $C = A/\mathfrak{c} = K[\overline{x}_1, \overline{x}_2, ...]$. Así temos que o ideal $\mathfrak{m} = (\overline{x}_1, \overline{x}_2, ...)$ é maximal, pois $C/\mathfrak{m} = K$, e vexamos que é o único primo. Sexa entón un primo $\mathfrak{p}$ de C. Como $\overline{x}_n^n = 0$ teremos que $\overline{x}_n \in \mathfrak{p}$ $\forall n$, ou sexa, $\mathfrak{m} = \mathfrak{p}$ e, polo tanto, $Spec(C) = \{\mathfrak{m}\}$ é noetheriano. Pero C non é noetheriano polo contrarecíproco de (2.11).

O máximo que podemos afirmar do recíproco é o seguinte resultado que involucra os ideais relacionados co espectro primo: os ideais primos.

Proposición 2.25. *$Spec(A)$ é un espazo topolóxico noetheriano para un anel A se, e só se, os ideais radicais deste satisfán a condición de cadea ascendente. En particular, $(Spec(A), \subset)$ cumple a condición de cadea ascendente.*

Demostración. A demostración deste resultado é un feito inmediato de (1.28). □

Corolario 2.26. *O conxunto de ideais primos minimais nun anel noetheriano é finito.*

Demostración. Sexa A un anel noetheriano. Por (2.23) X é un espazo noetheriano e por (2.21) teremos que X ten un conxunto finito de compoñentes irreducibles. Por (1.27) as compoñentes irreducibles de $X = Spec(A)$ son os conxuntos pechados de $V(\mathfrak{p})$ con $\mathfrak{p}$ un primo minimal. Polo tanto hai unha cantidade finita de primos minimales. □

Nota 2.27. Apoiándonos na nota (2.17) pódese dar unha intuición xeométrica máis asequible que a aritmética sobre as noción topolóxicas introducidas ao longo do capítulo 1 e 2. Se consideramos o anel $K[x_1, ..., x_n]$, con K corpo, os pechados de Zariski veñen a simbolizar o conxunto de variedades alxébricas que acollen un determinado espazo. De aí a que resulte que os complementarios destes con respecto ao espazo gocen de propiedades como a densidade. Ao mesmo tempo, os pechados irreducibles simbolizarán o conxunto mínimo de variedades que conforman un pechado de Zariski. A noetherianidade simplemente manifestará que toda concatenación inclusiva de variedades se estabiliza nunha variedade con caracter minimal.

Rematamos a sección e o capítulo comprobando como se transmite a noetherianidade topolóxica baixo certo tipo de transformacións e dependencias entre dous aneis. Isto móstrase no seguinte resultado:

Proposición 2.28. *Sexa $f : A \to B$ unha A-álxebra de tipo finito e a aplicación continua $f^* : Spec(B) \to Spec(A)$, con $f^*(\mathfrak{p}) = f^{-1}(\mathfrak{p}) = \mathfrak{p}^{\mathfrak{c}}$. Entón as fibras de f^* son espacios topolóxicos noetherianos.*

Demostración. Sexa $\mathfrak{p} \in Spec(A)$. Terase que $(f^*)^{-1}(\mathfrak{p}) = V(\mathfrak{p}B) \cong Spec(K(\mathfrak{p}) \otimes_A B)$ por (.29) onde $K(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = K(A/\mathfrak{p})$ é o corpo de fraccións de $A/\mathfrak{p}$ que denota o campo residual de $\mathfrak{p}$. Pero por (2.16) sabemos que $K(\mathfrak{p}) \otimes_A B$ é noetheriano ao ser unha $K(\mathfrak{p})$-álxebra de tipo finito. O resultado obtense aplicando (2.23).

□

Capítulo 3

Descomposición primaria

3.0.1. Introdución

Ao longo deste capítulo desenvolveremos o tema principal: a descomposición primaria. Un pilar fundamental tanto da xeometría alxébrica como da teoría de números. No noso estudo imos abordala dende este derradeiro marco teórico mencionado (de aí a que comecemos con moitas analoxías á factorización de números enteiros). Recordemos que o concepto de factorización é moi importante en álxebra debido á clasificación que esta nos dá dos elementos dun conxunto, no noso caso dos ideais deste. Non sempre podemos asegurar a súa existencia e, de ser certa esta, tamén non sempre teremos a unicidade. Para ver esto último basta considerar o exemplo $\mathbb{Z}[i\sqrt{5}]$ que non é un dominio de ideais principais pero hai factorización única de ideais. Sen embargo existen certos conxuntos operacionais con boas propiedades de segregación interna que nos permitirán asentar devanditas existencias e unicidades. Estes aneis serán os noetherianos, xa desenvolvemos no capítulo anterior, e o teorema que garantirá a existencia e unicidade de factorización de ideais nestes aneis será o teorema de Lasker-Noether.

O noso obxectivo é en primeiro lugar facer unha análise do concepto de descomposición primaria en aneis máis xenéricos para chegar aos dous teoremas de unicidade. Depois restrinxiremos a nosa mirada ao caso particular de aneis noetherianos. Cabe mencionar que ao longo deste capítulo farase referencia e uso dos conceptos do apéndice A sobre aneis de fraccións.

3.0.2. Descomposición primaria [1]

Ao longo do primer capítulo introducimos o concepto de ideal primo. Os cales, como xa sabemos, xeralizan aos números primos. Como o que buscamos é unha xeralización da factorización dun número por ideais primos debemos introducir a xeralización do concepto

potencia de primo. Comezamos entón cunha definición:

Definición 3.1. Dado un anel A decimos que un ideal $\mathfrak{q} \subsetneq A$ é *primario* se dado $xy \in \mathfrak{q}$ tense que ou $x \in \mathfrak{q}$ ou $y^n \in \mathfrak{q}$ para algún $n \in \mathbb{N}$.

Cabe notar que este concepto ten unha connotación semellante que a de número primo, pola propia caracterización. De feito todo ideal primo é primario. Polo tanto é natural, ao igual que o que ocorría con ideias primos e maximais, que tamén se traspase ao cociente propiedades interesantes tal e como observamos no seguinte resultado:

Proposición 3.2. *Dado un anel A dicimos que un ideal $\mathfrak{q} \subsetneq A$ é primario se, e só se, cada divisor de cero é nilpotente en $A/\mathfrak{q}$.*

Ao longo deste traballo destacamos a importancia dos ideais primos na descripción dos conxuntos operacionais dos aneis. Neste caso non temos unha descrición directa do ideal primario mais sí dun ideal que se lle achega, ou sexa, imos telo do seu ideal radical. Xorde así a seguinte proposición:

Proposición 3.3. *Dado un anel A e un ideal $\mathfrak{q} \subsetneq A$ primario temos que $r(\mathfrak{q})$ é primo e, así, o menor ideal primo que contén a $\mathfrak{q}$.*

Demostración. Vexamos primeiro que $\mathfrak{p} = r(\mathfrak{q})$ é un ideal primo. Tomamos un produto no ideal e vemos que unha das dúas compoñentes está nel. Así se $xy \in r(\mathfrak{q})$ teremos, pola definición de radical, $(xy)^m \in \mathfrak{q}$ para certo enteiro m. Pola definición de ideal primario temos que $x^m \in \mathfrak{q}$ ou $y^{nm} \in \mathfrak{q}$. De novo, pola defincón de radical, temos que $x \in r(\mathfrak{q})$ ou $y \in \mathfrak{q}$. A minimalidade ven pola caracterización do radical como a intersección de todos os primos que conteñen ao ideal. □

Imos restrinxir a nosa mirada a un conxunto particular de ideais primarios. Estes, ao igual que expuxemos no capítulo 1, van ter a característica de ser primos e polo tanto van ser os ideais adecuados á hora de realizar a descomposicón primaria dun ideal.

Definición 3.4. Dado un anel A e un ideal primario $\mathfrak{q}$ diremos que é un ideal $\mathfrak{p}$-*primario* se verifica que $r(\mathfrak{q}) = \mathfrak{p}$ para un certo ideal primo $\mathfrak{p}$ de A.

Exemplo 3.5. Non sempre vai ocorrer esa equivalencia aparente entre primarios e potencias de primos que se ten en $\mathbb{Z}$ tal e como se observan nos seguintes exemplos:

- Un ideal primario non é sempre potencia dun primo. Tomamos $K[x,y]/\mathfrak{q} \cong k[x]/(x^2)$ con $\mathfrak{q} = (x^2, y)$ e K un corpo. Así temos que $\mathfrak{q}$ é primario pero o seu radical é $r(\mathfrak{q}) = \mathfrak{p} = (x, y)$ tendo polo tanto $\mathfrak{p}^2 \subset \mathfrak{q} \subset \mathfrak{p}$.

- Unha potencia dun ideal primo non é necesariamente un ideal primario aínda que o radical da potencia sexa o primo. Para este contraexemplo, tomemos $K[x,y]/(x^2y)$ onde K é un corpo e tomemos o ideal primo $\mathfrak{p} = (\overline{x})$. Tense que $\mathfrak{p}^3 = (\overline{x}^3)$ non é primario.

Aínda que unha potencia dun primo non é necesariamente un ideal primario, e viceversa, o seguinte resultado danos unha situación na que si se cumple:

Proposición 3.6. *Se $r(\mathfrak{a})$ é maximal entón $\mathfrak{a}$ é un ideal primario.*

Demostración. Sexa $\mathfrak{a}$ un ideal tal que $r(\mathfrak{a}) = \mathfrak{m}$ para algún ideal maximal $\mathfrak{m}$. A imaxe de $\mathfrak{m}$ no cociente $A/\mathfrak{m}$ é o nilradical deste anel tendo este tan só un ideal primo que será maximal. Notemos que só hai un primo pola caracterización do racical e a noción de maximalidade (se houbera outro ideal significaría necesariamente que contén ao ideal cero e polo tanto o ideal maximal en A estaría contido noutro ideal). Así cada elemento do cociente será, polo tanto, unha unidade ou nilpotente e así cada divisor de cero será nilpotente. □

Corolario 3.7. *As potencias dun ideal maximal $\mathfrak{m}$ son $\mathfrak{m}$-primarias.*

Unha vez introducidos os conceptos básicos o que imos buscar é a descomposición dun ideal $\mathfrak{a} \subset A$ a partir da intersección dos ideais primarios, ao igual que no teorema fundamental da aritmética. Como resulta natural, unha vez construído o obxecto, imos centrarnos no seu comportamento con respecto a certas operacións. Por unha banda vainos interesar o feito de que un ideal primario con radical primo se transmita coa intersección, pois vai ser a clave na descomposición primaria do ideal. Así tense:

Lema 3.8. *Se $\mathfrak{q}_i$ con $i \in \{1, \dots n\}$ son $\mathfrak{p}$-primarios entón $\mathfrak{q} = \cap_{i=1}^n \mathfrak{q}_i$ é $\mathfrak{p}$-primario.*

Demostración. Tomamos $\mathfrak{q} = \cap_{i=1}^n \mathfrak{q}_i$. Polas propiedades do radical temos que $r(\mathfrak{q}) = r(\cap_{i=1}^n \mathfrak{q}_i) = \cap_{i=1}^n r(\mathfrak{q}_i) = \mathfrak{p}$. Vexamos que $\mathfrak{q}$ é $\mathfrak{p}$-primario. Tomamos $xy \in \mathfrak{q}$ con $y \notin \mathfrak{q}$. Para algún $i \in \{1, ..., n\}$ terase $xy \in \mathfrak{q}_i$ con $y \notin \mathfrak{q}_i$ tendo que $x \in \mathfrak{p}$ por ser $\mathfrak{q}_i$ $\mathfrak{p}$-primario. □

Por outra banda imos empregar o seguinte lema de carácter máis técnico:

Lema 3.9. *Sexa $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario e $x \in A$. Entón cúmplese:*

1. *Se $x \in \mathfrak{q}$ entón $(\mathfrak{q} : x) = (1)$*
2. *Se $x \notin \mathfrak{q}$ entón $(\mathfrak{q} : x)$ é $\mathfrak{p}$-primario.*
3. *Se $x \notin \mathfrak{p}$ entón $(\mathfrak{q} : x) = \mathfrak{q}$.*

Demostración.

1. Como x pertence a $\mathfrak{q}$ imos ter que $xy \in \mathfrak{q}$ para calquera $y \in A$. Ou sexa temos que $(\mathfrak{q} : x) = (1) = A$.

2. Vexamos primeiro que o radical é efectivamente o primo $\mathfrak{p}$. Se $y \in (\mathfrak{q} : x)$ entón por definición $xy \in \mathfrak{q}$. Como $x \notin \mathfrak{q} \subseteq r(\mathfrak{q}) = \mathfrak{p}$ necesariamente $y \in \mathfrak{p}$. Así $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$ polo que tomando radicais e a propiedade de compresión temos que $r(\mathfrak{q} : x) = \mathfrak{p}$.

   Vexamos agora que o ideal é primario. Sexa $yz \in (\mathfrak{q} : x)$ con $y \notin \mathfrak{q}$ entón $xyz \in \mathfrak{q}$. Así ao ser primario imos ter que $xz \in \mathfrak{q}$ e en consecuencia $z \in (\mathfrak{q} : x)$.

3. Como x non pertence a $\mathfrak{p}$ e ao ser $\mathfrak{q}$ $\mathfrak{p}$-primario cumple $\mathfrak{q} \subseteq r(\mathfrak{q}) = \mathfrak{p}$. Entón se $xy \in \mathfrak{q}$ terase que $y \in \mathfrak{q}$. Ou sexa temos que $(\mathfrak{q} : x) = \mathfrak{q}$.

□

A noción de descomposición dun ideal xorde de forma natural. Podería introducirse ao par que o concepto de ideal primario mais a partir de aquí xogará un papel central:

Definición 3.10. Dado un ideal $\mathfrak{a} \subset A$ dicimos que unha *descomposición primaria* é unha expresión de $\mathfrak{a}$ da forma $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ sendo os $\mathfrak{q}_i$ ideais primarios $i \in \{1, ...n\}$. Se ademais verifica que $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ $\forall i \neq j$ e que $\mathfrak{q}_i \subsetneq \cap_{i \neq j} \mathfrak{q}_j$ diremos que a descomposicón primaria é *minimal*. Se $\mathfrak{a}$ ten unha descomposición primaria diremos que é *descompoñible*.

Así chegamos ao primer teorema de unicidade, no que esencialmente afirmamos que se un ideal posee unha descomposición primaira entón os elementos $\mathfrak{p}$-primarios son independentes da descomposición, ou sexa, os elementos básicos son compartidos.

Teorema 3.11 (Primer teorema de unicidade)**.** *Dado un ideal $\mathfrak{a}$ descompoñible cunha descomposición primaria minimal da forma $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$. Se $\mathfrak{p}_i = r(\mathfrak{q}_i)$ con $i \in \{1, ... n\}$ entón son os ideais primos que aparecen nos ideais $r(a : x)$ con $x \in A$ independientemente da descomposición particular de $\mathfrak{a}$.*

Demostración. Para cada $x \in A$ terase polas propiedades do cociente e a descomposición de $\mathfrak{a}$ que $(\mathfrak{a} : x) = (\cap_{i=1}^{n} \mathfrak{q}_i : x) = \cap_{i=1}^{n} (\mathfrak{q}_i : x)$. Tendo en conta as propiedades do radical e o lema (3.9) teremos que $r(\mathfrak{a} : x) = r(\cap_{i=1}^{n} \mathfrak{q}_i : x) = \cap_{i=1}^{n} r(\mathfrak{q}_i : x) = \cap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i$. Só nos falta por ver que, efectivamente, os primos $\mathfrak{p}_j$ son xustamente os primos de $r(\mathfrak{a} : x)$. Vexamos as dúas inclusións:

$\subseteq$ Por un lado supoñamos que $r(\mathfrak{a} : x)$ é primo. Polo tanto $r(\mathfrak{a} : x) = \mathfrak{p}_i$ para un certo índice i. Temos así que cada ideal primo da forma $r(\mathfrak{a} : x)$ é un $\mathfrak{p}_i$.

$\supseteq$ Por outra banda, sexa i un índice tal que $\exists x_i \notin \mathfrak{q}_i$. Como a descomposición é minimal temos que $x_i \in \cap_{i \neq j} \mathfrak{q}_j$. Polo tanto $r(\mathfrak{a} : x_i) = \mathfrak{p}_i$.

□

Así mesmo, podemos clasificar os primos que interveñen na descomposición en función de como se comportan, inclusivamente, co ideal de $\mathfrak{a}$. Xorde entón a seguinte definición:

Definición 3.12. Os ideais primos do anterior teorema dícese que *pertencen* a $\mathfrak{a}$. No caso dos ideais primarios, estes tan só terán un único primo asociado. Por último, os elementos minimales do conxunto $\{\mathfrak{p}_i\}_{i=1}^n$ denomínanse *ideais primos minimales* ou *ideais primos illados*; o resto serán os *ideais primos inmersos.*

Nota 3.13. En [1] faise unha nota altamente esclarecedora sobre estes conceptos. Indica e cito textualmente: 'os termos *illado* e *inmerso* proceden da Xeometría. Así se $A = K[x_1, ..., x_n]$ onde K é un corpo alxébricamente pechado, o ideal $\mathfrak{a}$ dá lugar a unha variedade $X \subseteq K^n$. Os primos minimales $\mathfrak{p}_i$ corresponden ás compoñentes irreducibles de X e os primos inmersos corresponden ás subvariedades nas compoñentes irreducibles.' Ilustremos esto, así como a non unicidade para a descomposición primaria, cun exemplo. Sexa $A = K[x, y]$, con K un corpo, e consideramos $\mathfrak{a} = (x^2, xy)$. Imos ver que existen máis dunha descomposición para este ideal. Consideramos $\mathfrak{q}_1 = (x)$ e $\mathfrak{q}_a = (y - ax, x^2)$. Temos por unha banda que $\mathfrak{q}_1$ é primo, polo tanto primario, entón tomamos $\mathfrak{q}_1 = \mathfrak{p}_1$. Por outra banda temos que $\mathfrak{p}_2 = (x, y)$ é maximal e ademais cumple $\mathfrak{p}_2^2 \subset \mathfrak{q}_a \subset \mathfrak{p}_2$. Entón temos que $\mathfrak{q}_a$ é $\mathfrak{p}_2$-primario por (3.6). É fácil comprobar que $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_a$. Así, para cada $a \in K$ obtemos unha descomposición do ideal distinta, xa que para $a \neq b$ temos que $\mathfrak{q}_a \neq \mathfrak{q}_b$. Ou sexa, encontramos unha familia parametrizada de descomposicións para $\mathfrak{a}$. Neste caso temos que $\mathfrak{p}_1 \subset \mathfrak{p}_2$ sendo dous primos asociados tal que $\mathfrak{p}_1$ é minimal e $\mathfrak{p}_2$ inmerso.

Necesitamos entón poder garantir que se un ideal se descompón terá compoñentes irreducibles e dar unha caracterzación destas. Así vexamos que os ideais primos minimais dun ideal dado son, efectivamente, os elementos minimales do conxunto de todos os ideais primos que conteñen ao ideal. Isto será consecuencia inmediata da seguinte proposición:

Proposición 3.14. *Dado un ideal descompoñible* $\mathfrak{a}$ *temos que cada ideal primo que o contén ten un ideal primo minimal.*

Demostración. Tomamos entón un ideal primo $\mathfrak{p}$ tal que $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i \subset \mathfrak{p}$. Polas propiedades do radical temos que $\mathfrak{p} = r(\mathfrak{p}) \supset r(\mathfrak{a}) = r(\cap_{i=1}^n \mathfrak{q}_i) = \cap_{i=1}^n r(\mathfrak{q}_i) = \cap_{i=1}^n \mathfrak{p}_i$. Por (1.8) temos que que $\mathfrak{p}_i \subseteq \mathfrak{p}$ e polo tanto ten elemento minimal. □

Introducimos por último, apoiándonos sobre o apéndice, dous resultados que servirán de medio para chegar ao segundo teorema de unicidade. O primeiro deles indícanos como se comportan os ideais primarios, dun anel A, no seu paso a aneis de fraccións en función de como cortan ao conxunto que xera os inversos, S. Por outra banda, o segundo danos unha descomposición dos inversos, segundo S, dun ideal $\mathfrak{a}$ en función da interseción dos inversos segundo S cos ideais primarios asociados a $\mathfrak{a}$.

Proposición 3.15. *Dado un subconxunto multiplicativamente pechado $S \subset A$ e $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario, entón verifícase:*

1. *Se $S \cap \mathfrak{p} \neq \emptyset$ entón $S^{-1}\mathfrak{q} = S^{-1}A$.*
2. *$S \cap \mathfrak{p} = \emptyset$ entón $S^{-1}\mathfrak{q}$ é $S^{-1}\mathfrak{p}$-primario. Ademais a súa contración en A, $S(\mathfrak{a})$, será $\mathfrak{q}$.*

Demostración.

1. Claramente, como $\mathfrak{q} \subsetneq A$, tense que $S^{-1}\mathfrak{q} \subseteq S^{-1}A$. Vexamos a outra inclusión. Como, por hipótese, $S \cap \mathfrak{p} \neq \emptyset$ tomamos un s contido na intersección. Xa que $r(\mathfrak{q}) = \mathfrak{p}$ temos que $s \in S \cap r(\mathfrak{q})$ e, pola definición de radical, $s^n \in S \cap \mathfrak{q}$ para un certo n. Temos que $\frac{s^n}{1} \in S^{-1}\mathfrak{q}$ sendo unha unidade de $S^{-1}A$. Ou sexa temos que $S^{-1}A \subseteq S^{-1}\mathfrak{q}$ e, en consecuencia, a igualdade.

2. Imos ter de forma inmediata que $S^{-1}\mathfrak{q}$ é primo. Vexamos que $r(S^{-1}\mathfrak{q}) = S^{-1}\mathfrak{p}$. Por (.29) temos que $r(\mathfrak{q}^{\mathfrak{c}}) = r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$ tendo que o ideal é $S^{-1}\mathfrak{p}$-primario.

   Vexamos agora que a súa contracción é $\mathfrak{q}$. Como $S \cap \mathfrak{p} = \emptyset$ temos que se $s \in S$ e $as \in \mathfrak{q}$ entón teremos que $a \in \mathfrak{q}$. Así por (.29) $\mathfrak{q}^{\mathfrak{ec}} = (S^{-1}\mathfrak{q})^{\mathfrak{c}} = \mathfrak{q}$.

□

Proposición 3.16. *Dado un conxunto multiplicativamente pechado $S \subset A$ e $\mathfrak{a} \subset A$ un ideal descompoñible con descomposición minimal primaria $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$. Sexa $\mathfrak{p}_i = r(\mathfrak{q}_i)$ con $i \in \{1, \dots n\}$ tal que $S \cap \mathfrak{p}_i \neq \emptyset$ $\forall i \in \{m+1, \dots n\}$ e $S \cap \mathfrak{p}_i = \emptyset$ $\forall i \in \{1, \dots m+1\}$ entón :*

1. *$S^{-1}\mathfrak{a} = \cap_{i=1}^{m} S^{-1}\mathfrak{q}_i$*
2. *$S(\mathfrak{a}) = \cap_{i=1}^{m}\mathfrak{q}_i$*

Demostración.

1. Por unha banda temos por (3.15) e (.29) que $S^{-1}\mathfrak{a} = \cap_{i=1}^{n} S^{-1}\mathfrak{q}_i = \cap_{i=1}^{m} S^{-1}\mathfrak{q}_i$. Notemos que os $S^{-1}\mathfrak{p}_i$ son primos distintos ao selos $\mathfrak{p}_i$. Obtemos así unha descomposición minimal primaria.

2. Por outra banda, se contraemos ambos membros e aplicamos (3.15) obtemos que $S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^{\mathfrak{c}} = \cap_{i=1}^{m}(S^{-1}\mathfrak{q}_i)^{\mathfrak{c}} = \cap_{i=1}^{m}\mathfrak{q}_i$.

□

Imos empregar o resultado anterior no noso anel A. Imos definir un conxunto multiplicativamente pechado S, a través dunha definición para fundamentar o posterior desenvolvemento:

Definición 3.17. Sexa Σ o conxunto de ideais primos pertencentes a un ideal $\mathfrak{a}$. Diremos que Σ é *illado* se dado $\mathfrak{p}_1$ un ideal que pertencente a $\mathfrak{a}$ tal que $\mathfrak{p}_1 \subset \mathfrak{p} \in \Sigma$ verifica $\mathfrak{p}_1 \in \Sigma$.

Entón consideremos o conxunto Σ previamente descrito e consideramos o conxunto multiplicativamente pechado $S = A - \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$. Para cada ideal primo pertencente a $\mathfrak{a}$ vaise verificar:

- $\mathfrak{p}_1 \in \Sigma$ entón $\mathfrak{p}_1 \cap S = \emptyset$
- $\mathfrak{p}_1 \notin \Sigma$ entón $\mathfrak{p}_1 \cap S \neq \emptyset$

Así, estando nas hipóteses da proposición anterior chegamos ao segundo teorema de unicidade, o cal a diferencia do primeiro, vaise referir a unicidade dos elementos da descomposición:

Teorema 3.18 (Segundo teorema de unicidade)**.** *Dado un ideal descompoñible* $\mathfrak{a}$ *con descomposición minimal primaria* $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ *e sexa* $\{\mathfrak{p}_{i_j}\}_{j=1}^{m}$ *un conxunto illado de ideais primos de* $\mathfrak{a}$ *entón* $\cap_{j=1}^{m}\mathfrak{q}_{i_j}$ *é independente da descomposición.*

Corolario 3.19. *As compoñentes illadas primarias está determinadas polo ideal* $\mathfrak{a}$*.*

A descomposición primaria dun ideal $I \subset K[x_1, ..., x_n]$, con K corpo non sempre dá a descomposición da variedade asociada $V(I)$ nas súas compoñentes irreducibles. Para elo tomamos o seguinte exemplo:

Exemplo 3.20. Vexamos que, para K arbitrario, os primos minimales non corresponden ás compoñentes irreducibles (3.13). Sexa $K = \mathbb{R}$ e consideramos o ideal $\mathfrak{p} = (y^2 + x^2(x-1))$ [3]. Este é un ideal primo de $\mathbb{R}[x, y]$ mais $V(I) = \{P(0, 0), Q(1, 0)\}$ ten dúas compoñentes, mentres que o único primo minimal é $\mathfrak{p}$.

3.0.3. Descomposición primaria en aneis noetherianos [1]

Nesta subsección centrarémonos, unha vez máis, no caso de que o anel a tratar sexa noetheriano. Ao mesmo tempo imos poder xeralizar a relación que hai en $\mathbb{Z}$ entre os ideais e os radicais destes. Se pensamos o ideal xerado por (12) o seu radical xa vimos que era $r(12) = (6)$. O certo é que podemos garantir o contido de certas potencias do radical no ideal orixinal. No caso anterior tense $r(6)^2 \subset (12)$ mais $r(6) \nsubseteq r(12)$. Para aneis noetherianos tamén se vai cumplir:

Proposición 3.21. *Cada ideal $\mathfrak{a}$ dun anel noetheriano A contén unha potencia do seu radical.*

Demostración. Sexa $\mathfrak{a}$ un ideal dun anel noetheriano A e $r(\mathfrak{a})$ o seu radical. Supoñamos que este está xerado por un conxunto de elementos $\{a_1, ..., a_n\}$ ou sexa $a_i^{n_i} \in \mathfrak{a}$ con $i \in \{1, ...n\}$. Tomamos $m = \sum_{i=1}^{n}(n_i - 1) + 1$. Así $r(\mathfrak{a})^m$ estará xerado por $\{a_1^{r_1}, ..., a_n^{r_n}\}$ con $\sum_{i=1}^{n} r_i = m$. Tal e como os definimos imos ter que $r_i \leq n_i$ para certo índice i polo que necesariamente $a_1^{r_1}...a_n^{r_n} \in \mathfrak{a}$. Polo tanto $r(\mathfrak{a})^m \subseteq \mathfrak{a}$. □

A seguinte definición servirá de base para enunciar o teorema principal deste traballo:

Definición 3.22. Dado un anel A e $\mathfrak{a} \subseteq A$ un ideal deste. Dicimos que $\mathfrak{a}$ é *irreducible* se ao poñer este como intersección de ideais necesariamente é un deles, ou sexa, se $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ entón $\mathfrak{a} = \mathfrak{b}$ ou $\mathfrak{a} = \mathfrak{c}$.

Teorema 3.23 (Lasker-Noether)**.** *Dado un anel A noetheriano todo ideal $\mathfrak{a} \subseteq A$ ten descomposición primaria.*

Demostración. Temos que ver que cada ideal dun anel A noetheriano se pode poñer como unha intersección de ideais primarios. Para elo vemos que:

1. Vexamos que cada ideal de A é intersección finita de ideais irreducibles. Supoñamos o contrario para chegar a unha contradición. Consideremos Σ o conxunto dos ideais de A que non son intersección dun número finito de ideais. Por suposición este conxunto é non baleiro e polo lema de Zorn ten un elemento maximal $\mathfrak{a}$. Como $\mathfrak{a}$ é reducible imos poñer este como intersección de ideais, ou sexa, $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ con $\mathfrak{a} \subset \mathfrak{b}$ e $\mathfrak{a} \subset \mathfrak{c}$. Pola maximalidade de $\mathfrak{a}$ temos que $\mathfrak{b}, \mathfrak{c} \notin \Sigma$ e polo tanto podemos poñelo como intersección finita de ideais. Así $\mathfrak{a}$ pode poñerse como intersección finita de ideais sendo un absurdo con que $\mathfrak{a} \in \Sigma$.

2. Vexamos que cada ideal irreducible é primario. Consideremos un ideal $\mathfrak{a}$ e o anel $A/\mathfrak{a}$. Así ver que se o ideal $\mathfrak{a}$ de A é irreducible entón é primario é o mesmo que

ver que se o ideal $\overline{0}$ de $A/\mathfrak{a}$ é irreducible entón é primario. Tomamos $xy \in \overline{0}$, ou sexa, $xy = 0$ e vexamos se se cumple a definición de ideal primario. Tomamos $y \neq 0$ e vexamos que $x^n = 0$. Consideramos a cadea de ideais $Ann(x) \subseteq Ann(x^2) \subseteq ....$ Como A é noetheriano sabemos que $A/\mathfrak{a}$ tamén o será e como consecuencia a cadea estabilizarase nun certo N. Así $Ann(x^n) = Ann(x^{n+1})$ con $n \geq N$.

Empreguemos isto último para deducir que $(x^n) \cap (y) = 0$. Tomamos un $a \in (x^n) \cap (y)$. Terase que $ax = 0$ e que $a = bx^n$. Multiplicando a última expresión por x obtemos que $ax = bx^n x = bx^{n+1} = 0$ pois temos que $b \in Ann(x^{n+1}) = Ann(x^n)$. Tendo que $a = bx^n = 0$ tal e como queríamos ver. Entón temos que $(x^n) \cap (y) = 0$ e como $y \neq 0$ temos que $x^n = 0$ e polo tanto $x^n \in \overline{0}$ verificando $\overline{0}$ a definición de ser primario.

Así por (1) e (2) temos que cada ideal dun anel noetheriano ten descomposición primaria. □

Nota 3.24. Este teorema formaliza aínda máis esa idea de descomposición das subestruturas que recobre o concepto de ser noetheriano. Pode entenderse dende un punto de vista aritmético como a xeralización do teorema fundamental da aritmética para aneis máis xenéricos. Por outra banda pode entenderse dende un punto de vista xeométrico. Así na linguaxe da xeometría alxébrica vai manifestar a idea de descompoñer certas variedades alxébricas, representadas a través dos ceros de polinomios, como unha unión finita das súas compoñentes irreducibles como se puido ver para espacios noetherianos en (3.11).

Recuperamos co teorema de Lasker-Noether os resultado da sección anterior para aneis noetherianos. Así, a partir da condición de ser noetheriano, podemos caracterizar de forma directa os seus ideais primos como consecuencia de (3.11). En consecuencia, e como fixen fincapé ao longo do traballo, todo o relativo a nivel operacional vai estar perfectamente determinado no caso dos aneis noetherianos.

Proposición 3.25. *Dado un ideal noetheriano $\mathfrak{a} \subsetneq A$ entón os seus ideais primos son os ideais primos que aparecen no conxunto de ideais $\{(\mathfrak{a} : x)\}_{x \in A}$.*

Aneis de fraccións

Como xa sabemos os aneis que empregamos ao longo deste traballo non teñen por que ter inverso multiplicativo. Xa vimos, ademais, que existen estruturas máis restrictivas, con este tipo de elementos, que posuían un bo comportamento con respecto os seus ideais: os corpos. Xorde así de forma natural preguntarse como podemos, dado un anel A, construír outro anel C que teña certos inversos de elementos de A. Imos tomar como exemplo do anterior a construción de $\mathbb{Q}$ a partir de $\mathbb{Z}$. Isto realízase a partir dunha relación de equivalencia que nos dá a forma dos inversos. Tomamos un par $(x, y),\ (z, w) \in \mathbb{Z} \times \mathbb{Z}$ e diremos que están relacionados se verifican a identidade das fraccións equivalentes usuais, ou sexa:

$$(x, y) \sim (z, w) \Leftrightarrow xw - yz \ = \ 0$$

Isto poderíase estender aos aneis que, ao igual que $\mathbb{Z}$, son dominios. Mais, non sempre temos este tipo de aneis e teremos que ter en conta a existencia de certos divisores de cero para reformular a relación '$\sim$' anterior. Así, sexa A un anel e S un subconxunto multiplicativamente pechado, ou sexa, un subsemigrupo do semigrupo multiplicativo A. Dados $(x, y),\ (z, w) \in A \times S$ definimos a nova relación, '$\sim_S$', como segue:

$$(x, y) \sim_S (z, w) \ \Leftrightarrow \ (xw \ - \ yz)u \ = \ 0, \quad u \in S$$

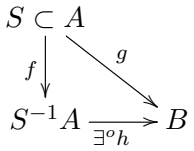
Ao multiplicar por un certo $u \in S$ imos poder demostrar a transitividade da relación e a constitución desta como unha relación de equivalencia. Denotaremos como '$\frac{x}{y}$' á clase de equivalencia do par (x, y) e chamarémoslle fracción. O conxunto de clases, neste caso das fraccións, denotarase como $S^{-1}A$. Este podemos dotalo das seguintes operacións para elaborar un novo anel: o *anel de fraccións*.

$$\begin{cases} (x/y) + (z/w) = \frac{(xw+yz)}{yw} \\ (x/y)(z/w) = \frac{xz}{yw} \end{cases}$$

Un dos feitos de maior importancia é que a partir deste anel poderemos factorizar calquera aplicación que leve os elementos de A en inversos dun anel B. É dicir, calquera

homomorfismo que leve elementos en inversos pode entenderse como un homomorfismo dende o anel de fraccións. Isto é o que se coñece como a propiedade universal do anel de fraccións e enúnciase así:

Proposición .26. *Dados dous aneis A, B e dous homomofismo $g : A \to B$, tal que $g(x)$ é unha unidade de B, e $f : A \to S^{-1}A$, dado por $f(x) = \frac{x}{1}$, con $x \in A$. Entón existe un único homomorfismo de aneis $h : S^{-1}A \to B$ que fai conmutativo o seguinte diagrama:*



Nota .27. O homomorfismo $f : A \to S^{-1}A$ non é polo xeral inxectivo. Podemos exemplificar isto tomando como anel $A = \mathbb{Z}_6$ e como conxunto $S = \{2, 4\}$.

Nota .28. Estas construcións podemos estendelas á teoría de módulos dun xeito análogo así como as subestruturas destes.

Rematamos introducindo a notación $A_{\mathfrak{p}} := S^{-1}A$ con $S = A - \mathfrak{p}$ e observando como se transmite aos aneis de fraccións as operacións que introducimos no capítulo 1 así como o comportamento dos ideais destes, na seguinte proposición:

Proposición .29. *Dado un anel A e un conxunto multiplicativamente pechado S verifícase:*

1. *Todo ideal de $S^{-1}A$ é un ideal estendido.*
2. *Se $\mathfrak{a} \subset A$ é un ideal entón $\mathfrak{a}^{ec} = \cap_{s \in S}(\mathfrak{a} : s)$. Ademais $\mathfrak{a}^{e} = (1)$ se, e só se, $\mathfrak{a} \cup S \neq \emptyset$.*
3. *Os ideais primos de $S^{-1}A$ está en correspondencia bixectiva cos ideais primos de A que non cortan a S.*
4. *A operación S^{-1} conmuta coa formación de sumas finitas, produtos, intersecciónes e radicais.*

Bibliografía

[1] Atiyah, M. F. & Macdonald, I. G. *Introducción al Álgebra Conmutativa* Reverté 1994.

[2] Boyer C. *Historia de la Matematica*, Alianza Editorial 1978.

[3] Fulton W. *Curvas Algebraicas*, Reverté 1969.

[4] Gray J. *Algebraic geometry between Noether and Noether - A forgotten chapter in the history of algebraic geometry* , Revue d'historie des mathématiques 3 (1997), 1-48.

[5] Kunz E. *Introduction to Conmutative Algebra and Algebraic Geometry*, BIRKHÄUSER 1985.