MAT426 - Ayudantía 3

Cristóbal Montecino

1. Hilbert's Nullstellensatz

En 1930, J. L. Rabinowitsch publica el articulo "*Zum Hilbertschen Nullstellensatz*". Del cual se destaca el conocido como *Truco de Rabinowitsch*. Este nos dice que solo basta demostrar el caso "débil"del teorema ya que el "fuerte", tras utilizar el truco de Rabinowitsch, se deduce del primero.

En 1947, se publica "*A new proof of Hilbert's Nullstellensatz*" por O. Zariski. La demostración del caso débil se basa en el lema de Zariski: *Si K/k es una extensión de cuerpo tal que K es una k-álgebra finitamente generada, entonces K es una extensión finita de k.*

En 2005, D. Allcock expone una demostración sencilla al Hilbert's Nullstellensatz que resulta ser una simplificación a la demostración de Zariski. Esta utiliza una versión débil al lema de Zariski que, en este documento, lo llamaremos lema de Zariski-Allcock: *Si K/k es una extensión de cuerpo tal que K es una k-álgebra finitamente generada, entonces K es una extensión algebraica de k.*

Esta ultima es la que demostraremos. Para ello, asumiremos conocimientos básicos sobre teoría de cuerpos y álgebras sobre un cuerpo. Aparte de anillos, espacios vectoriales y estructuras en general. El resto se complementara con la sección Complemento.

Lema 1.1 (Lema de Zariski-Allcock)**.** Sea K/k una extensión de cuerpo. Si K es una k-álgebra finitamente generada, entonces K es una extensión algebraica de k.

$\boxed{\text{Ejercicio}}$ Demuestre el lema de Zariski-Allcook. Para esto,

1. Suponga, por reducción al absurdo, que K es una extensión trascendente.
2. Demuestre que el caso cuando el grado de trascendencia es mayor a 1 se puede reducir al caso de grado de trascendencia igual a 1.

   Hint: Cómo K es una k-álgebra finitamente generada, existen $x_1, ..., x_n \in K$ tales que $K = k(x_1, ..., x_n)$.
3. Demuestre que se produce una contradicción cuando el grado de trascendencia es igual a 1. Para ello,

   a) Pruebe que $[K : k(\alpha)] < \infty$ con $\{\alpha\}$ una base de trascendencia de K/k.

   Hint: Existen $x_1, ..., x_n \in K$ tales que $K = k(x_1, ..., x_n)$.

   b) Pruebe que $k(\alpha) \cong \mathrm{Fr}(k[x])$.

   c) Obtenga $\frac{1}{r(\alpha)} \notin K$ para algún polinomio irreducible $r \in k[x]$.
   Hint: use a) y b) para mostrar que los denominadores solo pueden ser de cierta manera.

   d) Concluya por contradicción.

Teorema 1.1 (Hilbert's Nullstellensatz débil)**.** Sea k un cuerpo algebraicamente cerrado y $R := k[x_1, ..., x_n]$. Si $\mathfrak{m}$ es un ideal maximal de R, entonces existe $a \in k^n$ tal que

$$\mathfrak{m} = \mathfrak{m}_a$$

Además, si J es un ideal de R tal que $V(J) = \emptyset$, entonces $J = R$.

Ejercicio: Demuestre Hilbert's Nullstellensatz débil.

Teorema 1.2. (Hilbert's Nullstellensatz fuerte) Sea k un cuerpo algebraicamente cerrado, $R := k[x_1, ..., x_n]$. Entonces,

$$I(V(J)) = \sqrt{J}$$

para todo ideal J de R.

Ejercicio: Demuestre Hilbert's Nullstellensatz fuerte. Para ello,

1. Note que solo hay que demostrar $I(V(J)) \subseteq \sqrt{J}$.
2. Pruebe que existen $f_1, ..., f_m$ tales que generan J.

   Hint: Use el teorema de la base de Hilbert.
3. Truco de Rabinowitsch. Sea $g \in I(V(J))$. Entonces,

   $$V(\{f_1, ..., f_m, gx_{n+1} - 1\}) = \emptyset \text{ en } R[x_{n+1}]$$
4. Utilice el teorema débil y devuélvase a R de manera conveniente (i.e. para obtener la conclusión).
5. Concluya que alguna potencia de g pertenece J.

2. Cayley-Hamilton

Muchos resultados sobre matrices, usando la topología de Zariski, pueden resolverse solo considerando matrices con buenas propiedades, es decir, matrices diagonalizables, invertibles, con valores propios distintos, etc. Un buen ejemplo es el siguiente:

Teorema 2.1 (Cayley-Hamilton)**.** Sea k un cuerpo, A una matriz $n \times n$ sobre k, P_A el polinomio característico de A. Entonces,

$$P_A(A) = 0$$

Ejercicio: Demuestre Cayley-Hamilton. Para ello,

1. Note que basta con asumir que k es un cuerpo algebraicamente cerrado.
2. Sea $X \subseteq \mathbb{A}_k^{n^2}$ el conjunto de todos las matrices $n \times n$ tal que hacen cero a su polinomio característico:

   $$X := \{A \in \mathbb{A}_k^{n^2} \mid P_A(A) = 0\}$$

   Pruebe que X es un cerrado de Zariski.
3. Demuestre el teorema cuando A es una matriz con todos los valores propios distintos.

   Es decir, pruebe que $U := \{A \in \mathbb{A}_k^{n^2} \mid A \text{ tiene valores propios distintos}\}$ es subconjunto de X.
4. Pruebe que U es un abierto de Zariski.

   Hint: El discriminante de un polinomio es cero si y solo si tiene raíces repetidas.
5. Concluya por la irreducibilidad de $\mathbb{A}_k^{n^2}$ que $X = \mathbb{A}_k^{n^2}$.

   Hint: irreducibilidad $\implies$ abiertos densos

Referencia: *Using Zariski Topology to prove The Cayley Hamilton Theorem.*

3. Complemento

Teorema 3.1. Sea k un cuerpo. $k[x]$ contiene infinitos polinomios irreducibles.

Demostración. Supongamos que $k[x]$ tiene una cantidad finita de polinomios irreducibles: $p_1, ..., p_n$. Basta considerar el polinomio $p_1 \cdots p_n + 1$. Este tiene que ser irreducible y esto es una contradicción porque habría $n+1$ polinomios irreducibles. $\square$

Definición 3.1 (Depedencia algebraica)**.** Sea F/K una extensión de cuerpo. $S \subseteq F$ se dice *algebraicamente dependiente* sobre K ssi existen $\alpha_1, ..., \alpha_n \in S$ y algún polinomio $p \in K[x_1, ..., x_n]$: $p \neq 0$ tal que

$$p(\alpha_1, ..., \alpha_n) = 0 \text{ sobre } F$$

para algún $n \in \mathbb{N} : n \geq 1$.

Definición 3.2 (Indepedencia algebraica)**.** Sea F/K una extensión de cuerpo. $S \subseteq F$ se dice *algebraicamente independiente* ssi no es algebraicamente dependiente.

Proposición 3.1 (Extensión algebraica)**.** Sea F/K una extensión de cuerpo. F es una extensión algebraica de K si y solo si

$$\{\alpha\} \text{ es algebraicamente dependiente sobre } K$$

para todo $\alpha \in F$.

Definición 3.3 (Extensión trascendente)**.** Una extensión de cuerpo F/K se dice *transcendente* cuando no es una extensión algebraica.

Definición 3.4 (Base de trascendencia)**.** Sea F/K una extensión de cuerpo. $S \subset F$ es *una base de trascendencia de* F/K ssi

(1) S es algebraicamente independiente (sobre K). ("*Los elementos de* S *no se generan entre si*")

(2) F es una extensión algebraica de $K(S)$. ("*Los elementos de* $K(S)$ *generan* F")

$$\begin{array}{cl} F & \\ | & \leftarrow \text{(extensión algebraica)} \\ K(S) & \\ | & \\ K & \end{array}$$

Teorema 3.2 (Existencia de base de trascendencia)**.** Sea F/K una extensión de cuerpo. Existe alguna base de trascendencia de F/K.

Teorema 3.3. Sea F/K una extensión de cuerpo. Todas las bases de trascendencia de F/K tienen la misma cardinalidad.

Definición 3.5 (Grado de trascendencia)**.** Sea F/K una extensión de cuerpo. El grado de trascendencia de F/K es la cardinalidad de cualquier base de trascendencia de F/K.

Proposición 3.2. Sea F/K una extensión de cuerpo. F/K es una extensión trascendente si y solo si el grado de trascendencia es mayor o igual a 1.

Definición 3.6. Sea k un cuerpo, $R := k[x_1, ..., x_n]$ y $a \in k^n$. Se define

$$\mathfrak{m}_a := (x_1 - a_1, ..., x_n - a_n)$$

Proposición 3.3. Sea k un cuerpo, $R := k[x_1, ..., x_n]$ y $a \in k^n$.

$$\mathfrak{m}_a \text{ es un ideal maximal de } R.$$