USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Teorema dos ceros de Hilbert. Tema e variacións.

Alfonso Gallego Fernández

2020/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Teorema dos ceros de Hilbert. Tema e variacións.

Alfonso Gallego Fernández

Febreiro 2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Teorema dos ceros de Hilbert. Tema e variacións.
Breve descrición do contido
O teorema dos ceros (Nullstellensatz) é a xeneralización do teorema fundamental da álxebra a sistemas de ecuacións polinómicas en varias variábeis. Trátase de dar unha exposición deste resultado e explorar variantes en corpos con propiedades interesantes como son os corpos reais ou os finitos.
Recomendacións
Ter superado e comprendido os contidos das materias "Estruturas alxébricas" e "Ecuacións alxébricas". É de axuda pero non imprescindíbel ter cursado a materia "Álxebra, Números e Xeometría".
Outras observacións

Índice xeral

Resumo

Este traballo ten como obxectivo enunciar e demostrar o *Nullstellensatz*, ou *Teorema dos Ceros*, de Hilbert, un importante teorema alxébrico que fai de ponte entre a álxebra conmutativa e a xeometría alxébrica, permitindo deducir propiedades das variedades alxébricas afíns mediante o estudo dos ideais do anel de polinomios. Previamente enunciaranse os preliminares alxébricos e xeométricos necesarios para a realizar a proba e para comprender a súa conexión coa teoría de variedades alxébricas afíns. Logo abordarase a xeneralización do teorema a álxebras finitamente xeradas sobre aneis de Jacobson, non necesariamente sobre corpos alxebricamente pechados. Tamén enunciaranse e probaranse os casos particulares para corpos finitos e corpos reais pechados, usando as propiedades específicas que posúen cada un deses tipos de corpos.

Abstract

This work aims to show and prove Hilbert's *Nullstellensatz*, or *Theorem of Zeros*, a very important algebraic theorem which acts as a bridge between commutative algebra and algebraic geometry, allowing us to deduce properties of affine varieties by studying the ideals of the polynomial ring. Previously, we will show the algebraic and geometric preliminaries required for the proof and to comprehend its connection to the theory of affine varieties. Afterwards we will show the generalization of the theorem to finitely generated algebras over Jacobson rings, not necessarily over algebraicly closed fields. We will also show and prove the particular cases of finite fields and real closed fields, using the specific properties of each of those fields.

Introdución

Unha motivación básica da álxebra é a resolución de ecuacións. Os sistemas de ecuacións lineais son o cometido da álxebra lineal, que posúe unha ampla colección de resultados cun amplo rango de aplicacións. O caso non lineal máis sinxelo é o das ecuacións polinómicas nunha variábel, cuxa resolución a aborda a *Teoría de Galois*. Neste ámbito xurde o *Teorema Fundamental da Álxebra*, estudado intensamente por Gauss a finais do século XVIII e comezos do XIX. En linguaxe moderno, este teorema afirma que o corpo dos números complexos, $\mathbb{C}$, é alxebricamente pechado: todo polinomio dunha variábel con coeficientes complexos ten polo menos unha raíz complexa, e como consecuencia directa, un polinomio de grao n ten exactamente n raíces complexas, tendo en conta a súa multiplicidade.

A seguinte cuestión que xurde de forma natural é que condicións son necesarias para que un sistema de ecuacións polinómicas en varias variábeis teña solución. Este problema o resolve Hilbert co seu *Nullstellensatz* (que podería ser traducido do alemán como *Teorema de Localización dos Ceros*, aínda que habitualmente se lle chama *Teorema dos Ceros*), o cal enunciou e demostrou en 1893, e ten como consecuencia que todo sistema de ecuacións polinómicas en varias variábeis con coeficientes nun corpo alxebricamente pechado ten polo menos unha solución. Este resultado é de enorme importancia, pois abriu a porta ó estudo da xeometría alxébrica no espazo afín e proxectivo e converteu ós corpos alxebricamente pechados nas eleccións máis naturais para o estudo destes problemas.

Neste traballo propoñémonos dar unha demostración moderna deste resultado, xunto cos preliminares necesarios. Tamén pretendemos abordar xeneralizacións e variantes do teorema que xurdiron dende o traballo de Hilbert. Un aspecto que nos servirá para a xeneralización do teorema é a filosofía de que as solucións dun sistema de ecuacións polinómicas, que son os puntos dunha variedade alxébrica afín, correspóndense cos ideais maximais do anel de coordenadas desa variedade. Con esta abstracción do problema orixinal obtemos unha xeneralización do Nullstellensatz a unha clase de aneis, os chamados *aneis de Jacobson*, onde os maximais teñen un bo comportamento, e permiten deducir un enunciado similar ó do Nullstellensatz forte para calquera tipo de corpo.

Doutra banda, resulta natural impoñer outras condicións ó corpo no que se quere traballar, para caracterizar así os sistemas de ecuacións que se corresponden cos tipos de xeometrías que se queren abordar. Aínda que existen moitas posibilidades para escoller, nesta memoria centrámonos en dous casos especialmente interesantes: os corpos finitos e os corpos reais pechados.

No caso dos corpos finitos, estudar os subconxuntos do espazo afín que son solución de ecuacións polinómicas é esencialmente un problema diofántico. A solución deste pasa por construír un ideal que contén ós polinomios que se anulan en todo o espazo afín, para logo cocientar o anel de polinomios por ese ideal, recuperando así a correspondencia entre ideais e variedades.

Os corpos reais pechados son corpos ordenados maximais no sentido de que non posúen extensións alxébricas que admitan unha orde, polo que será necesario introducir elementos básicos da álxebra real. En poucas palabras, un sistema de ecuacións polinómicas con coeficientes nun corpo real pechado terá solución nese corpo se o ideal que xera é tal que o anel cociente por ese ideal admite unha orde compatíbel coas operacións.

Pasamos agora a describir brevemente o contido da memoria:

No primeiro tema enunciaranse os preliminares de álxebra conmutativa, con tres seccións: álxebras, extensións de corpos e extensións de aneis. Na sección de álxebras definirase o concepto esencial de álxebra finitamente xerada e probaranse dúas caracterizacións equivalentes do mesmo. Na sección de extensións de corpos recordaranse as definicións dos distintos tipos de extensións e as relacións entre eles, así como a definición de corpo alxebricamente pechado e as súas propiedades. Na sección de extensións de aneis é de especial importancia probar o teorema 1.3.9, que di que nunha extensión enteira de aneis, un deles é un corpo se e soamente se o outro tamén o é, pois se usa na proba do *Lema de Zariski*.

No segundo tema expoñeranse os preliminares da teoría de variedades afíns necesarios para entender a relación do Nullstellensatz coa xeometría alxébrica. Logo probaranse as dúas versións clásicas do Nullstellensatz: a débil e a forte, usando o *Lema de Zariski* para probar a versión débil e logo o *truco de Rabinowich* para probar a versión forte.

No terceiro tema definirase o concepto de *anel de Jacobson* e probaranse algunhas das súas propiedades para logo enunciar unha versión máis xeral do Nullstellensatz forte, que se pode aplicar a calquera anel de Jacobson, incluso os que non son álxebras sobre un corpo alxebricamente pechado, e así poder deducir máis propiedades sobre as variedades afíns dun corpo arbitrario.

No cuarto tema enunciarase e probarase a variante do Nullstellensatz para corpos finitos, que consiste basicamente en definir un ideal que contén ós polinomios que se anulan en todos os puntos, e logo cocientar o anel de polinomios por ese ideal, para así poder obter un enunciado similar ó do Nullstellensatz forte para este tipo de corpos.

No quinto e último tema introduciranse os preliminares alxébricos sobre a álxebra real, que inclúen o concepto de anel semirreal, real, ordenado, e as relacións entre os mesmos, tanto no caso dos aneis como no particular dos corpos. A continuación definirase o concepto de corpo real pechado, que non son máis que os corpos ordenados que son maximais respecto de admitir unha extensión alxébrica ordenada, e enunciaranse algunhas das súas propiedades máis relevantes para o traballo. Logo definirase o concepto de radical real dun anel, que se utilizará finalmente para dar un enunciado do Nullstellensatz para corpos reais pechados moi similar ó dado no tema 2 para o Nullstellensatz forte.

Capítulo 1

Preliminares Alxébricos

Antes de comezar cos preliminares, convén aclarar algunhas convencións que se tomarán durante o traballo. Sempre que se mencione un anel, supoñerase que se trata dun anel conmutativo e con neutro para o produto. Para un corpo supoñerase sempre que $0 \neq 1$, e as letras $x, x_1, \dots, x_n$ denotarán sempre as incógnitas dun anel de polinomios.

1.1. Álxebras

Definición 1.1.1. Sexa A un anel. Defínese unha ***A*-álxebra** como un par (B, φ), sendo B un anel e $\varphi : A \longrightarrow B$ un homomorfismo de aneis, que permite darlle a B unha estrutura de A-módulo mediante a operación $ab := \varphi(a)b \; \forall a \in A \; \forall b \in B$. Dado un ideal $\mathfrak{b} \lhd B$, denotarase $A \cap \mathfrak{b} := \varphi^{-1}(\mathfrak{b})$, que é un ideal de A.

Definición 1.1.2. Dise que unha A-álxebra (B, φ) é **finitamente xerada** se existen os elementos $b_1, \dots, b_n \in B$ tales que cada elemento de B pode ser expresado (de forma non necesariamente única) como unha expresión polinómica en $\{b_1, \dots, b_n\}$ con coeficientes en A, usando o produto de B como A-módulo para multiplicar os elementos de A polos b_i. Isto denotarase por $B = A[b_1, \dots, b_n]$.

Proposición 1.1.3. *Sexa (B, φ) unha A-álxebra. Entón son equivalentes:*

1. *B é finitamente xerada por $b_1, \dots, b_n \in B$.*
2. *Existen $b_1, \dots, b_n \in B$ e $\psi : A[x_1, \dots, x_n] \longrightarrow B$ un homomorfismo de aneis sobrexectivo tales que:*

$$\psi(a) = \varphi(a) \; \forall a \in A \qquad\qquad \psi(x_i) = b_i \; \forall i \in \{1, \dots, n\}$$

3. *Existe un ideal $\mathfrak{a} \lhd A[x_1, \dots, x_n]$ tal que $B \simeq A[x_1, \dots, x_n]/\mathfrak{a}$.*

Demostración.

"1 ⇒ 2" É evidente que se B está finitamente xerada polos elementos $b_1, \dots, b_n \in B$, entón pódese definir o homomorfismo de aneis $\psi : A[x_1, \dots, x_n] \longrightarrow B$ como:

$$\psi\left(\sum_{\nu\in\mathbb{N}^n} a_\nu M_\nu(x_1, \dots, x_n)\right) = \sum_{\nu\in\mathbb{N}^n} \varphi(a_\nu) M_\nu(b_1, \dots, b_n)$$

Sendo M_ν o monomio tal que $M_\nu(x_1, \dots, x_n) = x_1^{\nu_1} \cdots x_n^{\nu_n}$, con $\nu = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n$, e $a_\nu = 0$ para todos agás un número finito de ν. Desta forma, é evidente ver que compre as propiedades enunciadas no apartado 2.

"2 ⇒ 3" Tómase $\mathfrak{a} = \mathrm{Ker}(\psi)$. Aplicando o *Primeiro Teorema de Isomorfía* e tendo en conta que ψ é sobrexectivo, pódese definir o isomorfismo de aneis $\tilde{\psi} : A[x_1, \dots, x_n]/\mathfrak{a} \longrightarrow B$ como $\tilde{\psi}(f + \mathfrak{a}) = \psi(f)$, de forma que $B \simeq A[x_1, \dots, x_n]/\mathfrak{a}$.

"3 ⇒ 1" Sexa $\tau : B \longrightarrow A[x_1, \dots, x_n]/\mathfrak{a}$ un isomorfismo de aneis, e sexan $b_1, \dots, b_n \in B$ os elementos tales que $\tau(b_i) = x_i + \mathfrak{a}\ \forall i \in \{1, \dots, n\}$. É evidente ver que cada elemento de $A[x_1, \dots, x_n]/\mathfrak{a}$ pódese escribir como unha expresión polinómica en $\{x_1 + \mathfrak{a}, \dots, x_n + \mathfrak{a}\}$ con coeficientes en A, logo cada elemento de B pódese escribir como unha expresión polinómica en $\{b_1, \dots, b_n\}$ con coeficientes en A, é dicir, B é unha A-álxebra finitamente xerada. ■

Exemplo 1.1.4. Para un anel arbitrario A, un exemplo dunha A-álxebra finitamente xerada pode atoparse no seu anel de polinomios en n variábeis, $A[x_1, \dots, x_n]$, xunto co homomorfismo inclusión $\varphi : A \longrightarrow A[x_1, \dots, x_n]$ que leva cada $a \in A$ no polinomio constante $a \in A[x_1, \dots, x_n]$.

O homomorfismo ψ que se menciona no apartado 2 da proposición 1.1.3 sería a identidade de $A[x_1, \dots, x_n]$, e o ideal $\mathfrak{a} \lhd A[x_1, \dots, x_n]$ do apartado 3 sería o ideal 0.

1.2. Extensións de Corpos

Definición 1.2.1. Sexa K un corpo. Unha **extensión de corpos** de K é un corpo F do cal K é subcorpo, é dicir, $K \subset F$ e K é un corpo coa restrición ó mesmo das operacións de F. Denotarase por $F : K$. É doado comprobar que nesta situación F é un K-espazo vectorial, e tamén unha K-álxebra co homomorfismo inclusión.

Definición 1.2.2. Defínese o **grao dunha extensión** $F : K$ como a dimensión de F como K-espazo vectorial, e denótase por $[F : K] := \dim_K(F)$. Unha extensión dise que é **finita** se o seu grao é finito.

Definición 1.2.3. Sexa K un corpo. Defínese o **corpo de funcións racionais** de K en n variábeis, denotado por $K(x_1, \dots, x_n)$, como o corpo de fraccións do anel de polinomios $K[x_1, \dots, x_n]$, é dicir, o menor corpo que contén a $K[x_1, \dots, x_n]$, o cal admite a expresión:

$$K(x_1, \dots, x_n) = \left\{ \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \ / \ f, g \in K[x_1, \dots, x_n],\ g \neq 0 \right\}$$

Definición 1.2.4. Sexa $F : K$ unha extensión de corpos e $\alpha_1, \dots, \alpha_n \in F$. Denotarase:

$$K[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \ / \ f \in K[x_1, \dots, x_n]\}$$

$$K(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \ / \ f, g \in K[x_1, \dots, x_n],\ g \neq 0 \right\}$$

Con esta definición, $K(\alpha_1, \dots, \alpha_n)$ compre a propiedade de ser o menor corpo que contén a K e a $\alpha_1, \dots, \alpha_n$, e tense que:

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1)(\alpha_2, \dots, \alpha_n)$$

Dado un subconxunto arbitrario $S \subset F$, denotarase por $K[S]$ ó menor subanel de F que contén a K e a S, e por $K(S)$ ó menor subcorpo de F que contén a K e a S.

Definición 1.2.5. Sexa $F : K$ unha extensión de corpos. Un conxunto $S \subset F$ dise que é un **conxunto de xeradores** de F sobre K, ou que S **xera** F sobre K, se $F = K(S)$. Se ademais S é un conxunto finito, a extensión $F : K$ dise que é **finitamente xerada**.

Observación 1.2.6. Toda extensión de corpos finita $F : K$ é finitamente xerada. Un posíbel conxunto finito de xeradores de F é unha base do mesmo como K-espazo vectorial.

Observación 1.2.7. Sexa $F : K$ unha extensión de corpos. Entón F é unha K-álxebra co homomorfismo inclusión. Se F é finitamente xerado como K-álxebra, entón existen os elementos $\alpha_1, \dots, \alpha_n \in F$ tales que $F = K[\alpha_1, \dots, \alpha_n]$. Como F é un corpo, entón tense que $F = K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$, é dicir, a extensión $F : K$ é finitamente xerada.

Definición 1.2.8. Sexa $F : K$ unha extensión de corpos e $\alpha \in F$. Dise que α é un elemento **alxébrico** sobre K se existe un polinomio non nulo $f \in K[x]$ tal que $f(\alpha) = 0$. Noutro caso dise que α é **transcendente** sobre K. A extensión $F : K$ dise que é **alxébrica** se todo elemento de F é alxébrico sobre K.

Definición 1.2.9. Sexa $F : K$ unha extensión de corpos. O conxunto dos elementos de F que son alxébricos sobre K chamarase a **clausura alxébrica** de K en F, e denotarase por $\bar{K}^F$. Dise que K é **alxebricamente pechado** se todo polinomio non constante de $K[x]$ ten unha raíz en K. Defínese a **clausura alxébrica** de K, sen especificar en que extensión de corpos, como o menor corpo alxebricamente pechado do cal K é subcorpo.

Teorema 1.2.10. *Un corpo alxebricamente pechado K non admite extensións alxébricas distintas da trivial, $K : K$.*

Demostración. Sexa $f \in K[x]$ un polinomio. Como K é alxebricamente pechado, f ten unha raíz $\alpha_1 \in K$, logo existe un polinomio $g \in K[x]$ tal que $f = (x-\alpha_1)g$. Pódese aplicar o mesmo razoamento a g, chegando a que $f = (x-\alpha_1)\cdots(x-\alpha_n)$, onde $\alpha_1, \dots, \alpha_n \in K$ son as raíces de f, tendo en conta a súa multiplicidade.

Dada unha extensión alxébrica $F : K$ e un elemento $\alpha \in F$, este é raíz dun polinomio de $K[x]$, pero polo deducido anteriormente, isto implica que $\alpha \in K$. Logo, K non admite extensións alxébricas distintas da trivial, $K : K$. ■

Proposición 1.2.11. *Sexa $F : K$ unha extensión de corpos e $\alpha \in F$. Entón α é alxébrico sobre K se e soamente se a extensión $K(\alpha) : K$ é finita.*

Demostración. Ver [4], páxina 521, proposición 12. ■

Teorema 1.2.12. *Toda extensión de corpos finita é alxébrica.*

Demostración. Sexa $F : K$ unha extensión finita tal que $[F : K] = n \in \mathbb{N}$ e sexa $\alpha \in F$. Como F é un K-espazo vectorial de dimensión n, entón o conxunto $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ é linealmente dependente, pois ten $n+1$ elementos. Logo existen $\lambda_0, \dots, \lambda_n \in K$ tales que:

$$\lambda_n \alpha^n + \cdots + \lambda_0 = 0$$

É dicir, α é unha raíz do polinomio $f(x) = \lambda_n x^n + \cdots + \lambda_0 \in K[x]$, e polo tanto é alxébrico sobre K, logo a extensión $F : K$ é alxébrica. ■

Teorema 1.2.13. *Unha extensión de corpos $F : K$ é finita se e soamente se é finitamente xerada por elementos de F que son alxébricos sobre K.*

Demostración. Ver [4], páxina 526, teorema 17. ■

Teorema 1.2.14. *Sexa $F : K$ unha extensión de corpos. Entón $\bar{K}^F$ é un corpo.*

Demostración. Ver [4], páxina 527, corolarios 18 e 19. ■

Teorema 1.2.15. *Sexan $L : F$ e $F : K$ dúas extensións de corpos alxébricas. Entón $L : K$ tamén é alxébrica.*

Demostración. Ver [4], páxina 527, teorema 20. ■

Teorema 1.2.16. *Todo corpo ten unha clausura alxébrica, que é única salvo isomorfismos.*

Demostración. Ver [4], páxina 544, proposicións 30 e 31. ■

1.3. Extensións Enteiras

Definición 1.3.1. Sexa A un anel. Dise que B é unha **extensión de aneis de** A se A é subanel de B, é dicir, se $A \subset B$ e A é un anel coa restrición ó mesmo das operacións de B.

Definición 1.3.2. Sexa $A \subset B$ unha extensión de aneis. Un elemento $b \in B$ dise que é **enteiro sobre** A se é a raíz dun polinomio mónico dunha variábel con coeficientes en A, é dicir, se existen $\lambda_1, \dots, \lambda_n \in A$ tales que:

$$b^n + \lambda_1 b^{n-1} + \cdots + \lambda_n = 0$$

O concepto de elemento enteiro é similar ó de elemento alxébrico nas extensións de corpos, máis neste caso hai que esixir que o polinomio sexa mónico na definición, pois ó traballar con aneis, non sempre se pode multiplicar polo inverso do coeficiente principal para transformar un polinomio arbitrario nun mónico.

Definición 1.3.3. Sexa $A \subset B$ unha extensión de aneis. O conxunto dos elementos de B que son enteiros sobre A chamarase a **clausura íntegra** de A en B, e denotarase por $\bar{A}^B$.

Se todos os elementos de B son enteiros sobre A (é dicir, se $B = \bar{A}^B$), dirase que A é **integramente pechado** en B, que B é **enteiro sobre** A, ou que a extensión de aneis $A \subset B$ é **enteira**. Un dominio dirase que é **normal** ou **integramente pechado**, sen especificar en que extensión de aneis, se o é no seu corpo de fraccións.

Lema 1.3.4 (Lema de Gauss)**.** *Sexa K un corpo. Entón $K[x]$ é normal.*

Demostración. Hai que probar que se $\alpha \in K(x)$ é enteiro sobre $K[x]$, entón $\alpha \in K[x]$.

Sexa $\alpha = \frac{f}{g} \in K(x)$, con $f, g \in K[x]$ tales que f e g non teñen divisores en común e $g \neq 0$. Se α é enteiro sobre $K[x]$, entón existen $h_1, \dots, h_n \in K[x]$ tales que:

$$\left(\frac{f}{g}\right)^n + h_1 \left(\frac{f}{g}\right)^{n-1} + \cdots + h_{n-1}\frac{f}{g} + h_n = 0$$

Multiplicando por g^n a ambos lados da igualdade obtense:

$$f^n + h_1 f^{n-1} g + \cdots + h_{n-1} f g^{n-1} + h_n g^n = 0$$

$$f^n = -g(h_1 f^{n-1} + \cdots + h_{n-1} f g^{n-2} + h_n g^{n-1})$$

Logo g divide a f^n, pero como f e g non tiñan divisores comúns, entón $g = \pm 1$, e polo tanto tense que $\alpha = \pm f \in K[x]$. ■

Teorema 1.3.5 (Teorema de Cayley-Hamilton)**.** *Sexa A un anel, $\mathfrak{a} \triangleleft A$ un ideal do mesmo, M un A-módulo finitamente xerado e $\phi : M \longrightarrow M$ un homomorfismo de A-módulos tal que $\phi(M) \subset \mathfrak{a}M$. Entón existen $a_1, \dots, a_n \in \mathfrak{a}$ tales que:*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n I = 0$$

Denotando ϕ^i a composición de ϕ con si mesmo i veces e I a aplicación identidade.

Demostración. Ver [1], tema 10 (páxina 73). ■

Proposición 1.3.6. *Sexa $A \subset B$ unha extensión de aneis e $b \in B$. Entón equivalen:*

1. *b é enteiro sobre A.*
2. *$A[b]$ é un A-módulo finitamente xerado.*
3. *Existe un subanel $C \subset B$ tal que $A[b] \subset C$ e C é un A-módulo finitamente xerado.*

Demostración.
"1 $\Rightarrow$ 2" Se b é enteiro sobre A, entón existen $\lambda_1, \dots, \lambda_n \in A$ tales que:

$$b^n + \lambda_1 b^{n-1} + \cdots + \lambda_n = 0$$

Dado $r \in \mathbb{N}$, tense que:

$$b^n = -(\lambda_1 b^{n-1} + \cdots + \lambda_n)$$

$$b^{n+r} = -(\lambda_1 b^{n+r-1} + \cdots + \lambda_n b^r)$$

Isto quere dicir que toda potencia de b pode expresarse como unha combinación lineal dos elementos do conxunto $\{1, b, \dots, b^{n-1}\}$ con coeficientes en A, logo todo elemento de $A[b]$ é unha combinación lineal destes elementos, é dicir, $A[b]$ é un A-módulo finitamente xerado.

"2 $\Rightarrow$ 3" Basta con tomar $C = A[b]$.

"3 $\Rightarrow$ 1" Sexa $\phi : C \longrightarrow C$ o homomorfismo de A-módulos definido por $\phi(c) = bc$. É evidente ver que $\phi(C) \subset A[b]$, logo polo teorema de Cayley-Hamilton (1.3.5), existen os elementos $a_1, \dots, a_n \in A$ tales que $\phi^n + a_1\phi^{n-1} + \cdots + a_n I = 0$. Avaliando esta expresión en 1 obtense que $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, o cal implica que b é enteiro sobre A. ■

Corolario 1.3.7. *Sexa $A \subset B$ unha extensión de aneis. Se $b_1, \dots, b_n \in B$ son enteiros sobre A, entón $A[b_1, \dots, b_n]$ é un A-módulo finitamente xerado.*

Demostración. Probarase unicamente o caso de dous elementos, pois o de n elementos pode probarse facilmente mediante indución usando que $A[b_1, \dots, b_n] = A[b_1][b_2, \dots, b_n]$.

Na demostración da proposición anterior (1.3.6) probouse que, se b_1 e b_2 son enteiros sobre A, entón existen $r, s \in \mathbb{N}$ tales que $\{1, b_1, b_1^2, \dots, b_1^r\}$ xera $A[b_1]$ e $\{1, b_2, b_2^2, \dots, b_2^s\}$ xera $A[b_2]$. Entón é doado ver que o conxunto $\{b_1^i b_2^j \,/\, 1 \leq i \leq r,\ 1 \leq j \leq s\}$ xera $A[b_1, b_2]$. ■

Corolario 1.3.8. *Se $A \subset B$ e $B \subset C$ son extensións de aneis enteiras, entón a extensión $A \subset C$ tamén é enteira.*

Demostración. Sexa $c \in C$. Como C é enteiro sobre B, existen $b_1, \dots, b_n \in B$ tales que:

$$c^n + b_1 c^{n-1} + \cdots + b_n = 0$$

Logo c é tamén enteiro sobre $A[b_1, \dots, b_n]$. Polo corolario 1.3.7, $A[b_1, \dots, b_n]$ é un A-módulo finitamente xerado e $A[b_1, \dots, b_n, c]$ é un $A[b_1, \dots, b_n]$-módulo finitamente xerado, logo tamén é un A-módulo finitamente xerado. Entón, polo apartado 3. da proposición 1.3.6, c é enteiro sobre A. ■

Teorema 1.3.9. *Sexa $A \subset B$ unha extensión enteira de aneis tal que A e B son dominios. Entón A é un corpo se e soamente se B é un corpo.*

Demostración.

"⇒" Supoñamos que A é un corpo e sexa $y \in B \setminus \{0\}$. Este elemento é enteiro sobre A, logo existen $\lambda_1, \dots, \lambda_n \in A$ tales que:

$$y^n + \lambda_1 y^{n-1} + \cdots + \lambda_n = 0$$

$$-\lambda_n = y(y^{n-1} + \lambda_1 y^{n-2} + \cdots + \lambda_{n-1})$$

Supoñamos que se toma o n mínimo de entre os graos dos polinomios mónicos de $A[x]$ dos cales y é raíz. Entón tense que $y^{n-1} + \cdots + \lambda_{n-1} \neq 0$, e polo tanto $-\lambda_n \neq 0$ (pois B é un dominio). Como A é un corpo, existe λ_n^{-1}, e pódese multiplicar a igualdade anterior por $-\lambda_n^{-1}$, obtendo:

$$1 = -\lambda_n^{-1} y(y^{n-1} + \cdots + \lambda_{n-1})$$

Desta forma, probouse que o inverso de y existe e é $y^{-1} = -\lambda_n^{-1}(y^{n-1} + \cdots + \lambda_{n-1})$, logo B é un corpo.

"⇐" Supoñamos que B é un corpo e sexa $y \in A \setminus \{0\}$. Entón $y^{-1} \in B$, e é enteiro sobre A, logo existen $\lambda_1, \dots, \lambda_n \in A$ tales que:

$$(y^{-1})^n + \lambda_1 (y^{-1})^{n-1} + \cdots + \lambda_n = 0$$

Multiplicando a ambos lados da igualdade por λ^{n-1} obtense que:

$$y^{-1} + \lambda_1 + \lambda_2 y + \cdots + \lambda_n y^{n-1} = 0$$

$$y^{-1} = -(\lambda_1 + \lambda_2 y + \cdots + \lambda_n y^{n-1}) \in A$$

Probando así que A é un corpo. ■

Capítulo 2

Nullstellensatz Clásico

2.1. Preliminares de Variedades Afíns

A teoría de variedades afíns é moi importante para comprender as implicacións xeométricas do Nullstellensatz. Durante esta sección supoñerase que se traballa con un corpo K, mentres que K^n denotará o produto cartesiano de K consigo mesmo n veces, que ten estrutura de K-espazo vectorial.

Cometerase un certo abuso de notación ó denotar tamén por K^n o espazo afín sobre o espazo vectorial K^n, cuxos elementos son *puntos* en lugar de *vectores*, mais neste traballo non se utilizarán as súas propiedades como espazo afín. A cambio, isto fará máis intuitiva a notación.

Definición 2.1.1. Dado un subconxunto $S \subset K[x_1, \dots, x_n]$, defínese $V(S)$ como o conxunto dos puntos de K^n que anulan a todos os polinomios de S, é dicir:

$$V(S) := \{a \in K^n \,/\, f(a) = 0 \,\forall f \in S\}$$

Dise que un conxunto $\mathcal{V} \subset K^n$ é unha **variedade alxébrica afín**, a miúdo abreviado variedade, se existe un subconxunto $S \subset K[x_1, \dots, x_n]$ tal que $\mathcal{V} = V(S)$.

Definición 2.1.2. Dado un subconxunto $X \subset K^n$, defínese $I(X)$ como o conxunto dos polinomios de $K[x_1, \dots, x_n]$ que se anulan en todos os puntos de X, é dicir:

$$I(X) := \{f \in K[x_1, \dots, x_n] \,/\, f(a) = 0 \,\forall a \in X\}$$

Proposición 2.1.3. *Sexan os subconxuntos $S \subset K[x_1, \dots, x_n]$ e $X \subset K^n$. Entón tense que:*

1. $V(S) = V(\langle S \rangle)$
2. $I(X)$ *é un ideal de* $K[x_1, \dots, x_n]$.

Demostración.

1. É evidente ver pola definición que $V(\langle S\rangle) \subset V(S)$, así que probarase o outro contido. Sexan $a \in V(S)$ e $f \in \langle S\rangle$. Entón existen os polinomios $g_1, \dots, g_m \in K[x_1, \dots, x_n]$ e $f_1, \dots, f_m \in S$ tales que:
$$f = \sum_{i=1}^{m} g_i f_i$$
Polo tanto, avaliando f en a tense que:
$$f(a) = \sum_{i=1}^{m} g_i(a) f_i(a) = \sum_{i=1}^{m} g_i(a) \cdot 0 = 0$$
Concluíndo así que $a \in V(\langle S\rangle)$.

2. Sexan $f \in I(X)$, $g \in K[x_1, \dots, x_n]$ e $a \in X$. Entón tense que:
$$(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0$$
Polo tanto, $fg \in I(X)$, logo $I(X)$ é un ideal de $K[x_1, \dots, x_n]$.

■

Observación 2.1.4. A proposición anterior permite asumir que toda variedade alxébrica afín $\mathcal{V} \subset K^n$ é da forma $\mathcal{V} = V(\mathfrak{a})$, sendo $\mathfrak{a} \lhd K[x_1, \dots, x_n]$ un ideal. Para o caso particular dun ideal xerado por unha cantidade finita de elementos, $\mathfrak{a} = \langle f_1, \dots, f_m\rangle$, denotarase por $V(\mathfrak{a}) = V(f_1, \dots, f_m)$.

Proposición 2.1.5. *Tense as seguintes propiedades de V e I:*

1. *As aplicacións V e I inverten as inclusións, é dicir, se $\mathfrak{a} \subset \mathfrak{b}$, entón $V(\mathfrak{b}) \subset V(\mathfrak{a})$, e se $X \subset Y$, entón $I(Y) \subset I(X)$.*
2. *$V(0) = K^n$ e $V(K[x_1, \dots, x_n]) = \varnothing$*
3. *$I(\varnothing) = K[x_1, \dots, x_n]$ e, se K é un corpo infinito, $I(K^n) = 0$.*
4. *$V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ para todos ideais $\mathfrak{a}, \mathfrak{b} \lhd K[x_1, \dots, x_n]$.*
5. *$V\left(\bigcup_{\alpha\in A} \mathfrak{a}_\alpha\right) = V\left(\sum_{\alpha\in A} \mathfrak{a}_\alpha\right) = \bigcap_{\alpha\in A} V(\mathfrak{a}_\alpha)$ para toda familia de ideais $\{\mathfrak{a}_\alpha\}_{\alpha\in A}$.*
6. *$I\left(\bigcup_{\alpha\in A} X_\alpha\right) = \bigcap_{\alpha\in A} I(X_\alpha)$ para toda familia de conxuntos $\{X_\alpha\}_{\alpha\in A}$.*
7. *$V(I(V(\mathfrak{a}))) = V(\mathfrak{a})$ e $I(V(I(X))) = I(X)$.*

Demostración.

1. É inmediato pola definición.
2. É inmediato pola definición.
3. $I(\varnothing) = K[x_1, \dots, x_n]$ é inmediato pola definición, pero a segunda afirmación deste apartado é máis complexa, e require do Nullstellensatz forte para ser probada, así que non se probará ata que se enuncie e probe ese teorema. Sí é doado ver que, se K é un corpo finito, pódese construír un polinomio non nulo que se anule en todo K^n.
4. É inmediato ver que $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b}$, logo, polo apartado 1. tense que:

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) \subset V(\mathfrak{a} \cap \mathfrak{b}) \subset V(\mathfrak{ab})$$

   Para probar as outras inclusións, sexa $a \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$. Entón existen $f \in \mathfrak{a}$ e $g \in \mathfrak{b}$ tales que $f(a) \neq 0$ e $g(a) \neq 0$, logo $(fg)(a) \neq 0$, e $a \notin V(\mathfrak{ab})$.
5. Que $V\left(\bigcup_{\alpha \in A} \mathfrak{a}_\alpha\right) = \bigcap_{\alpha \in A} V(\mathfrak{a}_\alpha)$ é inmediato pola definición. O resto deste apartado dedúcese de que $\sum_{\alpha \in A} \mathfrak{a}_\alpha = \left\langle \bigcup_{\alpha \in A} \mathfrak{a}_\alpha \right\rangle$.
6. É inmediato pola definición.
7. É inmediato ver pola definición que $X \subset V(I(X))$ e que $\mathfrak{a} \subset I(V(\mathfrak{a}))$, logo isto implica que $V(\mathfrak{a}) \subset V(I(V(\mathfrak{a})))$ e $I(X) \subset I(V(I(X)))$, e aplicando o apartado 1, que $V(I(V(\mathfrak{a}))) \subset V(\mathfrak{a})$ e $I(V(I(X))) \subset I(X)$.

■

Definición 2.1.6. Un anel A dise que é **noetheriano** se toda cadea de ideais da forma $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset A$ é estacionaria, é dicir, existe un $r \in \mathbb{N}$ tal que $\mathfrak{a}_r = \mathfrak{a}_{r+t}\ \forall t \in \mathbb{N}$. Por exemplo, todo dominio de ideais principais é noetheriano, así como todo corpo.

Teorema 2.1.7. *Sexa A un anel. Entón son equivalentes:*

1. *A é un anel noetheriano.*
2. *Cada conxunto de ideais de A ten un elemento maximal respecto da inclusión.*
3. *Cada ideal de A é finitamente xerado.*

Demostración. Ver [4], páxina 656, teorema 2. ■

Teorema 2.1.8 (Teorema da Base de Hilbert)**.** *Se A é un anel noetheriano, entón o anel $A[x_1, \dots, x_n]$ tamén é noetheriano.*

Demostración. Ver [13], páxina 37, teorema 2.7. ■

Corolario 2.1.9. *Sexa $\mathcal{V} \subset K^n$ unha variedade. Entón existen $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ tales que $\mathcal{V} = V(f_1, \dots, f_m)$.*

Demostración. Como K é noetheriano por ser un corpo, aplicando o *Teorema da Base de Hilbert* (2.1.8), $K[x_1, \dots, x_n]$ tamén é noetheriano.

Como $\mathcal{V}$ é unha variedade, existe un ideal $\mathfrak{a} \triangleleft K[x_1, \dots, x_n]$ tal que $\mathcal{V} = V(\mathfrak{a})$. Polo teorema 2.1.7, $\mathfrak{a}$ é un ideal finitamente xerado, logo existen $f_1, \dots, f_n$ tales que $\mathfrak{a} = \langle f_1, \dots, f_n \rangle$, e polo tanto $\mathcal{V} = V(\mathfrak{a}) = V(f_1, \dots, f_n)$. ■

Proposición 2.1.10. *Sexa $a = (a_1, \dots, a_n) \in K^n$ un punto do espazo afín. Entón tense que $V(x_1 - a_1, \dots, x_n - a_n) = \{a\}$. En particular, todo subconxunto finito de K^n é unha variedade.*

Demostración. É evidente ver que $a \in V(x_1 - a_1, \dots, x_n - a_n)$, e que ningún outro punto de K^n anula simultaneamente ós polinomios $x_1 - a_1, \dots, x_n - a_n$. ■

Definición 2.1.11. Polas propiedades enunciadas na proposición 2.1.5, $\varnothing$ e K^n son variedades, a unión finita de variedades é unha variedade, e a intersección arbitraria de variedades é unha variedade. Polo tanto, as variedades forman o conxunto de pechados dunha topoloxía en K^n, a chamada **topoloxía de Zariski**, cuxos abertos son os complementarios das variedades.

Observación 2.1.12. No caso dos corpos $\mathbb{C}$ ou $\mathbb{R}$, a topoloxía de Zariski é máis grosa que a usual, é dicir, todo aberto de Zariski é aberto usual, mais existen abertos usuais que non son abertos segundo Zariski.

Definición 2.1.13. Sexa $\mathcal{V} \subset K^n$ unha variedade. Defínese o seu **anel de coordenadas** como $K[\mathcal{V}] = K[x_1, \dots, x_n]/I(\mathcal{V})$.

Este anel é de gran importancia para o estudo das variedades, pois dados dous polinomios $f, g \in K[x_1, \dots, x_n]$, estes son iguais en $\mathcal{V}$ se e soamente se $f + I(\mathcal{V}) = g + I(\mathcal{V})$ en $K[\mathcal{V}]$. É doado ver que $K[\mathcal{V}]$ ten estrutura de K-álxebra, que é finitamente xerada por $x_1 + I(\mathcal{V}), \dots, x_n + I(\mathcal{V})$.

Definición 2.1.14. Sexa A un anel e $\mathfrak{a} \triangleleft A$ un ideal do mesmo. Defínese o **radical** de $\mathfrak{a}$ como o conxunto:

$$\operatorname{rad}(\mathfrak{a}) := \{a \in A \,/\, a^n \in \mathfrak{a} \text{ para un certo } n \in \mathbb{N}\}$$

É doado ver que $\operatorname{rad}(\operatorname{rad}(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a})$, $\mathfrak{a} \subset \operatorname{rad}(\mathfrak{a})$ e que $\operatorname{rad}(\mathfrak{a})$ é sempre un ideal.

Proposición 2.1.15. *Sexa A un anel e $\mathfrak{a} \lhd A$ un ideal do mesmo. Entón o radical de $\mathfrak{a}$ é a intersección dos ideais primos de A que conteñen a $\mathfrak{a}$, é dicir:*

$$\operatorname{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(A) \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p}$$

Demostración. Ver [4], páxina 674, proposición 12. ■

Corolario 2.1.16. *Sexa $\mathfrak{m} \lhd K[x_1, \dots, x_n]$ un ideal maximal. Entón* $\operatorname{rad}(\mathfrak{m}) = \mathfrak{m}$.

Demostración. É inmediato usando a proposición anterior (2.1.15) e o feito de que $\mathfrak{m}$ é un ideal primo. Este corolario tamén pódese probar directamente probando que $\operatorname{rad}(\mathfrak{m})$ é un ideal propio, pois como $\mathfrak{m} \subset \operatorname{rad}(\mathfrak{m})$ e $\mathfrak{m}$ é maximal isto implica a igualdade buscada. ■

Proposición 2.1.17. *Sexa $X \subset K^n$ un subconxunto. Entón $I(X)$ é un ideal radical, é dicir,* $\operatorname{rad}(I(X)) = I(X)$.

Demostración. A inclusión $I(X) \subset \operatorname{rad}(I(X))$ é inmediata, así que probarase a restante. Sexa $f \in \operatorname{rad}(I(X))$. Entón existe un $m \in \mathbb{N}$ tal que $f^m \in I(X)$. Dado un $a \in X$, tense que $f(a)^m = 0$, logo $f(a) = 0$, e isto implica que $f \in I(X)$, como queríamos probar. ■

Proposición 2.1.18. *Sexa $a = (a_1, \dots, a_n) \in K^n$ un punto do espazo afín. Entón tense que $I(\{a\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$, e este ideal é maximal*

Demostración. É evidente ver que $I(\{a\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Sexa un homomorfismo de aneis $\varphi : K[x_1, \dots, x_n] \longrightarrow K[x_1, \dots, x_n]$ tal que $\varphi(x_i) = x_i - a_i \; \forall i \in \{1, \dots, n\}$, que é claramente un isomorfismo. Entón tense que:

$$K \simeq \frac{K[x_1, \dots, x_n]}{\langle x_1, \dots, x_n \rangle} \simeq \frac{K[x_1, \dots, x_n]}{\langle x_1 - a_1, \dots, x_n - a_1 \rangle}$$

Como K é un corpo, entón $\langle x_1 - a_1, \dots, x_n - a_1 \rangle$ é un ideal maximal. ■

Observación 2.1.19. Con esta última proposición (2.1.18) pódese deducir que os puntos de K^n correspóndense con ideais maximais de $K[x_1, \dots, x_n]$ mediante I, mais esta aplicación non é necesariamente sobrexectiva, pois poden existir ideais maximais que non se corresponden con puntos. Un exemplo pode atoparse en $\mathbb{R}[x]$ co ideal maximal $\mathfrak{m} = \langle x^2 + 1 \rangle$, que é tal que $V(\mathfrak{m}) = \varnothing$. Neste tema verase que se K é alxebricamente pechado, isto non pode ocorrer, e no seguinte tema falarase máis a fondo deste suceso e como caracterizalo para un corpo arbitrario, utilizando a versión xeral do Nullstellensatz.

2.2. Álxebras sobre un Corpo

Nesta sección probaranse os dous enunciados clásicos do Nullstellensatz: a versión débil e a forte. Antes diso, enunciarase un lema auxiliar, o *Lema de Zariski*, que empregarase para probar a versión débil. Logo utilizarase o chamado *truco de Rabinowich* para probar a versión forte a partir da débil.

Lema 2.2.1 (Lema de Zariski)**.** *Sexa $F : K$ unha extensión de corpos e $\alpha_1, \dots, \alpha_n \in F$. Se a K-álxebra finitamente xerada $K[\alpha_1, \dots, \alpha_n]$ é un corpo, entón cada α_i é alxébrico sobre K. En particular, se K é alxebricamente pechado, tense que $\alpha_i \in K \; \forall i \in \{1, \dots, n\}$.*

Demostración. Probarase mediante indución en n:

No caso de $n = 1$, se α_1 non fose alxébrico sobre K, entón $K[\alpha_1]$ sería isomorfo a un anel de polinomios, e polo tanto non podería ser un corpo.

Supoñamos que o lema verifícase para $n - 1$ elementos e que $K[\alpha_1, \dots, \alpha_n]$ é un corpo. Denotando por $E = K(\alpha_1)$, tense que:

$$K \subset K[\alpha_1] \subset E \subset K[\alpha_1, \dots, \alpha_n]$$

Sendo a última inclusión debida a que E é o corpo máis pequeno que contén a $K[\alpha_1]$.

A continuación probarase que $K[\alpha_1, \dots, \alpha_n] = E[\alpha_2, \dots, \alpha_n]$, sendo a inclusión "$\subset$" inmediata, pois $K[\alpha_1] \subset E$. Por outra parte, como $K[\alpha_1, \dots, \alpha_n]$ é un corpo, entón coincide co seu corpo de fraccións, $K(\alpha_1, \dots, \alpha_n)$, que é tal que $E[\alpha_2, \dots, \alpha_n] \subset K(\alpha_1, \dots, \alpha_n)$.

Entón tense que $E[\alpha_2, \dots, \alpha_n]$ é tamén un corpo, e aplicándolle a hipótese de indución, $\alpha_2, \dots, \alpha_n$ son alxébricos sobre E, é dicir, existen os polinomios $f_2, \dots, f_n \in E[x]$ tales que $f_i(\alpha_i) = 0 \; \forall i \in \{2, \dots, n\}$. Os seus coeficientes son elementos de $E = K(\alpha_1)$, é dicir, fraccións de polinomios con coeficientes en K avaliados en α_1. Ademais estes polinomios poden supoñerse mónicos debido a que E é un corpo.

Fixado un $i \in \{2, \dots, n\}$, existen $a_1, \dots, a_m \in E$ tales que:

$$f_i(x) = x^m + a_1 x^{m-1} + \cdots + a_m$$

$$f_i(\alpha_i) = \alpha_i^m + a_1 \alpha_i^{m-1} + \cdots + a_m = 0$$

Sexa $D \in K[\alpha_1]$ o produto dos denominadores dos coeficientes de todos os f_i. Multiplicando por D^m a ambos lados da igualdade anterior obtense:

$$D^m f_i(\alpha_i) = (D\alpha_i)^m + Da_1(D\alpha_i)^{m-1} + \cdots + D^m a_m = 0$$

Sexa $K[\alpha_1]_D$ a localización de $K[\alpha_1]$ no ideal xerado por D. Entón tense que $D\alpha_i$ é enteiro sobre $K[\alpha_1]$, e en particular sobre $K[\alpha_1]_D$, para todo $i \in \{2, \dots, n\}$. Como D ten inverso en $K[\alpha_1]_D$, entón cada α_i é enteiro sobre $K[\alpha_1]_D$, e a extensión de aneis $K[\alpha_1]_D \subset K[\alpha_1, \dots, \alpha_n]$ é enteira.

Aplicando o teorema 1.3.9, como $K[\alpha_1, \dots, \alpha_n]$ é un corpo, entón $K[\alpha_1]_D$ tamén é un corpo, e como está contido en $K(\alpha_1)$ pola súa definición, entón $K[\alpha_1]_D = K(\alpha_1)$.

Nesta situación, se α_1 non fose alxébrico sobre K, entón $K[\alpha_1]$ sería isomorfo a un anel de polinomios, e teríase unha contradición coa igualdade $K[\alpha_1]_D = K(\alpha_1)$, pois entón todas as fraccións de $K(\alpha_1)$ terían como denominador potencias dun único polinomio, D, mais este non pode ser o caso, pois existen infinitos polinomios irreducibles en $K[\alpha_1]$. Entón necesariamente α_1 é alxébrico sobre K. Por transitividade, $\alpha_2, \dots, \alpha_n$ son alxébricos sobre $K[y_1]$, que é unha extensión alxébrica de K polo caso de $n = 1$, e polo tanto son tamén alxébricos sobre K (teorema 1.2.15). ■

Teorema 2.2.2 (Nullstellensatz débil)**.** *Sexa K un corpo alxebricamente pechado e un ideal maximal $\mathfrak{m} \lhd K[x_1, \dots, x_n]$. Entón existen $a_1, \dots, a_n \in K$ tales que:*

$$f(a_1, \dots, a_n) = 0 \; \forall f \in \mathfrak{m}$$

Demostración. Tense que $L = K[x_1, \dots, x_n]/\mathfrak{m}$ é un corpo e unha K-álxebra finitamente xerada. Entón, polo *Lema de Zariski* (2.2.1), é tamén unha extensión alxébrica de K, pero como este corpo é alxebricamente pechado, entón $K \simeq L$, mediante o isomorfismo $\varphi : K \longrightarrow L$. Debido á definición de L, φ necesariamente ten que ser da forma $\varphi = \pi \circ i$, sendo $\pi : K[x_1, \dots, x_n] \longrightarrow L$ a proxección cociente e $i : K \longrightarrow K[x_1, \dots, x_n]$ a inclusión.

$$\begin{array}{ccc} K[x_1, \dots, x_n] & \xrightarrow{\pi} & L \\ {\scriptstyle i}\uparrow & \nearrow_{\varphi} & \\ K & & \end{array}$$

Sexan $a_1, \dots, a_n \in K$ os elementos tales que $\varphi(a_i) = x_i + \mathfrak{m} \; \forall i \in \{1, \dots, n\}$. Dado un polinomio $f \in \mathfrak{m}$ arbitrario, tense que:

$$\varphi(f(a_1, \dots, a_n)) = f(\varphi(a_1), \dots, \varphi(a_n)) = f(x_1 + \mathfrak{m}, \dots, x_n + \mathfrak{m}) = f(x_1, \dots, x_n) + \mathfrak{m} = 0 + \mathfrak{m}$$

Como φ é un isomorfismo, tense que $\mathrm{Ker}(\varphi) = 0$, logo $f(a_1, \dots, a_n) = 0$. ■

Corolario 2.2.3. *Sexa K un corpo alxebricamente pechado e $\mathfrak{a} \lhd K[x_1, \dots, x_n]$ un ideal propio. Entón existen $a_1, \dots, a_n \in K$ tales que $f(a_1, \dots, a_n) = 0 \; \forall f \in \mathfrak{a}$.*

Demostración. Como $\mathfrak{a}$ é un ideal propio, existe un ideal maximal $\mathfrak{m} \triangleleft K[x_1, \dots, x_n]$ tal que $\mathfrak{a} \subset \mathfrak{m}$. Aplicando o *Nullstellensatz débil* (2.2.2), existen os elementos $a_1, \dots, a_n \in K$ tales que $f(a_1, \dots, a_n) = 0 \; \forall f \in \mathfrak{m}$, o cal implica claramente que $f(a_1, \dots, a_n) = 0 \; \forall f \in \mathfrak{a}$ ■

Observación 2.2.4 (Conexión xeométrica). Unha consecuencia inmediata do Nullstellensatz débil é que no contexto das variedades afíns, se K é un corpo alxebricamente pechado e $\mathfrak{m} \triangleleft K[x_1, \dots, x_n]$ un ideal maximal, entón existe un $a = (a_1, \dots, a_n) \in V(\mathfrak{m}) \neq \varnothing$.

De feito, debido á construción deste punto na proba anterior, $V(\mathfrak{m}) = \{a\}$, e é tal que $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$, o cal permite establecer unha correspondencia bixectiva entre os ideais maximais de $K[x_1, \dots, x_n]$ e os puntos de K^n.

Por outra parte, o corolario 2.2.3 é equivalente a que toda variedade $V(\mathfrak{a})$ (sendo $\mathfrak{a}$ un ideal propio) sexa non baleira, é dicir, todo sistema de ecuacións polinómicas no que 1 non sexa combinación lineal das ecuacións ten solución, xeneralizando este resultado xa coñecido para unha variábel.

Dado un ideal $\mathfrak{a} \triangleleft K[x_1, \dots, x_n]$, debido a que toda variedade é a unión dos puntos que a conforman e os puntos correspóndense mediante I cos ideais maximais, tense que:

$$I(V(\mathfrak{a})) = I\left(\bigcup_{a \in V(\mathfrak{a})} a\right) = \bigcap_{a \in V(\mathfrak{a})} I(\{a\}) = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{a} \subset \mathfrak{m}}} \mathfrak{m}$$

Unha cuestión de interese para a xeometría alxébrica é cando un polinomio $f \in K[x_1, \dots, x_n]$ anúlase nos puntos dunha variedade afín $V(\mathfrak{a}) \subset K^n$, é dicir, cando $f \in I(V(\mathfrak{a}))$. O Nullstellensatz forte da unha resposta clara a esa pregunta, que é cando $f \in \operatorname{rad}(\mathfrak{a})$.

Teorema 2.2.5 (Nullstellensatz forte)**.** *Sexa K un corpo alxebricamente pechado e un ideal $\mathfrak{a} \triangleleft K[x_1, \dots, x_n]$. Entón tense que:*

$$\operatorname{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{a} \subset \mathfrak{m}}} \mathfrak{m} = I(V(\mathfrak{a}))$$

Demostración. Probaranse as dúas inclusións:

"$\subset$" Pola proposición 2.1.15, $\operatorname{rad}(\mathfrak{a})$ é a intersección dos ideais primos que conteñen a $\mathfrak{a}$, logo está contido na intersección dos maximais que conteñen a $\mathfrak{a}$.

"$\supset$" Sexa $f \in I(V(\mathfrak{a}))$. Para probar que f pertence a $\operatorname{rad}(A)$ utilizarase o chamado *truco de Rabinowich.*

Sexa $\mathfrak{a}^e \triangleleft K[x_1, \dots, x_n, x_{n+1}]$ o ideal extensión de $\mathfrak{a}$ a través do homomorfismo inclusión $i : K[x_1, \dots, x_n] \longrightarrow K[x_1, \dots, x_{n+1}]$, que é tal que $\mathfrak{a}^e = \mathfrak{a}K[x_1, \dots, x_{n+1}]$. Sexa o ideal $\mathfrak{b} = \mathfrak{a}^e + \langle 1 - x_{n+1} f \rangle$. Para cada $(a_1, \dots, a_{n+1}) \in K^{n+1}$ poden darse dous casos:

1. Todos os polinomios de $\mathfrak{a}$ anúlanse en $(a_1, \dots, a_n)$, é dicir, $(a_1, \dots, a_n) \in V(\mathfrak{a})$. Entón, como $f \in I(V(\mathfrak{a}))$, tense que $f(a_1, \dots, a_n) = 0$. Polo tanto, $1 - x_{n+1}f$ non pode anularse en $(a_1, \dots, a_{n+1})$.

2. Non todos os polinomios de $\mathfrak{a}$ anúlanse en $(a_1, \dots, a_n)$. Entón existe un elemento de $\mathfrak{a}^e$ que non é anulado por $(a_1, \dots, a_{n+1})$.

Logo tense que non existe ningún punto de K^{n+1} que anule a todos os polinomios do ideal $\mathfrak{b}$, polo que, debido ó corolario do *Nullstellensatz débil* (2.2.3), $\mathfrak{b}$ non pode ser un ideal propio, logo $1 \in \mathfrak{b}$, é dicir, existen os polinomios $Q_1, \dots, Q_k \in \mathfrak{a}$ e $R_1, \dots, R_k, S \in K[x_1, \dots, x_{n+1}]$ tales que:

$$1 = \sum_{j=1}^{k} R_j Q_j + S(1 - x_{n+1}f)$$

Denotando $\mathfrak{c} = \langle 1 - x_{x+1}f \rangle$ e pasando esta igualdade ó anel cociente $K[x_1, \dots, x_{n+1}]/\mathfrak{c}$, tense que:

$$1 + \mathfrak{c} = \sum_{j=1}^{k} R_j Q_j + \mathfrak{c}$$

Neste anel cociente, a clase de x_{n+1} é o inverso da de f, logo existe un $m \in \mathbb{N}$ tal que $f^m R_j \in K[x_1, \dots, x_n]\ \forall j \in \{1, \dots, k\}$, e polo tanto, como $Q_j \in \mathfrak{a}\ \forall j \in \{1, \dots, k\}$, tense que:

$$f^m = \sum_{j=1}^{k} (f^m R_j) Q_j \in \mathfrak{a}$$

■

Proposición 2.2.6. *Sexa K un corpo alxebricamente pechado (polo tanto infinito). Entón $I(K^n) = 0$.*

Demostración. É inmediato ver que $V(0) = K^n$, logo, polo *Nullstellensatz forte* (2.2.5) tense que:

$$I(K^n) = I(V(0)) = \mathrm{rad}(0) = 0$$

■

Capítulo 3

Xeneralización a Aneis de Jacobson

Neste capítulo introducirase o concepto de anel de Jacobson e algunhas das súas propiedades para enunciar unha versión máis xeral do Nullstellensatz, que trata con álxebras e aneis de Jacobson en lugar de corpos alxebricamente pechados, dando lugar a un teorema máis abstracto, pero que xeneraliza ó Nullstellensatz forte enunciado no tema anterior.

3.1. Preliminares de Aneis de Jacobson

Definición 3.1.1. Un anel A dise que é **de Jacobson** se para todo ideal primo $\mathfrak{p} \lhd A$, tense que:

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{p} \subset \mathfrak{m}}} \mathfrak{m}$$

Con esta definición é inmediato ver que todo corpo é un anel de Jacobson, e que todo anel local é de Jacobson se e soamente se o seu ideal maximal é o único ideal primo.

Observación 3.1.2. O radical dun ideal é a intersección dos ideais primos que o conteñen (proposición 2.1.15), mais nun anel de Jacobson, como os ideais primos son a intersección dos maximais que os conteñen, o radical dun ideal é a intersección dos maximais que o conteñen, o cal é unha compoñente importante do enunciado do Nullstellensatz forte. Non todo anel é de Jacobson, mais probarase que o anel de polinomios dun corpo sí o é.

Lema 3.1.3. *Sexa A un anel de Jacobson e $\mathfrak{a} \lhd A$ un ideal do mesmo. Entón $A/\mathfrak{a}$ é un anel de Jacobson.*

Demostración. Sexa $\mathfrak{p} \lhd A/\mathfrak{a}$ un ideal primo tal que $\mathfrak{p} = \mathfrak{q} + \mathfrak{a}$ para un certo ideal primo $\mathfrak{q} \lhd A$ tal que $\mathfrak{a} \subset \mathfrak{q}$. Por ser A de Jacobson, $\mathfrak{q}$ é intersección dos ideais maximais en A que o conteñen, e polo tanto, $\mathfrak{p}$ é intersección das clases deses ideais no cociente, que son claramente maximais e conteñen a $\mathfrak{p}$, probando así que $A/\mathfrak{a}$ é de Jacobson. ■

3.2. Nullstellensatz Xeral

Lema 3.2.1. *Sexa A un anel. Entón son equivalentes:*

1. *A é de Jacobson.*
2. *Se $\mathfrak{p} \lhd A$ é un ideal primo tal que en $A/\mathfrak{p}$ existe un elemento non nulo $a+\mathfrak{p} \in A/\mathfrak{p}$ para o cal $(A/\mathfrak{p})_{a+\mathfrak{p}}$ (que denota a localización $(A/\mathfrak{p})[(a+\mathfrak{p})^{-1}]$) é un corpo, entón $A/\mathfrak{p}$ é un corpo.*

Demostración.

"1 $\Rightarrow$ 2" Sexa $\mathfrak{p} \lhd A$ un ideal primo tal que existe un elemento non nulo $a+\mathfrak{p} \in A/\mathfrak{p}$ para o cal $(A/\mathfrak{p})_{a+\mathfrak{p}}$ é un corpo. Como A é de Jacobson e $\mathfrak{p}$ primo, entón $A/\mathfrak{p}$ é un dominio de Jacobson, polo que $0+\mathfrak{p}$ é primo, e é a intersección de todos os ideais maximais de $A/\mathfrak{p}$:

$$0+\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \lhd A/\mathfrak{p} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$$

Doutra banda, os ideais primos non nulos de $(A/\mathfrak{p})_{a+\mathfrak{p}}$ están en correspondencia bixectiva cos ideais primos de $A/\mathfrak{p}$ que non conteñen a $a+\mathfrak{p}$. Como $(A/\mathfrak{p})_{a+\mathfrak{p}}$ é un corpo, non ten ideais primos non nulos, polo que todos os ideais primos de $A/\mathfrak{p}$ conteñen a $a+\mathfrak{p}$. Logo, para que a intersección dos ideais maximais sexa $0+\mathfrak{p}$, como se probou antes, un deses maximais ten que ser o propio $0+\mathfrak{p}$, pois todos os maximais non nulos conteñen a $a+\mathfrak{p}$, que por hipótese é non nulo. Todo anel no que o ideal nulo é maximal é un corpo, probando así que $A/\mathfrak{p}$ é un corpo.

"2 $\Rightarrow$ 1" Sexa $\mathfrak{q} \lhd A$ un ideal primo e $\mathfrak{i}$ o ideal intersección de todos os ideais maximais de A que conteñen a $\mathfrak{q}$. Probarase que $\mathfrak{i} = \mathfrak{q}$, sendo a inclusión $\mathfrak{q} \subset \mathfrak{i}$ inmediata por definición.

Se ocorrese que $\mathfrak{q} \subsetneq \mathfrak{i}$, entón sexa $a \in \mathfrak{i} \setminus \mathfrak{q}$. Debido ó *Lema de Zorn*, existe un ideal $\mathfrak{p} \lhd A$ que é maximal entre os ideais de A que conteñen a $\mathfrak{q}$ mais non a a. É doado probar que este ideal é primo. Sexa $\mathfrak{m} \lhd A$ un ideal maximal tal que $\mathfrak{p} \subset \mathfrak{m}$. Logo tense que $\mathfrak{q} \subset \mathfrak{p} \subset \mathfrak{m}$, e como $a \in \mathfrak{i}$ e pola definición de $\mathfrak{i}$, tense que $a \in \mathfrak{m}$, logo $\mathfrak{p} \subsetneq \mathfrak{m}$, o cal implica que $\mathfrak{p}$ non é maximal e $A/\mathfrak{p}$ non é un corpo.

Por outra parte, vexamos que $\mathfrak{p}A[a^{-1}]$ é maximal en $A[a^{-1}]$. Sexa $\mathfrak{a}A[a^{-1}] \lhd A[a^{-1}]$ un ideal tal que $\mathfrak{p}A[a^{-1}] \subset \mathfrak{a}A[a^{-1}]$. Entón tense que $\mathfrak{p} \subset \mathfrak{a}$, e polo tanto, $\mathfrak{q} \subset \mathfrak{p} \subset \mathfrak{a}$, pero como $\mathfrak{p}$ era maximal entre os ideais que contiñan a $\mathfrak{q}$ mais non a a, entón ben $\mathfrak{p} = \mathfrak{a}$ ou $a \in \mathfrak{a}$. No segundo caso teríase que $a/a = 1 \in \mathfrak{a}A[a^{-1}]$, o cal implica que $\mathfrak{a}A[a^{-1}] = A[a^{-1}]$, probando así que $\mathfrak{p}A[a^{-1}]$ é maximal.

Desta forma, como $(A/\mathfrak{p})_{a+\mathfrak{p}} = A[a^{-1}]/\mathfrak{p}A[a^{-1}]$ e $\mathfrak{p}A[a^{-1}]$ é maximal, entón $(A/\mathfrak{p})_{a+\mathfrak{p}}$ é un corpo, mentres que $A/\mathfrak{p}$ non, contradicindo así o apartado 2. ■

Corolario 3.2.2. *Sexa A un dominio de Jacobson. Se existe un elemento $a \in A$ tal que $A[a^{-1}]$ é un corpo, entón A é un corpo.*

Demostración. Basta tomar o ideal primo 0 no enunciado do apartado 2 do lema anterior. ■

Lema 3.2.3. *Sexa A un anel, (B, φ) unha A-álxebra e $\mathfrak{b} \triangleleft B$. Entón $B/\mathfrak{b}$ é unha $A/A\cap\mathfrak{b}$-álxebra cuxo homomorfismo de aneis é inxectivo, é dicir, $A/A\cap\mathfrak{b}$ é isomorfo a un subanel de $B/\mathfrak{b}$.*

Demostración. Defínese o homomorfismo de aneis que fai a $B/\mathfrak{b}$ unha $A/A\cap\mathfrak{b}$-álxebra como:

$$\begin{aligned} \tilde{\varphi} : \frac{A}{A\cap\mathfrak{b}} &\longrightarrow \frac{B}{\mathfrak{b}} \\ a + A\cap\mathfrak{b} &\longrightarrow \varphi(a) + \mathfrak{b} \end{aligned}$$

Este homomorfismo está ben definido, pois dados $a, a' \in A$ tales que $a + A\cap\mathfrak{b} = a' + A\cap\mathfrak{b}$ (é dicir, $a - a' \in A\cap\mathfrak{b}$), tense que:

$$A\cap\mathfrak{b} = \varphi^{-1}(\mathfrak{b}) \Rightarrow \varphi(a-a') = \varphi(a) - \varphi(a') \in \mathfrak{b} \Rightarrow \varphi(a) + \mathfrak{b} = \varphi(a') + \mathfrak{b} \Rightarrow \tilde{\varphi}(a) = \tilde{\varphi}(a')$$

E ademais é inxectivo, pois dados $a, a' \in A$ tales que $\tilde{\varphi}(a + A\cap\mathfrak{b}) = \tilde{\varphi}(a' + A\cap\mathfrak{b})$, tense que:

$$\tilde{\varphi}(a + A\cap\mathfrak{b}) = \tilde{\varphi}(a' + A\cap\mathfrak{b}) \Rightarrow \varphi(a) + \mathfrak{b} = \varphi(a') + \mathfrak{b} \Rightarrow \varphi(a) - \varphi(a') = \varphi(a-a') \in \mathfrak{b} \Rightarrow$$

$$\Rightarrow a - a' \in \varphi^{-1}(\mathfrak{b}) = A\cap\mathfrak{b} \Rightarrow a + A\cap\mathfrak{b} = a' + A\cap\mathfrak{b}$$

Como queríamos probar. ■

Lema 3.2.4. *Sexa K un corpo. Entón o anel de polinomios $K[x]$ é de Jacobson, e para todo ideal maximal $\mathfrak{m} \triangleleft K[x]$, tense que $K\cap\mathfrak{m} = 0$, e $K[x]/\mathfrak{m}$ é unha extensión finita de K.*

Demostración. Sábese que $K[x]$ é un dominio de ideais principais. Ademais, cada ideal primo non nulo do mesmo está xerado por un polinomio mónico e irreducíbel, e polo tanto ese ideal é tamén maximal, pois os polinomios irreducíbeis non teñen divisores, é dicir, os ideais que xeran non están contidos noutros ideais. Ademais, $K[x]$ é unha K-álxebra co homomorfismo inclusión $i : K \longrightarrow K[x]$, que leva cada $a \in K$ no polinomio constante $a \in K[x]$.

Sexa $\mathfrak{m} \triangleleft K[x]$ un ideal maximal. Como K é un corpo e $K \cap \mathfrak{m}$ un ideal do mesmo, $K \cap \mathfrak{m}$ so pode ser 0 ou K, e no segundo caso teríase que $1 \in \mathfrak{m}$, logo $\mathfrak{m} = K[x]$, contradicindo o feito de que $\mathfrak{m}$ sexa maximal en $K[x]$. Polo tanto tense que $K \cap \mathfrak{m} = 0$, $K/K \cap \mathfrak{m} = K/0 = K$, e $K[x]/\mathfrak{m}$ é unha extensión de K finitamente xerada por $x + \mathfrak{m}$. Como $x + \mathfrak{m}$ é alxébrico sobre K (é raíz de calquera $f \in \mathfrak{m}$), entón a extensión é finita (teorema 1.2.13).

Falta probar que $K[x]$ é de Jacobson. Dado que os ideais primos non nulos de $K[x]$ son maximais, basta con probar que o ideal 0 é a intersección de todos os ideais maximais. Se probásemos que $K[x]$ ten infinitos polinomios mónicos irreducíbeis probaríase que ten tamén infinitos ideais maximais, e para que a intersección de todos eles fose distinta de 0 tería que existir un polinomio con infinitos factores irreducíbeis, o cal sábese que non existe, e así teríase probado que $K[x]$ é de Jacobson.

Para probar a infinidade dos polinomios mónicos irreducíbeis pódese usar o argumento de Euclides, co cal, a partir dunha lista finita deles, $f_1, \dots, f_n \in K[x]$, constrúese un novo da forma $f_{n+1} = 1 + \prod_{i=1}^{n} f_i$. ■

Teorema 3.2.5 (Nullstellensatz xeral)**.** *Sexa A un anel de Jacobson e (B, φ) unha A-álxebra finitamente xerada. Entón tense que:*

1. *B é un anel de Jacobson.*
2. *Se $\mathfrak{m} \triangleleft B$ é un ideal maximal, entón $A \cap \mathfrak{m}$ é un ideal maximal en A, e o corpo $B/\mathfrak{m}$ é unha extensión finita de $A/A \cap \mathfrak{m}$.*

Demostración. Probarase mediante indución en r, o número de xeradores de B como A-álxebra.

No caso de $r = 1$, polo lema 3.2.1, hai que probar que, se $\mathfrak{p} \triangleleft B$ é un ideal primo tal que existe un elemento non nulo $b + \mathfrak{p} \in B/\mathfrak{p}$ para o cal $(B/\mathfrak{p})_{b+\mathfrak{p}}$ é un corpo, entón $B/\mathfrak{p}$ é un corpo.

Sexa $\mathfrak{p} \triangleleft B$ un ideal primo. Entón $B/\mathfrak{p}$ é un dominio, e como $A \cap \mathfrak{p} = \varphi^{-1}(\mathfrak{p})$, entón $A \cap \mathfrak{p}$ é un ideal primo de A, $A/A \cap \mathfrak{p}$ é un dominio, e este é de Jacobson por selo A e polo lema 3.1.3. Polo lema 3.2.3, $B/\mathfrak{p}$ é unha $A/A \cap \mathfrak{p}$-álxebra finitamente xerada cuxo homomorfismo de aneis é inxectivo, logo $A/A \cap \mathfrak{p}$ é isomorfo a un subanel de $B/\mathfrak{b}$, é dicir, podemos reducirnos ó caso no que A e B son dominios tales que $A \subset B$, e temos que probar que se existe un $b \in B$ tal que $B[b^{-1}]$ é un corpo, entón B é un corpo. Probarase de feito que nese caso A é tamén un corpo, e que $B : A$ é unha extensión finita, probando así o apartado 2.

Sexa $t \in B$ o elemento que xera B como A-álxebra. Entón, pola proposición 1.1.3, existe un homomorfismo de aneis sobrexectivo $\psi : A[x] \longrightarrow B$ definido por:

$$\psi\left(\sum_{i=0}^{k} \lambda_i x^i\right) = \sum_{i=0}^{k} \varphi(\lambda_i) t^i$$

Polo *Primeiro Teorema de Isomorfía*, denotando $\mathrm{Ker}(\psi) = \mathfrak{q}$, pode definirse o isomorfismo de aneis $\tilde{\psi} : A[x]/\mathfrak{q} \longrightarrow B$ como:

$$\tilde{\psi}\left(\sum_{i=0}^{k} \lambda_i x^i + \mathfrak{q}\right) = \sum_{i=0}^{k} \varphi(\lambda_i) t^i$$

Entón tense que $B \simeq A[x]/\mathfrak{q}$, e como B é un dominio, o ideal $\mathfrak{q} \lhd A[x]$ é primo.

Primeiro probarase que $\mathfrak{q} \neq 0$. Supoñendo que existe un $b \in B$ tal que $B[b^{-1}]$ é un corpo e denotando por $S = A \setminus \{0\}$ e por K ó corpo de fraccións de A, tense que:

$$\left.\begin{array}{l} K[x] = S^{-1}A[x] \\ \mathfrak{q}K[x] = S^{-1}\mathfrak{q} \end{array}\right\} \Rightarrow \frac{K[x]}{\mathfrak{q}K[x]} = \frac{S^{-1}A[x]}{S^{-1}\mathfrak{q}} = S^{-1}\left(\frac{A[x]}{\mathfrak{q}}\right) \simeq S^{-1}B$$

Á súa vez, como $B[b^{-1}]$ é un corpo, tense que $B[b^{-1}] = S^{-1}B[b^{-1}]$, logo:

$$B[b^{-1}] = \frac{K[x]}{\mathfrak{q}K[x]}[b^{-1}]$$

Se $\mathfrak{q} = 0$, teríase que $K[x][b^{-1}]$ é un corpo, e como $K[x]$ é un anel de Jacobson por ser K un corpo (lema 3.2.4), entón $K[x]$ é un corpo (lema 3.2.1), mais isto non pode ser, pois $K[x]$ é un anel de polinomios.

Sexa $f(x) = \lambda_n x^n + \cdots + \lambda_0 \in \mathfrak{q}$ un polinomio non nulo. Como $\mathfrak{q} = \mathrm{Ker}(\psi)$, f é tal que:

$$\psi(f) = f(t) = \lambda_n t^n + \cdots + \lambda_0 = 0$$

Entón $B[\lambda_n^{-1}]$ é unha extensión enteira de $A[\lambda_n^{-1}]$, pois t, o elemento que xera B como A-álxebra, é raíz do polinomio mónico $\lambda_n^{-1} f \in A[\lambda_n^{-1}][x]$. Logo $b \in B \subset B[\lambda_n^{-1}]$ é tamén raíz dun polinomio mónico de $A[\lambda_n^{-1}][x]$, é dicir, existen $\alpha_1, \ldots, \alpha_m \in A[\lambda_n^{-1}]$ tales que:

$$b^m + \alpha_1 b^{m-1} + \cdots + \alpha_m = 0$$

Podemos supoñer que $\alpha_m \neq 0$, pois B é un dominio e b é non nulo. Multiplicando por $(\alpha_m b^m)^{-1}$ a ambos lados da igualdade anterior, tense que:

$$(b^{-1})^m + \frac{\alpha_1}{\alpha_m}(b^{-1})^{m-1} + \cdots + \frac{1}{\alpha_m} = 0$$

Polo tanto, o corpo $B[b^{-1}]$ é enteiro sobre sobre o anel $A[(\lambda_n\alpha_m)^{-1}]$, logo este anel é un corpo (teorema 1.3.9), A é un corpo (corolario 3.2.2), $A[x]$ é Jacobson (lema 3.2.4), e $A[x]/\mathfrak{q} \simeq B$ tamén é Jacobson (lema 3.1.3), logo B é un corpo (corolario 3.2.2). Entón tense que $A = A[(\lambda_n\alpha_m)^{-1}]$ e $B = B[b^{-1}]$, logo $B : A$ é unha extensión enteira de aneis, e alxébrica de corpos, e como é finitamente xerada, tamén é finita (teorema 1.2.13).

Supoñamos agora que o teorema é certo para $r-1$ xeradores, e que B está xerado por r elementos.

Para o apartado 1, sexa $B' \subset B$ a A-subálxebra de B xerada por $r-1$ dos r xeradores de B. Pola hipótese de indución, B' é de Jacobson, e polo caso de $r = 1$, B tamén o é, pois é unha B'-álxebra xerada por un elemento, o xerador restante.

Para o apartado 2, sexa $\mathfrak{m} \lhd B$ un ideal maximal. Entón, polo caso de $r = 1$, $B' \cap \mathfrak{m}$ é maximal en B', e pola hipótese de indución, $A \cap \mathfrak{m} = A \cap (B' \cap \mathfrak{m})$ é maximal en A. Como as extensións de corpos $A/A\cap\mathfrak{m} \subset B'/B'\cap\mathfrak{m} \subset B/\mathfrak{m}$ son finitas pola hipótese de indución, entón a extensión $A/A \cap \mathfrak{m} \subset B/\mathfrak{m}$ tamén o é, probando así o teorema. ■

Corolario 3.2.6. *Sexa K un corpo (polo tanto Jacobson) e $K[x_1, \dots, x_n]$ o seu anel de polinomios en n variábeis, que é unha K-álxebra finitamente xerada. Entón tense que:*

1. *$K[x_1, \dots, x_n]$ é de Jacobson e dado un ideal $\mathfrak{a} \lhd K[x_1, \dots, x_n]$, tense que:*

$$\operatorname{rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{a}\subset\mathfrak{m}}} \mathfrak{m}$$

2. *Se $\mathfrak{m} \lhd K[x_1, \dots, x_n]$ é un ideal maximal, entón $K \cap \mathfrak{m}$ é un ideal maximal de K (e como K é un corpo, entón $K \cap \mathfrak{m} = 0$) e $K[x_1, \dots, x_n]/\mathfrak{m}$ é unha extensión finita de K, e polo tanto tamén alxébrica.*

Demostración. Para enunciar este corolario basta con substituír no enunciado do *Nullstellensatz xeral* (3.2.5) $A = K$ e $B = K[x_1, \dots, x_n]$. O feito de que o radical dun ideal de $K[x_1, \dots, x_n]$ sexa a intersección dos maximais que o conteñen dedúcese directamente do feito de que $K[x_1, \dots, x_n]$ sexa un anel de Jacobson. ■

Corolario 3.2.7. *Sexa K un corpo e $\mathfrak{m} \lhd K[x_1, \dots, x_n]$ un ideal maximal. Entón existen os polinomios nunha variábel $f_1, \dots, f_n \in K[x]$ tales que:*

$$\mathfrak{m} = \langle f_1(x_1), \dots, f_n(x_n)\rangle$$

Ademais, os f_i poden escollerse irreducíbeis en $K[x]$, de forma que os $f_i(x_i)$ tamén sexan irreducíbeis en $K[x_1, \dots, x_n]$.

Demostración. Polo corolario anterior (3.2.6), para cada $i \in \{1, \dots, n\}$, $x_i + \mathfrak{m}$ é alxébrico sobre K, logo existe un polinomio $f_i \in K[x]$, que pode escollerse irreducíbel, tal que:

$$f_i(x_i + \mathfrak{m}) = f_i(x_i) + \mathfrak{m} = 0 + \mathfrak{m} \Rightarrow f_i(x_i) \in \mathfrak{m}$$

Logo tense que $\langle f_1(x_1), \dots, f_n(x_n)\rangle \subset \mathfrak{m}$. Para rematar a demostración, probarase que o ideal $\langle f_1(x_1), \dots, f_n(x_n)\rangle$ é maximal, o cal implicará a súa igualdade con $\mathfrak{m}$.

Sexa $\varphi : K[x_1, \dots, x_n] \longrightarrow K[x_1, \dots, x_n]$ un homomorfismo de aneis tal que $\varphi(x_i) = f_i(x_i)$. Entón é doado ver que o ideal contracción de $\langle f_1(x_1), \dots, f_n(x_n)\rangle$ a través do homomorfismo φ é $\langle x_1, \dots, x_n\rangle$. Denotando $L = K[x_1, \dots, x_n]/\langle f_1(x_1), \dots, f_n(x_n)\rangle$ e tendo en conta que $K[x_1, \dots, x_n]/\langle x_1, \dots, x_n\rangle \simeq K$, tense que L é unha extensión de aneis de K. Tamén é doado comprobar que esta extensión é enteira, logo polo teorema 1.3.9, como K é un corpo, entón L tamén é un corpo, é dicir, $\langle f_1(x_1), \dots, f_n(x_n)\rangle$ é un ideal maximal. ■

Proposición 3.2.8. *Sexa K un corpo e $\mathfrak{m} \lhd K[x_1, \dots, x_n]$ un ideal maximal. Entón son equivalentes:*

1. $K[x_1, \dots, x_n]/\mathfrak{m} \simeq K$
2. $\exists a = (a_1, \dots, a_n) \in K^n \,/\, \mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n\rangle$
3. $\exists a \in K^n \,/\, V(\mathfrak{m}) = \{a\}$
4. $V(\mathfrak{m}) \neq \varnothing$

Demostración. As implicacións "2 $\Rightarrow$ 3" e "3 $\Rightarrow$ 4" son inmediatas. Probarase "4 $\Rightarrow$ 2" para rematar de probar a equivalencia $2 \Leftrightarrow 3 \Leftrightarrow 4$, e logo probarase que 1 é equivalente a calquera dos outros tres apartados.

Polo corolario 3.2.7, existen os polinomios $f_1, \dots, f_n \in K[x]$, que poden escollerse irreducíbeis, tales que:

$$\mathfrak{m} = \langle f_1(x_1), \dots, f_n(x_n)\rangle$$

"4 $\Rightarrow$ 2" Sexa $a = (a_1, \dots, a_n) \in V(\mathfrak{m})$. Entón tense que $f_i(a_i) = 0 \,\forall i \in \{1, \dots, n\}$. Como os f_i son irreducíbeis e $a_i \in K$, entón necesariamente $f_i(x_i) = x_i - a_i$, probando 2.

"2 $\Rightarrow$ 1" Sexa o isomorfismo de aneis $\varphi : K[x_1, \dots, x_n] \longrightarrow K[x_1, \dots, x_n]$ definido por $\varphi(x_i) = x_i - a_i \,\forall i \in \{1, \dots, n\}$. Entón tense que $\varphi(\langle x_1, \dots, x_n\rangle) = \langle x_1 - a_1, \dots, x_n - a_n\rangle$, e:

$$K \simeq \frac{K[x_1, \dots, x_n]}{\langle x_1, \dots, x_n\rangle} \simeq \frac{K[x_1, \dots, x_n]}{\langle x_1 - a_1, \dots, x_n - a_n\rangle} = \frac{K[x_1, \dots, x_n]}{\mathfrak{m}}$$

"1 $\Rightarrow$ 4" Sexa $\psi : K[x_1, \dots, x_n]/\mathfrak{m} \longrightarrow K$ un isomorfismo, e sexan $a_1, \dots, a_n \in K$ tales que $\psi(x_i + \mathfrak{m}) = a_i \; \forall i \in \{1, \dots, n\}$. Entón, dado un $f \in \mathfrak{m}$ arbitrario, tense que:

$$f(a_1, \dots, a_n) = f(\psi(x_1 + \mathfrak{m}), \dots, \psi(x_n + \mathfrak{m})) = \psi(f(x_1 + \mathfrak{m}, \dots, x_n + \mathfrak{m})) =$$

$$= \psi(f + \mathfrak{m}) = \psi(0 + \mathfrak{m}) = 0$$

Entón tense que $a = (a_1, \dots, a_n) \in V(\mathfrak{m}) \neq \varnothing$. ■

Observación 3.2.9. Ó tomar un corpo arbitrario K, aínda que se pode deducir unha parte do enunciado que demostramos anteriormente para o *Nullstellensatz forte* (2.2.5), non se pode afirmar nun principio nada sobre $I(V(\mathfrak{a}))$ para un certo ideal $\mathfrak{a} \lhd K[x_1, \dots, x_n]$, pois a dedución de que é o radical de $\mathfrak{a}$ require do *Nullstellensatz débil* (2.2.2) para poder corresponder bixectivamente os ideais maximais do anel de polinomios cos puntos do espazo afín.

Sen embargo, co *Nullstellensatz xeral* (3.2.5) e a proposición 3.2.8, podemos caracterizar os ideais maximais de $K[x_1, \dots, x_n]$ que se corresponden con puntos do espazo afín. Denotando por M_K ó conxunto de ditos maximais e dado un ideal $\mathfrak{a} \lhd K[x_1, \dots, x_n]$, pódese deducir que:

$$I(V(\mathfrak{a})) = I\left(\bigcup_{a \in V(\mathfrak{a})} a\right) = \bigcap_{a \in V(\mathfrak{a})} I(\{a\}) = \bigcap_{\substack{\mathfrak{m} \in M_K \\ \mathfrak{a} \subset \mathfrak{m}}} \mathfrak{m}$$

Nos temas seguintes intentará darse unha caracterización máis precisa desta intersección para certos tipos concretos de corpos: os corpos finitos e os reais pechados.

Capítulo 4

Nullstellensatz Finito

4.1. Preliminares de Corpos Finitos

Definición 4.1.1. Sexa K un corpo. Defínese a súa **característica**, denotada por $\text{car}(K)$, como o menor número natural non nulo $p \in \mathbb{N}^+$ tal que $p \cdot a = 0 \; \forall a \in K$ (interpretándose esta operación como sumar a consigo mesmo p veces, ou $-a$ sumado $-p$ veces se p fose negativo). Se non existe tal número, dirase que K é de característica 0.

Proposición 4.1.2. *Sexa K un corpo de característica $p \in \mathbb{N}^+$. Entón p é primo.*

Demostración. Supoñamos que p non é primo. Entón existen $r, s \in \mathbb{N}^+$ tales que $p = rs$, e polo tanto tense que:

$$0 = p \cdot 1 = rs \cdot 1 = (r \cdot 1)(s \cdot 1)$$

Como K é un corpo, entón ben $r \cdot 1 = 0$ ou $s \cdot 1 = 0$, polo que p non é o menor número natural non nulo tal que $p \cdot 1 = 0$, chegando así a unha contradición. ■

Proposición 4.1.3. *Sexa K un corpo finito. Entón* $\text{car}(K) \neq 0$.

Demostración. Se $\text{car}(K) = 0$, entón $n \cdot 1 \neq 0 \; \forall n \in \mathbb{N}^+$. Supoñamos agora que existen $m, k \in \mathbb{N}^+$ tales que $m > k$ e $m \cdot 1 = k \cdot 1$. Entón tense que:

$$0 = m \cdot 1 - k \cdot 1 = (m - k) \cdot 1$$

Chegando a unha contradición co feito de que $\text{car}(K) = 0$. Logo tense que K contén o conxunto $\{n \cdot 1 \,/\, n \in \mathbb{N}^+\}$, o cal non pode conter elementos repetidos, é dicir, o seu cardinal é $\aleph_0$, contradicindo así o feito de que K sexa finito. ■

Proposición 4.1.4. *Sexa K un corpo finito de característica $p \in \mathbb{N}^+$. Entón, o cardinal de K é p^n, para un certo $n \in \mathbb{N}^+$.*

Demostración. Sexa $\phi : \mathbb{Z} \longrightarrow K$ o homomorfismo de aneis definido por $\phi(n) = n \cdot 1$. Como $\text{car}(K) = p$, entón tense que $\text{Ker}(\phi) = p\mathbb{Z}$, e polo *Primeiro Teorema de Isomorfía*, $L = \phi(\mathbb{Z}) \simeq \mathbb{Z}/\text{Ker}(\phi) = \mathbb{Z}_p$.

Como K é un corpo finito, é unha extensión finita de L, de grao $[K : L] = n \in \mathbb{N}^+$. É dicir, considerando K como un L-espazo vectorial, existen $k_1, \dots, k_n \in K$ tales que cada elemento de K pode ser expresado de forma única como unha combinación lineal de $\{k_1, \dots, k_n\}$ con coeficientes en L. Como L ten p elementos, existen p^n desas combinacións lineais, e polo tanto, p^n elementos en K. ■

Teorema 4.1.5. *Para cada $p \in \mathbb{Z}$ primo e $n \in \mathbb{N}^+$ natural non nulo, existe un corpo finito con $q = p^n$ elementos, que é único salvo isomorfismos e denotarase por $\mathbb{F}_q$. Ademais, todos os elementos de $\mathbb{F}_q$ anulan ó polinomio $x^q - x \in \mathbb{F}_q[x]$.*

Demostración. Ver [11], páxina 246, teorema 5.1. ■

4.2. O Nullstellensatz para Corpos Finitos

Durante toda esta sección, considerarase unha extensión alxébrica $K : \mathbb{F}_q$.

Definición 4.2.1. Un polinomio $f \in K[x_1, \dots, x_n]$ dise que é **reducido** se o seu grao en cada variábel é menor que $q - 1$, é dicir, $\partial_{x_i} f \leq q - 1 \; \forall i \in \{1, \dots, n\}$. O conxunto dos polinomios reducidos de $K[x_1, \dots, x_n]$ denotarase por $\mathfrak{R}_K$. Nótese que para $n = 0$ tense que $\mathfrak{R}_K = K$.

É doado probar que $\mathfrak{R}_K$ é un espazo vectorial sobre K de dimensión q^n, cuxa base é o conxunto $\{x_1^{i_1} \dots x_n^{i_n} \; / \; 0 \leq i_j \leq q - 1 \; \forall j \in \{1, \cdots, n\}\}$.

Lema 4.2.2. *Tense que $\mathfrak{R}_K \cap I(\mathbb{F}_q^n) = \{0\}$.*

Demostración. Probarase mediante indución en n, sendo o caso de $n = 0$ inmediato. Sexa $n \geq 1$ e supoñamos que o lema verifícase para polinomios de $n - 1$ ou menos variábeis.

Sexa $f \in \mathfrak{R}_K \cap I(\mathbb{F}_q^n)$. Por ser f reducido, existen $f_0, \dots, f_{q-1} \in K[x_1, \dots, x_{n-1}]$ tales que:

$$f = f_{q-1} x_n^{q-1} + f_{q-2} x_n^{q-2} + \cdots + f_0$$

Entón, fixado un $(a_1, \dots, a_{n-1}) \in \mathbb{F}_q^{n-1}$, tense que o polinomio $f(a_1, \dots, a_{n-1}, x_n) \in K[x_n]$ ten grao menor ou igual que $q-1$, mais ten polo menos q raíces en K (pois f anúlase en todo $\mathbb{F}_q$), polo que ten que ser o polinomio nulo, é dicir, $f_i(a_1, \dots, a_{n-1}) = 0 \; \forall i \in \{0, \dots, q-1\}$. Pola hipótese de indución, cada f_i é o polinomio nulo, e entón tamén o é f. ■

Definición 4.2.3. Defínese o ideal $\Gamma_q(K) \lhd K[x_1, \dots, x_n]$ como:

$$\Gamma_q(K) = \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle$$

Debido ó teorema 4.1.5, os polinomios de $\Gamma_q(K)$ anúlanse en todos os puntos de $\mathbb{F}_q^n$, é dicir, $\Gamma_q(K) \subset I(\mathbb{F}_q^n)$. Logo, aplicando o lema anterior (4.2.2), tense que $\mathfrak{R}_K \cap \Gamma_q(K) = \{0\}$.

Lema 4.2.4. *Cada polinomio $f \in K[x_1, \dots, x_n]$ pode ser escrito de forma única como $f = g + \gamma$, con $g \in \mathfrak{R}_K$ e $\gamma \in \Gamma_q(K)$, é dicir, $S = \mathfrak{R}_K \oplus \Gamma_q(K)$ como espazos vectoriais.*

Demostración. A unicidade da descomposición é inmediata grazas a que $\mathfrak{R}_K \cap \Gamma_q(K) = \{0\}$ e a que tanto $\mathfrak{R}_K$ como $\Gamma_q(K)$ son espazos vectoriais sobre K. Para probar a existencia, basta probala para un monomio da forma $f = x_1^{i_1} \cdots x_n^{i_n}$. Supoñamos que f non é reducido, pois doutra forma é inmediato. Entón existe un $j \in \{1, \dots, n\}$ tal que $i_j \geq q$. Pode supoñerse, sen perda de xeneralidade, que $j = 1$. Logo tense que:

$$x_1^{i_1} = x_1^{i_1 - q} x_1^q = x_1^{i_1 - q}(x_1^q - x_1 + x_1)$$

No anel cociente $K[x_1, \dots, x_n]/\Gamma_q(K)$ tense que:

$$x_1^q - x_1 + \Gamma_q(K) = 0 + \Gamma_q(K) \Rightarrow x_1^{i_1} + \Gamma_q(K) = x_1^{i_1 - q + 1} + \Gamma_q(K)$$

Entón tense que:

$$f + \Gamma_q(K) = x_1^{i_1 - q + 1} \cdots x_n^{i_n} + \Gamma_q(K)$$

Repetindo este proceso para todos os $j \in \{1, \dots, n\}$ tales que $i_j \geq q$, chégase á igualdade no cociente $f + \Gamma_q(K) = g + \Gamma_q(K)$, sendo $g \in \mathfrak{R}_K$ un monomio reducido. Entón $f - g \in \Gamma_q(K)$, e existe un $\gamma \in \Gamma_q(K)$ tal que $f = g + \gamma$. ■

Teorema 4.2.5. *Sexa K unha extensión alxébrica de $\mathbb{F}_q$. Entón tense que:*

1. *$I(\mathbb{F}_q^n) = \Gamma_q(K)$.*
2. *Sexa $\mathcal{V} = V(\mathfrak{a}) \subset K^n$ unha variedade tal que $\mathfrak{a} \lhd K[x_1, \dots, x_n]$ é un ideal xerado por polinomios de $\mathbb{F}_q[x_1, \dots, x_n]$. Entón tense que:*

$$I(V(\mathfrak{a})) = \mathfrak{a} + \Gamma_q(K)$$

Demostración.

1. A inclusión $\Gamma_q(K) \subset I(\mathbb{F}_q^n)$ é evidente, así que probarase a restante. Sexa $f \in I(\mathbb{F}_q^n)$. Polo lema 4.2.4, existen $g \in \mathfrak{R}_K$ e $\gamma \in \Gamma_q(K) \subset I(\mathbb{F}_q^n)$ tales que $f = g + \gamma$, e entón tense que $g = f - \gamma \in I(\mathbb{F}_q^n)$, polo que g anúlase en todo $\mathbb{F}_q^n$, logo $g = 0$ (lema 4.2.2), e $f = \gamma \in \Gamma_q(K)$.

2. É evidente ver que $\mathfrak{a} + \Gamma_q(K) \subset I(V(\mathfrak{a}))$. Polo *Teorema da Base de Hilbert* (2.1.8) e o seu corolario 2.1.9, o ideal $\mathfrak{a}$ está xerado por unha cantidade finita de polinomios $f_1, \dots, f_r \in \mathbb{F}_q[x_1, \dots, x_n]$. Por outra parte, sexan:

$$g = 1 - \prod_{i=1}^{r}(1 - f_i^{q-1})$$

$$h = 1 - g = \prod_{i=1}^{r}(1 - f_i^{q-1})$$

É evidente que $g, h \in \mathbb{F}_q[x_1, \dots, x_n]$ e $g \in \mathfrak{a}$. Ademais tense que, fixado un $a \in K^n$:

$$g(a) = \begin{cases} 0 & \text{se } a \in V(\mathfrak{a}) \\ 1 & \text{noutro caso} \end{cases} \qquad h(a) = \begin{cases} 1 & \text{se } a \in V(\mathfrak{a}) \\ 0 & \text{noutro caso} \end{cases}$$

Sexa agora $f \in I(V(\mathfrak{a}))$. Entón $fg \in \mathfrak{a}$, e como $g + h = 1$ e aplicando o apartado 1, tense que $f = f(g + h) = fg + fh \in \mathfrak{a} + \Gamma_q(K)$, polo que $I(V(\mathfrak{a})) = \mathfrak{a} + \Gamma_q(K)$.

■

Corolario 4.2.6 ($\mathbb{F}_q$-Nullstellensatz afín)**.** *Sexa $\mathfrak{a} \lhd \mathbb{F}_q[x_1, \dots, x_n]$ un ideal. Entón:*

1. $I(\mathbb{F}_q^n) = \Gamma_q(\mathbb{F}_q)$
2. $I(V(\mathfrak{a})) = \mathfrak{a} + \Gamma_q(\mathbb{F}_q)$.

Demostración. Basta con tomar $K = \mathbb{F}_q$ no enunciado do teorema anterior (4.2.5). ■

Observación 4.2.7. Como consecuencia deste corolario, pódese ver que os puntos de $\mathbb{F}_q^n$ correspóndense cos ideais maximais de $\mathbb{F}_q[x_1, \dots, x_n]$ que conteñen a $\Gamma_q(\mathbb{F}_q)$, é dicir, cos ideais maximais de $\mathbb{F}_q[x_1, \dots, x_n]/\Gamma_q(\mathbb{F}_q)$, que é un anel finito.

Capítulo 5

Nullstellensatz Real

Neste capítulo expoñerase unha versión do Nullstellensatz para corpos reais pechados. Antes diso expoñeranse os conceptos de anel real e semirreal, de orde dun anel, e as relacións entre os mesmos tanto para aneis como no caso particular dos corpos. Logo introducirase unha variación da definición de radical dun ideal que permita obter un resultado similar ó Nullstellensatz forte nas liñas do xa deducido no capítulo 3.

5.1. Aneis Reais

Notación 5.1.1. Denotarase por $\sum A^2 = \{a_1^2 + \cdots + a_n^2 \ / \ a_1, \ldots, a_n \in A\}$ ó conxunto das sumas de cadrados dun anel A.

Definición 5.1.2. Sexa A un anel. Dise que A é **semirreal** se $-1 \notin \sum A^2$. Noutro caso, existen os elementos $a_1, \ldots, a_n \in A$ tales que $0 = 1 + a_1^2 + \cdots + a_n^2$, e A dise que é irreal.

Dise que A é (formalmente) **real** se para todos $a_1, \ldots, a_n \in A$ tense que:

$$a_1^2 + \cdots + a_n^2 = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Un ideal $\mathfrak{a} \lhd A$ dise que é **semirreal** ou **real** se $A/\mathfrak{a}$ é respectivamente semirreal ou real.

Observación 5.1.3. Todo anel real non nulo é tamén semirreal, mais o anel nulo é semirreal e non real. Así mesmo, todo ideal real dun anel non nulo é tamén semirreal.

Proposición 5.1.4. *Sexa A un anel e $\mathfrak{a} \lhd A$ un ideal do mesmo. Entón tense que:*

1. *O ideal $\mathfrak{a}$ é real se e soamente se para todos os elementos $a_1, \ldots, a_n \in A$ tales que $a_1^2 + \cdots + a_n^2 \in \mathfrak{a}$, tense que $a_1, \ldots, a_n \in \mathfrak{a}$.*
2. *O ideal $\mathfrak{a}$ é semirreal se e soamente se $(1 + \sum A^2) \cap \mathfrak{a} = \varnothing$.*

Demostración.

1. O ideal $\mathfrak{a}$ é real se e soamente se $A/\mathfrak{a}$ é un anel real, é dicir, se dados os elementos $a_1+\mathfrak{a},\dots,a_n+\mathfrak{a}\in A/\mathfrak{a}$ tales que $\sum_{i=1}^n a_i^2+\mathfrak{a}=0+\mathfrak{a}$ (é dicir, $\sum_{i=1}^n a_i^2\in\mathfrak{a}$), tense que $a_i+\mathfrak{a}=0+\mathfrak{a}\,\forall i\in\{1,\dots,n\}$, é dicir, $a_i\in\mathfrak{a}\,\forall i\in\{1,\dots,n\}$.

2. O ideal $\mathfrak{a}$ é semirreal se e soamente se $A/\mathfrak{a}$ é semirreal, é dicir, $-1+\mathfrak{a}\notin\sum(A/\mathfrak{a})^2$. Isto é equivalente a que, para todos $a_1+\mathfrak{a},\dots,a_n+\mathfrak{a}\in A/\mathfrak{a}$, tense que $-1+\mathfrak{a}\neq\sum_{i=1}^n a_i^2+\mathfrak{a}$, é dicir, $1+\sum_{i=1}^n a_i^2\notin\mathfrak{a}$, e isto á súa vez é equivalente a que $\left(1+\sum A^2\right)\cap\mathfrak{a}=\varnothing$.

■

Proposición 5.1.5. *Sexa A un dominio e K o seu corpo de fraccións. Se A é real, entón K é real.*

Demostración. Sexan $\frac{a_1}{b_1},\dots,\frac{a_n}{b_n}\in K$, con $b_i\neq 0\,\forall i\in\{1,\dots,n\}$ tales que:

$$\sum_{i=1}^n\left(\frac{a_i}{b_i}\right)^2=0$$

Denótese por $b=\prod_{i=1}^n b_i$ e $c_i=a_i\prod_{\substack{j=1\\ j\neq i}}^n b_j$. Multiplicando por b^2 a ambos lados da igualdade anterior, obtense que:

$$b^2\sum_{i=1}^n\left(\frac{a_i}{b_i}\right)^2=0\Rightarrow\sum_{i=1}^n c_i^2=0$$

Logo, como A é real, tense que $c_i=0\,\forall i\in\{1,\dots,n\}$, e como $b_i\neq 0\,\forall i\in\{1,\dots,n\}$, entón $a_i=0\,\forall i\in\{1,\dots,n\}$, probando así que K é real. ■

Proposición 5.1.6. *Sexan A e B aneis e $\varphi:A\longrightarrow B$ un homomorfismo de aneis. Entón tense que:*

1. *Se B é semirreal, entón A é semirreal.*

2. *Se φ é inxectivo e B é real, entón A é real. En particular e tendo en conta a proposición 5.1.5, un dominio é real se e soamente se tamén o é o seu corpo de fraccións.*

3. *Se $\mathfrak{b}\lhd B$ é un ideal semirreal ou real, entón $\varphi^{-1}(\mathfrak{b})\lhd A$ é respectivamente un ideal semirreal ou real. Se ademais φ é sobrexectivo, entón $\mathfrak{b}$ é semirreal ou real se e soamente se $\varphi^{-1}(\mathfrak{b})$ tamén o é.*

Demostración.

1. Supoñamos que A non é semirreal, é dicir, que $-1 \in \sum A^2$ e existen $a_1, \dots, a_n \in A$ tales que $-1 = \sum_{i=1}^{n} a_i^2$. Entón tense que:

$$-1 = \varphi(-1) = \varphi\left(\sum_{i=1}^{n} a_i^2\right) = \sum_{i=1}^{n} \varphi(a_i)^2$$

   Logo $-1 \in \sum B^2$, contradicindo que B sexa semirreal.

2. Supoñamos que A non é real, é dicir, que existen $a_1, \dots, a_n \in A$ tales que $\sum_{i=1}^{n} a_i^2 = 0$ e $a_1 \neq 0$. Entón tense que:

$$0 = \varphi(0) = \varphi\left(\sum_{i=1}^{n} a_i^2\right) = \sum_{i=1}^{n} \varphi(a_i)^2$$

   E como φ é inxectivo, tense que $\varphi(a_1) \neq 0$, contradicindo así que B sexa real.

3. Denótese $\mathfrak{a} = \varphi^{-1}(\mathfrak{b})$ e defínase o homomorfismo de aneis $\tilde{\varphi} : A/\mathfrak{a} \longrightarrow B/\mathfrak{b}$ como $\tilde{\varphi}(a+\mathfrak{a}) = \varphi(a)+\mathfrak{b}$. Este homomorfismo é claramente inxectivo, logo, se $\mathfrak{b}$ é semirreal ou real, $B/\mathfrak{b}$ é semirreal ou real respectivamente, e entón polos apartados 1 e 2, $A/\mathfrak{a}$ tamén o é, probando que $\mathfrak{a} = \varphi^{-1}(\mathfrak{b})$ é respectivamente semirreal ou real.

   Se φ é sobrexectivo, entón $\tilde{\varphi}$ é un isomorfismo, e pódese aplicar o mesmo argumento para ver que se $\mathfrak{a} = \varphi^{-1}(\mathfrak{b})$ é semirreal ou real, entón $\mathfrak{b}$ tamén o é.

■

Proposición 5.1.7. *Sexa A un anel. Entón son equivalentes:*

1. *A é semirreal.*
2. *A ten un ideal semirreal.*
3. *A ten un ideal real propio.*
4. *A ten un ideal primo e semirreal.*
5. *A ten un ideal primo e real.*

Demostración. Ver [10], páxina 773, teorema 2.3. ■

Proposición 5.1.8. *Sexa A un anel real. Entón o seu único elemento nilpotente é o 0.*

Demostración. Sexa $a \in A$ un elemento nilpotente non nulo, e sexa $n \geq 2$ o menor número natural tal que $a^n = 0$. Poden darse dous casos:

- Se n é par, existe un $k \in \mathbb{N}$ tal que $n = 2k$, logo tense que:

$$a^n = a^{2k} = (a^k)^2 = 0$$

  Como A é real, entón $a^k = 0$, chegando a unha contradición coa definición de n.

- Se n é impar, existe un $k \in \mathbb{N}$ tal que $n = 2k + 1$, logo tense que:

$$a^{n+1} = a^{2k+2} = (a^{k+1})^2 = 0$$

  Como A é real, entón $a^{k+1} = 0$, chegando a unha contradición coa definición de n.

■

Proposición 5.1.9. *Sexa A un anel semirreal. Entón o anel de polinomios $A[x_1, \dots, x_n]$ é semirreal.*

Demostración. Basta con probar que $A[x]$ é semirreal, pois o caso de n variábeis séguese de forma inmediata ó ter en conta que $A[x_1, \dots, x_n] = A[x_1, \dots, x_{n-1}][x_n]$. Supoñamos entón que $A[x]$ non é semirreal. Entón $-1 \in \sum A[x]^2$, e existen $f_1, \dots, f_n \in A[x]$ tales que:

$$-1 = \sum_{i=1}^{n} f_i(x)^2 \; \forall x \in A$$

Logo, ó avaliar estes polinomios en 0, tense que -1 é unha suma de cadrados de A, contradicindo o feito de que A sexa semirreal. ■

5.2. Teoría de Aneis Ordenados de Artin-Schreier

Definición 5.2.1. Sexa A un anel. Defínese unha **preorde** de A como un subconxunto $T \subset A$ tal que:

1. T é pechado baixo a suma e o produto, é dicir: $a + b, ab \in T \; \forall a, b \in T$
2. As sumas de cadrados de A pertencen a T, é dicir: $\sum A^2 \subset T$
3. $-1 \notin T$

Denotando por $-T = \{-a \,/\, a \in T\}$, tense que $T \cap -T$ é o subgrupo aditivo máis grande contido en T, o cal chamarase **soporte** de T, e denotarase por $\text{sop}(T)$.

Proposición 5.2.2. *Sexa A un anel e $T \subset A$ unha preorde do mesmo. Se $T \cup -T = A$, entón $\text{sop}(T)$ é un ideal de A.*

Demostración. Sexan $a \in A$ e $b \in \text{sop}(T)$. Probarase que $ab \in \text{sop}(T)$. Como $A = T \cup -T$, entón ben $a \in T$ ou $-a \in T$, mentres que sempre tense que $b \in T$ e $-b \in T$.

- Se $a \in T$, entón $ab \in T$, e $a(-b) = -ab \in T$, é dicir, $ab \in -T$.
- Se $-a \in T$, entón $(-a)(-b) = ab \in T$, e $(-a)b = -ab \in T$, é dicir, $ab \in -T$.

En ambos casos probouse que $ab \in T \cap -T = \text{sop}(T)$. ■

Definición 5.2.3. Sexa A un anel e $T \subset A$ unha preorde do mesmo. Dise que T é unha **orde** de A se:

1. $T \cup -T = A$
2. $\text{sop}(T) = T \cap -T$ é un ideal primo de A.

Dirase entón que (A, T) é un **anel ordenado**, sendo T o seu conxunto de elementos **positivos**, e $-T$ o de elementos **negativos**.

Observación 5.2.4. Unha orde $T \subset A$ permite definir unha relación de orde total en A, que denotarase "$\leq_T$" e é tal que:

$$a \leq_T b \Leftrightarrow b - a \in T$$

Tamén permite definir a relación (xa non de orde) "$<_T$" como:

$$a <_T b \Leftrightarrow b - a \notin -T$$

Normalmente omitirase o subíndice a non ser que se requira especificar a orde escollida.

Teorema 5.2.5. *Un anel é semirreal se e soamente se admite unha orde.*

Demostración. Ver [10], páxina 779, teorema 3.9. ■

Proposición 5.2.6. *Sexa A un dominio semirreal e K o seu corpo de fraccións. Entón K é semirreal.*

Demostración. Polo teorema 5.2.5, A admite unha orde $T_A \subset A$, e basta con probar que K admite unha orde $T \subset K$. Esta orde definirase da seguinte forma: Un elemento de K pertence a T se e soamente se admite un representante $\frac{a}{b}$ con $a, b \in T_A$ e $b \neq 0$. É evidente comprobar que $-1 \notin T$.

Dados $\frac{a}{b}, \frac{c}{d} \in T$ con $a, b, c, d \in T_A$ e $b, d \neq 0$, como T_A é pechado baixo a suma e o produto, tense que $ad + bc, bd, ab, cd \in T_A$, logo:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in T \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd} \in T$$

Sexa $\sum_{i=1}^{n}(\frac{a_i}{b_i})^2 \in \sum K^2$. Como $\sum A^2 \subset T_A$, para cada $i \in \{1, \dots, n\}$ tense que $a_i^2, b_i^2 \in T_A$, entón $(\frac{a_i}{b_i})^2 \in T$, e como xa se probou que T é pechado baixo a suma, $\sum_{i=1}^{n}(\frac{a_i}{b_i})^2 \in T$, logo $\sum K^2 \subset T$.

Ata agora probouse que T é unha preorde de K. Para probar que é tamén unha orde basta con ver que $K = T \cup -T$, pero isto é evidente usando o feito de que $-\frac{a}{b} = \frac{-a}{b}$, o cal implica que $-T = (K \setminus T) \cup \{0\}$. ■

5.3. Propiedades dos Corpos Reais e Ordenados

Proposición 5.3.1. *Sexa (K, T) un corpo ordenado e $a \in T \setminus \{0\}$. Entón tense que $a^{-1} \in T$.*

Demostración. Supoñamos que $a^{-1} \notin T$. Entón tense que:

$$\left.\begin{array}{c} a^{-1} \notin T \\ K = T \cup -T \end{array}\right\} \Rightarrow a^{-1} \in -T \Rightarrow -a^{-1} \in T \Rightarrow a(-a^{-1}) = -1 \in T$$

Chegando así a unha contradición con que T sexa unha orde de K. ■

Proposición 5.3.2. *Sexa (K, T) un corpo ordenado. Entón $T \cap -T = \{0\}$.*

Demostración. Pola proposición 5.2.2, $T \cap -T$ é un ideal de K, mais como é un ideal propio e K é un corpo, entón so pode ser o ideal 0. ■

Proposición 5.3.3. *Sexa K un corpo e $T, T' \subset K$ dúas ordes do mesmo tales que $T' \subset T$. Entón tense que $T = T'$.*

Demostración. Se $T \neq T'$, entón sexa $a \in T \setminus T' \subset K \setminus T' \subset -T'$, que polo tanto é tal que $-a \in T' \subset T$, logo $a \in T \cap -T = \{0\}$, pero como $0 \in T'$, chegouse a unha contradición co feito de que $a \notin T'$. ■

Proposición 5.3.4. *Un corpo é real se e soamente se é semirreal.*

Demostración. É evidente ver que todo corpo real é semirreal, así que sexa K un corpo semirreal e supoñamos que K non é real. Entón existen os elementos $a_1, \dots, a_n \in K$ tales que $a_1 \neq 0$ e $\sum_{i=1}^{n} a_i^2 = 0$. Logo tense que:

$$-a_1^2 = \sum_{i=2}^{n} a_i^2$$

Como K é un corpo e $a_1 \neq 0$, entón existe o seu inverso, e pódese multiplicar a ambos lados da igualdade por $(a_1^{-1})^2 = (a_1^2)^{-1}$, obtendo:

$$-1 = \sum_{i=2}^{n} \left(a_i a_1^{-1}\right)^2 \in \sum K^2$$

Contradicindo así o feito de que K sexa semirreal. ■

Corolario 5.3.5. *Sexa A un anel. Un ideal maximal $\mathfrak{m} \lhd A$ é real se e soamente se é semirreal.*

Demostración. É inmediato usando a proposición anterior e o feito de que $A/\mathfrak{m}$ é un corpo:

$$\mathfrak{m} \text{ é real} \Leftrightarrow A/\mathfrak{m} \text{ é real} \Leftrightarrow A/\mathfrak{m} \text{ é semirreal} \Leftrightarrow \mathfrak{m} \text{ é semirreal}$$

■

Lema 5.3.6. *Sexa K un corpo real. Entón o corpo de funcións racionais $K(x_1, \dots, x_n)$ é real.*

Demostración. Pola proposición 5.3.4, K é un corpo semirreal, e basta con probar que $K(x_1, \dots, x_n)$ é semirreal. Pola proposición 5.1.9, $K[x_1, \dots, x_n]$ é un anel semirreal. Pola proposición 5.2.6, o seu corpo de fraccións, $K(x_1, \dots, x_n)$, tamén é semirreal. ■

Teorema 5.3.7. *Un corpo é real se e soamente se admite unha orde.*

Demostración. É inmediato aplicando que un anel é semirreal se e soamente se admite unha orde (teorema 5.2.5) e que un corpo é real se e soamente se é semirreal (proposición 5.3.4). Para unha proba alternativa, pódese ver [6], páxina 14, corolario 1.10. ■

Proposición 5.3.8. *A característica dun corpo real é* 0.

Demostración. Sexa K un corpo real. Se existise un $n \in \mathbb{N}^+$ tal que $n \cdot 1 = 0$, teríase unha suma de cadrados ($1 = 1^2$ sumado consigo mesmo n veces) igualada a 0, e como K é real isto implica que $1 = 0$, chegando a unha contradición. ■

Proposición 5.3.9. *Sexa $L : K$ unha extensión de corpos e $T \subset L$ unha orde de L. Entón $T \cap K$ é unha orde de K, que chamarase a orde **inducida** por (L, T) en K.*

Demostración. Como $-1 \notin T$, é evidente que $-1 \notin T \cap K$, e como T e K son pechados baixo a suma e o produto, $T \cap K$ tamén o é. Por outra parte tense que:

$$\sum K^2 \subset \left(\sum L^2\right) \cap K \subset T \cap K$$

Para rematar, é doado ver que $-(T \cap K) = (-T) \cap K$, logo tense que:

$$(T \cap K) \cup -(T \cap K) = (T \cap K) \cup (-T \cap K) = (T \cup -T) \cap K = L \cap K = K$$

Probando así que $T \cap K$ é unha orde de K. ■

Lema 5.3.10. *Sexa K un corpo real e $\mathcal{F}$ o conxunto de todas as ordes de K. Entón tense que $\sum K^2 = \bigcap_{T \in \mathcal{F}} T$. É dicir, un elemento de K é suma de cadrados se e soamente se é positivo en todas as ordes de K.*

Demostración. Ver [6], páxina 16, proposición 1.19. ■

5.4. Corpos Reais Pechados

Definición 5.4.1. Sexa K un corpo. Dise que K é **real pechado** se é real e non admite ningunha extensión de corpos alxébrica e real. Dise que o corpo L é unha **clausura real** de K se L é real pechado e $L : K$ é unha extensión alxébrica de corpos.

Teorema 5.4.2. *Sexa K un corpo. Entón son equivalentes:*

1. *K é real pechado.*
2. *$\sum K^2$ é a única orde de K e todo polinomio de $K[x]$ de grao impar ten polo menos unha raíz en K.*
3. *K é real, para todo $a \in K$ existe un $b \in K$ tal que ben $a = b^2$ ou $a = -b^2$ e todo polinomio de $K[x]$ de grao impar ten polo menos unha raíz en K.*
4. *K non é alxebricamente pechado, e a súa clausura alxébrica é $K(\sqrt{-1})$.*

Demostración. En [6], páxina 19, teorema 1.29, demóstrase un teorema moi similar a este. Completarase a proba cos lemas seguintes. ■

Lema 5.4.3. *Se K é un corpo real, entón non é alxebricamente pechado.*

Demostración. Basta con tomar o polinomio $f(x) = x^2 + 1$. Como K é real, se existira un $a \in K$ que fose raíz de f isto implicaría que $a = 1 = 0$, logo f non ten raíces en K. ■

Lema 5.4.4. *Sexa K un corpo. Se $\sum K^2$ é unha orde de K, entón é a única orde que admite K.*

Demostración. Polo lema 5.3.10, $\sum K^2$ é a intersección de todas as ordes de K. Logo, pola proposición 5.3.3, como $\sum K^2$ é unha orde de K, entón é a única orde que admite K. ■

Lema 5.4.5. *Sexa K un corpo. Entón $\sum K^2$ é unha orde de K se e soamente se para todo $a \in K$ existe un $b \in K$ tal que ben $a = b^2$ ou $a = -b^2$.*

Demostración.

"$\Rightarrow$" Sexa $a \in K$. Basta con probar que se $a \in \sum K^2$ entón $\sqrt{a} \in K$. Supoñamos que $a \in \sum K^2$ mais $\sqrt{a} \notin K$. Como $\sqrt{a}$ é unha raíz do polinomio $x^2 - a$, entón pertence a $K(i)$, denotando $i = \sqrt{-1}$ unha raíz do polinomio $x^2 + 1$. Entón existen $b_1, \dots, b_n, c, d \in K$ tales que:

$$a = \sum_{i=1}^{n} b_i^2$$

$$\sqrt{a} = c + di \Rightarrow a = c^2 - d^2 + 2cdi$$

$$\sum_{i=1}^{n} b_i^2 = c^2 - d^2 + 2cdi \Rightarrow 2cd = 0 \Rightarrow c = 0 \text{ ou } d = 0$$

Se ocorrese que $d = 0$ entón $\sqrt{a} = c \in K$, chegando a unha contradición, mais se $c = 0$, entón $\sqrt{a} = di$ e $a = -d^2 \in -\sum K^2$, logo $a = 0$ e $\sqrt{a} = 0 \in K$, chegando tamén a unha contradición.

"$\Leftarrow$" Denotando $K^2 = \{a^2 \,/\, a \in K\}$, tense que $A = K^2 \cup -K^2$, e como $K^2 \subset \sum K^2$, entón $K = \sum K^2 \cup -\sum K^2$. $\sum K^2$ satisfai trivialmente as outras propiedades das ordes: é pechado baixo a suma e o produto, contén a $\sum K^2$ e $-1 \notin \sum K^2$, logo $\sum K^2$ é unha orde de K. ■

Teorema 5.4.6. *Sexa K un corpo real e $T \subset K$ unha orde do mesmo. Entón tense que:*

1. *Existe unha clausura real L de K que induce a orde T en K.*

2. *Dadas L_1 e L_2 dúas clausuras reais de K que inducen a orde T en K, existe un único isomorfismo de aneis $\phi : L_1 \longrightarrow L_2$ tal que $\phi(a) = a \; \forall a \in K$.*

Demostración. Ver [6], páxina 34, teorema 2.15. ■

Teorema 5.4.7 (Teorema de Artin-Schreier)**.** *Sexa L un corpo alxebricamente pechado e $K \subsetneq L$ un subcorpo do mesmo tal que $L : K$ é unha extensión de corpos finita. Entón tense que K é real pechado e $L = K(i)$, sendo $i \in L$ unha raíz do polinomio $x^2 + 1$.*

Demostración. Ver [12], páxina 362, teorema 2. ■

5.5. Espectro Real e Radical Real

Definición 5.5.1. Defínese o **espectro real** dun anel A como o conxunto dos ideais primos reais do mesmo, e denotarase por r-Spec(A). Nótese que para un ideal primo $\mathfrak{p} \lhd A$, é equivalente que ese ideal sexa real con que o corpo de fraccións de $A/\mathfrak{p}$ sexa real (apartado 2 da proposición 5.1.6)

Definición 5.5.2. Sexa A un anel e $\mathfrak{a} \lhd A$ un ideal do mesmo. Defínese o **radical real** de $\mathfrak{a}$ como a intersección dos ideais primos reais de A que o conteñen:

$$\text{r-rad}(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \in \text{r-Spec}(A) \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p}$$

Teorema 5.5.3. *Sexa A un anel, $\mathfrak{a} \lhd A$ un ideal do mesmo e $f \in A$. Entón son equivalentes:*

1. $f \in \text{r-rad}(\mathfrak{a})$
2. *Existen $m, n \in \mathbb{N}$ e $a_1, \dots, a_n \in A$ tales que $f^{2m} + a_1^2 + \cdots + a_n^2 \in \mathfrak{a}$.*

Demostración.
"1 $\Rightarrow$ 2" Pasando ó anel cociente $A/\mathfrak{a}$ e tendo en conta que hai unha correspondencia bixectiva entre os ideais primos de $A/\mathfrak{a}$ e os ideais primos de A que conteñen a $\mathfrak{a}$, pódese supoñer sen perda de xeneralidade que $\mathfrak{a} = 0$.

Denotando por $D(f) = \{\mathfrak{p} \in \text{Spec}(A) \,/\, f \notin \mathfrak{p}\}$ ó conxunto dos ideais primos de A que non conteñen a f, é doado ver que $f \in \text{r-rad}(0)$ se e soamente se $D(f) \cap \text{r-Spec}(A) = \varnothing$. Tendo en conta que existe unha correspondencia bixectiva entre os ideais primos de $A[f^{-1}]$ e os ideais primos de A que non conteñen a f, pódese ver que r-Spec($A[f^{-1}]$) $= \varnothing$. Logo, o anel $A[f^{-1}]$ non é semirreal (proposición 5.1.7, equivalencia 1 $\Leftrightarrow$ 5), e existen $b_1, \dots, b_n \in A$ e $m_1, \dots, m_n \in \mathbb{N}$ tales que:

$$1 + \left(\frac{b_1}{f^{m_1}}\right)^2 + \cdots + \left(\frac{b_n}{f^{m_n}}\right)^2 = 0$$

Denotando $m = \prod_{i=1}^{n} m_i$ e $a_i = b_i \prod_{\substack{j=1 \\ i \neq j}}^{n} f^{m_j}$, e multiplicando a ambos lados da igualdade por f^{2m}, tense que:

$$f^{2m}\left(1 + \left(\frac{b_1}{f^{m_1}}\right)^2 + \cdots + \left(\frac{b_n}{f^{m_n}}\right)^2\right) = 0$$

$$f^{2m} + a_1^2 + \cdots + a_n^2 = 0 \in \mathfrak{a}$$

"2 $\Rightarrow$ 1" Sexa $\mathfrak{p} \in$ r-Spec(A) tal que $\mathfrak{a} \subset \mathfrak{p}$. Entón $f^{2m} + a_1^2 + \cdots + a_n^2 \in \mathfrak{a} \subset \mathfrak{p}$. Pola proposición 5.1.4 e por ser $\mathfrak{p}$ real, tense que $f^m \in \mathfrak{p}$, e por ser $\mathfrak{p}$ primo, $f \in \mathfrak{p}$, logo:

$$f \in \bigcap_{\substack{\mathfrak{p} \in \text{r-Spec}(A) \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p} = \text{r-rad}(\mathfrak{a})$$

■

Proposición 5.5.4. *Sexa A un anel. Entón tense que:*

1. *A é real se e soamente se* r-rad$(0) = 0$.
2. *Un ideal $\mathfrak{a} \lhd A$ é real se e soamente se* r-rad$(\mathfrak{a}) = \mathfrak{a}$.

Demostración.

1. "$\Rightarrow$" Supoñamos que A é real e sexa $f \in$ r-rad(0). Pola proposición 5.5.3, existen $m, n \in \mathbb{N}$ e $a_1, \ldots, a_n \in A$ tales que:

   $$f^{2m} + a_1^2 + \cdots + a_n^2 = 0$$

   Como A é real, pola proposición 5.1.4 tense que $f^m = 0$, é dicir, f é nilpotente. Pola proposición 5.1.8, o único elemento nilpotente de A é o 0, logo $f = 0$.

   "$\Leftarrow$" Supoñamos que r-rad$(0) = 0$ e A non é real, e sexan os elementos $a_1, \ldots, a_n \in A$ tales que $\sum_{i=1}^n a_i^2 = 0$ e $a_1 \neq 0$. Entón tense que $a_1 \notin$ r-rad$(0) = 0$, e polo teorema 5.5.3, $\sum_{i=1}^n a_i^2 \neq 0$ (pois doutra forma o teorema implicaría que $a_1 \in$ r-rad(0)). Desta forma chegouse a unha contradición, e A ten que ser real.

2. É doado ver que no anel cociente $A/\mathfrak{a}$:

   $$\text{r-rad}(0 + \mathfrak{a}) = \text{r-rad}(\mathfrak{a}) + \mathfrak{a}$$

   Logo, aplicando o apartado 1, tense que:

   $$\mathfrak{a} \text{ é real} \Leftrightarrow A/\mathfrak{a} \text{ é real} \Leftrightarrow \text{r-rad}(0 + \mathfrak{a}) = 0 + \mathfrak{a} \Leftrightarrow \text{r-rad}(\mathfrak{a}) \subset \mathfrak{a}$$

   A outra inclusión é evidente pola definición, logo tense que r-rad$(\mathfrak{a}) = \mathfrak{a}$.

■

5.6. Nullstellensatz Real

Teorema 5.6.1 (Teorema de Homomorfismos de Artin-Lang)**.** *Sexa K un corpo real pechado e A un dominio real que é unha K-álxebra finitamente xerada. Entón existe un homomorfismo de K-álxebras $\varphi : A \longrightarrow K$.*

Demostración. Ver [10], páxina 791, corolario 5.5. ■

Corolario 5.6.2. *Sexa K un corpo real pechado, A un dominio real que é unha K-álxebra finitamente xerada e $f_1, \dots, f_n \in A \setminus \{0\}$. Entón existe un homomorfismo de K-álxebras $\varphi : A \longrightarrow K$ tal que $\varphi(f_i) \neq 0 \, \forall i \in \{1, \dots, n\}$.*

Demostración. Basta con aplicar o teorema 5.6.1 ó dominio real $A[(f_1 \cdots f_n)^{-1}]$. ■

Corolario 5.6.3. *Sexa K un corpo real pechado e A un anel semirreal que é unha K-álxebra finitamente xerada. Entón existe un homomorfismo de K-álxebras $\varphi : A \longrightarrow K$.*

Demostración. Pola proposición 5.1.7, A ten un ideal primo real $\mathfrak{p} \in \text{r-Spec}(A)$. O corolario séguese de aplicar o teorema 5.6.1 ó dominio real $A/\mathfrak{p}$. ■

Corolario 5.6.4. *Sexa K un corpo real pechado, A unha K-álxebra finitamente xerada e $f_1, \dots, f_n \in A$. Se existe unha orde $T \subset A$ tal que $f_i >_T 0 \, \forall i \in \{1, \dots, n\}$ (respectivamente $f_i \geq_T 0 \, \forall i \in \{1, \dots, n\}$), entón existe un homomorfismo de K-álxebras $\varphi : A \longrightarrow K$ tal que $\varphi(f_i) > 0 \, \forall i \in \{1, \dots, n\}$ (respectivamente $\varphi(f_i) \geq 0 \, \forall i \in \{1, \dots, n\}$), sendo "$\leq$" a relación de orde inducida pola única orde que admite K.*

Demostración. Ver [10], páxina 792, corolario 5.5.(C) ■

Teorema 5.6.5 (Problema 17 de Hilbert)**.** *Sexa K un corpo real pechado e $f \in K[x_1, \dots, x_n]$ tal que $f(a) \geq 0 \, \forall a \in K^n$. Entón f é unha suma de cadrados de $K(x_1, \dots, x_n)$.*

Demostración. A resolución (afirmativa) deste problema foi dada por Emil Artin en 1927. Aquí darase unha versión moderna da súa proba.

Denótese por $L = K(x_1, \dots, x_n)$ e supóñase que $f \notin \sum L^2$. Polo lema 5.3.6, L é un corpo real. Entón, polo lema 5.3.10, existe unha orde $T \subset L$ tal que $f <_T 0$, é dicir, $-f >_T 0$. Nótese que esta orde induce tamén unha orde en K. Aplicando o corolario 5.6.4, existe un homomorfismo de K-álxebras $\varphi : K[x_1, \dots, x_n] \longrightarrow K$ tal que $\varphi(-f) > 0$, sendo "$\leq$" a relación de orde inducida pola única orde que admite K.

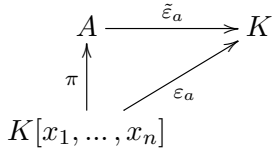
Denotando $a_i = \varphi(x_i) \, \forall i \in \{1, \dots, n\}$, tense que:

$$f(a_1, \dots, a_n) = f(\varphi(x_1), \dots, \varphi(x_n)) = \varphi(f(x_1, \dots, x_n)) = \varphi(f) = -\varphi(-f) < 0$$

Chegando así a unha contradición coa definición de f. ■

Teorema 5.6.6 (Nullstellensatz real)**.** *Sexa K un corpo real pechado, $\mathfrak{a} \lhd K[x_1, \dots, x_n]$ un ideal e $A = K[x_1, \dots, x_n]/\mathfrak{a}$ unha K-álxebra finitamente xerada. Entón A é un anel semirreal se e soamente se $V(\mathfrak{a}) \neq \varnothing$.*

Demostración.
"$\Leftarrow$" Supoñamos que $V(\mathfrak{a}) \neq \varnothing$ e sexa $a = (a_1, \dots, a_n) \in V(\mathfrak{a})$. Sexa o homomorfismo avaliación en a, $\varepsilon_a : K[x_1, \dots, x_n] \longrightarrow K$, definido por $\varepsilon_a(f) = f(a)\ \forall f \in K[x_1, \dots, x_n]$. É evidente ver que $\mathfrak{a} \subset \mathrm{Ker}(\varepsilon_a)$, logo existe un homomorfismo de K-álxebras $\tilde{\varepsilon}_a : A \longrightarrow K$ definido por $\tilde{\varepsilon}_a(f + \mathfrak{a}) = f(a)$, que é tal que $\varepsilon_a = \tilde{\varepsilon}_a \circ \pi$, sendo $\pi : K[x_1, \dots, x_n] \longrightarrow A$ a proxección no cociente.



Como K é un corpo real, entón é semirreal (proposición 5.3.4), logo polo apartado 1 da proposición 5.1.6, A é semirreal.

"$\Rightarrow$" Se A é un anel semirreal, entón polo corolario 5.6.3 existe un homomorfismo de K-álxebras $\varphi : A \longrightarrow K$. Denotando $a_i = \varphi(x_i + \mathfrak{a})$ e dado un $f \in \mathfrak{a}$ tense que:

$$f(a_1, \dots, a_n) = f(\varphi(x_1 + \mathfrak{a}), \dots, \varphi(x_n + \mathfrak{a})) = \varphi(f(x_1 + \mathfrak{a}, \dots, x_n + \mathfrak{a})) =$$

$$= \varphi(f + \mathfrak{a}) = \varphi(0 + \mathfrak{a}) = 0$$

Logo tense que $(a_1, \dots, a_n) \in V(\mathfrak{a}) \neq \varnothing$. ■

Lema 5.6.7. *Sexa K un corpo real e $\mathfrak{a} \lhd K[x_1, \dots, x_n]$ un ideal. Entón $I(V(\mathfrak{a}))$ é un ideal real de $K[x_1, \dots, x_n]$.*

Demostración. Sexan $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ polinomios tales que $f_1^2 + \cdots + f_r^2 \in I(V(\mathfrak{a}))$. Entón tense que:

$$(f_1^2 + \cdots + f_r^2)(a) = f_1(a)^2 + \cdots + f_r(a)^2 = 0\ \forall a \in V(\mathfrak{a})$$

Como K é un corpo real, entón tense que $f_1(a) = \cdots = f_r(a) = 0\ \forall a \in V(\mathfrak{a})$, é dicir, $f_1, \dots, f_r \in I(V(\mathfrak{a}))$. Pola proposición 5.1.4, isto implica que o ideal $I(V(\mathfrak{a}))$ é real. ■

Teorema 5.6.8. *Sexa K un corpo real pechado e $\mathfrak{p} \in \mathrm{Spec}(K[x_1, \dots, x_n])$ un ideal primo. Entón tense que $I(V(\mathfrak{p})) = \mathfrak{p}$ se e soamente se $\mathfrak{p} \in \text{r-Spec}(K[x_1, \dots, x_n])$.*

Demostración.
"⇒" Supoñamos que $\mathfrak{p}$ non é real. Entón existen os polinomios $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ tales que $f_1^2 + \cdots + f_r^2 \in \mathfrak{p}$, mais $f_1 \notin \mathfrak{p}$. Polo lema 5.6.7, $I(V(\mathfrak{p}))$ é un ideal real, e pola definición é evidente que $\mathfrak{p} \subset I(V(\mathfrak{p}))$, logo, pola proposición 5.1.4, tense que $f_1 \in I(V(\mathfrak{p}))$, mais como $f_1 \notin \mathfrak{p}$, entón $I(V(\mathfrak{p})) \neq \mathfrak{p}$, como queríamos probar.

"⇐" Supoñamos que $\mathfrak{p}$ é real e sexa $f \notin \mathfrak{p}$. Probarase que entón $f \notin I(V(\mathfrak{p}))$. Como no anel cociente $A = K[x_1, \dots, x_n]/\mathfrak{p}$ tense que $f + \mathfrak{p} \neq 0 + \mathfrak{p}$, polo corolario 5.6.2 existe un homomorfismo de K-álxebras $\varphi : A \longrightarrow K$ tal que $\varphi(f + \mathfrak{p}) \neq 0$. Denotando $a_i = \varphi(x_i + \mathfrak{p})$ e dado un $g \in \mathfrak{p}$ arbitrario tense que:

$$g(a_1, \dots, a_n) = g(\varphi(x_1 + \mathfrak{p}), \dots, \varphi(x_n + \mathfrak{p})) = \varphi(g(x_1 + \mathfrak{p}, \dots, x_n + \mathfrak{p})) =$$

$$= \varphi(g + \mathfrak{p}) = \varphi(0 + \mathfrak{p}) = 0$$

Logo tense que $a = (a_1, \dots, a_n) \in V(\mathfrak{p})$. De forma análoga pódese ver que:

$$f(a) = \varphi(f + \mathfrak{p}) \neq 0$$

Logo tense que $f \notin I(V(\mathfrak{p}))$. ■

Teorema 5.6.9 (Nullstellensatz real forte)**.** *Sexa K un corpo real pechado e $\mathfrak{a} \triangleleft K[x_1, \dots, x_n]$ un ideal. Entón tense que $I(V(\mathfrak{a})) = \text{r-rad}(\mathfrak{a})$.*

Demostración.
"⊃" Sexa $f \in \text{r-rad}(\mathfrak{a})$. Entón, polo teorema 5.5.3, existen $m, r \in \mathbb{N}$ e os polinomios $g_1, \dots, g_r \in K[x_1, \dots, x_n]$ tales que $f^{2m} + g_1^2 + \cdots + g_r^2 \in \mathfrak{a}$. Logo para cada $a \in V(\mathfrak{a})$ tense que:

$$(f^{2m} + g_1^2 + \cdots + g_r^2)(a) = f(a)^{2m} + g_1(a)^2 + \cdots + g_r(a)^2 = 0$$

Como K é un corpo real, entón tense que $f(a)^m = 0$, logo $f(a) = 0 \; \forall a \in V(\mathfrak{a})$, é dicir, $f \in I(V(\mathfrak{a}))$.

"⊂" Sexa $\mathfrak{p} \in \text{r-Spec}(A)$ un ideal primo real tal que $\mathfrak{a} \subset \mathfrak{p}$. Entón tense que $V(\mathfrak{p}) \subset V(\mathfrak{a})$, e $I(V(\mathfrak{a})) \subset I(V(\mathfrak{p})) = \mathfrak{p}$, sendo a última igualdade debida ó teorema 5.6.8. Logo tense que:

$$I(V(\mathfrak{a})) \subset \bigcap_{\substack{\mathfrak{p} \in \text{r-Spec}(A) \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p} = \text{r-rad}(\mathfrak{a})$$

■

Bibliografía

[1] Allen B. Altman and Steven L. Kleiman: *A Term of Commutative Algebra*. Worldwide Center of Mathematics, 2019.

[2] Michael F. Atiyah and Ian G. MacDonald: *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[3] Alexey Beshenov: *Introducción al álgebra conmutativa*. Universidad de El Salvador, 2018.
`https://cadadr.org/san-salvador/2018-08-algebra-conmutativa/algebra-conmutativa.pdf`

[4] David S. Dummit and Richard M. Foote: *Abstract Algebra*. John Wiley and Sons Inc, 2003.

[5] David Eisenbud: *Commutative Algebra with a View Towards Algebraic Geometry*. Springer, 1989.

[6] José F. Fernando and J. Manuel Gamboa: *Real Algebra from Hilbert's 17th Problem*. Pisa & Madrid, July 2012.
`http://www.mat.ucm.es/~josefer/articulos/rgh17.pdf`

[7] Sudhir R. Ghorpade: *A Note on Nullstellensatz over Finite Fields*. June 26, 2018.
`https://arxiv.org/abs/1806.09489`

[8] Kriti Goel, Dilip P. Patil and Jugal Verma: *Nullstellensätze and Applications*. September 8, 2018.
`https://arxiv.org/abs/1809.02818`

[9] Thomas W. Judson: *Abstract Algebra, Theory and Applications*. 2020.
`http://abstract.ups.edu/`

[10] Tsit Yuen Lam: *An Introduction to Real Algebra*. Rocky Mountain J. Math, Volume 14, Number 4 (1984), 767-814.

[11] Serge Lang: *Algebra*, 3rd edition. Springer, 2005.

[12] Odilon Otávio Luciano: *A Really Simple Proof of the Artin-Schreier Characterization of Real Closed Fields*. South American Journal of Logic Vol. 2, n. 2, pp. 361–377, 2016. http://www.sa-logic.org/sajl-v2-i2/10-Luciano-SAJL.pdf

[13] James S. Milne: *Algebraic Geometry*. March 19, 2008. https://www.jmilne.org/math/CourseNotes/AG510.pdf

[14] Bernd Sturmfels: *Nullstellensätze*. Notes for the lecture in the IMPRS Ringvorlesung "Introduction to Nonlinear Algebra", May 15, 2018. https://personal-homepages.mis.mpg.de/michalek/may15.pdf