TEORÍA DE MODELOS Y GEOMETRÍA ALGEBRAICA EN LA DEMOSTRACIÓN DE LA CONJETURA DE MORDELL-LANG

Universidad Nacional Autónoma de México

Facultad de Ciencias

Matemáticas

Tesis de Lincenciatura

Carlos Alfonso Ruiz Guido

Director de Tesis: Timothy Gendron Thornton

México Distrito Federal - 22 de agosto de 2012

ÍNDICE

1. INTRODUCCIÓN

Este texto resume el trabajo que hice para obtener el grado de licenciatura en Matemáticas en la Facultad de Ciencias de la Universidad Nacional Autónoma de México. Agradezco muy en particular al Dr. Timothy Gendron por su gran ayuda y entusiasmo sobre el tema. Su enorme disposición y sus consejos fueron fundamentales para el desarrollo de este trabajo. La meta es dar una demostración detallada de la conjetura de Mordell-Lang. Su demostración es fascinante por varios aspectos. Por un lado es un teorema importante dentro del área de Geometría Diofantina, pues establece un resultado análogo a la Conjetura de Lang para los campos de funciones; a su vez, la importancia de esta última radica en ser una generalización (bastante fuerte) de la conjetura de Mordell, ahora teorema de Faltings.

Por el otro lado, la demostración es un parteaguas en la interacción entre geometría algebraica y teoría de modelos. La prueba fue hecha por Ehud Hrushovski en el año 1996, y en lugar de utilizar técnicas como alturas, aproximación diofantina o geometría algebrica avanzada (como en las demostraciones de la conjetura de Mordell y la conjetura de Lang), Hrushovski utilizó fuertes resultados de Saharon Shelah, Boris Zilber y del mismo Hrushovski sobre teoría de modelos.

La teoría de modelos es un área de la Lógica Matemática. En su versión actual es consecuencia, por un lado, de las interacciones entre la lógica y teoría de conjuntos, análisis matemático o geometría algebraica; por el otro lado, del estudio de los modelos de una teoría arbitraria sobre un lenguaje dado. A esto último es lo que se le conoce como teoría de modelos pura. Resulta un poco paradójico que aquellas técnicas que durante algún tiempo se consideraron exclusivas de la teoría de modelos pura, son precisamente las que utilizó Hrushovski en su demostración. Incluso son las mismas que actualmente se están utilizando en muchas áreas aparentemente alejadas a la lógica como: combinatoria enumerativa, integración motívica, teoría de módulos, geometría Khäleriana o álgebra diferencial. Considero que la teoría de modelos es un lenguaje que puede ayudar a resolver problemas de la matemática en general y que sus técnicas -además de eficientes- son muy bellas.

El lector interesado en seguir a detalle mi trabajo debe haber llevado un primer curso de Lógica Matemática y cursos de Álgebra abstracta sobre grupos, anillos y campos. Aquellos que sepan sobre geometría algebraica en el lenguaje de variedades (Hrushovski lo hizo todo sobre esquemas, pero al no perder generalidad en las técnicas he decidido usar variedades) y teoría de modelos básica ganarán mucho tiempo en la lectura. Sin embargo, en el apéndice introduzco definiciones desde los primeros requisitos que mencioné.

También debo advertir de las dificultades que se pueden enfrentar para leer este trabajo. Por un lado el enunciado de la conjetura de Mordell-Lang es muy técnico, por eso he decidido no escribirlo hasta la sección 7.2, donde es precedido por una sección en la que se motiva su formulación y se hace un recuento histórico-matemático de su significado. Para aquellos que no aguanten la curiosidad, el enunciado que demostraremos es el último de la sección 8.

Si el lector decide leer mi trabajo en orden (como debería de ser) es posible que se encuentre con la dificultad de no saber hacia dónde voy. Me disculpo de antemano con aquellos lectores que se enfrenten a ese problema y me justifico con la gran cantidad de teoría que se utiliza en la demostración. También me permito darles una sugerencia sobre otro posible órden de lectura. Empezar con las secciones 2.1 y 3 que es dónde se encuentra lo básico de teoría de modelos. Inmediatamente después ir a la sección 8 que es donde se encuentra la demostración de Mordell-Lang y regresar a aquellas secciones que ustedes vayan juzgando necesarias conforme su avance. Debo mencionar que en ningún momento

será mi intención perder a ningún lector con los resultados que vaya exponiendo, así que en todas las secciones encontrarán ejemplos y referencias relevantes a la demostración de Hrushovski.

A continuación daré un pequeño resúmen respecto a la organización del trabajo y la relevancia de cada sección dentro de la demostración de Mordell-Lang.

En la primera sección incluyo los preliminares del trabajo, es decir: ideas básicas de la teoría de modelos. También decidí agregar una sección sobre un tema mucho menos clásico en matemáticas: los Campos diferenciales. Esta parte se incluye porque la teoría que se utilizará para hacer la demostración de Mordell-Lang es la de los campos diferencialmente cerrados.

En la sección dos encontrarán objetos y propiedades de la teoría de modelos que son análogos a los ideales y a las extensiones algebraicas. También explicaremos por qué es posible incluir algunas hipótesis sobre los modelos en los que trabajaremos y por qué son útiles. Las hipótesis son saturación y ω-estabilidad.

En el capitulo tres se estudiará una extensión canónica de cualquier estructura y lenguaje llamada la estructura de los imaginarios. Las proposiciones más importantes para demostrar Mordell-Lang están dadas en la estructura de los imaginarios, sin embargo necesitamos que esas propiedades sean ciertas en la estructura original (y no la de los imaginarios). En la teoría que vamos a utilizar, siempre es posible hacer esto.

La sección cuatro es quizás la más necesaria para entender la prueba. Desarrollaré lo necesario de la teoría geométrica de la Estabilidad. La teoría de Estabilidad se utilizó para dar la clasificación de los modelos de una teoría dada. Este trabajo fue hecho por Shelah y se enmarca dentro de la teoría de modelos pura. Sin embargo, hoy en día sus aplicaciones a otras áreas de las matemáticas se cuentan por montón. Quiero recalcar que los conceptos que ahí se definirán tienen traducciones de cosas ya conocidas en los campos algebraicamente cerrados. Uno de estos conceptos generalizará la dimensión de Krull para anillos, otro la dependencia lineal (espacios vectoriales) y la dependencia algebraica (campos), mientras que otro generalizará extensiones trascendentes (campos). La relación más profunda entre la teoría de modelos y geometría algebraica se encuentra en este tipo de equivalencias. Las últimas 4 subsecciones son bastante técnicas, pues incluyen muchos métodos y proposiciones que se utilizarán en la prueba de Mordell-Lang. Estas últimas secciones se podrían englobar bajo el título de grupos ω-estables.

En la sección cinco se habla sobre las geometrías de Zariski. A grandes rasgos las geometrías de Zariski son modelos con condiciones topológicas que cumplen con parecerse a la topología que se utiliza en la geometría algebraica. Resultan ser generalizaciones de variedades algebraicas, pero lo más importante es que en ellas es cierta la conjetura de tricotomía de Boris Zilber. Esta tricotomía es fundamental en la prueba de Mordell-Lang. A grandes rasgos dice que si tenemos un modelo con condiciones geométricas básicas sobre sus conjuntos definibles, entonces pasa alguna de las siguientes cosas: su geometría es la trivial (solo son conjuntos), es parecida a la de los espacios vectoriales o existe un campo algebraicamente cerrado dentro del modelo. Notemos lo fantástico que resulta poder encontrar un campo algebraicamente cerrado en un conjunto muy arbitrario.

La sección seis se acerca peligrosamente a la demostración y está dividido en tres secciones. En la primera se enuncian y demuestran algunos teoremas que ya utilizan la mayoría de las secciones anteriores y serán usados en la demostración. La segunda es la motivación histórico-matemática de la conjetura de Mordell-Lang y la tercera habla precisamente sobre una traducción que existe entre la teoría de modelos y Mordell-Lang.

La última sección incluye la demostración detallada y así cumplimos con el objetivo de la tesis. Es importante mencionar que a pesar de que la prueba de Hrushovski involucra campos de característica arbitraria, yo sólo expondré el caso de característica 0. La idea es muy parecida en ambos casos, pero los detalles son más complicados para característica p.

El apéndice incluye una introducción autocontenida sobre la geometría algebraica. Es importante mencionar que no incluyo ninguna de las demostraciones. Recomiendo a quienes no estén familiarizados con la geometría algebraica leer cuidadosamente esta sección y en caso de querer profundizar en los detalles consultar [7], [8] o [9].

Con el objetivo de ir dejando las ideas claras, me atrevo a dar una idea MUY VAGA sobre la demostración de Hrushovski. El enunciado de la conclusión de Mordell-Lang es del tipo «entonces A o B», mientras que la conjetura de tricotomía de Zilber (dadas las hipótesis de Mordell-Lang) se convierte en una dicotomía. Como la tritotomía de Zilber es cierta para los campos diferenciales, entonces sólo faltaría demostrar que las implicaciones de la dicotomía de Zilber implican a su vez A y B respectivamente. Esto último se hace en los teoremas 5.87 y 7.16.

Por último me gustaría agradecer a personas que fueron muy importantes para que esta tesis fuera posible. A Octavio Páez Osuna por su incondicional ayuda y sus excelentes enseñanzas a lo largo de estos cuatro años. A mi amigo Iván Ongay por revisar los primeros capítulos sin esperar nada a cambio. A Zabdi Rojas por mejorar mi redacción y ortografía. A mi amiga Brenda Pazos también por mejorar mi ortografía. Por su puesto soy yo el responsable de cualquier error en la redacción, ortográfico o matemático.

2. PRELIMINARES

Esta sección se dividirá en tres, en la primera daré una introducción autocontenida de la teoría de modelos, los resultados de esa sección son fundamentales tanto para el resto del texto como para poder leer cualquier otro respecto a la teoría de modelos, por lo cual recomiendo ampliamente que el lector no familiarizado dedique el tiempo suficiente a entender bien los resultados. Más detalles se pueden consultar en [3], [4] u [11].

En la segunda parte daré una introducción sobre un tema menos clásico en matemáticas que es la teoría de campos diferenciales. El objetivo es dar las definiciones básicas y hacer una analogía entre ellos y los campos algebraicos en lo que respecta a los teoremas importantes para hacer geometría algebraica.

Por último daré un acercamiento a los campos algebraicamente cerrados utilizando teoría de modelos.

2.1. Ideas básicas de la teoría de modelos. El objeto de estudio de la teoría de modelos son las estructuras. Pero lo más importante de las estructuras es el conjunto de los definibles dentro de ella. Existen dos maneras distintas de definir a las estructuras, la principal diferencia radica en que en una de ellas es bastante sencillo hablar del conjunto de los definibles. A continuación daré esa definición, sin embargo no la utilizaremos en el futuro pues puede ser un poco tediosa. La incluyo a manera de motivación de lo que son los conjuntos definibles en una estructura dada.

Definición 2.1. *Una **estructura** **M*** es una pareja $\left(M,(B_i)_{i\in I}\right)$ donde M es un conjunto no vacío, y la familia $(B_i)_{i\in I}$ son subconjuntos de $\cup_{n\geq 1}M^n$. A los $(B_i)_{i\in I}$ los llamaremos **conjuntos atómicos**. Por convención en este texto, agregaremos la condición de que la diagonal en M^2 siempre es un B_i para algún $i\in I$.

Definición 2.2. *Sea* $\boldsymbol{M}=\left(M,(B_i)_{i\in I}\right)$ una estructura. Definimos a la familia de **conjuntos definibles** en M (denotados por $Def\,(M)$) como la familia más pequeña de subconjuntos en $\cup_{n\geq 1}M^n$ de tal forma que se cumplan las siguientes propiedades:

1. Para cada $i\in I$ se tiene que $B_i\in Def\,(M)$
2. $Def\,(M)$ es cerrado bajo combinaciones booleanas finitas, ie. si $A,B\subseteq M^n$ para algún n, con $A,B\in Def\,(M)$, entonces $A\cup B, A\cap B\in Def\,(M)$ y $M^n\backslash A\in Def\,(M)$.
3. $Def\,(M)$ es cerrado bajo productos cartesianos, ie. si $A,B\in Def\,(M)$, entonces $A\times B\in Def\,(M)$.
4. $Def\,(M)$ es cerrado bajo proyecciones, ie. si $A\subseteq M^{n+m}$, $A\in Def\,(M)$ y $\pi_n\,(A)$ es la imagen de la proyección canónica que va de M^{n+m} a M^n, entonces $\pi_n\,(A)\in Def\,(M)$.
5. $Def\,(M)$ es cerrado bajo especializaciones, ie. si $A\in Def\,(M)$, $A\subseteq M^{n+k}$ y $m\in M^n$, entonces
$$A\,(m)=\left\{b\in M^k:(m,b)\in A\right\}\in Def\,(M)$$
6. $Def\,(M)$ es cerrado bajo permutación de coordenadas, i.e. si $A\in Def\,(M)$, $A\subseteq M^n$ y σ es una permutación de $\{1,2,\ldots,n\}$ entonces
$$\sigma\,(A)=\left\{\left(a_{\sigma(1)},a_{\sigma(2)},\ldots,a_{\sigma(n)}\right):(a_1,a_2,\ldots,a_n)\in A\right\}\in Def\,(M)$$

Comenzaremos con algunos ejemplos:

Ejemplo 2.3. ***[Campos algebraicamente cerrados]***Consideremos la estructura $\boldsymbol{K}$ donde el conjunto K es un campo algebraicamente cerrado y la familia $(B_i)_{i\in I}$ consiste (para cada

i) de las soluciones de polinomios con coeficientes en K en n variables para algún $n \in \mathbb{N}$. ¿Cómo entendemos las propiedades 1-6 para los campos algebraicamente cerrados?

1. Para la propiedad dos notemos que la multiplicación de dos polinomios es un polinomio (así que la unión está). Por otro lado debemos agregar a $Def\,(K)$ los complementos de todo conjunto de soluciones a un polinomio. Las intersecciones estarán por las leyes de De Morgan. Así están todas las combinaciones booleanas.
2. Para la propiedad 3: si tenemos un polinomio en n variables y otro en m variables, consideremos la suma del primer polinomio en las variables $x_1, \ldots, x_n$ y el segundo en las variables $x_{n+1}, \ldots, x_{n+m}$ (las $n+m$ son distintas). El conjunto de soluciones de este polinomio (llamémosle S) contiene a las que queremos. Si S_1 y S_2 son los conjuntos de soluciones del polinomio 1 y 2 respectivamente, entonces el producto cartesiano que queremos considerar será igual a $(S \cap S_1) \cup (S \cap S_2)$.
3. Para las especializaciones: si $p\,(x)$ es un polinomio en $n+m$ variables y a es una m-ada, entonces al evaluar las coordenadas de a en las últimas m variables, obtenemos un polinomio en n variables, y su conjunto de soluciones es el que queremos.
4. Como la suma de elementos en el campo es conmutativa, entonces las soluciones de un polinomio y las de permutar sus variables son las mismas.
5. La propiedad que no es para nada trivial es probar que los definibles son cerrados bajo proyecciones. El resultado es un teorema de Chevalley y es un ejemplo de una importante propiedad en la teoría de modelos llamada eliminación de cuantificadores. Más adelante daremos una definición precisa de este concepto.

Así obtenemos a los conjuntos definibles dentro de los campos algebraicamente cerrados.

Ejemplo 2.4. *Consideremos a los números reales $\mathbb{R}$. Tomemos por subconjuntos atómicos los conjuntos de la siguiente forma: si $p\,(x_1, \ldots, x_n)$ un polinomio con coeficientes en $\mathbb{R}$, consideramos*

$$\{a \in \mathbb{R}^n : p\,(a) = 0\}\, o\, \{a \in \mathbb{R}^n : p\,(a) > 0\}$$

El análisis de qué conjuntos debemos agregar para obtener $Def\,(\mathbb{R})$ es muy similar al anterior.

La primera desventaja de esta definición de estructura es que es muy complicado encontrar una definición apropiada para los «morfismos» entre estructuras, pues no queda muy claro ¿qué tipo de propiedades debe cuidar una función entre estructuras?

Otra razón para buscar una nueva definición es que el contestar las siguientes preguntas es muy complicado con nuestra primera definición:

- Si $\overline{\mathbb{Q}}$ denota una cerradura algebraica de $\mathbb{Q}$, consideramos a $Def\left(\overline{\mathbb{Q}}\right)$ y a $Def\,(\mathbb{C})$ como los conjuntos definibles de un campo algebraicamente cerrado. ¿Hay alguna forma de extender un conjunto definible en $\overline{\mathbb{Q}}$ a uno en $\mathbb{C}$?
- Sea $D \subseteq \overline{\mathbb{Q}}^n$ definible en $\overline{\mathbb{Q}}$, ¿será que su intersección con $\mathbb{Q}^n$ es un definible? Resulta que para nuestros ejemplos las respuestas a esas preguntas son afirmativas, sin embargo, ¿eso ocurre para otro tipo de estructuras?

Debido a que los conjuntos B_i fueron escogidos de manera sumamente arbitraria es necesario dar una nueva definición que las aclare. Nuestra nueva definición dirá que un conjunto es definible si existe una fórmula en el lenguaje formal que lo caracteriza unívocamente. La ventaja inmediata de esto es que, de acuerdo a cómo construiremos las fórmulas es posible hacer inducción sobre ellas. Además, tendremos dos maneras DISTINTAS de referirnos a un conjunto definible: una es por sus elementos y la otra por la fórmula que lo define. La analogía a tener en cuenta son las soluciones de un polinomio y

el polinomio que los define. Fue Groethendieck quien hizo notar que estas dos maneras de ver al mismo conjunto son tan distintas.

A continuación la definición oficial de estructura:

Definición 2.5. *Una **estructura** M* consta de lo siguiente:

- Un conjunto no vacío al que denotaremos también por M. Este abuso de notación será recurrente: M puede referirse a la estructura o al conjunto.
- Una familia $\left(R_i^M\right)_{i\in I}$ de subconjuntos de $\cup_{n\geq 1}M^n$ de tal forma que para cada $i \in I$, $R_i^M \subseteq M^{n_i}$. A estos conjuntos les llamamos relaciones. A manera de notación, $R_i^M(a)$ significa que $a \in R_i^M$. Notemos que a denota una i-ada en M^{n_i}.
- Nuevamente agregamos a la diagonal en M^2 como uno de los R_i^M's. Esta relación corresponde a la igualdad ($=$).
- Una familia de funciones $\left(f_j^M\right)_{j\in J}$, donde cada f_j^M es una función n_j-ria que va de M^{n_j} en M.
- Un conjunto de constantes $\left(c_k^M\right)_{k\in K}$ de tal forma que cada $c_k^M \in M$.

Respecto a nuestra primera definición, hasta ahora estamos considerando sólo un subconjunto de los $B_{i's}$.

La primera distinción entre los conjuntos y las fórmulas que los definen es la siguiente:

Definición 2.6. *El **lenguaje** L_M* asociado a la estructura M consta de:

- Símbolos lógicos: $\wedge, \vee, \neg$
- Paréntesis.
- Símbolo de pertenencia $\in$.
- Cuantificadores $\forall$, $\exists$.
- Para cada relación R_i^M, un símbolo de relación R_i de aridad n_i.
- Como la diagonal en M^2 es una relación considerada, siempre hay una relación binaria en L que coincide con la igualdad en M.
- Para cada función f_j^M, un símbolo de función f_j de aridad n_j.
- Para cada constante c_k^M, un símbolo de constante c_k.

Decimos que R^M es una interpretación de R.

Una ventaja de este acercamiento a las estructuras es que podemos considerar lenguajes arbitrarios $L = \left(\wedge, \vee, =, (,), \in, \forall, \exists, (R_i)_{i\in I}, (f_j)_{j\in J}, (c_k)_{k\in K}\right)$ tan sólo como un conjunto de símbolos. Si el lenguaje L_M asociado a una estructura M coincide con L, diremos que M es una L estructura. Es interesante cuando fijamos un lenguaje L y consideramos la familia de todas las L-estructuras, más adelante hablaremos de esta familia de estructuras.

Recordemos que en la primera definición que dimos de estructura nunca se mencionó nada sobre el lenguaje, veamos cuáles son los lenguajes en los ejemplos que dimos:

- El lenguaje de los campos algebraicamente cerrados es el siguiente: $(+, \cdot, 0, 1)$. A este lenguaje lo llamaremos $L_{anillos}$ pues la familia de las $L_{anillos}$-estructuras contiene a todos los anillos. También contiene a todos los campos.
- Es posible agrandar este lenguaje para un anillo dado. Sea R un anillo, consideremos a $L_R = L_{anillos} \cup \{f_r\}_{r\in R}$ donde cada f_r es la función uno-aria que multiplica al argumento por $r \in R$:
$$f_r : R \longrightarrow R$$
$$f_r(s) = rs$$
- Los reales (como campo ordenado) tienen un lenguaje más amplio: $L_{\mathbb{R}} = (<, \cdot, +, 0, 1)$.
- El lenguaje de los grupos es el siguiente: $L_{grupos} = (G, \cdot, e)$.

Un primer acercamiento al concepto de morfismo entre estructuras es el siguiente:

Definición 2.7.
- *Sean M, N L-estructuras. Una función $h : M \longrightarrow N$ es un **morfismo*** si se cumple lo siguiente:
  1. Para cada relación n-aria $R \in L$, si $R^M(a)$ con $a \in M^n$, entonces $R^N(h(a))$.
  2. Para cada función n-aria $f \in L$, y para cada $a \in M^n$ se tiene que $h\left(f^M(a)\right) = f^N(h(a))$.
  3. Para cada símbolo de constante $c \in L$, $h\left(c^M\right) = c^N$.
- Si h es un morfismo entre estructuras M y N, decimos que h es una **inclusión** cuando h sea inyectiva.
- Un morfismo h es un **isomorfismo** si es biyectivo.
- Un isomorfismo h es un **automorfismo** cuando $M = N$.

Ahora podemos definir subestructuras:

Definición 2.8. *Si M y N son L-estructuras, entonces N es una L-**subestructura*** de M cuando $N \subseteq M$, y además la inclusión (como conjuntos) de N en M sea una inclusión de estructuras. Se denotará por $N \subseteq_L M$.

Por ejemplo, $(\mathbb{Z}, +, 0) \subseteq_{L_{grupos}} (\mathbb{R}, +, 0)$.

Como ya habíamos dicho, nuestra segunda definición de estructuras nos permite hablar de $Def(M)$ de una manera más práctica:

Fijemos un lenguaje L, y agreguémosle un conjunto infinito de variables $x_1, x_2, \ldots$. Ahora queremos definir fórmulas en el lenguaje L, pero antes de definir las fórmulas en general hablaremos del conjunto más básico de fórmulas: los términos. Para definirlos procedemos inductivamente:

Definición 2.9. *El conjunto de L-**términos*** es el más pequeño que contiene lo siguiente:

1. Las variables x_i,
2. Todas las constantes $c_i \in L$,
3. Si f es una función n-aria en L, y $t_1, \ldots, t_n$ son términos, entonces $f(t_1, \ldots, t_n)$ también es un término.

Ejemplo 2.10. *Sea R un anillo, consideremos el lenguaje L_R antes definido. Un término es precisamente un polinomio en n-variables: $f_{r_1}(x_1^{n_1}) + f_{r_2}(x_2^{n_2}) + \ldots + f_{r_m}(x_m^{n_m})$ con $r_i \in R$, x_i variables y $n_i \in \mathbb{N}$. Este ejemplo es bastante inspirador pues en un lenguaje arbitrario los términos jugarán el papel de los "polinomios lógicos".*

Recordemos que un término es una serie de símbolos en un lenguaje L, sin embargo no es del todo claro cuál es la relación entre un término y una L-estructura M. La siguiente definición resuelve el problema:

Definición 2.11. *Sea M una L-estructura, a cada término t en L que involucra las variables $x_1, \ldots, x_n$ se le asocia inductivamente una función $s_{t^M} : M^n \longrightarrow M$ de la siguiente forma:*

- *Si $t = x_i$ es una variable, entonces $s_{t^M}(a) = a \; \forall a \in M^1$.*
- *Si $t = c_i$ es una constante, entonces $s_{t^M}(a) = c_i \; \forall a \in M^1$.*
- *Si $t = f(t_1, \ldots, t_n)$ donde f es una función y t_i es un término $\forall i$, entonces $s_{t^M}(a) = f\left(s_{t_1^M}(a), \ldots, s_{t_m^M}(a)\right), \forall a \in M$.*

Ahora definimos fórmulas más complejas:

Definición 2.12. *Una **fórmula atómica*** es una expresión de la forma $R(t_1, \ldots, t_n)$ donde R es una relación n-aria en L y los t_i's son términos. Ya que las fórmulas atómicas están formadas por términos y estos a su vez involucran variables, escribiremos $R(t_1, \ldots, t_n)(x_1, \ldots, x_n)$ para hacer explícitas a las variables.

Las fórmulas atómicas darán lugar a los subconjuntos atómicos de la definición 2.1.

Notemos que como la igualdad siempre es una relación considerada, si t, t' son términos, entonces $t = t'$ es una fórmula atómica.

En el caso de L_R para algún anillo R, las fórmulas atómicas son de la forma $p(\bar{x}) = q(\bar{y})$ con $p(\bar{x}), q(\bar{y})$ polinomios. Las fórmulas atómicas en un lenguaje arbitrario L serán nuestras «ecuaciones lógicas», la parte más importante de las ecuaciones son sus soluciones:

Definición 2.13. *Sea M una L-estructura. Si $\phi(x_1, \ldots, x_n)$ es una fórmula atómica en el lenguaje L, decimos que $a = (a_1, \ldots, a_n) \in M^n$ **satisface** a $\phi(x_1, \ldots, x_n)$* cuando $\phi(a_1, \ldots, a_n)$. Denotaremos lo anterior por $M \models \phi(a_1, \ldots, a_n)$.

Como una fórmula atómica se ve de la forma $R(t_1(x_1, \ldots, x_n), \ldots, (t_m(x_1, \ldots, x_n)))$ con R una relación m-aria y $t_i(x_1, \ldots, x_n)$ términos en n variables, $\phi(a_1, \ldots, a_n)$ será cierto cuando ocurra que $R^M\left(s_{t_1^M}(a_1, \ldots, a_n), \ldots, s_{t_m^M}(a_1, \ldots, a_n)\right)$.

Ejemplo 2.14. *Un ejemplo de lo anterior es lo siguiente: consideremos el lenguaje $L_{anillos}$, tomemos un campo de característica p (primo) $\mathbb{F}_p$. Entonces $\mathbb{F}_p$ es una $L_{anillos}$-estructura. En esa estructura tenemos lo siguiente:*

$$\mathbb{F}_p \models 1 + \ldots + 1 = 0,$$

cuando en la fórmula anterior el 1 sea sumado p veces.

Ahora sí redefinimos a los $B_{i's}$ de la definición 2.1.

Definición 2.15. *Consideremos $S \subseteq M^n$. Decimos que S es un **conjunto atómico*** cuando $S = \{(a_1, \ldots, a_n) : M \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}$ para alguna fórmula ϕ en $n + m$ variables y $b_i \in M$ para cada $i \in \{1, \ldots, m\}$. Notemos que los $b_{i's}$ no son elementos del lenguaje. Decimos entonces que S está definido con los parámetros $b_{i's}$.

Regresando al caso de L_R con R un anillo, como 0 está en el lenguaje podemos hablar de la ecuación que define a un conjunto algebraico[1]. En este caso, el hecho de considerar parámetros significa poder usar a los elementos de R no sólo como funciones sino como constantes. Continuando con la analogía: los conjuntos atómicos son las "variedades lógicas".

Ahora vamos a definir las fórmulas en general, las cuales darán lugar al conjunto $Def(M)$:

Definición 2.16. *Las **fórmulas*** están descritas así:

1. Todas las fórmulas atómicas son fórmulas.
2. Si $\phi(x_1, \ldots, x_n)$ y $\psi(x_1, \ldots, x_n)$ son dos fórmulas, entonces
   - $\phi \wedge \psi(x_1, \ldots, x_n)$ también es una fórmula.
   - $\phi \vee \psi(x_1, \ldots, x_n)$ es una fórmula.
   - $\neg\phi(x_1, \ldots, x_n)$ es una fórmula.
   - $\exists x_n \phi(x_1, \ldots, x_n)$ es una fórmula.
   - $\forall x_n \phi(x_1, \ldots, x_n)$ es una fórmula.

[1] Las soluciones de una ecuación $p(\bar{x}) = 0$ con $p(\bar{x})$ un polinomio con coeficientes en R.

Nuevamente $\phi(x_1, \ldots, x_n)$ significa que en ϕ ocurren las variables $x_1, \ldots, x_n$.

Anteriormente llamamos a las fórmulas atómicas «ecuaciones lógicas», pues en el caso de L_R coinciden con las ecuaciones algebraicas. Debido a que las fórmulas son bastante más generales que las fórmulas atómicas, podemos pensar en la teoría de modelos y sus fórmulas como una generalización de la geometría algebraica y sus polinomios.

Supongamos que M es una L-estructura. Si tenemos $A \subseteq M$, podemos agrandar el lenguaje L de la siguiente manera: $L(A) = L \cup \{c_a^M : a \in A\}$. Es inmediato que podamos considerar a M como una $L(A)$-estructura. Si tenemos $a_1, \ldots, a_n \in A$, $\phi(x_1, \ldots, x_m, a_1, \ldots, a_n)$ es una $L(A)$-fórmula.

Denotamos por $Form(L)$ al conjunto de L-fórmulas. Es inmediato que $Form(L) \subseteq Form(L(A))$.

La definición de satisfacibilidad para fórmulas en general es la siguiente:

Definición 2.17. *Sea M una estructura de un lenguaje L, definimos la* ***satisfacibilidad*** de una fórmula arbitraria de manera inductiva: si $\phi(x_1, \ldots, x_n)$ y $\psi(x_1, \ldots, x_n)$ son dos L fórmulas, y $a_1, \ldots, a_n \in M$, entonces:

- $M \models \phi \wedge \psi(a_1, \ldots, a_n)$ cuando ocurra que $M \models \phi(a_1, \ldots, a_n)$ y además $M \models \psi(a_1, \ldots, a_n)$.
- $M \models \phi \vee \psi(a_1, \ldots, a_n)$ cuando ocurra que $M \models \phi(a_1, \ldots, a_n)$ ó $M \models \psi(a_1, \ldots, a_n)$.
- $M \models \neg\phi(a_1, \ldots, a_n)$ cuando no sea cierto que $M \models \phi(a_1, \ldots, a_n)$.
- $M \models \exists x_n \phi(a_1, \ldots, a_{n-1}, x_n)$ cuando exista un $b \in M$ de tal forma que $M \models \phi(a_1, \ldots, a_n, b)$
- $M \models \forall x_n \phi(a_1, \ldots, a_{n-1}, x_n)$ cuando para cualquier $a \in M$ se tiene que $M \models \phi(a_1, \ldots, a_{n-1}, a)$

Al igual que las fórmulas atómicas definen subconjuntos atómicos, las fórmulas definen conjuntos definibles:

Definición 2.18.

- *Consideremos $S \subseteq M^n$. Decimos que este subconjunto es un subconjunto* ***definible sin parámetros*** cuando $S = \{(a_1, \ldots, a_n) : M \models \phi(a_1, \ldots, a_n)\}$ para alguna L-fórmula $\phi(x_1, \ldots, x_n)$.
- $S \subseteq M^n$ se dice **definible con parámetros** en A cuando $\phi(x_1, \ldots, x_n)$ sea una $L(A)$-fórmula.
- Diremos que una relación R en n variables es definible cuando su gráfica en M^n lo sea.

Estas son nuestras «variedades lógicas» en general.

Es muy importante tener en cuenta la diferencia entre ser definible con parámetros y sin parámetros, por ejemplo: consideremos el lenguaje $L_{\mathbb{R}}$ con $\mathbb{R}$ como un anillo. ¿$\{\pi\} \subseteq \mathbb{R}$ es definible en $L_{\mathbb{R}}$? Como π es trascendente, no es $L_{\mathbb{R}}$-definible, sin embargo sí es $L_{\mathbb{R}}(\{\pi\})$-definible.

La siguiente propiedad es muy útil pues nos da otra equivalencia a ser definible, su demostración se encuentra en [4].

Proposición 2.19. *Sea M una L-estructura, $D \subseteq M^n$ es $A \subseteq M$-definible si y sólo si $\sigma(D) = D$ $\forall \sigma Aut(M)$ tales que $\sigma_A = Id_A$.*

Nota. *Es cierto que ambas definiciones de $Def(M)$ coinciden, sin embargo para que esto sea cierto es necesario considerar un lenguaje bastante amplio para M. Algunos detalles se pueden encontrar en* [12].

Definición 2.20. *Decimos que una familia $(E_i)_{i\in I}$ de conjuntos definibles en M^n es **uniformemente definible*** cuando existe una fórmula $\phi(x,y)$ en el lenguaje L y $(b_i)_{i\in I}$ con $b_i \in M^m$ de tal forma que para cada i, $E_i = \{a \in M^n : M \models \phi(a, b_i)\}$.

Ejemplo 2.21. *En los campos algebraicamente cerrados, una familia algebraica de conjuntos afines es una familia uniformemente definible i.e. supongamos que $p(x,y) \in K[x,y]$ es un polinomio en dos variables y $\{a_i\}_{i\in I} \subset K$, entonces $\{X_i\}_{i\in I}$ es un conjunto uniformemente definible donde $X_i = \{a \in K : p(a, a_i) = 0\}$.*

Definición 2.22. *Cuando todas las variables en una fórmula estén cuantificadas, por ejemplo: $\forall x \exists y \phi(x,y)$, diremos que ϕ **no tiene variables libres***. A este tipo de fórmulas las llamaremos **oraciones**. Si $\phi(x_1, \ldots, x_n)$ es una oración, simplemente escribiremos ϕ.

Definición 2.23. *A un conjunto T de L-oraciones se le llama **teoría** .*

A continuación algunos ejemplos:

- Los axiomas de la teoría de campos algebraicamente cerrados son una teoría; la denotaremos por ACF por sus siglas en inglés.
- Consideremos una familia F de L-estructuras. La teoría asociada a F es el conjunto de oraciones que son ciertas en todas las estructuras en F. Los axiomas de la teoría de campos son la teoría asociada a la familia de todos los campos.

Definición 2.24. *Sea T una teoría de un lenguaje L, decimos que una L-estructura M es **modelo*** de T cuando $M \models \phi$ para todo $\phi \in T$. A este hecho lo denotaremos por $M \models T$.

Si K es un campo algebraicamente cerrado, $K \models ACF$.

Definición 2.25. *Si para cada L-oración σ, $\sigma \in T$ o $\neg\sigma \in T$ decimos que la teoría T es **completa***.

A continuación algunos ejemplos de teorías completas y no completas:

1. Sea M una L estructura. La teoría asociada a M y denotada $Teo(M)$ es el conjunto de todas las L-fórmulas de tal manera que M las satisfaga. Notemos que por el principio del tercero excluido, $Teo(M)$ siempre es una teoría completa.
2. Consideremos los axiomas de los campos algebraicamente cerrados; la teoría generada[2] por este conjunto de axiomas no es completa. En efecto, si K es un campo algebraicamente cerrado de característica $p \geq 0$ para $k \in K$, $n \in \mathbb{N}$ denotaremos por nk a la suma n veces de k en K. Consideremos la $L_{anillos}$-oración $\phi_p(x)$ que dice $\forall x, px = 0$. Esta oración expresa la característica del campo, y ni $\phi_p(x)$ ni $\neg\phi_p(x)$ son consecuencias lógicas[3] de la teoría de los campos algebraicamente cerrados. El teorema de completud de Gödel[4] nos da una demostración de ese hecho pues no es cierto que $\phi_p(x)$ o $\neg\phi_p(x)$ sea cierta para cada campo algebraicamente cerrado.
3. El primer teorema de incompletud de Gödel dice que la teoría generada por los axiomas de Peano no es completa (de hecho Gödel demostró que no existe una manera «razonable» de completar la teoría).

---

[2]El conjunto de «consecuencias lógicas» . Ver la siguiente nota al pie.

[3]Que exista una cantidad finita de pasos lógicos entre los axiomas de los campos algebraicamente cerrados y la conclusión. Para una definición más precisa ver [4].

[4]Teorema de Completud de Gödel. Si T es una teoría, entonces para cada oración ϕ: ϕ es una consecuencia lógica de T si y sólo si $T \models \phi$. $T \models \phi$ significa que $M \models \phi$ para todo M tal que $M \models T$

Definición 2.26. *Consideremos un conjunto Σ de oraciones en un lenguaje L. Decimos que Σ es **consistente*** cuando no exista una L-oración ϕ de tal forma que $\phi \in \Sigma$ y además $\neg\phi \in \Sigma$.

El primer teorema de completud de Gödel nos da una equivalencia de ser consistente:

Corolario 2.27. *Un conjunto Σ de L-oraciones es consistente si y sólo si existe una L-estructura M de tal forma que para toda oración $\sigma \in \Sigma$, $M \models \sigma$.*

Por ejemplo, los axiomas de los campos son un conjunto de fórmulas consistentes. Por otro lado, el siguiente conjunto no es consistente: $\{\neg\phi, \phi\}$.

Una de las propiedades más importantes de las teorías es la siguiente:

Definición 2.28. *Supongamos que T es una teoría en un lenguaje L con al menos un símbolo de constante. Decimos que T tiene **eliminación*** de cuantificadores si para toda L-fórmula $\phi(x_1, \ldots, x_n)$ con variables libres $x_1, \ldots, x_n$ (posiblemente $n = 0$), existe $\psi(x_1, \ldots, x_n)$, una fórmula sin cuantificadores de tal forma que

$$T \models \forall x_1, \forall x_2, \ldots, \forall x_{n-1}, \forall x_n \left(\phi(x_1, \ldots, x_n) \Leftrightarrow \psi\right)$$

No toda teoría tiene eliminación de cuantificadores:

Consideremos la estructura que tiene como lenguaje a $L_{\mathbb{R}}$ y como conjunto a $\mathbb{R}$. El orden en los reales se puede definir de la siguiente manera:

$$x < y \Leftrightarrow \exists z, z \neq 0 \wedge x + z^2 = y$$

Si hubiera eliminación de cuantificadores para $Teo(\mathbb{R})$, este conjunto sería las soluciones de una combinación booleana de polinomios con coeficientes en $\mathbb{R}$ (porque las fórmulas que no tienen cuantificadores son combinaciones booleanas de fórmulas atómicas, las cuales son polinomios). Sin embargo, no es posible ver al orden en los reales como una combinación booleana de polinomios.

Existe una equivalencia de tener eliminación de cuantificadores que es más fácil de utilizar:

Proposición 2.29. *Una teoría T tiene eliminación de cuantificadores si y sólo si:*

- *Si A, B son modelos de T y $C \subseteq A, B$, entonces $A \models \phi(a)$ si y sólo si $B \models \phi(a)$ $\forall a \in C$, $\forall \phi(x)$.*

La demostración de este hecho se encuentra en [3]. Lo anterior, junto con el siguiente lema, nos permitirá demostrar la eliminación de cuantificadores para los campos algebraicamente cerrados.

Lema 2.30. *Para demostrar la eliminación de cuantificadores de una teoría T es suficiente demostrar lo siguiente: para cada fórmula $\exists v \phi(v, \bar{w})$ con $\phi(v, \bar{w})$ libre de cuantificadores, existe una fórmula libre de cuantificadores $\psi(\bar{w})$ tal que $T \models \forall \bar{w} \left(\phi(v, \bar{w}) \Leftrightarrow \psi(\bar{w})\right)$.*

La eliminación de cuantificadores de los campos algebraicamente cerrados fue demostrada por Tarski. Es notable que fue enunciada en términos puramente algebro-geométricos.

Teorema 2.31. *Los campos algebraicamente cerrados tienen eliminación de cuantificadores.*

Demostración. Utilizaré la proposición y el lema anterior. Sean K y L campos algebraicamente cerrados y F un subcampo contenido en ambos. Supongamos que $\phi(v, w)$ es una fórmula sin cuantificadores, y $a \in F$. Queremos demostrar que $K \models \exists v \phi(v, a)$ si y sólo

si $L \models \phi(v,a)$, así que supongamos $b \in K$ de tal forma que $K \models \phi(b,a)$. Queremos demostrar que existe un $c \in L$ de tal forma que $L \models \phi(c,a)$.

Como $\phi(v,w)$ es una fórmula sin cuantificadores, existen polinomios $f_{i,j}, g_{i,j} \in F[x]$ (alguno de ellos no es constante pues si no podríamos escribir $\phi(w)$ en lugar de $\phi(v,w)$ de tal forma que $\phi(w,a)$ es equivalente a

$$\vee_{i=1}^{l}\left(\left(\wedge_{j=1}^{m} f_{i,j}(v)=0\right)\wedge\left(\wedge_{j=1}^{n} g_{i,j}(v)\neq 0\right)\right).$$

Eso quiere decir que $K \models \wedge_{j=1}^{m} f_{i,j}(b)=0 \wedge \wedge_{j=1}^{n} g_{i,j}(b)\neq 0$ para algún i.

Consideremos $\bar{F}$ una cerradura algebraica de F. Podemos ver a $\bar{F}$ como un subconjunto tanto de K como de L. Si ocurre que exista un $f_{i,j}$ que no es idénticamente cero para algún j, entonces $b \in \bar{F} \subseteq L$ y ya habremos terminado.

De otra forma supongamos que todos son idénticamente cero. Por otro lado, como estamos suponiendo que $K \models \wedge_{j=1}^{n} g_{i,j}(b) \neq 0$ y todos los $f_{i,j}$ son constantes, existe $g_{i,j}(X)$ no constante. Así que tiene un número finito de soluciones. Consideremos al conjunto $\{c_1, c_2, \ldots, c_s\} \subseteq L$, de todas las raíces de polinomios no constantes $g_{i,j}$. Como los campos algebraicamente cerrados son infinitos, tomemos $d \notin \{c_1, c_2, \ldots, c_s\}$. Entonces $L \models \phi(d,a)$, y así hemos terminado.

□

Corolario 2.32. *Todo conjunto definible en un conjunto algebraicamente cerrado es finito o cofinito.*

Demostración. Por la eliminación de cuantificadores, cualquier conjunto definible es una combinación booleana de conjuntos de la forma $\{a \in K : f(a)=0\}$, los cuales son cofinitos o finitos dependiendo si f es o no constante. □

Ahora resolveremos un problema que habíamos mencionado con anterioridad: comparar estructuras.

Ya dijimos cuándo dos estructuras son isomorfas, sin embargo esa definición es bastante restrictiva pues más adelante veremos un teorema (el teorema 2.38) que nos dice que dos estructuras distintas (como conjuntos) son isomorfas si y sólo sí son finitas Así que si hablamos de estructuras infinitas, la teoría de modelos se reduciría a la Teoría de Conjuntos. Como queremos hacer las cosas más interesantes haremos algo parecido a lo que se hace en topología, donde en lugar de estudiar aquellos espacios isomorfos se estudian aquellos espacios que sean homótopos (lo cual ya es suficientemente interesante). La siguiente definición se podría ver como la equivalencia homótopa para estructuras:

Definición 2.33. *Sean M y N dos L estructuras, decimos que M y N son* ***elementariamente equivalentes*** cuando para toda L-oracion σ, $M \models \sigma$ si y sólo si $N \models \sigma$. Otra forma de decir lo anterior es: $Teo(M) = Teo(N)$. Lo denotaremos $M \equiv N$.

Existe una definición más apropiada para comparar estructuras:

Definición 2.34.

- *Supongamos que $M \subseteq_L N$. Decimos que M es una* ***substructura elementaria*** de N (o **N es un extensión elementaria de M**) cuando para cada fórmula $\phi(x_1,\ldots,x_n) \in L$ y cada $(a_1,\ldots,a_n) \in M^n$, se tiene que

$$M \models \phi(a_1,\ldots,a_n) \Leftrightarrow N \models \phi(a_1,\ldots,a_n)$$

  Lo denotaremos por $M \prec N$.
- Una función $f : M \longrightarrow N$ con M, N, L estructuras es una **inclusión elementaria** entre M y N si para cada fórmula $\phi(x_1,\ldots,x_n) \in L$ y cada $(a_1,\ldots,a_n) \in M^n$, se tiene que

$$M \models \phi(a_1, \ldots, a_n) \Leftrightarrow N \models \phi(f(a_1), \ldots, f(a_n))$$

Algunas observaciones inmediatas:

- Como toda oración es en particular una fórmula, entonces tenemos que $M \prec N \Rightarrow M \equiv N$.
- De hecho, $(M \prec N) \Leftrightarrow (M \equiv N$ como $L(M)$-estructuras).
- No toda inclusión es elementaria, un ejemplo son los racionales considerados como campo dentro de los reales igualmente considerados como campo, pues en el lenguaje de los campos hay muchas más cosas ciertas sobre los reales que sobre los racionales.
- Todo isomorfismo entre estructuras es una inclusión elementaria.

Por otro lado, si tenemos que $M \prec N$ y $S \subseteq M$ definible, entonces S tiene una extensión natural S' a N dada por el conjunto de elementos en N que satisfacen la fórmula que define a S. Esto corresponde a considerar las soluciones de un polinomio en un campo más grande que aquél donde viven sus coeficientes.

Notemos que cuando intersectamos S' con M obtenemos a S. Así solucionamos un problema planteado anteriormente.

La definición de inclusión elementaria tiene relevancia en nuestra discusión sobre las teorías completas: una teoría T es completa si y sólo si para cualesquiera dos modelos $M, N \models T$, M y N son elementariamente equivalentes. Para una demostración de este hecho ver [4].

Ya antes habíamos visto que la teoría ACF no es completa, sin embargo, si agregamos la oración que describe a la característica del campo, entonces la teoría de los campos algebraicamente cerrados de característica p (denotado por ACF_p) sí es completa. Esto se puede encontrar en [12].

Esta observación de la teoría de modelos, tiene un corolario en geometría algebraica conocido como el Principio de Lefschetz de primer orden.

Corolario 2.35. *Un enunciado ϕ en el lenguaje de los anillos es cierto para $\mathbb{C}$ si y sólo si es cierto para todo campo que modele ACF_0.*

Demostración. Por lo dicho hace un par de párrafos, una teoría es completa si y sólo si cualesquiera dos modelos son elementariamente equivalentes. Así que si ACF_0 es completa implica que cualquier campo algebraicamente cerrado es elementariamente equivalente a $\mathbb{C}$.

□

El principio de Lefschetz es más general, pues involucra enunciados que no precisamente son de primer orden.

Ahora regresemos a propiedades generales de las extensiones elementarias:

Teorema 2.36. ***[El test de Tarski-Vaught.]***. Supongamos que $M \subseteq_L N$. Entonces $M \prec N$ si y sólo si para todo $(m_1, \ldots, m_n) \in M^n$, $N \models \exists x \phi(x, m_1, \ldots, m_n) \Rightarrow M \models \exists x \phi(x, m_1, \ldots, m_n)$.

En términos de conjuntos definibles esto quiere decir que $M \prec N$ si y sólo si para todos los conjuntos no vacíos $E \subseteq N$ definibles en M, entonces $E \cap M$ es no vacío.

Otro teorema fundamental en la teoría de modelos es el siguiente:

Teorema 2.37. ***[Teorema de Compacidad.]***

Si Σ es un conjunto de L fórmulas, entonces Σ es consistente si y sólo si todo subconjunto finito de Σ es consistente.

Se llama teorema de compacidad porque garantiza la compacidad de cierto espacio topológico, en la proposición 3.8 daremos los detalles.

En términos de conjuntos definibles, el teorema de compacidad dice lo siguiente: Si tenemos una familia $F = \{D_i\}_{i\in I}$ de conjuntos definibles en M^n que tiene la propiedad de la intersección finita[5], entonces en alguna extensión elementaria $M \prec N$, la familia F (en realidad es una familia F' pues consideramos a los definibles en N con fórmulas en M) tiene intersección no vacía.

Es muy importante mencionar que el teorema de compacidad es el que nos permitirá trabajar sobre extensiones suficientemente grandes de un modelo. Pensemos esto como campos donde nuestras ecuaciones ya tienen solución. El siguiente teorema es un corolario inmediato del teorema de compacidad, su demostración abre la puerta a la teoría de modelos como se le conoce actualmente.

Teorema 2.38. ***[Löwenheim-Skolem.]***

- Sea M una L-estructura infinita y $X \subseteq M$. Existe una estructura $M_0 \prec M$ de tal forma que $X \subseteq M_0$ y además $|M_0| = |X| + |L|$.
- Sea M una L estructura infinita. Para cada cardinal $\kappa > |M|$ existe una extensión elementaria $M \prec N$ con $|N| = \kappa$.

Por el teorema anterior, si tenemos una estructura infinita, es imposible que todos sus modelos sean isomorfos.

Podríamos decir que la teoría de modelos básica incluye todo lo anterior y pocas cosas más. Ahora mencionaré resultados un poco más modernos sobre la teoría de modelos. Enunciaré teoremas y definiciones que parecerán un poco aislados entre ellos, sin embargo, serán de suma importancia para continuar desarrollando la teoría.

Uno de los problemas teóricos más importantes de la teoría de modelos es el de la clasificación de estructuras de Shelah. La pregunta es: dada una teoría, ¿es posible clasificar a todos los modelos de esa teoría bajo algún invariante? Este problema está resuelto en gran parte. Para quienes estén interesados en conocer más sobre el problema de clasificación de Shelah vea [5].

Existen algunas teorías que son muy simples de estudiar, por ejemplo los espacios vectoriales sobre un campo fijo K. Debido a que dos espacios vectoriales con la misma cardinalidad de la base son isomorfos, entonces dada una cardinalidad fija, los modelos de la teoría de los espacios vectoriales son únicos salvo isomorfismo. Este tipo de teorías reciben un nombre especial:

Definición 2.39. *Decimos que una teoría T es κ-**categórica*** cuando todos los modelos de cardinalidad κ son isomorfos.

Por ejemplo, los espacios vectoriales son κ categóricos para todo κ.

El siguiente teorema tuvo una repercusión mayúscula en el desarrollo de la teoría de modelos. Fue demostrado por Morley.

Teorema 2.40. ***[Morley]*** Si una teoría T es κ-categórica para algún κ no numerable, entonces T es θ-categórica para todos los $\theta > \kappa$.

---

[5]La propiedad de la intersección finita: para cada subconjunto finito $J \subseteq I$, la intersección sobre J es no vacía

2.2. Campos diferenciales. Una de las cualidades sobresalientes en la demostración de Hrushovski es el uso de la teoría de los campos diferencialmente cerrados. Cabe mencionar que agregar una diferencial a los campos para atacar la conjetura se le debe a Buium en su articulo [43]. Hrushovski utilizó la diferencial para agrandar el lenguaje de los campos, y así prácticamente todos los objetos en el enunciado de Mordell-Lang son definibles.

En esta sección hablaremos de sus propiedades algebraicas. La mayor parte de las demostraciones se pueden encontrar en [26].

Definición 2.41. *Sea R un anillo conmutativo, decimos R es un* ***anillo es diferencial*** cuando exista $\delta : R \longrightarrow R$ de tal forma que

$$\delta(rs) = r\delta(s) + s\delta(r), \delta(r+s) = \delta(r) + \delta(s).$$

A δ le llamamos una diferencial.

La primera propiedad sobre estos anillos es la siguiente:

Lema 2.42. *Sea (R, δ) un anillo diferencial, entonces $\delta(x^n) = nx^{n-1}\delta(x)$*

Demostración. Por inducción sobre n: $\delta\left(x^1\right) = 1\delta(x)$. Ahora: $\delta\left(x^{n+1}\right) = \delta(xx^n) = x\delta(x^n) + x^n\delta(x) = nxx^{n-1}\delta(x) + x^n\delta(x) = nx^n\delta(x) + x^n\delta(x) = (n+1)x^n\delta(x)$. Justo como se quería. □

Lema 2.43. *Sea b una unidad (ie. $\exists a \in R$ tal que $a \cdot b = 1_R$) en R. Entonces $\delta(a/b) = \frac{b\delta(a) - a\delta(b)}{b^2}$*

Demostración. Notemos que $\delta(a) = \delta(ba/b) = b\delta(a/b) + (a/b)\delta(b)$. Entonces: $(1/b)\delta(a) - \left(a/b^2\right)\delta(b) = \frac{b\delta(a)-a\delta(b)}{b^2} = \delta(a/b)$, como se quería. □

Algunos ejemplos de estos anillos son los siguientes:

1. Cuando $\delta(r) = 0$ para cualquier r.
2. Sea O_U el anillo de funciones analíticas $f : U \longrightarrow \mathbb{C}$ con $U \subseteq \mathbb{C}$. Entonces la δ es la derivación usual.
3. Así como los polinomios de un anillo forman un anillo, los polinomios diferenciales forman un anillo diferencial: Sea R un anillo diferencial. Defino $R\{X\}$ como el anillo diferencial en una variable de R: Como conjunto, $R\{X\}$ es el anillo de polinomios en las siguientes variables: $X, X^{(1)}, X^{(2)}, \ldots$. A un polinomio en $R\{x\}$ lo denotaremos como $p\{x\}$. En este anillo, los siguientes elementos son distintos: $x^{(2)}$ y x^2, de hecho existe el siguiente elemento: $(x^{(2)})^2$.

   Para definir una diferencial en $R\{X\}$, extendemos a δ de manera lineal con $\delta\left(X^{(n)}\right) = X^{(n+1)}$. A $R\{X\}$ con δ le llamamos el anillo de polinomios diferenciales en una variable.

Definición 2.44. *Si R es un anillo diferencial con δ. Consideremos el conjunto $r \in R$ de tal forma que $\delta(r) = 0$. A este conjunto le llamamos el* ***anillo de constantes*** de R, es fácil probar que es un anillo. Se denota por R_C.

Notemos que si $c \in R_C$ entonces $\delta(cx) = c\delta(x)$.

En el caso de que $R = K$ sea un campo, entonces a K le llamamos un campo diferencial, también es claro que K_C es un campo.

La siguiente definición da lugar a una teoría de ideales diferenciales que extiende la de los ideales:

Definición 2.45. *Sea R un anillo diferencial. $I \subseteq R$ es un* ***ideal diferencial*** cuando siempre que $r \in I$, entonces $\delta(r) \in I$. A estos les llamaremos δ-ideales.

El concepto de δ-ideal primo es el mismo que en los ideales. A partir de ahora consideraremos el anillo $R\{X\}$ para un anillo diferencial R.

Definición 2.46. *Sea $f \in R\{X\}$. Se define el* ***orden de*** f (denotado por $ord(f) = n$) como el mayor entero n de tal forma que $a_n X^{(n)}$ sea un sumando en f, con $a_n \neq 0$ y a_n un polinomio en las variables $X, X^{(1)}, \ldots, X^{(n-1)}$.

Definición 2.47. *Si $f \in R\{X\}$ tiene orden n, definimos su* ***separante*** : $s(X)$ como la derivada parcial (la usual) respecto a la variable $X^{(n)}$.

Por ejemplo, si $f = \left(X^{(2)}\right)^2 + X^1$, entonces $s(X) = 2X^{(2)}$. No es difícil dar una fórmula explícita para obtener el separante.

Definición 2.48. *Si $f \in R\{X\}$, definimos a $I(f) = \left\{g(x) \in R\{X\} : \exists k, s(X)^k g(X) \in \langle f \rangle\right\}$* donde $\langle f \rangle$ es el ideal generado por f.

A partir de ahora ya no escribiré las demostraciones.

Proposición 2.49. *Si $f \in R\{X\}$, entonces $I(f)$ es un δ-ideal primo.*

De hecho se tiene más.

Proposición 2.50. *Siempre que $J \subseteq R\{x\}$ sea un δ-ideal primo, entonces $J = I(f)$ para algún único $f \in R\{x\}$. Al polinomio f le llamamos el polinomio minimal de J.*

Definición 2.51. *Si I es un δ-ideal, definimos su* ***rango diferencial*** $RD(I)$ como el orden de su polinomio mínimo. Cuando R es un campo, se puede pensar en RD como el grado de trascendencia.

Definición 2.52. *Definimos al δ-**ideal generado*** por un conjunto S como el menor ideal que contenga a S. Se denotará por $\{S\}$.

Desgraciadamente los anillos diferenciales no cumplen con la condición ascendente de cadena [6], y no se puede enunciar un teorema como el de la base de Hilbert[7]. Veamos un contraejemplo:

Defino $I_n = \left\{X^2, \left(X^{(1)}\right)^2, \left(X^{(2)}\right)^2, \ldots, \left(X^{(n)}\right)^2\right\}$. Notemos que $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$, sin embargo esta cadena no se estabiliza. Notemos que para esto no importó cómo fuera el anillo R. Sin embargo, hay forma de enunciar un equivalente al teorema de la base de Hilbert.

Definición 2.53. *Si I es un δ-ideal, definimos $\sqrt{I} = \{f \in R\{X\} : \exists n, f^n \in I\}$. Se dice que un ideal diferencial es* ***radical*** cuando $I = \sqrt{I}$

Teorema 2.54. ***[Teorema de la base de Ritt-Raudenbush.]*** Si R es un anillo diferencial, entonces todo ideal diferencial radical es finitamente generado.

Con el teorema anterior es posible hacer geometría algebraica de manera muy parecida a como se hace con campos algebraicamente cerrados.

---

[6] Si $A_1 \subseteq A_2 \subseteq \ldots$ es una cadena de ideales, entonces existe un $N \in \mathbb{N}$ de tal forma que si $n > N$ entonces $A_{n+1} = A_n$.

[7] Teorema de la base de Hilbert. Sea K un campo algebraicamente cerrado. Todo ideal en $K[X]$ es finitamente generado. Este teorema es muy importante en geometría algebraica pues recordemos si tenemos un conjunto de polinomios A, entonces el ideal generado por A ($\langle A \rangle$) y A definen el mismo conjunto algebraico. Así que este teorema nos permite trabajar con una cantidad finita de polinomios en lugar de cualquier conjunto.

Sin embargo, existe otra propiedad de los campos que se utiliza mucho en geometría algebraica: Dado un campo cualquiera es posible construir un campo que lo extienda y además sea algebraicamente cerrado, de tal forma que es el más pequeño que cumple con esas dos propiedades. No es en lo absoluto inmediato que podamos hacer algo parecido para los campos diferenciales (encontrar su cerradura diferencial). De hecho no hemos hablado nada sobre lo que podría significar ser diferencialmente cerrado. Para esta discusión y para demostrar que la cerradura diferencial existe haremos uso de la teoría de modelos.

2.3. La teoría de modelos en los campos diferenciales. De momento ni siquiera es claro cuál sería una definición apropiada de ser «diferencialmente cerrado», más adelante lo definiremos correctamente. De momento enunciaré algunas cosas importantes sobre el concepto de cerradura diferencial:

- Un campo diferencialmente cerrado, será en particular algebraicamente cerrado.
- ¡No existe un ejemplo concreto de un campo diferencialmente cerrado!
- Que todo campo tenga una cerradura algebraica necesita insalvablemente (hasta ahora) de la teoría de modelos.

Definición 2.55. *La teoría de campos diferencialmente cerrados de característica cero se abrevia DFC_0. El lenguaje de esta teoría es el mismo que el de los campos más un símbolo de función unaria δ que se interpreta de la manera obvia. Los axiomas de esta teoría son:*

1. *Los de los campos de característica cero.*
2. $\forall x, y\, \delta(xy) = x\delta(y) + y\delta(x), \delta(x+y) = \delta(x) + \delta(y)$
3. ***Cerradura diferencial*** Para cuales quiera dos polinomios $f, g \in K\{X\}$ tales que el orden de $g\{X\}$ es menor al orden de $f\{X\}$, existe un $a \in K$ de tal forma que $f\{a\} = 0$ y $g\{a\} \neq 0$. Notemos que como K es un campo diferencial con diferencial δ, evaluar $f\{X\} = a_0X + a_1X^{(1)} + \ldots a_nX^{(n)}$ en $a \in K$ es igual a $a_0a + a_1\delta(a) + \ldots a_n\delta^n(a)$.

Por convención, si $f\{X\} \in K\{X\}$ y además tiene orden 0, entonces denotaremos a $f\{X\}$ como $f(X)$.

Definición 2.56. *Sean K, L campos diferenciales con diferencial δ tales que $K \subseteq L$. Diremos que un elemento $a \in L$ es **algebraico*** cuando lo sea en el sentido usual ($\exists p(X) \in K[X] \setminus K$ tal que $p(a) = 0$ con p no constante). Mientras que diremos que es **δ-algebraico** cuando $p\{X\} \in K\{X\}$ y además $p\{a\} = 0$.

Proposición 2.57. *Todo campo K que sea modelo de DFC_0 es algebraicamente cerrado.*

Demostración. Sea $f(X)$ de órden cero, definimos $g(X) = 1$. Debido a que estos dos polinomios cumplen las hipótesis del último axioma de DFC_0, entonces existe un $a \in K$ que es solución para f. □

Lo que queremos es construir una cerradura diferencial para un campo diferencial k. Es decir, queremos una prueba de existencia y unicidad de una extensión $k \subseteq K$. La existencia consiste en construir al campo K de tal forma que sea diferencialmente cerrado (esto no necesita de la teoría de modelos) y además sea «única» (aquí es donde se utilizará teoría de modelos). La demostración de existencia la damos a continuación mientras que la de unicidad debe esperar aún más.

Proposición 2.58. *Sea un campo diferencial k con diferencial δ. Existe una extensión $k \subseteq K$ con K diferencialmente cerrado.*

Demostración. La demostración de esto es tan parecida a la que se usa para las extensiones algebraicamente cerradas de los campos que sólo daremos la primera parte de la demostración, pues sólo al principio difieren. Demostraré que dado un polinomio diferencial $f\{X\} \in k\{X\}$ con orden n, siempre existe una extensión L donde hay un $a \in L$ de tal forma que $f\{a\} = 0$. Consideremos un $g\{X\}$ de orden menor a n. Sea $f_1$un factor irreducible de f que también tenga orden n. Defino a $I = I(f_1)$ como anteriormente. Ya que el orden de g es menor, $g \notin I$. Sea F el campo de fracciones de $K\{X\}/I$. Notemos que la regla del cociente para una diferencial δ que probamos anteriormente nos permite extender a F nuestra diferencial. Sea a la imagen de X en el campo F. Como $f \in I$, entonces $f(a) = 0$ y como $g \notin I$, $g\{a\} \neq 0$. Ahora es cuestión de repetir la demostración para campos algebraicamente cerrados usando el lema de Zorn. □

La primera definición de DFC_0 que se dio históricamente es distinta a la que dimos anteriormente. Fue Blum quien demostró la equivalencia (ver [26]).

Definición 2.59. *Consideremos una familia de estructuras K de un lenguaje L. Decimos que $A \in K$ es* ***existencialmente cerrada*** cuando: siempre que tengamos $A \prec B$ con $B \in K$, entonces para cualquier $L(A)$-fórmula ($L(A)$ denota el lenguaje L unión todos los símbolos de constantes que denotan elementos en A) sin cuantificadores $\phi(w)$, se tiene lo siguiente: si $B \models \exists w \phi(w)$ entonces $A \models \exists w \phi(w)$.

Nota. *La primera definición que se dio de DCF_0 es: aquellos modelos de los campos diferenciales que son existencialmente cerrados.*

Así como los campos tienen eliminación de cuantificadores, los campos diferencialmente cerrados también la tienen:

Teorema 2.60. *DCF_0 tiene eliminación de cuantificadores.*

3. TIPOS, SATURACIÓN Y ESTABILIDAD

Los tres conceptos que estudiaremos en esta sección son fundamentales para desarrollar una teoría más rica. Gracias al primero podemos hablar de una generalización de conjuntos definibles (tipos). Los dos conceptos siguientes justifican la importancia de los tipos pues de acuerdo a sus propiedades podemos obtener información de la estructura.

3.1. Tipos. Recordemos que dada una estructura (M, L), no todo subconjunto $X \subseteq M$ será definible en el lenguaje L, sin embargo será útil poder «aproximar» a los conjuntos no definibles por medio de conjuntos definibles. La definición de tipo nos ayuda con eso:

Definición 3.1. *Sea T una teoría, $M \models T$ una estructura y $A \subseteq M$. Consideremos $\Sigma(x_1, \dots x_n)$ un conjunto de $L(A)$-fórmulas con $x_1, \dots, x_n$ variables libres. Decimos que $\Sigma(x_1, \dots x_n)$ es **finitamente satisfacible*** cuando para cualquier $\sigma(x_1, \dots x_n) \subseteq \Sigma(x_1, \dots x_n)$ finito existe $a \in M^n$ tal que $M \models \phi(a), \forall \phi \in \sigma$. Ya antes habíamos notado que esto es equivalente a que las fórmulas sean consistentes.

Definición 3.2. *Un n-**tipo*** sobre A es un conjunto de $L(A)$-fórmulas $\Sigma(x_1, \dots x_n)$ que es finitamente satisfacible. Decimos que un $n - tipo$ es **completo** cuando para toda $L(A)$-fórmula $\phi(\bar{x})$, $\phi(\bar{x}) \in \Sigma(x_1, \dots x_n)$ ó $\neg\phi(\bar{x}) \in \Sigma(x_1, \dots x_n)$.

Ejemplo 3.3. *Existe una forma inmediata para obtener tipos completos: sea $\bar{c} \in M^n$, $A \subseteq M$. Consideremos el tipo $tp(\bar{c}/A)$ que consiste de todas las $L(A)$-fórmulas $\phi(\bar{x})$ tales que $M \models \phi(\bar{c})$. Por el principio del tercero excluido, éste es un tipo completo. Notemos que la última definición corresponde a considerar el conjunto de subconjuntos definibles de M con parámetros en A que contienen a $\bar{c}$.*

El siguiente ejemplo justifica por qué decimos que los tipos aproximan conjuntos no definibles.

Ejemplo 3.4. *Sea K/L una extensión de campos, si $\alpha \in K$ es un elemento trascendente sobre L [8], entonces α no es definible en el lenguaje de los anillos.*

Sin embargo, en algunos casos es posible aproximar elementos trascendentes (no definibles) utilizando elementos algebráicos (definibles). Supongamos $K = \mathbb{R}, L = \mathbb{Q}$. $e \in \mathbb{R}$ no es $\emptyset$-definible en el lenguaje de los anillos. Sin embargo consideremos el siguiente tipo:

$$p(x) = \left\{ x \geq 1 + 0, x \geq 1 + \frac{1}{1!}!, x \geq \left(1 + \frac{1}{2!}\right)^2, x \geq \left(1 + \frac{1}{3!}\right)^3, \dots \right\}$$

El conjunto de elementos en $\mathbb{R}$ que satisfacen cada una de las fórmulas es justamente $[e, \infty)$. Si aproximamos a e por otra sucecsión, pero esta vez por el lado izquierdo, al intersectar los tipos obtenemos a e.

Definición 3.5. ▪ *Si $\bar{c}$ satisface todas las fórmulas de un tipo $\Sigma(\bar{x})$ diremos que $\bar{c}$ **realiza** a $\Sigma(\bar{x})$.*

La siguiente propiedad será de mucha ayuda:

Proposición 3.6. *Sean $\bar{c}, \bar{d} \in M^n$. Entonces $tp(\bar{c}/A) = tp\left(\bar{d}/A\right)$ si y sólo si existe un automorfismo f de M que fije a A punto a punto y además $f(\bar{c}) = \bar{d}$.*

Su demostración se puede encontrar en [4].

Por la proposición anterior podemos pensar en los tipos como «puntos» (salvo la existencia de algún automorfismo), de hecho esa idea geométrica nos ayudará:

[8] No existe un polinomio no nulo con coeficientee en L del cual α es raíz.

Definición 3.7. ***[Espacios de Stone.]*** Sean $n \in \mathbb{N}$ y $A \subseteq M$, definimos al conjunto $S_n(A)$ como el conjunto de todos los n-tipos completos sobre A. A este espacio lo llamamos un espacio de Stone.

Es posible darle una topología a $S_n(A)$: sea ϕ una $L(A)$-fórmula con n variables libres. Defino a $[\phi] = \{p \in S_n(A) : \phi \in p\}$. Notemos que si $\phi \vee \psi \in p$, entonces $\phi \in p$ o $\psi \in p$. Así que $[\phi \vee \psi] = [\phi] \cup [\psi]$. De la misma forma se tiene que $[\phi \wedge \psi] = [\phi] \cap [\psi]$.

Definimos una topología para $S_n(A)$ como la generada por los $[\phi]$ considerados como abiertos para cada ϕ $L(A)$-fórmula con n variables libres. Notemos que para cada tipo p, $\phi \in p$ o $\neg\phi \in p$, entonces $[\phi] = S_n(A) \setminus [\neg\phi]$. Así que todo abierto también es cerrado. Enunciamos algunas propiedades topológicas que son importantes, las demostraciones se encuentran en [4].

Proposición 3.8.
1. *$S_n(A)$ es un espacio topológico compacto para toda n (¡teorema de compacidad!).*
2. *$S_n(A)$ es totalmente disconexo, es decir: si $p, q \in S_n(A)$ con $p \neq q$, entonces existe un conjunto X que es abierto y cerrado a la vez en la topología, de tal forma que $p \in X$ y $q \notin X$.*

Como los tipos son finitamente satisfacibles, el teorema de compacidad también nos permite asegurar la existencia de una estructura que extienda a la inicial donde los tipos se realizan, así que buscar estructuras donde un tipo sea cierto no será ningún problema.

Por otro lado, no es claro que existan modelos donde no haya elementos que satisfagan un tipo.

Definición 3.9. *Cuando un tipo p no es realizado en M decimos que M* ***omite*** a p.

La existencia de modelos que omitan un tipo es equivalente a una condición topológica para los espacios de Stone:

Teorema 3.10. ***[Teorema de Omisión de Tipos.]*** Sea L un lenguaje numerable y T una teoría completa de L. Si para cada $n \in \mathbb{N}$ existe X_n un conjunto magro de $S_n(\emptyset)$, entonces existe un modelo M que es numerable donde se omiten todos los tipos sobre $\cup X_n$.

Para tener intuición sobre los tipos vamos a dar más ejemplos, el tercero es de suma importancia.

Ejemplo 3.11. *Consideremos a la estructura $(\mathbb{Z}, >)$. El conjunto de fórmulas $\{x > 1, x > 2, \ldots\}$ es un tipo porque para cualquier $n \in \mathbb{N}$, existe un $m \in \mathbb{Z}$ de tal forma que $m > n$, así que es finitamente satisfacible. El teorema de compacidad nos garantiza la existencia de una estructura $(\mathbb{Z}^*, >)$ con un elemento mayor que todos los enteros. Este es el llamado modelo no estándar de $\mathbb{Z}$.*

Ejemplo 3.12. *Supongamos que K es un campo algebraicamente cerrado. Existe una biyección entre $S_n(k)$ donde $k \subseteq K$ es un campo y $Spec(k[x_1, \ldots, x_n])$, en el siguiente ejemplo daremos una idea de cómo se hace la asginación.* [9]*. De hecho se puede probar que el mapeo que manda un tipo en un ideal primo es continuo con la topología que describimos para $S_n(k)$ y la de Zariski para $Spec(k[x_1, \ldots, x_n])$. Una demostración de esto se encuentra en*[4]*. Usando este hecho se puede demostrar que $Spec(k[x_1, \ldots, x_n])$ es compacto.*

[9] Si R es un anillo, definimos a $Spec(A)$ como el conjunto de ideales primos.

Ejemplo 3.13. *Ahora consideremos K un campo diferencialmente cerrado, $k \subseteq K$ un campo diferencial. La afirmación es que existe una biyección entre $S_1(k)$ y los δ-ideales primos de $k\{X\}$. Sea $p \in S_1(k)$. Definimos $I_p = \{f \in k\{X\} : "`f(\bar{a}) = 0"' \in p\}$, usando el hecho de que un campo es un dominio entero, se tiene que el ideal I_p es un δ-ideal primo. El siguiente lema se puede encontrar en* [4]

Lema 3.14. *La asignación $p \longmapsto I_p$ que describimos anteriormente es una biyección continua entre $S_1(k)$ y el espacio de los δ-ideales primos en $k\{X\}$.*

La siguiente definición coincidirá con una noción de la teoría de modelos llamada el Rango de Morley.

Definición 3.15. *Sea $p \in S_1(k)$, definimos al* ***rango diferencial*** de p como $RD(p) = RD(I_p)$

3.2. Saturación. Ahora hablaremos de una generalización a ser trascendente en campos, la analogía vendrá si pensamos en las fórmulas como polinomios y en los elementos que las satisfacen como raíces de polinomios.

Definición 3.16. *Sea κ un cardinal infinito. Una L-estructura M es* ***κ-saturada*** cuando para todo $A \subseteq M$ con $|A| < \kappa$ y para todo tipo $p \in S_n(A)$, existe $\bar{c} \in M^n$ tal que $M \models \phi(\bar{c}), \forall \phi(\bar{x}) \in p$. Diremos que M es saturado cuando sea $|M|$-saturado.

Por ejemplo, $\mathbb{Q}$ (como campo ordenado) no es $\aleph_1$-saturado debido a que $e \notin \mathbb{Q}$ y existe un tipo que es finitamente satisfacible (ver el ejemplo 3.4) con una cantidad numerable de parámetros. Este ejemplo no contradice el hecho de que $\mathbb{Q}$ sea $\aleph_0$-saturado pues la cantidad de parámetros para definir a e es numerable.

Usando el Teorema de Compacidad iteradamente lo siguiente es cierto:

- Sea κ un cardinal infinito y M una L-estructura, entonces existe una L-estructura N que es κ-saturada y además: $M \prec N$.

La siguiente proposición justifica nuestra presentación de saturación como una generalización de ser trascendente:

Proposición 3.17. *Si K es un campo algebraicamente cerrado, entonces K es $\aleph_0$-saturado si y sólo si el grado de trascendencia de K es infinito sobre su campo primo.*

No es inmediato que para todo cardinal κ exista una estructura N de cardinalidad κ que además sea κ-saturada i.e. una estructura saturada. El siguiente teorema ilustra un poco las dificultades a las que nos enfrentamos cuando queremos considerar estructuras saturadas:

Teorema 3.18. *Sea T una teoría. Supongamos que la Hipótesis Generalizada del Continuo es cierta. Entonces existe M con $M \models T$ tal que $|M| = \kappa^+$ y además es saturado para todo cardinal κ.*

Tener estructuras que cumplan lo anterior será bastante útil pues ellas cumplen con la siguiente propiedad:

Definición 3.19. *Decimos que una L-estructura M de cardinalidad κ es* ***homogénea*** si para cada dos conjuntos $A, B \subseteq M$ con cardinalidad estrictamente menor a κ y para cualquier inclusión elementaria $f : A \longrightarrow B$, es posible extender f a un automorfismo de M. Para ver con detalle por qué las estructuras saturadas cumplen con ser homogéneas recomiendo [12].

Además de la homogeneidad, los modelos saturados son muy útiles porque están determinados (salvo isomorfismo) por su cardinalidad:

Teorema 3.20. *Supongamos que M y N son modelos saturados de una teoría T. Entonces $M \cong N$.*

Ya que la hipótesis generalizada del contínuo no es un hecho trivial en matemáticas, en general existen obstrucciones para que una teoría tenga modelos saturados para todos los cardinales κ, sin embargo existen dos maneras de salvar este asunto; de ambas se hablará con detalle más adelante.

1. La primera tiene que ver con el concepto de estabilidad, pues en una teoría ω-estable (más adelante precisaremos lo que eso significa), sí podemos encontrar estructuras κ saturadas para cardinales arbitrarios. Resulta que las teorías que se usan en la demostración de Mordell-Lang son todas ω-estables.
2. Lo siguiente es considerar un modelo $\mathbb{M}$ al que se le llamará el modelo monstruo. Este modelo es el análogo al campo de definición en la geometría algebraica y es, a grandes rasgos, un modelo suficientemente grande para una discusión matemática (una demostración por ejemplo). En una teoría débil de conjuntos este modelo no será un conjunto, de hecho (como ya vimos anteriormente) la existencia de modelos κ-saturados para cardinales muy grandes necesita hipótesis en teoría de conjuntos muy fuertes, la hipótesis del continuo por ejemplo. El modelo monstruo está caracterizado por lo siguiente (para una discusión más precisa del modelo monstruo, recomendamos [13]):
   - Es saturado para un cardinal muy grande κ
   - Todo modelo del que se hable en la discusión matemática es incluible elementariamente en $\mathbb{M}$.
   - Es homogéneo.

Al modelo monstruo lo utilizaremos muy poco en lo que resta del trabajo, sin embargo no es posible aislarnos por completo de él.

Por último, motivamos la definición de estabilidad por medio del siguiente teorema que involucra tipos y saturación.

Teorema 3.21. *Sea T una teoría completa sobre un lenguaje numerable L. T tiene un modelo numerable y saturado si y sólo si $S_n(\emptyset)$ es numerable $\forall n \in \mathbb{N}$.*

3.3. Estabilidad. Otra definición fundamental para la teoría de modelos es la de estabilidad. Es importante mencionar que la noción de estabilidad le permitió a Shelah dar una clasificación de los modelos en una teoría arbitraría.

Definición 3.22. *Sea T una teoría completa en un lenguaje numerable L, κ un cardinal infinito. Decimos que T es κ-**estable*** cuando para todo modelo $M \models T$ y $A \subseteq M$ con $|A| = \kappa$ entonces $|S_n(A)| = \kappa$. Se dice que un modelo M es κ-estable cuando $Teo(M)$ sea κ-estable.

Por razones un poco extrañas diremos ω-estable en lugar de $\aleph_0$-estable pues así se hace en la literatura.

El primer teorema importante sobre estabilidad es el siguiente, su demostración se encuentra en [4]:

Teorema 3.23. *Si T es una teoría completa en un lenguaje numerable y además es ω-estable, entonces T es κ-estable para todos los cardinales infinitos.*

A continuación daré ejemplos de teorías que no son ω-estables y de otras que sí lo son:

Ejemplo 3.24. *Consideremos $(\mathbb{Q}, <)$, este modelo no es ω-estable pues cada sucesión de Cauchy (pensada como un tipo) utiliza una cantidad numerable de parámetros sin embargo*

es posible definir a todos los irracionales con sucesiónes de Cauchy, los cuales no son numerables.

Teorema 3.25. DCF_0 *es* ω*-estable.*

Demostración. Supongamos que K es un campo diferencialmente cerrado de característica 0. Sea $A \subseteq K$. Consideremos a k, como el campo diferencial generado por A. Queremos demostrar que $|S_n(k)| = |k|$ para todo n. Haré el caso cuando $n = 1$, para hacer la demostración en general es necesario usar inducción y el teorema 2.54. Veamos el caso $n = 1$: como hay una biyección entre $S_1(k)$ y los δ-ideales primos de $k\{X\}$, sería suficiente con demostrar que la cantidad de estos últimos es igual a $|k|$. Por el lema 3.14 cada ideal primo en $k\{X\}$, corresponde unívocamente a un $I(f)$ con $f \in k\{X\}$. Así que $|S_1(k)| = |k\{X\}| = |k|$. De esta forma terminamos. □

Con este hecho demostrado vamos a probar que en los campos diferencialmente cerrados existe la cerradura diferencial.

Definición 3.26. *Decimos que un modelo M de una teoría T es* ***primo*** sobre $A \subseteq M$ cuando para todo modelo $N \models T$ con $A \subseteq N$ existe una inclusión elementaria de M en N.

Recordemos que lo que nos hacía falta para tener una cerradura diferencial de un campo diferencial k es justo la idea de modelo primo sobre k. El siguiente teorema se debe a Morley y Shelah, su demostración se encuentra en [26].

Teorema 3.27. *Si una teoría T es ω-estable entonces para cualquier modelo M de T existe $M_0 \prec M$ donde M_0 es primo.*

Corolario 3.28. *Existe la cerradura diferencial en* DFC_0.

4. INTERPRETABILIDAD E IMAGINARIOS

En esta sección hablaremos de una teoría llamada T^{eq} que extiende a cualquier teoría T (i.e. $T \subseteq T^{eq}$). T^{eq} fue introducida por Shelah. Es importante por lo siguiente: si $M \models T^{eq}$ y E es una relación de equivalencia sobre M y definible, es posible trabajar con las clases laterales del cociente M/E como «elementos» y no como subconjuntos, lo cuál nos permite continuar en un lenguaje de primer órden. Esto no es posible cuando $M \models T$ en general. Resulta que hay algunas teorías para las cuáles «$T = T^{eq}$», por ejemplo $DCF = DCF^{eq}$. La siguiente sección da definiciones precisas de lo que significa $T = T^{eq}$ así como algunos ejemplos. Respecto a su importancia en la demostración de Mordell-Lang, aunque de ninguna manera quiero trivializarla, advierto al lector que en una primera lectura es posible saltarse la definición formal de la eliminación de imaginarios siempre y cuando tengamos en cuenta que «$DCF = DCF^{eq}$». Para que sea cierta la demostración de Mordell-Lang este hecho es indispensable.

También hablaremos de las llamadas «bases canónicas», las cuales nos permiten hablar en términos más sencillos de los subconjuntos definibles en una estructura.

Así como podemos definir conjuntos, funciones o relaciones dentro de una estructura, es posible definir estructuras dentro de otra estructura.

Definición 4.1. *Sea A una estructura en un lenguaje L. Decimos que una estructura A' en el lenguaje L' es **definible en** A* cuando exista:

1. $S \subseteq A^n$ $\emptyset$-definible para algún $n \in \mathbb{N}$.
2. Para cada símbolo de constante $c' \in L'$, un subconjunto $\emptyset$-definible $c^A \subseteq S$.
3. Para cada símbolo de m-relación $R' \in L'$, un subconjunto $\emptyset$-definible $R^A \subseteq S^m$.

De tal forma que S y A' sean isomorfos como L' estructuras.

Para explicar lo anterior, veamos un par de ejemplos:

Ejemplo 4.2. *Consideremos un modelo K de la teoría de campos (el lenguaje es $(K, +, *, 0, 1)$). Afirmo que el grupo $GL_2(K)$ (en el lenguaje $(G, \circ, e)$) es definible en K. Sea $X = \left\{(a, b, c, d) \in K^4 : ad - bc \neq 0\right\}$, el cual es claramente definible en el lenguaje de los campos. Definimos $f : X^2 \longrightarrow X$ por*

$$f\left((a_1, b_1, c_1, d_1), (a_2, b_2, c_2, d_2)\right) = (a_1a_2 + b_1c_2, a_1b_2 + b_1c_2, c_1a_2 + d_1c_2, c_1b_2 + d_1d_2)$$

, la cual también es claramente definible en el lenguaje de los campos. Si vemos a los elementos de X como matrices de 2×2 no invertibles y a f como la multiplicación de matrices, también es claro que ello es isomorfo al grupo $GL_2(K)$ con la composición como su operación.

Ejemplo 4.3. *Sea K un campo, veremos que K es definible en un subgrupo G de $GL_2(K)$.*

Consideremos al conjunto G de matrices con entradas en un campo K de la siguiente forma:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

Donde $a, b \in K$ y $a \neq 0$. Es inmediato que este conjunto forma un subgrupo de $GL_2(K)$. Consideremos este subgrupo como una estructura de la teoría de grupos. Sean

$$\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}$$

Con $\tau \neq 0$. Sea

$$A = \{g \in G : g\alpha = \alpha g\} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in K \right\}$$

y

$$B = \{g \in G : g\beta = \beta g\} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x \neq 0 \right\}$$

Por su puesto que A y B son definibles. Notemos que podemos definir una acción de B en A:

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y/x \\ 0 & 1 \end{pmatrix}$$

Ahora consideremos la función $i : A\backslash\{1\} \longrightarrow B$ de la siguiente forma: $i \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$. Notemos que, en principio, esta función no tiene porque ser definible. Sin embargo: si $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in A$, entonces existe (¡de hecho es única! y por eso será posible definir a i) $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in B$ de tal forma que:

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \alpha$$

y como tanto la conjugación como α son definibles en G, entonces i también lo será. Ahora definamos una operación $*$ en A de la siguiente manera: $a * b = i(b)^{-1} a i(b)$ cuando $b \neq 1$ y $a * b = 1$ cuando $b = 1$. La afirmación es que $(K, +, \cdot, 0, 1)$ es isomorfo como estructura a $(A, \cdot, *, 1, \alpha)$. No haré los detalles que demuestran esa afirmación, pero daré una idea de por qué eso es cierto. Como A es un subgrupo de G, entonces para que la operación $\cdot$ junto con 1 se comporte como $+, 0$ del campo sólo faltaría que A fuera conmutativo, pero eso está en la definición de A. La parte más interesante es que $*, \alpha$ se comporten como $\cdot, 1$ en el campo: Por la definición: $a * 1 = 1$. Mientras que

$$1 * b = i(b)^{-1} a i(b) = \begin{pmatrix} 1/y & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

Por otro lado, afirmo que para cualquier $a \in A\backslash\{1\}$, existe $b \in A$ de tal forma que $a * b = \alpha$. Sea $a = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ Buscamos una $b = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ tal que

$$\begin{pmatrix} 1/y & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y/x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Así que si considero a $y = 1/x$ entonces tengo lo que quería. Eso existe porque si $a \neq 1$, entonces $x \neq 1$. Por último, veremos que $\alpha * b = b$ para todo $b \in A$.

$$i(\alpha)^{-1} b i(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

La conmutatividad y asociatividad de $*$, así como sus distributividades con $+$ las omito por razones de espacio.

Ahora hablaremos de una generalización del concepto «ser definible» dentro de una estructura.

Definición 4.4. *Sea A una estructura en un lenguaje L. Decimos que una estructura A' en un lenguaje L' es* ***interpretable*** en A cuando existan:

1. $S \subseteq A^n$ $\emptyset$-definible y una relación de equivalencia E de A^n que sea $\emptyset$-definible.
2. Para cada símbolo de constante $c' \in L'$,un subconjunto $\emptyset$-definible (en L) $c^A \subseteq S$ de tal forma que si aEb con $a \in c^A$, entonces $b \in c^A$.
3. Para cada símbolo de m-relación $R' \in L'$, existe un subconjunto -definible (en L) $R^A \subseteq S^m$ de tal forma que si aEb con $a \in \left(R^A\right)^m$, entonces $b \in \left(R^A\right)^m$.

Se pide que S/E y A' sean isomorfos como L' estructuras.

A continuación un ejemplo:

Ejemplo 4.5. *Sea K un campo. Consideremos $X = \left\{(a_0, \dots a_n) \in K^{n+1} : \exists i, a_i \neq 0\right\}$. Definimos una relación de equivalencia para $a, b \in X$: aRb si existe $\lambda \in K^*$ de tal forma que $a = \lambda b$. Entonces $X/R = \mathbb{P}^n(K)$. Por otro lado, sea f un polinomio homogéneo sobre K en n variables, defino a $V = \{x \in X : f(x) = 0\}$. Como el polinomio es homogéneo, entonces V es R-invariante, así que podemos interpretar a $(\mathbb{P}^n(K), V/R)$ en K.*

Con la definición de interpretabilidad podemos definir dos tipos de elementos de una estructura A:

1. $a \in A^n$, a los que llamaremos **elementos reales.**
2. $\bar{a} \in S/E$ donde S es un conjunto $\emptyset$-definible en A^n para algún n y E es una clase de equivalencia $\emptyset$-definible. A estos elementos los llamaremos **imaginarios.**

Si A es una L-estructura vamos a construir un nuevo lenguaje y una nueva estructura de tal forma que contengan a A y a L. Pero lo más importante es que los elementos imaginarios de esta nueva estructura van a ser todos reales en algún sentido que explicaremos más adelante.

Definición 4.6. *Dado un lenguaje L, definimos L^{eq}* como el lenguaje que tiene a todos los símbolos de L más algunos nuevos. Para cada relación de equivalencia $\emptyset$-definible E de A^n:

1. Un símbolo de relación 1-aria A_E.
2. Un símbolo de función n-aria π_E.

Definición 4.7. A^{eq} será la estructura para L^{eq} de la siguiente forma:

1. El universo de A^{eq} es la unión disjunta de A^n/E con E una relación de equivalencia $\emptyset$-definible. Para cada relación de equivalencia E el símbolo A_E se interpretan como el conjunto A^n/E.
2. Los símbolos π_E se interpretan como las proyecciones canónicas de A^n a A^n/E
3. Notemos que como $=$ es una relación de equivalencia en A^n $\forall n$, A^n está contenido en la estructura A^{eq}. Los símbolos del lenguaje L se interpretan de la manera usual en esos A^n.

La ventaja inmediata de A^{eq} es que si A' es interpretable en A, entonces A' es definible en A^{eq}. Por otro lado, si A' es definible en A, entonces también lo es en A^{eq}, esto último es consecuencia directa de que $=$ es una relación de equivalencia. Además, si $X \subseteq A^n$ es definible en A^{eq}, entonces también lo era definible en A.

Enuncio el siguiente lema sin demostración, pues además de ser sencillo se puede encontrar en[5]:

Lema 4.8. *Si A y B son estructuras de un lenguaje L de tal forma que $A \equiv B$, entonces $A^{eq} \equiv B^{eq}$.*

El lema anterior nos permite definir $T^{eq} = Teo(A^{eq})$ cuando $T = Teo(A)$ sin temor a que esta definición dependa del modelo que estemos tomando. La siguiente propiedad es de suma importancia, pues en aquellas teorías en las que se cumple, las construcciones anteriores NO complican las cosas.

Definición 4.9. *Una estructura A de un lenguaje L tiene* ***eliminación de imaginarios*** cuando para cada relación de equivalencia E de A^n que sea $\emptyset$-definible y $a \in A^n$, entonces existe una fórmula $\phi(u, v)$ de L y una única $b \in A^n$ de tal forma que si $\bar{a}$ representa la clase de equivalencia de a en A^n/E,

$$\bar{a} = \phi(A^n, b)$$

El siguiente teorema nos dice por qué cuando una estructura A tiene eliminación de imaginarios, entonces no es necesario construir A^{eq}.

Teorema 4.10. *Sea A una estructura para un lenguaje L. Las siguientes propiedades son equivalentes:*

1. *A elimina imaginarios.*
2. *Para cada n y cada relación de equivalencia E sobre A^n que sea $\emptyset$-definible en A, existe una función $F_E : A^n \longrightarrow A^m$ que es $\emptyset$-definible de tal forma que $\forall a, a' \in A^n$:*

$$aEa' \Leftrightarrow F_E(a) = F_E(a')$$

Esto quiere decir que para cada relación de equivalencia E, las clases de equivalencia de E pueden ser pensadas como elementos de A^m, es decir elementos en la estructura. Como la imagen de una función definible es definible, entonces aquellos elementos imaginarios en realidad son reales.

Demostración. $\Rightarrow$:Para cada $a \in A^n$, definimos $F_E(a) = b$. $\Leftarrow$: Tomemos a $\phi(u, v)$ como la fórmula que define "'$F_E(u) = v$"' y $b = F_E(a)$. □

El siguiente teorema se prueba usando técnicas muy parecidas. Su demostración se puede ver en [5]

Teorema 4.11. *Una estructura A elimina imaginarios si y sólo si toda clase $\emptyset$-definible en A^{eq} está en $\emptyset$-biyección con una $\emptyset$-definible subclase de A^n para algún n.*

Existe otra equivalencia de eliminar imaginarios que puede ser de gran ayuda. Hablaremos de las bases canónicas, las cuales se pueden pensar como una base (como la base de un grupo) pero esta vez en lugar de respetar la estructura algebraica va a respetar la estructura de los conjuntos definibles.

Definición 4.12. *Sea $\mathbb{D}$ un conjunto definible. Se dice que una tupla $\bar{a} \in M^n$ es una* ***base canónica*** de $\mathbb{D}$ cuando $\bar{a}$ es fijado entrada a entrada justamente por aquellos automorfismos de M que fijan a $\mathbb{D}$ como conjunto. Denotamos $cb(\mathbb{D}) = \bar{a}$.

No es inmediato que las bases canónicas existan, pero el siguiente ejemplo nos ayuda a intuir cuándo existirán:

- Sea $\mathbb{D}$ el conjunto que representa una clase de equivalencia de una relación $\emptyset$-definible sobre un modelo A. Notemos que $\mathbb{D}$ es un elemento de A^{eq}. Así, cuando consideramos a $\mathbb{D}$ como un elemento de la estructura A^{eq}, éste es una base canónica de $\mathbb{D}$ pues los automorfismos que fijan un elemento son precisamente aquellos que lo fijan como conjunto en A^{eq}.

Ahora podemos establecer la equivalencia buscada de tener eliminación de imaginarios:

Teorema 4.13. *Una teoría elimina imaginarios si y sólo si todo conjunto definible tiene una base canónica.*

Demostración. Una de las equivalencias de tener eliminación de imaginarios es que todo elemento de A^{eq} es definible con parámetros en A. Pero ya sabemos que X es $\bar{b}$-definible (con $\bar{b} \in A^n$) si y sólo si X se queda fijo como conjunto justo por aquellos morfismos que dejan fijo a $\bar{b}$ por la propocisión 2.19, lo cual termina la demostración. □

En lo posterior necesitaremos de la siguiente definición.

Definición 4.14. *Si consideramos el modelo monstruo $\mathbb{M}$ de una teoría T, decimos que T* ***tiene eliminación de imaginarios*** cuando $\mathbb{M}$ la tiene.

Proposición 4.15. *T^{eq} tiene eliminación de imaginarios.*

La demostración de este teorema es inmediata con el primer inciso del siguiente lema. El segundo inciso nos da una equivalencia entre ser definible con parámetros y saber dónde encontrar a la base canónica:

Lema 4.16.
1. *Si X es definible en el grupo monstruo $\mathbb{M}$ de una teoría T, entonces existe $\alpha \in \mathbb{M}^{eq}$ una base canónica.*
2. *Sea X un conjunto definible (muy probablemente usando parámetros) que tiene una base canónica c. Si A es un conjunto, entonces X es definible sobre A si y sólo si $c \in dcl\,(A)$.*

Demostración. Sólo demostraré el primer inciso. Si X esta definido por la fórmula $\phi\,(x, \bar{a})$ con $a \in A \subseteq \mathbb{M}$. Definimos la siguiente relación de equivalencia:

$$\bar{b} E \bar{c} \Leftrightarrow \left(\phi\left(x, \bar{b}\right) = \phi\,(x, \bar{c})\right)$$

Proponemos $\alpha = \bar{a}_E \in \mathbb{M}^{eq}$. Como X es definible sobre $\bar{a}$ si y sólo si todo morfismo en $\mathbb{M}$ que fija a X como conjunto, también fija a $\bar{a}$(como elemento), entonces α es una base canónica.

□

Para finalizar esta sección damos un ejemplo de cuándo la eliminación de imaginarios no es cierta (recuerda que estamos estrenando una convención!) y otro cuando sí es cierta para reforzar los conceptos aprendidos.

Proposición 4.17. *Sea K un campo finito con al menos 3 elementos. V un espacio vectorial de dimensión mayor o igual a 2 sobre K. Entonces V no elimina imaginarios.*

Demostración. Supongamos por contradicción que sí tiene eliminación de imaginarios. Como K es finito, podemos considerar la fórmula

$$E\,(v, w) = \vee_{k \in K \backslash 0}\,(v = kw)$$

Esta fórmula define una relación de equivalencia en V: v está relacionado con w cuando pase que $E\,(v, w)$ sea cierta en V. Tomenos $a \in V \backslash 0$. Como supusimos que hay eliminación de imaginarios, existe una L_K-fórmula $\phi\,(v, \bar{z})$ y un $\bar{b} \in V^m$ de tal forma que

$$E\,(V, a) = \phi\left(V, \bar{b}\right)$$

Pero K tiene por lo menos 3 elementos, así que podemos tomar $k \in K \backslash 0, 1$. Como $E\,(V, a) = \phi\left(V, \bar{b}\right)$ entonces para todo $x \in V$:

$$k^{-1}x \in E\,(V, a) \Leftrightarrow k^{-1}x \in \phi\left(V, \bar{b}\right)$$

Pero la multiplicación por k es un automorfismo, entonces tenemos:

$$x \in E(V, ka) \Leftrightarrow x \in \phi\left(V, k\bar{b}\right)$$

Lo cual significa que son iguales como conjuntos: $E(V, ka) = \phi\left(V, k\bar{b}\right)$. Pero por la defincón de E: $E(V, a) = E(V, ka)$. Así que $E(V, a) = E(V, ka) = \phi\left(V, k\bar{b}\right)$. Eso implica (nuevamente por la definición de E) que $k\bar{b} = \bar{b}$, y como $k \neq 0, 1$ entonces $\bar{b} = 0$. Así que en lugar de $\phi(v, \bar{z})$ podemos poner a $\phi(v)$ y $\phi(V) = E(V, a)$.

Pero los espacios vectoriales en el lenguaje L_K tienen eliminación de cuantificadores, así que $\phi(v)$ es una combinación booleana finita de elementos de la forma

$$v = v, v = 0$$

Como V tiene dimensión por lo menos igual a dos, entonces no hay forma de que $E(V, a)$ sea igual a una combinación booleana de fórmulas atómicas como las anteriores. Así terminamos.

□

Ahora enunciaremos un par de ejemplos donde sí es cierta la eliminación de imaginarios. Omitimos sus demostraciones por razones de espacio. Es importante mencionar que será el segundo ejemplo el que utilizaremos en la demostración de la conjetura de Mordell-Lang.

También quisiera recalcar que no es para nada trivial cuando una teoría tiene eliminación de imaginarios, y el hecho de que Hrushovski decidiera trabajar en la teoría de los campos diferencialmente cerrados (en lugar de los campos algebraicamente cerrados que es donde se enuncia naturalmente Mordell-Lang) es un hecho notable dentro de su fantástica demostración. Hrushovski le atribuye la fuente de inspiración de este hecho al enfoque que le dio Buium a Mordell-Lang en [43]. La importancia de trabajar en una teoría con eliminación de imaginarios radica en que muchas de las proposiciones previas a la demostración de Mordell-Lang están enunciadas en T^{eq} como se podrá ver en la sección 5, gracias a la eliminación de imaginarios se puede trabajar en T sin ningún problema.

Teorema 4.18. *Los espacios vectoriales sobre un campo algebraicamente cerrado tienen eliminación de imaginarios.*

Teorema 4.19. DCF_0 *elimina imaginarios.*

5. TEORÍA DE LA ESTABILIDAD

Esta sección quizás contiene el sesenta por ciento de la teoría que se va a utilizar en la demostración de Mordell-Lang. Su lectura es absolutamente obligada para entender la demostración. Contiene una pequeña porción de la teoría de estabilidad iniciada por Shelah para solucionar el problema de la clasificación. Por su puesto que no pretendo que la exposición sea exhaustiva (pues no hay forma de serlo cuando la teoría es tan rica), en cambio espero que una persona que no sepa nada sobre teoría de la estabilidad sea capaz de entender la demostración de Hrushovski (lo relevante de ésta) con el material expuesto en esta sección.

El enfoque de la teoría de la estabilidad que estudiaremos en esta sección es el de la teoría geométrica de la estabilidad, que consiste en estudiar propiedades «geométricas» de una estructura. Comenzaremos con aquellas que son las más sencillas en términos de la geometría de sus conjuntos definibles: **Las fuertemente minimales** . Después daremos una definición cuantitativa (usando ordinales) de por qué las fuertemente minimales son las más sencillas: **Rango de Morley** .

Las siguientes dos secciones están dedicadas al **forking** y a la **independencia** . Estos conceptos generalizan propiedades geométricas que se cumplen en los conjuntos fuertemente minimales para estructuras un poco más complejas (respecto al rango de Morley).

En la sección 5 todos los esfuerzos están dirigidos a entender la **Conjetura de Tricotomía de Zilber** , para ello damos una generalización de las estructuras fuertemente minimales, pero esta vez la generalización no se hace respecto al rango de Morley sino a propiedades estrictamente «geométricas».

Después hablaremos de las teorías **1-basadas** , las cuales traducen en términos de la teoría de la estabilidad ideas de geometría algebraica. En esta sección sólo hablaremos de las propiedades que tienen las teorías uno basadas con respecto a la teoría de la estabilidad, no será hasta la sección 7.3 cuando hablemos de su traducción a la geometría algebraica.

También se incluye una sección dedicada a la **ortogonalidad** , que es una propiedad que generaliza el hecho que la topología de Zariski extienda a la topología producto. Esta generalización tiene sentido en los modelos $\omega-$ estables y tiene una traducción en términos de estabilidad.

Por último, incluimos una sección que consiste en demostrar un teorema para grupos que involucra toda la teoría anterior. Ese teorema se utilizará en la demostración de Mordell-Lang. Esta sección tambien incluye resultados técnicos que se utilizarán directamente en la demostración de Mordell-Lang.

5.1. Conjuntos fuertemente minimales.

Definición 5.1.

- *Sea M una L-estructura, decimos que un conjunto definible infinito $D \subseteq M^n$ es **minimal*** si cumple lo siguiente: Si $Y \subseteq D$ es definible, entonces ya sea que Y es finito, o $D \backslash Y$ es finito.
- Supongamos que $D \subseteq M^n$ está definido por $\phi(\bar{x})$, decimos que D es **fuertemente minimal** cuando $\phi(M')$ es minimal $\forall M \prec M'$.

Por la dualidad tipo Grothendieck entre fórmulas y subconjuntos definibles algunas veces hablaremos de conjuntos fuertemente minimales y otras de fórmulas «fuertemente minimales», notemos que en este caso no habrá ambigüedad.

Un ejemplo de un conjunto fuertemente minimal son los campos algebraicamente cerrados pues las soluciones de un polinomio dado son finitas o cofinitas.

Una parte importante en la demostración de Mordell-Lang consistirá en demostrar que podemos reducir el caso a los conjuntos definibles fuertemente minimales. Como la teoría

en la que demostraremos la conjetura de Mordell-Lang será la de los campos diferencialmente cerrados, entonces conviene preguntarnos si en esa teoría existen los conjuntos fuertemente minimales (no en todas las teorías existen...). Recordemos que los campos diferencialmente cerrados son ω-estables. La siguiente proposición hace plausible nuestro plan:

Proposición 5.2. *Supongamos que una teoría T es ω-estable. Si $M \models T$, entonces existe un conjunto minimal en M.*

Su demostración se encuentra en [4].

La principal cualidad de los conjuntos fuertemente minimales es su comportamiento respecto a la siguiente definición:

Definición 5.3. *Sea M una estructura. Un elemento $a \in M^n$ se dice que es **algebraico sobre** A* cuando esté contenido en un conjunto A-definible que además sea finito.

Definición 5.4.
- *Sea $A \subseteq M^n$, definimos $acl(A) =$* los a que son algebraicos sobre A.
- Sea $A \subseteq M^n$, definimos $dcl(A) =$ los a que son definibles sobre A.

Una observación inmediata es que $dcl(A) \subseteq acl(A)$ pues si a es definible, en particular $a \in \{a\}$ el cuál es un conjunto finito.

Ejemplo 5.5. *Sea K es un campo algebraicamente cerrado, la cerradura algebraica (el campo algebraicamente cerrado generado) de un conjunto $X \subseteq K$ coincide con $acl(\langle X \rangle)$ donde $\langle X \rangle$ es el campo generado por X. Esto es cierto pues -por eliminación de cuantificadores en los campos algebraicamente cerrados- cualquier definible sobre $\langle X \rangle$ consiste de combinaciones booleanas de ceros de polinomios con coeficientes en $\langle X \rangle$, dicho de otra manera son los elementos algebraicos sobre X.*

Ejemplo 5.6. *Sea V un espacio vectorial infinito sobre un campo K, lo consideramos como una estructura en el siguiente lenguaje: $L = (+, 0, \lambda_a : a \in K)$, donde cada λ_a es una función que se interpreta de la siguiente manera: $\lambda_a(x) = ax$. De esa forma (V, L) es fuertemente minimal, ver* [4].

Cuando una estructura $M = D$ es un conjunto fuertemente minimal definimos $acl_D(A) = acl(A) \cap D$. En lo posterior denotaremos $acl_D = acl$. La pareja (D, acl_D) cumple propiedades muy importantes:

Lema 5.7.
- $A \subseteq acl(A)$.
- $acl(A) = acl(acl(A))$.
- *Si $A \subseteq B$, entonces $acl(A) \subseteq acl(B)$.*
- *Si $a_0 \in acl(A)$, entonces existe $A_0 \subseteq A$ finito, de tal forma que $a_0 \in acl(A_0)$.*

Demostración.
- Si $a \in A$, entonces la fórmula $x = a$ define a a.
- Por el anterior: $acl(A) \subseteq acl(acl(A))$. Sea $a \in acl(acl(A))$, esto quiere decir que a es algebraico para una fórmula $\phi(x, \bar{b})$ con parámetros en $acl(A)$. Pero como una fórmula es finita, sólo se ocuparon una cantidad finita de parámetros, digamos $(b_1, \ldots, b_m)$. A su vez, cada b_i es algebraico sobre A, i.e. existen fórmulas $\phi_i(y, \overline{c_i})$ que definen conjuntos finitos, y los parámetros $\overline{c_i}$ están en A. Propongo la siguiente fórmula: $\phi(x, y_1, \ldots, y_m) \wedge \phi_1(y_1, \overline{c_1}) \wedge \ldots \wedge \phi_m(y_1, \overline{c_m})$. Como las realizaciones de cada una de las conjunciones es finita, las realizaciones de esta nueva fórmula también serán finitas. Como sus parámetros están en A ya terminamos.

- Sea $a \in acl(A)$, como $A \subseteq B$, entonces los parámetros que se necesitan para definir a A, en particular están en B, así que $a \in acl(B)$.
- a está en un conjunto definido por una fórmula con parámetros en A, como las fórmulas son finitas, sólo necesitamos una cantidad finita de parámetros para definir a a.

□

De hecho los conjuntos fuertemente minimales satisfacen otra propiedad mucho más importante que las anteriores:

Lema 5.8. *Supongamos que D es un conjunto fuertemente minimal y que $A \subseteq D$, $a, b \in D$. Si $acl(A \cup b) \setminus acl(A)$, entonces $b \in acl(A \cup a)$.*

Demostración. Escribiré $acl(A, b)$ para denotar $acl(A \cup b)$. Por otro lado, x, y, w serán variables.

Supongamos que $a \in acl(A, b) \setminus acl(A)$. Sea ϕ de tal forma que $M \models \phi(a, b)$ donde ϕ es una fórmula con parámetros A y además $|\{x \in D : \phi(x, b)\}| = n$. Sea $\psi(w)$ la fórmula que dice que $|\{x \in D : \phi(x, w)\}| = n$ (ψ se ve como: existe un w tal que lo anterior, y además existe uno distinto que lo anterior y ... existe otro tal que lo anterior pero que es distinto a todos los que ya dijimos; esto se puede expresar en una fórmula finita). Si fuera el caso que $\psi(w)$ define un conjunto finito, entonces $b \in acl(A)$ pues la fórmula $\phi(x, w)$ tiene parámetros en A. Pero entonces tendríamos una contradicción porque si b es algebraico sobre A y a es algebraico sobre $A \cup b$, entonces a sería algebraico sobre A, pero habíamos supuesto que $a \notin acl(A)$. Como D es fuertemente minimal, entonces $\psi(w)$ define un conjunto cofinito.

Ahora consideraré el siguiente conjunto: $S = \{y \in D : \phi(a, y) \wedge \psi(y)\}$. Ese conjunto puede ser finito o cofinito; supongamos que es finito. Entonces (como b esta ahí), $b \in acl(A, a)$ pues la fórmula $\phi(a, y) \wedge \psi(y)$ es una $A \cup a$-fórmula y eso es lo que queríamos.

Afirmo que sólo puede ocurrir que S sea finito. Por contradicción supongamos que $\{y \in D : \phi(a, y) \wedge \psi(y)\} = n$ es cofinito. Entonces $|D \setminus \{y : \phi(a, y) \wedge \psi(y)\}| = l$ para algún l. Si $\chi(x)$ es la fórmula que define lo siguiente:

$$\{D \setminus \{y : \phi(x, y) \wedge \psi(y)\}\}$$

y suponemos que $\chi(D)$ es finito, entonces $a \in acl(A)$ (pues $D \models \chi(a)$) y eso es nuevamente una contradicción. Así que $\chi(D)$ debe ser cofinito.

Como es cofinito, podemos encontrar $a_1, a_2, \ldots, a_{n+1}$ para algun n, tales que $\chi(a_i)$ para cada i. Definimos los conjuntos: $B_i = \{w \in D : \phi(a_i, w) \wedge \psi(w)\}$ para cada i. Por definición, B_i es cofinito para cada $i \leq n + 1$. Debido a que todos ellos son cofinitos, entonces existe $b' \in \cap^n B_i$. b' existe porque podemos tomar una cantidad arbitraria de a_i's, y como cada B_i es cofinito, entonces aquello que no esté en una cantidad finita de B_i's al mismo tiempo no puede ser infinito, luego entonces, con elementos de ese tipo no nos podemos acabar a D (que es infinito), así que b' sí existe. Por definición de b', $\phi(a_i, b')$ es cierto para cada $i \leq n+1$, entonces $|\{x \in D : \phi(x, b')\}| \geq n+1$, lo cual contradice que $\psi(b')$. Así terminamos.

□

La propiedad anterior es de suma importancia, no la perdamos de vista. Gracias a ella es posible definir una buena noción de dependencia para los conjuntos fuertemente minimales, la cuál generalizará la dependencia algebraica y la dependencia lineal en campos algebraicamente cerrados y espacios vectoriales respectivamente.

Definición 5.9. *Supongamos que D es fuertemente minimal, $A, B \subseteq D$ y $a \in M^n$.*

- *Decimos que a y A son **independientes*** cuando $a \notin acl(A)$.
- Decimos que a y A son **independientes sobre** B cuando $a \notin acl(A \cup B)$.
- Decimos que A es **independiente** cuando para todo $b \in A$, b y $(A \setminus \{b\})$ son independientes.
- Decimos que A es **independiente sobre** B cuando para todo $b \in A$, b y $(A \cup B) \setminus \{b\}$ son independientes sobre B.

Definición 5.10. *Sea D un conjunto fuertemente minimal, si $A \subseteq Y \subseteq D$ decimos que A es una **base*** para Y, cuando $acl(A) = acl(Y)$ y además A es independiente.

La demostración del siguiente lema se puede encontrar en [4], no es difícil pero por cuestión de espacio prefiero omitirla:

Lema 5.11. *Si D es fuertemente minimal y $A, B \subseteq Y \subseteq D$ y además A, B son bases, entonces $|A| = |B|$.*

Así que podemos definir una dimensión:

Definición 5.12. *Si $Y \subseteq D$, definimos la **dimensión*** de Y como la cardinalidad de alguna base de Y. Denotaremos $dim(Y)$ a la dimensión de Y.

Hasta el momento es súmamente difícil calcular la dimensión de los conjuntos, un primer ejemplo es el siguiente: si D no es numerable y el lenguaje L es numerable, entonces $dim(D) = |D|$, esto es inmediato pues $acl(A)$ es numerable para todo $A \subseteq D$ numerable.

Nuestra definición de conjuntos fuertemente minimales fue para conjuntos, pero también se puede hablar de teorías fuertemente minimales. Decimos que una teoría es fuertemente minimal cuando $v = v$ define a un conjunto fuertemente minimal para todo $M \models T$. Con lo anterior queremos decir que el universo de todo modelo de T es un conjunto fuertemente minimal.

Con el siguiente teorema (cuya demostración se puede encontrar en [4]) terminamos momentáneamente la discusión sobre conjuntos fuertemente minimales.

Teorema 5.13. *Supongamos que T es una teoría fuertemente minimal, sean $M, N \models T$, entonces $M \cong N$ si y sólo si $dim(M) = dim(N)$.*

Ya dijimos que en las teorías ω-estables siempre existen conjuntos fuertemente minimales, y por otro lado, en las últimas líneas hemos expuesto por qué los conjuntos fuertemente minimales simplifican el estudio de los subconjuntos definibles. Entonces sería bueno poder decir cuál es la relación entre los conjuntos fuertemente minimales en un modelo y el resto de los conjuntos definibles. El Rango de Morley contesta esa pregunta.

5.2. Rango de Morley. Así como pudimos asignarle un número a los subconjuntos definibles de un conjunto fuertemente minimal, en teoría de modelos se busca hacer eso para modelos más generales que los fuertemente minimales. A estas asignaciones se les conoce como rango, en general no es posible definir un rango que cumpla con propiedades interesantes para todos los definibles.

Definición 5.14. *Supongamos que M es una L estructura y que $\phi(u)$ es una fórmula en el lenguaje L_M. Definimos $RM^M(\phi)$, **el Rango de Morley*** de ϕ en M. Primero definiré inductivamente $RM^M(\phi) \geq \alpha$ para un ordinal α:

1. $RM^M(\phi) \geq 0$ si $\phi(M)$ es no vacío.
2. $RM^M(\phi) \geq \alpha$ para α un ordinal límite, si $RM^M(\phi) \geq \beta$ para todo $\beta < \alpha$.

3. $RM^M(\phi) \geq \alpha + 1$, cuando existan fórmulas en L_M: $\psi_1(v), \ldots$ de tal forma que $\psi_1(M), \ldots$ es una familia disjunta de subconjuntos de $\phi(M)$ de tal forma que $RM^M(\psi_i(v)) \geq \alpha$ para toda i.

Cuando $\phi(M) = \emptyset$, entonces $RM^M(\phi) = -1$ y si $RM^M(\phi) \geq \alpha$ pero no pasa que $RM^M(\phi) \geq \alpha + 1$, entonces $RM^M(\phi) = \alpha$

La definición del Rango de Morley que dimos hace referencia al modelo M, mientras que una fórmula no es más que un elemento dentro de una teoría, así que quisiéramos quitar la dependencia de la definición anterior al modelo M. Los siguientes lemas se encargaran de eso, las demostraciones se pueden encontrar en [4].

Lema 5.15. *Supongamos que $\phi(u, v)$ es una L-fórmula, M es $\aleph_0$-saturado, $a, b \in M$ tales que $tp^M(a) = tp^M(b)$, entonces $RM^M(\phi(u, a)) = RM^M(\phi(u, b))$*

Lema 5.16. *Supongamos que M y N son modelos $\aleph_0$-saturados de una teoría T, tales que $M \prec N$. Si ϕ es una L_M-fórmula, entonces $RM^M(\phi) = RM^N(\phi)$*

Corolario 5.17. *Supongamos que M es una L estructura, ϕ una L_M fórmula y N_0, N_1 son extensiones $\aleph_0$-saturadas de M. Entonces $RM^{N_0}(\phi) = RM^{N_1}(\phi)$.*

El corolario anterior nos permite definir al rango de Morley de la siguiente manera:

Definición 5.18. *Si M es una estructura de un lenguaje L y ϕ es una L-fórmula, definimos el **rango de Morley*** de ϕ por $RM(\phi) = RM^N(\phi)$ donde N es una extensión elementaria de M que además es $\aleph_0$-saturada.

El rango de Morley va a ser muy importante para demostrar Mordell-Lang, y ya que en las extensiones $\aleph_0$-saturadas su definición no depende de la elección del modelo, será necesario considerar campos $\aleph_0$-saturados para demostrar Mordell-Lang.

Éstas son algunas de las propiedades del rango de Morley:

Proposición 5.19. *Sea M una L-estructura y $X, Y \subseteq M^n$ subconjuntos definibles, entonces se cumple lo siguiente:*

1. *Si $X \subseteq Y$, entonces $RM(X) \leq RM(Y)$.*
2. *$RM(X \cup Y)$ es el máximo entre $RM(X)$ y $RM(Y)$.*
3. *Si X no es vacío, entonces $RM(X) = 0$ si y sólo si X es finito.*

Demostración.

1. Supongamos que $X \subseteq Y$, por la manera como definimos el Rango de Morley, es suficiente con demostrar que si $RM(X) \geq \alpha$, entonces $RM(Y) \geq \alpha$. Hagámoslo por inducción transfinita: Si $\alpha = 0$, supongamos que $RM(X) \neq \emptyset$, entonces $RM(Y) \neq \emptyset$. Si α es límite, supongamos que $RM(X) \geq \beta, \forall \beta < \alpha$. Por hipótesis de inducción, $RM(Y) \geq \beta, \forall \beta < \alpha$, lo cual significa que $RM(Y) \geq \alpha$. Si $\alpha = \beta + 1$, supongamos que $RM(X) \geq \alpha$. Eso quiere decir que existe una familia infinita $X_1, \ldots \subseteq X$ de tal forma que $RM(X_i) \geq \beta$, pero en particular esos $X_i \subseteq Y$, así que $RM(Y) \geq \alpha$. Así que $RM(X) \leq RM(Y)$.
2. Notemos que $X, Y \subseteq X \cup Y$, entonces por el ejercicio anterior tenemos que $max\{RM(X), RM(Y)\} \leq RM(X \cup Y)$. Ahora vamos a demostrar la otra desigualdad: nuevamente tenemos que demostrar si $max\{RM(X), RM(Y)\} \geq \alpha$ implica que $RM(X) \geq \alpha$ o $RM(X) \geq \alpha$. Lo haremos por inducción. Sea $\alpha = 0$, sin pérdida de generalidad podemos suponer que $RM(X) = max\{RM(X), RM(Y)\}$. Supongamos que $max\{RM(X), RM(Y)\} \geq 0$, entonces X es no vacío, eso quiere decir que $X \cup Y \neq \emptyset$, entonces $RM(X) \geq 0$, así que $RM(X) \geq \alpha$ o $RM(Y) \geq \alpha$.

Si α es un cardinal límite, entonces $max\{RM(X), RM(Y)\} \geq \beta$ para todo $\alpha > \beta$, entonces $RM(X) \geq \beta$, entonces $RM(X) \geq \alpha$, en el otro caso $RM(Y) \geq \alpha$. Si $\alpha = \beta+1$, supongamos que $max\{RM(X), RM(Y)\} \geq \alpha$. Sin pérdida de generalidad digamos $max\{RM(X), RM(Y)\} = RM(X)$, entonces $RM(X) \geq \alpha$ y terminamos.

3. Como X es no vacío, $RM(X) \geq 0$. Primero supongamos que X es finito, entonces X no puede ser partido en una cantidad infinita de subconjuntos, así que no es cierto que $RM(X) \geq 1$, entonces $RM(X) = 0$. Para el otro sentido, por contrapuesta: supongamos que X es infinito, sean $x_1, x_2, \ldots$ elementos en X, entonces X puede ser partido en $\{x_1\}, \{x_2\}, \ldots$, los cuales no son vacíos, entonces $RM(\{x_i\}) \geq 0$, así que $RM(X) \geq 1$.

□

Supongamos que $RM(X) = \alpha$, entonces X no puede ser partido en una cantidad infinita de subconjuntos con rango de Morley mayor o igual a α. De hecho existe un $d \in \mathbb{N}$ de tal forma que X no puede ser partido en más de d subconjuntos con rango de Morley mayor o igual a α. La demostración de ese hecho es un poco complicada, y nos la ahorraremos porque nos desviaría de los objetivos de este trabajo:

Proposición 5.20. *Supongamos que $RM(X) = \alpha$, entonces existe $d \in \mathbb{N}$ de tal forma que si existen $X_1, X_2, \ldots X_e$ disjuntos, de tal forma que $RM(X_i) \geq \alpha$, entonces $e \leq d$. A este natural lo llamaremos el* ***grado de Morley*** , se denotará por $gr_M(X)$.

Con el uso del rango y grado de Morley es posible dar una definición alternativa de los conjuntos fuertemente minimales.

Lema 5.21. *Un conjunto definible D de un modelo M es fuertemente minimal si y sólo si $RM(D) = gr_M(D) = 1$.*

Demostración. Supongamos que D es fuertemente minimal, como D es infinito, entonces $RM(X) \geq 1$, como todos los subconjuntos de D son finitos o cofinitos, entonces D no puede ser dividido en dos subconjuntos disjuntos que sean infinitos (si $D = D_1 \cup D_2$ con D_1 infinito, entonces D_2 debería ser finito), así que $gr_M(X) = 1$, en particular $RM(X) = 1$.

Por otro lado, supongamos que $RM(D) = gr_M(D) = 1$. Como $RM(D) \neq 0$, entonces D es infinito. Sea $X \subseteq D$ definible, entonces $X' = D \backslash X$ también es definible. Como $gr_M = 1$, entonces no puede suceder que X, X' sean infinitos, así que alguno de ellos será finito. Eso significa que cualquier definible es finito o cofinito.

□

Gracias a este resultado tenemos una relación tangible entre los conjuntos fuertemente minimales y el resto de los definibles. Además podemos cuantificar el hecho de que los conjuntos fuertemente minimales son los más sencillos.

Además del lema anterior existe otra forma de relacionar a los conjuntos fuertemente minimales con el rango de Morley. Recordemos que en los conjuntos fuertemente minimales es posible definir una noción de dimensión. Así que nos preguntamos ¿existe alguna relación entre el Rango de Morley y la dimensión en los conjuntos fuertemente minimales? El siguiente lema contesta satisfactoriamente a esa pregunta, incluso es posible generalizarlo. Enunciaremos esa generalización en un par de secciones posteriores. Su demostración se encuentra en [13]:

Proposición 5.22. *Si D es un conjunto fuertemente minimal y $a_1, a_2, \ldots, a_n \in D$ entonces $RM(a_1, \ldots, a_n/\emptyset) = dim(a_1, \ldots, a_n)$.*

Por otro lado, no es cierto que cualquier conjunto (o fórmula) tenga rango de Morley distinto a ∞:

Definición 5.23. *Una teoría se llamará* ***totalmente trascendente*** cuando el rango de Morley de cualquier conjunto es distinto a ∞.

Ya antes habíamos dicho que la estabilidad es una propiedad muy importante, la siguiente proposición refuerza esta idea (su demostración se encuentra en [12]):

Proposición 5.24. *Una teoría T es totalmente trascendente si y sólo si es ω-estable.*

Para característica 0, la demostración de Mordell-Lang utiliza teorías ω-estables, a saber, los campos diferencialmente cerrados.

Así como definimos el rango de Morley para una fórmula, podemos definir el rango de Morley para tipos.

Definición 5.25. *Sea $p \in S(A)$ un tipo, definimos el* ***rango de Morley de*** p como $RM(p) = \text{ínf}\{RM(\phi) : \phi \in p\}$ cuando exista alguna fórmula ϕ con rango de Morley distinto a ∞. De otra manera $RM(p) = \infty$.

Definición 5.26. *El* ***grado de Morley de*** p es $gr_M(p) = \text{ínf}\{gr_M(\phi) : \phi \in p, RM(\phi) = RM(p)\}$.

A lo largo del trabajo utilizaremos la siguiente notación: $RM(a/A) = RM(tp(a/A))$.

Los lemas a continuación (cuyas demostraciones nos saltaremos), se usarán para dar la demostración de un teorema que utilizaremos para probar Mordell-Lang.

Lema 5.27. *Sea M es una estructura y X un conjunto definible en M. $RM(X) = sup\{RM(a/A) : a \in X, A \subset M, X \subseteq dcl(A)\}$.*

Lema 5.28. *Sea M es una estructura, $A \subseteq M$ y $a, b \in M$ con $b \in acl(A \cup a)$ entonces $RM(a \cup b/A) = RM(a/A)$.*

Lo que este lema quiere decir es que el rango de Morley no distingue a los elementos algebraicos, algo así sucede en los campos algebraicamente cerrados, donde el grado de trascendencia no distingue el grado de las extensiones algebraicas. Ya dijimos que ser algebraico en teoría de modelos coincide con ser algebraico en el sentido de los campos y de hecho tenemos una traducción completa:

Proposición 5.29. *Sea $k \subseteq K$ un subcampo de un campo algebráicamente cerrado K y $a \in K^n$. Entonces $RM(a/k)$ es igual al grado de trascendencia de $k(a)$ sobre k.*

Una demostración de este hecho se puede encontrar en [49].

El siguiente teorema nos dice que el rango de Morley se porta bien respecto a funciones definibles.

Teorema 5.30. *Supongamos que una teoría T es ω-estable. Si existe una función definible, suprayectiva y con fibras finitas $f : X \longrightarrow Y$ entre dos conjuntos definibles, entonces $RM(X) = RM(Y)$.*

Demostración. Primero haremos la siguiente observación: si X, Y, f son definibles sobre $A \subset M$ y $f(c) = d$, entonces d es definible sobre $A \cup c$, en particular: $d \in acl(A \cup c)$. Pero como las fibras de f son finitas, entonces también $c \in acl(A \cup d)$. Por el lema 5.28, tenemos que $RM(a/A) = RM(a, b/A) = RM(b/A)$. Todo lo anterior, es cierto para cuales quiera c, d que cumplan las condiciones dadas.

Por otro lado, como T es ω-estable, entonces todos los conjuntos tienen rango de Morley distinto a infinito, así que en el lema 8, el supremo se alcanza. Sean $a, b \in X, Y$ tales que $RM(X) = RM(a/A)$, $RM(Y) = RM(b/A)$.

De la definición de supremo tenemos la siguiente desigualdad:

$$RM(Y) \geq RM(f(a)/A)$$

Pero por la primera observación:

$$RM(f(a)/A) = RM(a/A) = RM(X)$$

Asi que $RM(Y) \geq RM(X)$.

Para la otra desigualdad, como f es suprayectiva, entonces existe $a' \in X$ de tal forma que $f(a') = b$ (la b de la que ya habíamos hablado). Nuevamente por la definición de supremo y por la primera observación tenemos que

$$RM(X) \geq RM(a'/A) = RM(b/A)$$

Pero como la b era la misma de hace rato, $RM(b/A) = RM(Y)$. Por las dos desigualdades se tiene que $RM(X) = RM(Y)$, así que terminamos.

□

La siguiente proposición nos dice que estudiar conjuntos definibles respecto a su rango de Morley tiene importancia más allá de la lógica matemática, pues interactúa fuertemente con la teoría de anillos:

Proposición 5.31. *El Rango de Morley coincide con la dimensión de Krull*[10].

5.3. Forking. Así como es interesante considerar extensiones de ideales, también será interesante extender tipos: si p, q son tipos, q se dirá una extensión de p cuando $p \subseteq q$. Existen propiedades de las extensiones que nos dan información sobre la complejidad de una teoría.

Cuando se está trabajando en una teoría ω-estable existen por lo menos dos maneras equivalentes de definir las extensiones de tipos que no separan (en inglés llamadas forking). La primera de ellas es bastante intuitiva, sin embargo es muy difícil trabajar con ella. Es por lo anterior que la definición oficial será un poco más técnica; ella involucra al Rango de Morley. La primera definición es la siguiente.

Definición 5.32. *Sean $p \in S(A), q \in S(B)$ tales que $A \subseteq B$ y $p \subseteq q$. Se dice que q es un **heredero*** de p cuando para cualquier $\bar{b} \in B$ y cualquier fórmula $\phi(x, \bar{b})$ en el lenguaje $L(A)$ tal que $\phi(x, \bar{b}) \in q$ existe un $\bar{a} \in A$ de tal forma que $\phi(x, \bar{a}) \in p$.

Si pensamos en $A \subseteq B$ como dos campos algebraicamente cerrados y a $p \in Spec(A[x]), q \in Spec(B[x])$ con $p \subseteq q$. ¿Qué significa en términos algebraicos que p y q sean herederos? Para contestar esa pregunta es necesario utilizar una definición equivalente de ser herederos:

Ahora vamos con una definición más técnica, pero antes es importante hacer la siguiente observación: Si tenemos $p \in S(A), q \in S(B)$ tales que $A \subseteq B$ y $p \subseteq q$, entonces $RM(q) \leq RM(p)$ por la definición del ínfimo.

Definición 5.33. *Consideremos una estructura M, sea $A \subseteq B$ subconjuntos del universo de M. Sean $p \in S(A)$, $q \in S(B)$ tipos tales que $p \subseteq q$. Decimos que q es una **extensión de p que no separa*** cuando el rango de Morley de p es el mismo que el rango de Morley de q. En caso de que $RM(q) < RM(p)$ se dice que q es una **extensión de p que separa.**

[10]Si R es un anillo, la dimensión de Krull se define como el supremo de las longitudes de cadenas propias de ideales primos.

Proposición 5.34. *Sea T una teoría ω-estable, si $A \subseteq B$ son subconjuntos de un modelo M de T, $p \in S(A)$, $q \in S(B)$ tales que $p \subseteq q$, entonces q es heredero de p si y sólo si es una extensión que no separa.*

Ahora tratemos de ejercitar un poco nuestra intuición con esta definición: supongamos que k es un subcampo de un campo algebraicamente cerrado K. Ya vimos anteriormente que si $a \in K$ es trascendente sobre k, entonces $RM(tp(a/k)) = 1$, supongamos que tenemos otro campo $k \subseteq l$. Como $tp(a/l)$ es una extensión de $tp(a/k)$ nos podemos preguntar si ésta es una extensión que separa. Por la primera observación, $RM(a/l) \leq RM(a/k) = 1$, así que $RM(a/l) = 0$ o $RM(a/l) = 1$. En caso que $RM(a/l) = 1$, entonces la extensión no separa, y eso coincide justamente cuando a sigue siendo trascendente sobre l. Si en cambio $RM(a/l) = 0$, entonces a sería algebraico sobre l. Con lo anterior podemos decir que $tp(a/l)$ separa si y sólo si a es trascendente sobre l.

Notemos que en el ejemplo anterior, los tipos son un poco menos arbitrarios:

Definición 5.35. *Sea p es un tipo completo y A un conjunto de parámetros, decimos que p* ***no separa sobre*** *A* cuando p es una extensión de p_A (que denota la restricción de sus parámetros a A) que no separa.

Ahora vamos a enunciar y demostrar algunas propiedades sobre las extensiones que no separan:

Proposición 5.36. ***Transitividad.*** Sean $p \subseteq q \subseteq r$ una cadena de tipos. Entonces r es una extensión de p que no separa si y sólo si q es una extensión de p que no separa y además r es una extensión de q que no separa.

Demostración. $\Rightarrow$: Notemos que por la definición de ínfimo: $RM(r) \leq RM(q) \leq RM(p)$. Así que si $RM(r) = RM(p)$, entonces ya terminamos.

$\Leftarrow$: La igualdad es transitiva...

□

Proposición 5.37. ***Continuidad.*** Sea B un conjunto de parámetros, $q \in S(B)$ y $A \subseteq B$.

- q no separa sobre un conjunto un conjunto finito $B_0 \subseteq B$.
- Si q separa sobre A, existe $B_0 \subseteq B$ finito de tal forma que $q_{A \cup B_0}$ separa sobre A.

Demostración.

- Sea $\phi \in q$ de tal forma que $RM(\phi) = RM(q)$ (en [13] se demuestra que es posible). consideramos B_0 como el conjunto de parámetros en ϕ. Entonces q no separa sobre B_0.
- Por hipótesis, tenemos que $RM(q) < RM(q_A)$. Por el inciso anterior: existe $B_0 \subseteq B$ de tal forma que $RM(q_{B_0}) = RM(q)$. Así que $RM(q_{B_0}) < RM(q_A)$. Pero como $q_{B_0} \subseteq q_{B_0 \cup A}$, entonces $RM(q_{B_0 \cup A}) \leq RM(q_{B_0})$, así que $RM(q_{B_0 \cup A}) < RM(A)$. Entonces $q_{B_0 \cup A}$ separa sobre A.

□

En teoría de modelos (y en general en matemáticas) las extensiones que se buscan son aquellas que no separan, pues corresponde a los casos estables (en un sentido amplio).

Las propiedades importantes de este tipo de extensiones requieren que la teoría sea ω-estable (de hecho requieren una más débil pero no hablaré de eso...), a partir de ahora lo asumiremos. La demostración del siguiente teorema se puede encontrar en [4].

Teorema 5.38. *Supongamos que $A \subseteq B$ y $p \in S(A)$. Entonces:*

- *Existe $q \in S(B)$ una extensión de p que no separa.*
- *Existen a lo más $gr_M(p)$ extensiones en $S(B)$ de p que no separan.*

- *Cuando un modelo M es $\aleph_0$-saturado, con $A \subset M$, entonces existe justamente $gr_M(p)$ extensiones que no separan.*
- *Existe a lo más una extensión $q \in S(B)$ que no separa con $gr_M(p) = gr_M(q)$*
- *En particular, si $gr_M(p) = 1$, entonces existe una única extensión que no separa en $S(B)$*

Ya antes hablamos de la importancia de tener un conjunto con grado de Morley igual a uno (los conjuntos fuertemente minimales). Pero así como podemos hablar indistintamente entre fórmulas y conjuntos, también es posible hablar de tipos en lugar de conjuntos. Así que si ya antes habíamos dicho que los conjuntos con rango de Morley igual a uno son importantes, también los tipos con Rango de Morley serán importantes. Gracias al teorema anterior, tener rango de Morley se traduce en tener exactamente una extensión que no separa:

Definición 5.39. *Un tipo $p \in S(A)$ es **estacionario*** si tiene exactamente una extensión que no separa para cada $A \subseteq B$.

La demostración del siguiente teorema se puede encontar en [13]

Teorema 5.40. *Si A es un conjunto de parámetros tal que $acl^{eq}(A) = A$, entonces todo tipo con parámetros en A es estacionario.*

La definición que viene a continuación será necesaria para enunciar una propiedad de las teorías llamada uno-basada, la cual será importante para demostrar Mordell-Lang. Esta definición es la misma que la de las bases canónicas, sin embargo esta vez generalizaremos su definición para tipos. Recordemos que así como los conjuntos definibles se pueden pensar como fórmulas (a saber, la fórmula que lo define), también podemos pensar en un tipo como el conjunto de sus realizaciones, lo cual es un subconjunto en la estructura.

Definición 5.41. *Sea p un tipo, $bc(p) \subseteq M^n$ es una **base canónica*** de p cuando sea fijada punto a punto precisamente por aquellos automorfismos que fijan a p como conjunto.

Su existencia dentro de las teorías ω-estables está garantizada por el siguiente lema, su demostración se encuentra en [4]:

Lema 5.42. *Supongamos que M es ω-estable y $p \in S_n(M)$. Entonces p tiene una base canónica en M^{eq}.*

Ya que sabemos que en M^{eq} siempre existen las bases canónicas el siguiente teorema las reivindica y nos será de utilidad dentro de un par de secciones:

Teorema 5.43. *Sea M una estructura, si $p \in S_n(M)$ y $A \subseteq M$ un conjunto de parámetros, entonces*

- *p no separa sobre A si y sólo si $cb(p) \subseteq acl^{eq}(A)$.*

5.4. Independencia. Por medio del forking vamos a definir una noción de independencia entre un elemento a y un subconjunto B. Esta noción de independencia busca generalizar la dependencia algebraica y la dependencia lineal. Es importante notar la generalidad de lo que estamos haciendo, pues todo lo siguiente se puede hacer en cualquier teoría que cumpla con ser ω-estables.

Definición 5.44. *Sea M una estructura L-estructura, decimos que $\bar{a} \in M^n$ y B son **independientes*** sobre $A \subseteq M^n$, cuando $tp(\bar{a}/A \cup B)$ es una extensión de $tp(\bar{a}/A)$ que no separa. Lo denotamos de la siguiente forma: $a \underset{A}{\downarrow} B$

Si suponemos que $A = \emptyset$, decir que $\bar{a} \bigcirc\!\!\!\!\!\!\perp B$ significa que el rango de Morley es incapaz de distinguir entre los conjuntos $\emptyset$-definibles a los que pertenece $\bar{a}$ y los conjuntos B-definibles a los que pertenece $\bar{a}$. Esto quiere decir que los parámetros en B no enriquecen (en el sentido del rango de Morley) a los conjuntos que pertenece $\bar{a}$. Comenzamos con algunas propiedades importantes de la independencia:

Lema 5.45. ***Monotonía*** Si $a \underset{A}{\perp} B$ y $C \subseteq B$, entonces $a \underset{A}{\perp} C$.

Demostración. $RM\left(a/A\right) \geq RM\left(a/A \cup C\right) \geq RM\left(a/A \cup B\right)$, y si $a \underset{A}{\perp} B$ entonces $RM\left(a/A\right) = RM\left(a/A \cup B\right)$ así que $RM\left(a/A \cup C\right) = RM\left(a/A\right)$, por tanto $a \underset{A}{\perp} C$. □

Lema 5.46. ***Transitividad*** $a \underset{A}{\perp} \{b, c\}$ si y sólo si $a \underset{A}{\perp} \{b\}$ y $a \underset{A \cup \{b\}}{\perp} \{c\}$.

Demostración. Notemos que $tp\left(a/A\right) \subseteq tp\left(a/A \cup \{b\}\right) \subseteq tp\left(a/A \cup \{b\} \cup \{c\}\right)$, así que por la transitividad de extensiones que no separan tenemos el resultado.

□

Lema 5.47. ***Base finita*** $a \underset{A}{\perp} B$ si y sólo si $a \underset{A}{\perp} B_0$ para cualquier subconjunto finito $B_0 \subseteq B$.

Demostración. $\Rightarrow$: Es inmediato del lema anterior.

$\Leftarrow$: Supongamos que $\neg\left(a \underset{A}{\perp} B\right)$, por la proposición 5.37, existe un $B_0 \subseteq B$ de tal forma que $\neg\left(a \underset{A}{\perp} B_0\right)$, lo cual contradice nuestra suposición.

□

La demostración del siguiente hecho es bastante extensa, nos la ahorraremos, pero se puede encontrar en [4]

Lema 5.48. ***Simetría*** $a \underset{A}{\perp} b$ si y sólo si $b \underset{A}{\perp} a$.

De la simetría se sigue el siguiente corolario:

Corolario 5.49. $a \underset{A}{\perp} acl\left(A\right)$ *para cualquier* a.

Demostración. Por la propiedad de la base finita es suficiente demostrar el corolario para cada $\bar{b} \in acl\left(A\right)$. Notemos que $RM\left(\bar{b}/A \cup \{a\}\right) \leq RM\left(\bar{b}/A\right)$, pero como $\bar{b}$ es algebraico sobre A, entonces está contenido en un conjunto A-definible que además es finito. En particular $RM\left(\bar{b}/A\right) = RM\left(\phi\left(\bar{x}\right)\right)$ donde $\phi\left(M\right)$ es finito (por ser el infimo). Pero ya habíamos demostrado que si X es finito, entonces $RM\left(X\right) = 0$. Así que $RM\left(\bar{b}/A \cup \{a\}\right) = RM\left(\bar{b}/A\right) = 0$. Eso -por definición- quiere decir que $\bar{b} \underset{A}{\perp} a$, finalmente por simetría tenemos que $a \underset{A}{\perp} \bar{b}$.

□

El corolario anterior es una propiedad deseada para cualquier noción de independencia, quiere decir que a a le da igual tener los parámetros en A o tenerlos en $acl\left(A\right)$ (respecto al rango de Morley). De alguna manera es creíble pues los elementos en $acl\left(A\right)$ no están demasiado lejos de A.

Se puede extender la definición de independencia para dos conjuntos:

Definición 5.50. *Sean A, B y C conjuntos definibles. Decimos que A, B son **independientes** sobre C: $A \underset{C}{\downarrow} B$, cuando $a \underset{C}{\downarrow} B$, $\forall a \in A$.*

Para demostrar que esta noción de independencia generaliza la independencia lineal de los espacios vectoriales regresaremos a los conjuntos fuertemente minimales (pues los espacios vectoriales son ejemplos de conjuntos fuertemente minimales).

Lema 5.51. *Sea D un conjunto fuertemente minimal con $a \in D^n$, $A, B \subseteq D$ con a independiente sobre A entonces $a \underset{A}{\downarrow} B \Leftrightarrow a \in acl(A) \vee a \notin (A \cup B)$.*

Por el momento no demostraré el lema pues aún necesitamos una propiedad importante de la siguiente sección. Suponiendo el lema obtenemos un corolario inmediato al recordar que $acl(U) = \langle U \rangle$ donde $\langle U \rangle$ denota el subespacio vectorial generado por U.

Corolario 5.52. *La noción de independencia definida en esta sección coincide con la de independencia lineal.*

5.5. Pregeometrías y la conjetura de Tricotomía. El objetivo de esta sección es formular la conjetura de Tricotomía de Zilber para conjuntos fuertemente minimales.

Anteriormente hablamos de la estructura que tienen los conjuntos fuertemente minimales junto con la operación acl_D, ahora vamos a generalizar esas ideas.

Definición 5.53. *Sea X un conjunto con una operación $cl : \wp(X) \longrightarrow \wp(X)$. Decimos que la pareja anterior es una **pregeometría*** cuando se satisfagan las siguientes condiciones:

1. Si $A \subseteq X$ entonces $A \subseteq cl(A)$
2. $cl(cl(A)) = cl(A)$.
3. Si $A \subseteq B \subseteq X$ entonces $cl(A) \subseteq cl(B)$.
4. Intercambio. Si $A \subseteq X$, $a, b \in X$ y $a \in cl(A \cup \{b\})$ entonces $a \in cl(A)$ o $b \in cl(A \cup a)$
5. Si $A \subseteq X$ y $a \in cl(A)$, entonces existe $A_0 \subseteq A$ finito, de tal forma que $a \in cl(A_0)$.

Decimos que un conjunto $A \subseteq X$ es cerrado cuando $cl(A) = A$.

Un ejemplo inmediato de pregeometría es el siguiente:

Ejemplo 5.54. *Sea V un espacio vectorial sobre un campo K y $S \subseteq V$. definimos $cl(S) = \langle S \rangle$ como el subespacio vectorial generado por S. Esta pareja resulta ser una pregeometría:*

1. *Por definición: $S \subseteq \langle S \rangle$*
2. *Como $\langle S \rangle$ ya es un subespacio vectorial, entonces $\langle \langle S \rangle \rangle = \langle S \rangle$.*
3. *Nuevamente por definición: si $S \subseteq R$, entonces $\langle S \rangle \subseteq \langle R \rangle$ (pues todo espacio vectorial que contenga a R, también contiene a S).*
4. *Supongamos que $a \in \langle S \cup \{b\} \rangle$. Quiero demostrar que $a \in \langle S \rangle$ o $b \in \langle S \cup \{a\} \rangle$. Por hipótesis, tenemos que $a = \Sigma_{i=1}^{n} r_i s_i + r_0 b$ con $r_i \in K$ y $s_i \in S$. Entonces $r_0' b = \Sigma_{i=1}^{n} r_i s_i + a$, supongamos que $a \notin \langle S \rangle$, entonces $r_0' \neq 0$, asi que $b = \Sigma_{i=1}^{n} r_i' s_i + r'^{-1} a$, asi que $b \in \langle S \cup \{a\} \rangle$.*
5. *Supongamos que $a \in \langle S \rangle$, entonces $a = \Sigma_{i=1}^{n} r_i s_i$ con $s_i \in V, r_i \in K$, asi que $a \in \langle S_0 = \{s_1, \ldots, s_n\} \rangle$.*

Resulta que este ejemplo será prototípico de una pregeometría.

De hecho en la primera sección de este capítulo demostramos lo siguiente:

Ejemplo 5.55. *Todo conjunto fuertemente minimal es una pregeometría.*

Es posible generalizar todas las ideas de independencia y de dimensión que vimos para conjuntos fuertemente minimales, esta vez para las pregeometrías:

Definición 5.56. *Si (X, cl) es una pregeometría con $a \in X$ y $A, B \subseteq X$*

- *Decimos que a y A son **independientes*** cuando $a \notin cl(A)$.
- Decimos que a y A son **independientes sobre** B cuando $a \notin cl(A \cup B)$.
- Decimos que A es **independiente** cuando para todo $b \in A$, b y $(A \setminus \{b\})$ son independientes.
- Decimos que A es **independiente sobre** B cuando para todo $b \in A$, b y $(A \cup B) \setminus \{b\}$ son independientes sobre B.

Ya habíamos dicho antes que en el caso de los campos algebraicamente cerrados, si $X \subseteq K$ entonces $acl(X)$ es la cerradura algebraica del campo generado por X. Afirmo que ser independiente en el sentido de las pregeometrías, coincide con ser algebraicamente independiente lo cual significa lo siguiente:

Definición 5.57. *Sean $K \subseteq L$ dos campos algebraicamente cerrados y $S \subseteq L$ cualquier conjunto. Decimos que S es **independiente*** en L sobre K cuando para todos $\alpha_1, \alpha_2, \ldots, \alpha_n \in S$ distintos y $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ tal que $p(\alpha_1, \ldots, \alpha_n) = 0$ entonces p es el polinomio constante igual a cero.

En particular $\alpha \in L$ es independiente sobre K si y sólo si es trascendente sobre K: α es independiente sobre K si y sólo si $\alpha \notin \overline{K[a]} \setminus \overline{K}$, lo cual significa que sea trascendente.

Recordando el lema 5.51 de la sección anterior obtenemos el siguiente corolario:

Corolario 5.58. *La independencia (forking independencia) generaliza a la independencia algebraica en campos algebraicamente cerrados.*

Continuemos con el estudio de las pregeometrías:

Definición 5.59. *Si $B \subseteq X$ es independiente, decimos que B es una **base*** para $Y \subseteq X$ cuando $cl(Y) = cl(B)$.

En pregeometrías arbitrarias también es cierto lo siguiente:

Lema 5.60. *Supongamos que (X, cl) es una pregeometría, con $Y \subseteq X$ y $B_1, B_2 \subseteq X$ bases para Y. Entonces $|B_1| = |B_2|$. A esa cardinalidad la llamaremos la dimensión de Y y se denotará por $dim(Y)$.*

Definición 5.61. *Si (X, cl) es una pregeometría y $A \subseteq X$. Definimos $cl_A(B) = cl(A \cup B)$. A esta nueva operación la llamaremos la **localización*** de B por A.

Notemos que si (X, cl) es una pregeometría y $Y \subseteq X$, Y es independiente sobre $A \subseteq X$ cuando Y sea independiente en (X, cl_A). A la dimensión de Y sobre A (se defiende de la misma manera que en el caso anterior) se le denotará por $dim(Y/A)$.

Lema 5.62. *Si (X, cl) es una pregeometría y $A \subseteq X$, entonces (X, cl_A) es una pregeometría.*

Demostración. Sea $B \subseteq X$.

- Como $B \subseteq A \cup B$, entonces $B \subseteq cl(B) \subseteq cl(A \cup B) = cl_A(B)$.
- Supongamos que $B \subseteq C$, entonces $B \cup A \subseteq C \cup A$ así que $cl_A(B) \subseteq cl_A(B)$.

- $cl_A(cl_A(B)) = cl(A \cup cl(A \cup B))$, pero $A \subseteq cl(A \cup B)$ así que $A \cup cl(A \cup B) = cl(A \cup B)$. Por tanto $cl(cl(A \cup B)) = cl(A \cup B) = cl_A(B)$.
- Supongamos que $a \in cl_A(B \cup \{b\})$ y $a \notin cl_A(B)$. Entonces $a \in cl(A \cup B \cup \{b\})$ y $a \notin cl(A \cup B)$, por tanto $b \in cl(A \cup B \cup \{a\}) = cl_A(B\{a\})$.
- Supongamos que $a \in cl_A(B) = cl(A \cup B)$, entonces existe $B_0 \subseteq A \cup B$ finito tal que $a \in cl(B_0) \subseteq cl(A \cup B_0) = cl_A(B_0)$.

□

Veamos un ejemplo del concepto de localización:

Ejemplo 5.63. *Sea K un campo y V un espacio vectorial sobre K, definimos la operación en la potencia de V de la siguiente forma: $S \subseteq V$, $cl(S)$ igual al espacio afín generado por S. Recordemos que un espacio afín es el trasladado de un subespacio vectorial, por ejemplo: en $\mathbb{R}$ sería una recta fuera del origen. La única diferencia con el subespacio generado $\langle - \rangle$ es que este no forzosamente contiene al origen. Sin embargo si localizamos por 0_V obtenemos $cl_{0_V} = \langle - \rangle$.*

Gracias al concepto de localización podemos enunciar una generalización del lema 5.22:

Proposición 5.64. *Si D es un conjunto fuertemente minimal, $A \subseteq D$ y $a_1, a_2, \ldots, a_n \in D$ entonces $RM(a_1, \ldots, a_n/A) = dim(a_1, \ldots, a_n/A)$. Donde $dim(a/A)$ se refiere a la dimensión de a en la pregeometría D localizada por A.*

Como ya habíamos dicho, su demostración se puede encontrar en [12].
También es cierto lo siguiente:

Proposición 5.65. *Sea (X, cl) una pregeometría y $a_1, \ldots, a_n \in X$ entonces $a_1, \ldots, a_n$ son independientes sobre A si y sólo si $dim(a_1, \ldots, a_n) = n$.*

Estas proposiciones también nos permiten saldar una cuenta que teníamos pendiente sobre la independencia (en el sentido de forking), pues ahora podemos demostrar el lema 5.51, el cual decía lo siguiente: Sea D un conjunto fuertemente minimal con $a \in D^n$, $A, B \subseteq D$ con a independiente sobre A. Entonces $a \underset{A}{\downarrow} B \Leftrightarrow a \in acl(A) \vee a \notin (A \cup B)$.

Demostración. Por definición de forking $a \underset{A}{\downarrow} B$ si y sólo si $RM(a/A) = RM(a/A, B)$, pero por la proposición 5.64 se tiene que $dim(a/A) = dim(a/A, B)$. Por la proposición 5.65 tenemos que $dim(a/A) = n$ así que $dim(a/A, B) = n$ con lo cual terminamos.

□

Así hemos saldado nuestra deuda.

De acuerdo a los ejemplos que existen de pregeometrías, notaremos que son de particular importancia aquellas que cumplan con la siguiente propiedad: Al aplicar la operación cl a conjuntos con un elemento el resultado sea trivial:

Definición 5.66. *Se dice que una pregeometría (X, cl) es una* ***geometría*** cuando $cl(\{a\}) = \{a\}, \forall a \in X$ y $cl(\emptyset) = \emptyset$.

Ejemplo 5.67.
Supongamos que X es un conjunto con por lo menos dos elementos, definimos $cl(\{a\}) = \{a\}$, $cl(\emptyset) = \emptyset$ y $cl(A) = \cup_{a \in A} cl(\{a\})$ cuando A no sea como los anteriores. Afirmo que es una geometría:

1. *Hay tres casos:* $A = \emptyset, \{a\}$ *o ninguno de ellos. Si* $A = \emptyset$*, notemos que* $\emptyset \subseteq \emptyset$*. Si* $A = \{a\}$*, entonces* $\{a\} \subseteq \{a\} = cl(\{a\})$*. Si* A *no cae en los otros casos:* $cl(A) = \cup_{a \in A} cl(\{a\})$ *por definición, sea* $a \in A$*, notemos que* $\{a\} \subseteq cl(\{a\})$*, así que* $A \subseteq cl(A)$*.*
2. *Si* $A = \emptyset$*, notemos que* $cl(cl(\emptyset)) = cl(\emptyset)$*. Si* $A = \{a\}$*, entonces* $cl(cl(\{a\})) = cl(\{a\})$*. Si* A *es distinto,* $cl(cl(A)) = cl(\cup_{a \in A} \{a\}) = cl(A)$
3. *Supongamos que* $a \in cl(A)$*, sólo puede pasar que* $cl(A) = \cup_{b \in A} cl(\{b\}) = \cup_{b \in A} \{b\}$*. Así que* $a \in \{b\} = cl(\{b\})$ *para algún* b *y terminamos.*
4. *Supongamos que* $a \in cl(A)$*, hay tres casos: Si* $A = \emptyset, \{a\}$*, notemos que* $cl(A) = \emptyset, \{a\}$*, entonces* $B_0 = \emptyset, \{a\}$ *funcionan.*
5. *Por definición, cumple con la propiedad de ser geometría.*

Resulta que este caso también será prototípico cuando queremos estudiar las pregeometrías.
Por otro lado, si tomamos un espacio vectorial V *se tiene* $\langle \emptyset \rangle = \{0_V\}$*, por tanto no es una geometría. Más adelante veremos cómo podemos construir una geometría de una manera bastante canónica cuando tenemos este tipo de problemas.*

Definición 5.68. *Decimos que* (X, cl) *es* ***trivial*** cuando $cl(A) = \cup_{a \in A} cl(\{a\})$ para cualquier $A \subseteq X$.

Teorema 5.69. *Si* (X, cl) *es una pregeometría, entonces existe una geometría* $\left(\overline{X}, \overline{cl}\right)$ *asociada a* (X, cl)*.*

Demostración. Como conjunto: $\overline{X} = \{cl(\{a\}) : a \in X \backslash \emptyset\}$, si $A \subseteq \overline{X}$, entonces $A = \{cl(\{a\}) : a \in A' \subseteq X\}$. Defino la operación de la siguiente forma: $\overline{cl}(A) = \{cl(\{b\}) : b \in cl(A')\}$.
$\left(\overline{X}, \overline{cl}\right)$ es una geometría:

- Supongamos $A \subseteq \overline{X}$, quiero demostrar que $A \subseteq \overline{cl}(A)$. $A = \{cl(\{a\}) : a \in A' \subseteq X\}$ pero notemos que $A' \subseteq cl(A')$, entonces si $cl(\{a\}) \in A$, entonces $cl(\{a\}) \in \overline{cl}(A)$.
- Ahora quiero demostrar que $\overline{cl}\left(\overline{cl}(A)\right) = \overline{cf}(A)$. $\overline{cl}\left(\overline{cl}(A)\right) = \left\{cl(\{a\}) : a \in cl\left(\overline{cl}(A)'\right)\right\}$. Pero $\overline{cl}(A) = \{cl(\{b\}) : b \in cl(A)\}$, entonces $\overline{cl}(A) = \{b : b \in cl(A)\} = cl(A)$. Así que $\overline{cl}\left(\overline{cl}(A)\right) = \{cl(\{a\}) : a \in cl(cl(A))\} = \{cl(\{a\}) : a \in cl(A)\} = \overline{cl}(A)$.
- Supongamos que $A \subseteq B \subseteq \overline{X}$. Reescribiendo: $A = \{cl(\{a\}) : a \in A' \subseteq X\}$ y $B = \{cl(\{b\}) : b \in B' \subseteq X\}$. Por la hipótesis, $A' \subseteq B'$. Por definición: $\overline{cl}(A) = \{cl(\{a'\}) : a' \in cl(A')\}$ y $\overline{cl}(B) = \{cl(\{b'\}) : b' \in cl(B')\}$, pero como $A' \subseteq B' \subseteq X$, entonces $cl(A') \subseteq cl(B')$. así que $\overline{cl}(A) \subseteq \overline{cl}(B)$.
- La propiedad de intercambio la omito por razones de espacio, se puede encontar en [25].
- Supongamos $cl(a) \in \overline{cl}(A) = \{cl(\{a\}) : a \in cl(A')\}$ para algún $A = \{cl(\{a\}) : a \in A' \subseteq X\}$. Como existe un $A'_0 \subseteq A'$ finito de tal forma que $a \in cl(A'_0)$, entonces hacemos $A_0 = \{cl(\{a\}) : a \in A'_0 \subseteq X\}$, el cual nuevamente es finito y $cl(a) \in \overline{cl}(A_0)$.
- Sea $cl(a) \in \overline{X}$. $\overline{cl}(\{cl(a)\}) = \{cl(\{x\}) : x \in cl(\{a\})\} = \{cl(\{a\})\}$ que es justo lo que se quería. Es inmediato que $\overline{cl}(\emptyset) = \emptyset$

□

Un ejemplo de lo anterior es el espacio proyectivo asociado a un espacio vectorial, pues la construcción consiste en tomar como «puntos» a las rectas que pasan por el origen y como $\langle \{a\} \rangle$ es el subespacio vectorial uno dimensional que contiene a a, así que estamos haciendo lo mismo.

Además nos interesarán aquellas geometrías que cumplan una propiedad parecida a la de los espacios vectoriales respecto a la dimensión:

Definición 5.70. *Consideremos una pregeometría* (X, cl)*,*

1. *Decimos que* (X, cl) *es* ***modular*** cuando para cuales quiera dos conjuntos cerrados $A, B \subseteq X$ de dimensión finita, se tenga la siguiente igualdad:

$$dim\,(A \cup B) = dim\,(A) + dim\,(B) - dim\,(A \cap B)$$

2. Decimos que (X, cl) es **localmente modular** cuando (X, cl_A) es modular para algún $A \subseteq X$.

Para que las definiciones sean consistentes se necesitan los siguientes lemas cuyas demostraciones omitiremos:

Lema 5.71. *Si* (X, cl) *es modular, entonces* (X, cl_A) *es modular* $\forall A \subseteq X$.

Lema 5.72. *Si una pregeometría* (X, cl) *es modular, entonces su geometría asociada* $\left(\overline{X}, \overline{cl}\right)$ *también es modular.*

Notemos que las geometrías triviales siempre son modulares. Por su parte los espacios vectoriales cumplen con ser modulares por la muy conocida fórmula para espacios vectoriales. Finalmente, si consideramos la localización en el cero de un espacio vectorial con la cerradura afín, está geometría es modular; así que los espacios afines son un ejemplo de pregeometrías localmente modulares.

Por otro lado, existe un ejemplo de geometrías que no son localmente modulares:

- Si K es un campo algebraicamente cerrado con grado de trascendencia infinita sobre su campo primo, entonces K con la cerradura algebraica acl no es localmente modular. Este hecho es fundamental, no incluyo su demostración porque es bastante engorrosa, se puede encontar en [22].

A manera de resumen enunciaré aquellas geometrías que son de gran relevancia para la conjetura de Zilber:

1. Sea X un conjunto, definimos $cl\,(\{a\}) = \{a\}$. Esta resulta ser una geometría trivial.
2. Si $P\,(V)$ denota la geometría asociada a la de un espacio vectorial V; tenemos una geometría modular.
3. Si K es un campo algebraicamente cerrado, esta geometría no es localmente modular.

Notemos que todos estos ejemplos son conjuntos fuertemente minimales.

Existe una buena clasificación de las estructuras de geometrías triviales y modulares:

- Respecto a las geometrías triviales es fácil demostrar que todas coinciden con un estructuras de un lenguaje trivial.
- Zilber demostró que es posible identificar las geometrías modulares por espacios proyectivos sobre un anillo con división.
- Hasta 1988 no se conocían otros ejemplos geometrías no localmente modulares y fuertemente minimales más allá de los campos algebraicamente cerrados. Debido a la importancia antes mencionada sobre conocer a los conjuntos fuertemente minimales, Zilber conjeturó lo siguiente:

  Conjectura. *Si* X *es un conjunto fuertemente minimal que no es localmente modular, entonces* X *interpreta (en el sentido que ya definimos en la sección 3) a un campo algebraicamente cerrado.*

La conjetura es falsa en general, y los contraejemplos los dio Hrushovski. De hecho construyó contraejemplos en los que ni siquiera es posible interpretar un grupo.

Sin embargo, la conjetura no está muy alejada de ser verdad pues existen clases muy grandes de conjuntos fuertemente minimales donde la conjetura es cierta. En este trabajo hablaremos de una de ellas, que es la de las Geometrías de Zariski. Es notable el hecho que para que la conjetura sea cierta se necesitan condiciones topológicas sobre las estructuras. El hecho de que esta conjetura sea cierta para las geometrías de Zariski será absolutamente clave en la demostración de Mordell-Lang.

5.6. Uno-basado. Si bien la conjetura de Zilber (por su profundidad) para las geometrías de Zariski será el teorema más importante que utilizaremos en la demostración de Mordell-Lang, existe un concepto de la Teoría de la estabilidad que coincide con una de las hipótesis de Mordell-Lang. Este concepto es el de ser uno-basado. Así que podemos adelantar una idea de la demostración: siempre podremos suponer que la teoría en la que desarrollaremos la demostración no es uno basada. Por otro lado, no ser uno-basado coincidirá (en nuestro caso) con no ser localmente modular, así que con esta traducción podremos aplicar la conjetura de Zilber para geometrías de Zariski.

Hay dos maneras de motivar la defincón de ser uno-basado. Una de ellas es bastante bonita pues involucra geometría. Supongamos una curva C definida sobre un campo algebráicamente cerrado. Dado un punto $p \in C$, ¿es posible recuperar la curva C (i.e. las ecuaciones que la definen) mediante las coordenadas de p? Esto núnca es posible para campos algebráicamente cerrados, por eso diremos que los campos algebraicamente cerrados no son uno-basados. Ver [28].

La otra forma de motivar la definición es en términos de la teoría de estabilidad, vamos a demostrar una propiedad que « ser uno-basado » generaliza y que además tienen todas las pregeometrías:

Proposición 5.73. *Si (X, cl) es una pregeometría con $A, B \subseteq X$ entonces ser localmente modular es equivalente a que A y B son independientes sobre $A \cap B$.*

Para demostrarlo utilizaré los siguientes lemas cuyas demostraciones se encunetran en [4]:

Lema 5.74. *Sea (X, cl) una pregeometría con $A, B \subseteq X$, si $dim(A), dim(B) < \infty$ entonces la dimensión es aditiva:*

$$dim(A \cup B) = dim(A/B) + dim(B)$$

Lema 5.75. *Sea (X, cl) una pregeometría con $A, B \subseteq X$, si $dim(A), dim(B) < \infty$ entonces $dim(A \backslash B) = dim(A) - dim(B)$*

Demostración. Demostración de la proposición 5.73. Si $dim(A) = \infty$ o $dim(B) = \infty$ entonces la ecuación de ser localmente modular es cierta. Así que podemos suponer que sus dimensiones son finitas. Por el primero de los lemas anteriores tenemos que $dim(A \cup B) = dim(A/B) + dim(B)$. Recordando la definición **??**, A, B son independientes sobre $A \cap B$ si y sólo si $dim(A/B) = dim(A/A \cap B)$ (pues $dim(A)$ es finita), así que usando esas dos cosas, A, B son independientes sobre $A \cap B$ si y sólo si:

$dim(A \cup B) = dim(A/A \cap B) + dim(B)$, pero usando el segundo de los lemas obtenemos que $dim(A \cup B) = dim(A) - dim(A \cap B) + dim(B)$ que es lo que queríamos. □

Así que buscando el análogo a la modularidad, tiene sentido preguntarnos por una generalización de este concepto para teorías:

Definición 5.76. *Sea T una teoría ω-estable, T es **uno-basada*** si para toda $C \models T$ se cumple lo siguiente en C^{eq}: Cualesquiera dos conjuntos acl^{eq}-cerrados A y B son independientes sobre $A \cap B$.

Un modelo M es uno-basado cuando $Teo(M)$ sea uno-basada.

El siguiente lema nos da una equivalencia en términos de tipos y bases canónicas:

Lema 5.77. *C es uno-basado si y sólo si la base canónica de cualquier tipo estacionario $tp(a/B)$ es algebraica sobre a.*

Demostración. $\Rightarrow$: Sean $a \in C^{eq}$, $B \subseteq C^{eq}$. Definimos a $A = acl^{eq}(a)$, entonces A es acl^{eq}-cerrado. Como $tp(a/acl^{eq}(B))$ no separa sobre B, entonces podemos suponer sin pérdida de generalidad que $B = acl^{eq}(B)$. Notemos que $a \in acl^{eq}(A)$. Como estamos suponiendo que C es uno-basado, entonces $A \underset{A\cap B}{\downarrow} B$. En particular tenemos que $a \underset{A\cap B}{\downarrow} B$, y por el teorema 5.43, entonces $cb(tp(a/B)) \subseteq A \cap B \subseteq A = acl^{eq}(a)$.

$\Leftarrow$:Sean $A, B \subseteq C^{eq}$ tales que $A = acl^{eq}(A), B = acl^{eq}(B), a \in A$. Recordemos que para cualquier teoría ω-estable, $cb(tp(a/B)) \subseteq acl^{eq}(B) = B$, entonces como estamos suponiendo que $cb(tp(a/B)) \subseteq acl^{eq}(a)$ y por otro lado $acl^{eq}(a) \subseteq A$, entonces $cb(tp(a/B)) \subseteq A \cap B$, y por 5.43, tenemos que $tp(a/B)$ no separa sobre $A \cap B$. Como nos tomamos a arbitrario, entonces tenemos que $A \underset{A\cap B}{\downarrow} B$, que es lo que queríamos.

□

El siguiente teorema es el más importante de esta sección, su demostración se encuentra en [12]. Es importante mencionar que nuestra definición de ser uno-basado es para la teoría de un modelo, mientras que la de localmente modular es para una estructura dada. El siguiente teorema no se sigue de la proposición 5.73 porque la definición de ser uno-basado involucra a C^{eq}.

Teorema 5.78. *Si C es un conjunto fuertemente minimal, entonces C es localmente modular si y sólo si C es uno-basado.*

La relevancia de este teorema en Mordell-Lang es que en la sección 7.3 vamos a dar una equivalencia entre una hipótesis de Mordell-Lang y no ser uno-basado. Como trabajaremos sobre un conjunto fuertemente minimal B entonces siempre podemos suponer (porque es una hipótesis de Mordell-Lang) que nuestra teoría no es uno basada, así que por el teorema anterior obtendremos que B no es localmente modular. Como para B se cumplirá la conjetura de tricotomía de Zilber entonces B interpreta a un campo algebraicamente cerrado que coincidirá con el campo que estemos usando en Mordell-Lang.

Aunque no dimos la demostración del teorema 5.78 sí vamos a demostrar el tercero de los siguientes lemas. Éste se usará directamente en la prueba de Mordell-Lang y su demostración es muy parecida a la del teorema 5.78. La demostración de los dos primeros lemas es bastante sencilla y se puede encontrar en [44].

Lema 5.79. ***Interalgebraicos.***

Sea M una estructura con $H, B \subseteq M^n$. Supongamos que $H \subseteq acl(B)$ con B fuertemente minimal. Para cada $h \in H$ existen elementos independientes $a_1, \ldots a_m, b_1, \ldots, b_n \in M$, de tal forma que h es independiente de $a_1, \ldots, a_m$ y además $acl(b_1, \ldots, b_n, a_1, \ldots, a_m) = acl(h, a_1, \ldots, a_n)$. Cuando pasa esto decimos que a y $b_1, \ldots, b_n$ son interalgebraicos.

Lema 5.80. *Sean p y q dos tipos. Si p es una extensión de q que no separa, entonces sus bases canónicas son iguales.*

Sus demostraciónes se pueden encontrar en [4].

Lema 5.81. *Sea T una teoría con eliminación de imaginarios, $M \models T$ y $H, B \subseteq M^n$. Si $H \subseteq acl(B)$ con B uno-basado entonces H también es uno-basado.*

Recordemos que $B \subseteq acl(B)$, así que este lema nos dice algo aún más fuerte que lo siguiente: la propiedad de ser uno-basado se mantiene cuando tomamos elementos algebraicos, para ver esto supongamos $H = alc(B)$.

Demostración. Primero notemos que como la teoría tiene eliminación de imaginarios, entonces puedo considerar $acl = acl^{eq}$.

Para demostrar que H es uno-basado, voy a utilizar la equivalencia de ser uno-basado dada por el lema 5.77, i.e. quiero demostrar que si $c \in H^n$ y $F \subseteq H$ con $acl(F) = F$ entonces $cb(tp(c/F)) \in acl(c)$.

La primera afirmación es que es posible considerar a F de tal forma que $F \cup c \bigcup A$. Esto es porque...

Así que en particular $tp(c/F \cup A)$ es una extensión de $tp(c/F)$ que no separa, y por el lema 5.80 las bases canónicas de estos dos tipos son iguales. Guardemos esta observación.

Por el lema 5.79, existe un $b \subseteq B$ acl-independiente y finito de tal forma que b y c son interalgebraicos sobre un A (cuya existencia también la postula el lema) finito. Además es cierto que $A \underset{\emptyset}{\downarrow} c$.

Como estamos suponiendo que B es uno-basado, si tomamos $A \cup b, F \cup A \subseteq B$, entonces $A \cup b \underset{acl(A \cup b) \cap (F \cup A)}{\downarrow} F \cup A$. Pero además tenemos que $c \subseteq A \cup b$, entonces por monotonía: $c \underset{acl(A \cup b) \cap (F \cup A)}{\downarrow} F \cup A$. Si llamamos $e = cb(tp(c/F))$, entonces por el lema 5.43 tenemos que $e \subseteq acl(b \cup A) \cap (F \cup A) \subseteq acl(b \cup A)$. Pero como b y c son interalgebraicos sobre A, entonces $e \subseteq acl(c \cup A)$.

Por otro lado, como $A \subseteq acl(A \cup b)$, entonces $acl(A \cup b) \cap (F \cup A) = acl(A \cup b) \cap F$. Como ya habíamos dicho que e también es una base canónica para $tp(c/F)$, entonces usando nuevamente el lema 5.43, tenemos que $e \subseteq acl(A \cup b) \cap F \subseteq F$. Así que $e \subseteq F$.

Al principio de la demostración dijimos que era posible considerar $F \cup c \bigcup A$, eso implica que (transitividad) $F \underset{c}{\downarrow} A$, pero porque $e \subseteq F$ y por la monotonía de la independencia, entonces $e \underset{c}{\downarrow} A$.

Para terminar, recordemos que ya habíamos probado en 5.51 que para los conjuntos fuertemente minimales, entonces $e \underset{c}{\downarrow} A \Leftrightarrow e \in acl(c) \vee e \notin (c \cup A)$. Pero como en este caso tenemos que $e \subseteq acl(c \cup A)$, entonces $e \subseteq acl(c)$ que es lo que se quería. □

El estudio de los grupos uno-basados es muy interesante, el siguiente teorema sobre ellos se utilizará para demostrar Mordell-Lang.

Teorema 5.82. *Sea M una estructura. Supongamos que $G \subseteq M$ es un grupo uno-basado definido sobre F_0.*

- *Sea $H \leq G$ un subgrupo conectado y definible, entonces si c es la base canónica de H, se tiene que $c \in acl(F_0)$.*
- *Supongamos $p \in S(G)$ y denotemos $X = p(M)$. Si G actúa en M, entonces existe $a \in G$ de tal forma que $X = a + \{g \in G : g + X \subseteq X\}$.*

Su demostración se encuentra en [14].

Nota.
- *El primer inciso nos dice que H es definible sobre $acl(F_0)$ por el lema 4.16 y porque $dcl \subseteq acl$.*
- *El misterioso conjunto $\{g \in G : g + X \subseteq X\}$ se llamará el estabilizador. Pensemos en M como una variedad abeliana, G un subgrupo de puntos racionales y X un subconjunto de puntos racionales. Incluso existe una manera natural de hacer actuar a un grupo de la estructura en $S_n(G)$, ver* [14].

5.7. Ortogonalidad. Ahora definiremos la ortogonalidad entre un par de subconjuntos definibles, para dar una idea de lo que se trata: cuando nuestros conjuntos definibles sean variedades algebraicas nunca dos de ellos serán ortogonales.

Definición 5.83. *Decimos que dos conjuntos definibles $\mathbb{D}$,$\mathbb{E}$ son **ortogonales*** cuando $\forall n, m \in \mathbb{N}$, todo conjunto definible $X \subseteq \mathbb{D}^n \times \mathbb{E}^m$ es unión finita de conjuntos de la forma $X_1 \times X_2$ con X_i definibles en $\mathbb{D}$ y $\mathbb{E}$ respectivamente. Denotamos la relación de ortogonalidad como $\mathbb{D} \perp \mathbb{E}$.

Notemos que esto no es cierto para dos conjuntos algebráicos A, B pues la topología de Zariski de $A \times B$ extiende (propiamente) al producto de las topologías en A y B.

Una observación inmediata es que si $\mathbb{F} \subseteq \mathbb{D}$, y $\mathbb{D}$ es ortogonal con $\mathbb{E}$, entonces $\mathbb{F}$ es ortogonal con $\mathbb{D}$. Nuestra definición es muy intuitiva sin embargo es poco útil, existe una equivalencia en términos de la teoría de estabilidad que hemos venido utilizando:

Proposición 5.84. *Supongamos que T es ω-estable, $M \models T$ una estructura. Dos clases $\mathbb{D}$,$\mathbb{E}$ definibles (posiblemente con parámetros) son ortogonales si y sólo si para cualquier conjunto de parámetros A sobre el cual $\mathbb{D}$ y $\mathbb{E}$ se definen y todos los $d \in \mathbb{D}$,$e \in \mathbb{E}$ se tiene $d \underset{A}{\perp} e$.*

La demostración se encuentra en [45].

Cuando uno de los conjuntos es fuertemente minimal, la definición se reduce bastante. Ésta será la equivalencia de ortogonalidad que usaremos en la demostración de Mordell-Lang.

Lema 5.85. *Supongamos que D es fuertemente minimal. $D \not\perp E$ si y sólo si $D \subset acl(A \cup E)$ para algún conjunto finito de parámetros A sobre el que se definen E y D.*

Demostración. Supongamos $D \subset acl(A \cup E)$ con A finito. Como A es un conjunto finito de parámetros es posible tomar un $d \in D \backslash acl(A)$ (si es necesario se agregan algunos de esos parámetros al lenguaje y D seguirá siendo fuertemente minimal por definición). Luego consideremos un conjunto mínimo $\{e_1, \ldots, e_n\} \subseteq E$ de tal forma que $d \in acl(A \cup \{e_1, \ldots, e_n\})$. Por el lema 5.51 tenemos que $d \underset{\{e_1,\ldots,e_{n-1}\}}{\not\perp} e_n$ que es lo que se quería.

Ahora supongamos que $d \underset{A}{\not\perp} e$ para algunos $d \in D$ y $e \in E$ y A sobre el cual D y E se definen. Nuevamente usando el lema 5.51 obtenemos que $d \in acl(A \cup e) \backslash acl(A)$. Pero en [13] se puede ver que para cualesquiera dos elementos $d, d \in D \backslash acl(A)$ se tiene que $tp(d/A) = tp(d'/A)$, así que usando lo anterior tenemos que para cualquier $d \in D \backslash acl(A)$ se tiene que $d \in acl(A \cup e) \subseteq acl(A \cup E)$, es decir: $D \backslash acl(A) \subseteq acl(A \cup E)$. Pero por otro lado es claro que $acl(A) \subseteq acl(A \cup E)$, así que $D \subseteq acl(A \cup E)$ como se quería.

□

Otro lema muy importante es el siguiente:

Lema 5.86. *Para conjuntos fuertemente minimales, la no-ortogonalidad es una relación de equivalencia.*

Demostración. Sean D, E fuertemente minimales.

- Ya sabíamos que $D \subseteq acl(D)$, así que $D \not\perp D$ por el lema anterior.
- Por la simetría de la independencia se sigue de inmediato que si $D \not\perp E$, entonces $E \not\perp D$.
- Para la transitividad recomiendo checar [13].

□

Respecto a la ortogonalidad los siguientes resultados son los más importantes que veremos. El siguiente teorema es una de las consecuencias de la dicotomía de Zilber que se utilizarán para Mordell-Lang, por eso debemos considerarlo como una piedras angular. El lema en cambio es más técnico. Sus demostraciones se pueden encontrar en [13].

Teorema 5.87. *Lo siguiente ocurre en T^{eq}. Un grupo abeliano infinito $\mathbb{G}$ que sea casi fuertemente minimal es ortogonal a una clase definible $\mathbb{E}$ si y sólo si existe un grupo definible $\mathbb{H} \subseteq dcl^{eq}(\mathbb{E})$ y un homomorfismo definible y suprayectivo $h : \mathbb{G} \longrightarrow \mathbb{H}$ con kernel finito.*

Lema 5.88. *Supongamos que G es un grupo abeliano tal que $G \subseteq D$ con D fuertemente minimal. E una clase definible cualquiera. Si $H \subseteq acl^{eq}(E)$, entonces $G \perp E \Rightarrow D \perp H$.*

5.8. Grupos y el rango de Morley. Esta sección tendrá relevancia directa en la demostración de Mordell-Lang. Debido a que es bastante técnica y a que es difícil no considerar aisladas a las proposiciones que enunciaremos, recomendamos al lector afrontar su lectura tan sólo como un conjunto de aplicaciones del rango de Morley.

Lo aquí expuesto se enmarca en el análisis de las propiedades de los grupos que tienen rango de Morley finito y son ω-estables. Éste es un tema de suma importancia dentro de la teoría de modelos, la investigación comenzó aproximadamente en 1970 cuando Boris Zilber introdujo técnicas de Shelah (que éste a su vez utilizó para su programa de clasificación) en el análisis de propiedades algebraicas de los grupos. Es un hecho notable que los resultados de Zilber de esa época fueron los que lo motivaron la formulación su conjetura de tricotomía. Recientemente Hrushovski encontró aplicaciones del trabajo de Zilber a la combinatoria aditiva. Incluyo la siguiente conjetura de Zilber y Cherlin como uno de los problemas más importantes respecto a los grupos con rango de Morley finito a pesar de que no tiene relevancia alguna en la demostración de Mordell-Lang.

Conjectura. *Si G es un grupo con rango de Morley finito que además es divisible, entonces G es un grupo algebraico sobre un campo algebraicamente cerrado.*

Comenzamos suponiendo que G es un grupo tal que $Teo(G)$ es ω-estable.

Lema 5.89. *Supongamos que H es un subgrupo definible de G. Entonces $\forall a \in G$, se tiene que $RM(aH) = RM(Ha) = RM(H)$.*

Demostración. Usando el teorema 5.30 y porque existen biyecciones definibles entre H y aH, y entre H y Ha, se tiene el resultado. □

Como corolarios inmediatos tenemos que:

Corolario 5.90. *Supongamos que $H \subseteq H'$ son subgrupos definibles de G. Si $RM(H') = RM(H)$, entonces $[H', H]$ es finito.*

Corolario 5.91. *No existe una secuencia infinita, descendiente y propia de subgrupos definibles.*

Este corolario motiva la siguiente definición:

Definición 5.92. *Decimos que G es **conectado*** si no tiene subgrupos definibles propios con índice finito.

La equivalencia fundamental de este concepto es la siguiente:

Lema 5.93. *G está conectado si y sólo si tiene rango de Morley igual a uno.*

La demostración de este hecho se puede encontrar en [14].

Definición 5.94. *Sea G un grupo y X un subconjunto definible de G. Decimos que X es **indescomponible*** si para cada subgrupo $H \subseteq G$ que sea definible, el conjunto $\{xH : x \in X\}$ es infinito o tiene un sólo elemento.

Lema 5.95. *Si X es el conjunto de realizaciones de un tipo estacionario, entonces X es indescomponible.*

Este lema se usa en Mordell-Lang, su demostración de puede encontrar en [25].

Teorema 5.96. ***El teorema de Indescomponibilidad de Zilber.*** Sea $(X_i : i \in I)$ un conjunto de subconjuntos definibles e indescomponibles de G. Supongamos que cada uno de ellos contiene a la identidad $e \in G$. Entonces el grupo H generado por $\cup_{i \in I} X_i$ es definible y conectable.

Concluimos la sección de estabilidad con un importante teorema sobre los grupos con Rango de Morley finito que además son ω-estables. Este teorema se utilizará en la demostración de Mordell-Lang.

Teorema 5.97. *Si H es un grupo ω-estable con rango de Morley finito, entonces existe un subgrupo $G \subseteq H$ de tal forma que:*

- *G es conectable, existe un F finito de tal forma que $G \subseteq acl\,(F \cup Y_1 \cup \ldots \cup Y_n)$ con Y_i fuertemente minimal, δ-definible y G es máximo con esas propiedades.*
- *$G = G_1 + \ldots + G_k$ donde cada G_i es casi fuertemente minimal, conectable, δ-definible subgrupo de G y los $G_{i's}$ son ortogonales en parejas.*

Para su demostración usaremos dos proposiciones cuya demostración se puede encontrar en [14].

Demostración. Demostración del teorema 5.97. Notemos que siempre existe $X \subseteq H$ fuertemente minimal porque G es ω estable. Denotamos por B_X al conjunto que contiene a todos los $B \leq G$ concectados y tales que existra un F finito con $B \subseteq acl\,(F \cup X)$. Si B_X tiene un único elemento maximal, lo denotaremos también por B_X. B_X no es vacío por la siguiente proposición:

Proposición 5.98. *Sea H un grupo con Rango de Morley finito. Si $X \subseteq H$ es fuertemente minimal, entonces existe un subgrupo $F \subseteq H$ de tal forma que $F \subseteq acl\,(X)$.*

Como el rango de Morley de H es finito, entonces existe un elemento en B_X con rango de Morley maximal. De hecho es único: Sean B_1,B_2 elementos en B_X, entonces el subgrupo generado por $B_1 \cup B_2$ también está en B_X. Así que B_X tiene un único elemento maximal. Abusando de la notación lo denotaremos por B_X.

Ahora consideremos B la clase de subgrupos $G \leq H$ conectados, de tal forma que existan $X_1, \ldots, X_n$ conjuntos fuetemente minimales con $G \subseteq acl\,(X_1 \cup \ldots \cup X_n \cup F)$

con F finito. Es inmediato que B contiene a B_X para todo X fuertemente minimal. Nuevamente B tiene un único elemento maximal al que denotaremos por G.

Para finalizar la demostración el siguiente teorema nos dice cómo se descompone G.

Proposición 5.99. *Sea H un grupo con Rango de Morley finito. Si $G \leq H$ es maximal, conectado y $G \subseteq acl(F \cup, Y_1, \ldots, Y_m)$ para F finito y $Y_{i's}$ fuertemente minimales. Entonces existen conjuntos fuertemente minimales $X_1, X_2, \ldots, X_n$ de tal forma $G = B_{X_1} + \ldots B_{X_n}$ (aquí B_{X_i} denota al elemento maximal de la familia, en la demostración del teorema 5.97 veremos porqué exixte). Más aún los $X_{i's}$ son ortogonales a pares.*

□

6. GEOMETRÍAS DE ZARISKI

Las geometrías de Zariski fueron introducidas por Boris Zilber y Ehud Hrushovski en [46], su importancia radica en que resuelven dos problemas fundamentales: por un lado dan una generalización de la topología de Zariski por medio de axiomas que no involucran en lo absoluto a un campo algebraicamente cerrado. A saber, para una estructura que tenga una topología, nos dan axiomas geométricos que únicamente involucren el concepto de dimensión (notemos que esto es muy abstracto pues hay muchas formas de darle dimensión a objetos geométricos) y obtendremos una topología que se comporta muy parecida a la topología de Zariski en la geometría algebraica. Cuando la estructura sea un campo, la topología que se obtiene como geometría de Zariski coincide con la topología de Zariski.

Por el otro lado, las geometrías de Zariski nos dan ejemplos (vastísimos) de conjuntos fuertemente minimales donde la conjetura de tricotomía de Zilber es cierta. Eso quiere decir que con los axiomas topológicos y de dimensión que incluimos sobre la estructura, podemos interpretar (ver la sección 3) un campo algebraicamente cerrado. Las consecuencias de que esto sea cierto para variedades algebraicas es el eje fundamental en la demostración de la conjetura de Mordell-Lang.

6.1. Estructuras topológicas. En esta primera sección hablaremos de las condiciones topológicas que le pedimos a una estructura para ser una geometría de Zariski sin considerar su interacción con la dimensión.

Definición 6.1. *Consideremos una estructura M con un lenguaje L. Sea $C \subseteq \cup_n Def_{M^n}$, a los elementos de C les llamaremos* ***cerrados*** . Las relaciones que definen los cerrados serán las relaciones primitivas de nuestro lenguaje. (M, C) es una **estructura topológica** si se cumple lo siguiente:

- La intersección arbitraria de cerrados es cerrada.
- La unión finita de cerrados es cerrada.
- M es cerrada y $\emptyset$ es cerrado.
- La gráfica de la diagonal es cerrada.
- Si $m \in M$, entonces $\{m\} \in C$ (los puntos son cerrados).
- Si $A, B \in C \Rightarrow A \times B \in C$.
- La imagen de un cerrado bajo la permutación de coordenadas es cerrada.
- Si $a \in M^k$, $S \in C$ con $S \subseteq M^{k+l}$, de tal forma que S está definido por la fórmula $S(\bar{x}, \bar{y})$, entonces $S\left(a, M^l\right) \in C$. A $S\left(a, M^l\right)$ se le llama la fibra sobre a.

Observacion. *Si definimos $pr_{i_1,i_2,\ldots,i_m} : (x_1, x_2, \ldots, x_n) \longmapsto (x_{i_1}, x_{i_2}, \ldots x_{i_m})$ con $i_1, i_2, \ldots, i_m \in \{1, 2, \ldots, n\}$ como las proyecciones, entonces $pr_{i_1,i_2,\ldots,i_m}$ son continuas. Lo anterior es porque si $S \subseteq_{cr} M^m$ (S es cerrado en la topología inducida en M^m), $pr^{-1}_{i_1,i_2,\ldots,i_m}(S) = S \times M^{n-m}$ salvo un reordenamiento de las coordenadas. Pero uno de nuestros axiomas dice que M es cerrado y como el producto finito de cerrados es cerrado, $S \times M^{n-m}$ lo es.*

Lo anterior implica que la topología de M^{n+m} extiende a la topología producto de $M^n \times M^m$ pues esta última es por definición la más gruesa (con menos cerrados) que hace continua a las proyecciones.

Recordando que los cerrados C en M son un subconjunto de los definibles en el lenguaje de M definimos otra estructura sobre (M, C). Al lenguaje L de M, le agregamos un símbolo al que denotaremos por S para cada cerrado $S \in C$, a este nuevo lenguaje le llamaremos L_M. El universo de nuestra estructura seguirá siendo M.

A las combinaciones booleanas de elementos en C le llamaremos **constructibles** .

A la unión finita de elementos de la forma $pr_{i_1,i_2,\ldots,i_m}(S)$ con S constructible se le llama **proyectivo** .

Una estructura topológica M se dice **completa** cuando $pr_{i_1,i_2,\ldots,i_m}(S)$ es cerrado con $S \in C$. Esto se traducirá en eliminación de cuantificadores.

Una estructura topológica M es **cuasi compacta** cuando es completa y además cumple que: para toda familia finitamente consistente de cerrados $\{c_t : t \in T\}$ entonces $\cap_{t\in T} c_t$ es no vacía.

Observacion. *Notemos que lo anterior es equivalente a decir que cada cubierta abierta de M contiene una subcubierta finita.*

Demostración. Primero demostraré: lo anterior implica que M sea cuasi compacta. Sea una familia $\{c_t : t \in T\}$ de cerrados finitamente consistente. Por el teorema de completud, quiere decir que esta familia es finitamente satisfacible. Supongamos por contradicción que $\cap c_t \subseteq \emptyset$. Eso implica que $M \subseteq \cup c_t^c$ donde c_t^c denota al complemento de c_t, eso quiere decir que $\cup c_t^c$ es una cubierta abierta de M. Por nuestra hipótesis, existe un número finito de c_t^c's de tal forma que $M \subseteq c_1^c \cup, \ldots, \cup c_n^c$. Eso significa que $\cap_{j=1}^n c_j \subset \emptyset$ lo cual contradice que nuestra familia sea finitamente satisfacible.

Para la otra implicación, sea $M \subseteq \cup_{t\in T} U_t$ una cubierta abierta. Eso significa que $\cap_{t\in T} U_t^c \subseteq \emptyset$. Por el teorema de compacidad: $\cap_j^n U_j^c \subseteq \emptyset \ \forall n$. Entonces $M \subset \cup_{j=1}^n U_j$ para alguna n. Que es lo que queríamos. □

Definición 6.2. *Se dice que un espacio topológico es **noetheriano*** cuando toda cadena descendiente de cerrados $\ldots \subset S_2 \subset S_1 \subset S_0$ se estabiliza. Cuando una estructura topológica cumple esa condición se le llama una **estructura topológica noetheriana.**

Definición 6.3. *Los conjuntos **definibles irreducibles*** son aquellos subconjuntos definibles que no se pueden expresar como unión de dos cerrados propios. En [6] se puede ver una demostración del siguiente hecho:

Proposición 6.4. *En un espacio topológico noetheriano cualquier cerrado S se puede expresar únicamente como $S = S_1 \cup \ldots S_m$ con S_i irreducibles, cerrados y propios. A estos subconjuntos se les llama los componentes irreducibles.*

Definición 6.5. *Supongamos que X es un espacio topológico noetheriano. Definimos una **dimensión*** para todo $C \subseteq X$ que sea cerrado, irreducible y no vacío. Lo haremos inductivamente.

1. Si $C = \{a\}$, entonces $dim\,(C) = 0$.
2. $dim\,(C) = sup\,\{dim\,(F) + 1 : F \subset C\}$ donde tomamos a esos F que sean irreducibles, cerrados y no vacíos.

Cuando C sea cerrado, entonces definimos $dim\,(C)$ como el máximo de las dimensiones de sus componentes irreducibles.

Debido a la definición de noetheriano y a la proposición anterior, esta definición siempre nos da a un número natural.

Por último, supongamos que un conjunto $S \in C$ está definido por la fórmula $S\,(x, y)$. El conjunto definido por $\forall x S\,(x, y)$ también define un cerrado. Sea $\forall S$ el conjunto definible dado por la fórmula $\forall x S\,(x, y)$. Notemos que $\forall S = \cap_{m\in M} S\,(m, M)$. Pero la fibra $S\,(m, M)$ es cerrada , mientras que la intersección de cerrados también lo es. Así que $\forall S$ es un cerrado.

6.2. Geometrías de Zariski. Ahora daremos la axiomatización de las deometrías de Zariski noetherianas unidimensionales. Como ya dijimos antes, estos axiomas hablan de la interacción entre la topología y alguna noción de dimensión que se pueda definir en la estructura. Debido a que dentro de nuestras hipótesis estará considerar estructuras noetherianas, entonces la noción de dimensión que utilizaremos es la de la definición 6.5, sin embargo para geometrías de Zariski más generales es posible omitir la hipótesis de noetherianidad y la conjetura de tricotomía de Zilber aún será cierta.

A pesar de que incluiremos algunas demostraciones para ilustrar cómo consideraciones topológicas, nos dan información de teoría de modelos, me disculpo de antemano por la gran cantidad de demostraciones que me ahorraré. Recomiendo consultarlas en [6].

Definición 6.6. *Si M es una estructura topológica noetheriana, M es una* ***geometría de Zariski unidimensional*** cuando se cumplan los siguientes axiomas:

- Eliminación de cuantificadores débil (Z1). Si $C \subseteq D^n$ es cerrado e irreducible y $\pi : D^n \longrightarrow D^m$ es una proyección, entonces existe un subconjunto cerrado $F \subset \overline{\pi(C)}$ de tal forma que $\overline{\pi(C)} \backslash F \subseteq \pi(C)$.
- Unidimensionalidad uniforme (Z2). Supongamos que $C \subseteq D^n \times D$ es cerrado e irreducible. Para $a \in D^n$, sea $C(a) = \{x \in D : (a, x) \in C\}$. Entonces $C(a) = M$ o existe un natural N de tal forma $|C(a)| \leq N$.
- Axioma de la dimensión (Z3). Sea $C \subseteq D^n$ cerrado e irreducible. Para todo $W \subseteq \Delta^n_{i,j} \cap C$ irreducible y no vacío se tiene que $dim(C) - 1 \leq dim(W)$.

A primera vista estos axiomas nos pueden parecer un poco extraños, sin embargo son más naturales de lo que parecen:

1. Notemos que $Z1$ es una forma débil de completud (o eliminación de cuantificadores).
2. $Z2$ nos dice que todo subconjunto propio y cerrado de D será finito. Esto es una forma débil de ser un subconjunto fuertemente minimal, es débil pues no todo definible tiene que ser cerrado sino podría ser combinaciones booleanas de cerrados.
3. Para tratar de entender $Z3$ pensemos en C como una curva. Las diagonales las podemos pensar como rectas que «agotan» las posibles posiciones del espacio donde vive C (por ejemplo, el espacio vectorial generado por las diagonales en $\mathbb{R}^m$ tiene dimensión n). Como las diagonales «agotan» el espacio, la intersección de una diagonal con C representa elegir un punto «genérico» (de los que «hay más») de C. Por otro lado veremos a los W como los espacios tangentes en alguno de esos puntos genéricos. Después de tanta imaginación, $(Z3)$ nos dice que el espacio tangente a la mayoría de los puntos en una «curva de Zariski» tiene dimensión mayor o igual a la de la curva menos uno. Lo que quiere decir es que la curva es «genéricamente lisa». Esta propiedad es fundamental para las geometrías de Zariski.

Con estos axiomas es posible demostrar propiedades sencillas (pero deseables) de las geometrías de Zariski uno dimensionales:

Proposición 6.7. *Sea D una geometría de Zariski uno dimensional, entonces:*

1. *D^k es irreducible $\forall k \in \mathbb{N}$.*
2. *Si $S_1 \subseteq M^k$, $S_2 \subseteq M^l$ son irreducibles entonces $S_1 \times S_2$ es irreducible.*
3. *Bajo las hipótesis anteriores: $dim(S_1 \times S_2) = dim(S_1) + dim(S_2)$.*

Demostración. Sólo demostraré la primera de las propiedades, el resto se pueden encontrar en [6]. Haré su demostración por inducción. Por $Z2$, D es irreducible. Supongamos ahora

que $S_1 \cup S_2 = M^{k+1}$ con S_1, S_2 cerrados. Defino a

$$S_i' = \left\{a \in M^k : a, x \in S_i \forall x \in M\right\}$$

Es cierto que S_i' son cerrados, pues son la intersección de fibras de conjuntos cerrados (las cuales son cerradas).

Por otro lado, para cada $a \in M^k$ tenemos que $S_1(a) \cup S_2(a) = M$, pero como M es irreducible, sin pérdida de generalidad podemos suponer que $S_1(a) = M$. Pero eso quiere decir que $S_1' \cup S_2' = M^k$, y por hipótesis de inducción obtenemos que $S_i' = M^k$ para alguna i. Así que $S_i = M^{k+1}$ para alguna i. □

Las siguiente propiedad es menos básica que las anteriores. Boris Zilber le llama «prelisidad» (pre-smoothness en inglés), su nombre viene del hecho que generaliza a $(Z3)$. Es una condición clave para poder demostrar la conjetura de tricotomía.

Proposición 6.8. *Sean $S_1, S_2 \subseteq M^k$ irreducibles y cerrados con $dim(S_i) = d_i$. Si W es cualquier componente irreducible de $S_1 \cap S_2$ entonces $dim(W) \geq d_1 + d_2 - k$.*

Su demostración se puede encontrar en [6].

La siguiente proposición justifica el nombre de las geometrías de Zariski:

Proposición 6.9. *Sea C una curva lisa y proyectiva sobre un campo algebraicamente cerrado, entonces C como estructura topológica con la topología de Zariski para cada D^n, es una geometría de Zariski.*

Demostración. $Z1$ es cierta porque como C es proyectiva entonces C es completa[11] con lo cuál si tomamos a $F = \emptyset$ terminamos. Por la eliminación de cuantificadores para los campos algebraicamente cerrados $Z1$ es cierta incluso cuando C es cuasi-proyectiva.

$Z2$ se sigue de que cualquier definible en C es finito o cofinito.

$Z3$ (de hecho su generalización, es decir la proposición 6.8) es un teorema de geometría algebraica que se puede encontrar en [18]. □

Es importante mencionar que la condición de lisidad sobre la curva C es indispensable para que sea una geometría de Zariski en el sentido de nuestra definición. Esto contrasta con lo que habíamos dicho anteriormente de que toda variedad algebraica es una geometría de Zariski. Para que toda variedad algebraica sea una geometría de Zariski es necesario cambiar un poco la definición, lo cual no haremos en este trabajo, sin embargo es posible encontrarlo en [6].

Cuando hablamos de los cerrados en las estructuras topológicas los consideramos como un subconjunto de los definibles (con parámetros) de tal forma que fueran cerrados bajo algunos criterios. Pero en nuestra definición de estructura, un conjunto definible está dado por el conjunto de elementos de una estructura que satisfacen una fórmula, así que en realidad es posible pensar en los cerrados como fórmulas en el lenguaje L_D (el lenguaje inicial L junto a un símbolo para cada cerrado en D). De hecho no sólo los cerrados, sino también los constructibles y las proyecciones de combinaciones booleanas: los elementos que satisfacen $\exists x \phi(x, y)$ se pueden ver como la proyección del conjunto de realizaciones de $\phi(x, y)$. Resulta que la estructura (D, L_D) tiene propiedades importantes en la teoría de modelos.

Proposición 6.10. *Sea D una geometría de Zariski. La estructura (D, L_D) tiene eliminación de cuantificadores.*

La demostración de esto se encuentra en [6].

[11] La proyección de cerrados es cerrada

Proposición 6.11. *Si D es una geometría de Zariski entonces*

- *D es un conjunto fuertemente minimal.*
- *D tiene rango de Morley finito.*

Demostración.
- Sea $E \subseteq M^n \times M$ un conjunto definible, es suficiente con demostrar que $E(a)$ es finito o cofinito. Se deja al lector demostrar es posible expresar todo conjunto definible E como $E = S \backslash F$ con S, F cerrados. Notemos que si $S(a)$ es finito entonces ya acabamos. Supongamos que $S(A)$ es infinito, entonces por $Z2$ tenemos que $S(A) = M$. Si ahora suponemos que $F(a)$ es infinito, entonces ya acabamos (pues $E(a) = \emptyset$). De otra forma $F(a)$ es finito, así que $E(a)$ es cofinito y así terminamos.
- De hecho se tiene aún más: si $X \subseteq M^n$ entonces $MR(X) = dim\left(\bar{X}\right)$ donde dim se refiere a la dimensión como estructura noetheriana. Su demostración se encuentra en [6].

□

La siguiente proposición nos permite pensar en la categoría de geometrías de Zariski vistas como L_D-estructuras cuando los morfismos entre geometrías de Zariski son equivalencias elementarias:

Proposición 6.12. *Supongamos que D es una geometría de Zariski y M una extensión elementariamente equivalente de D. Si consideramos a los cerrados de M como $X = \left\{\bar{b} \in M^n : M \models C\left(\bar{a}, \bar{b}\right)\right\}$ con $C \subseteq M^n \times M^m$ un cerrado básico en D y $\bar{a} \in M^m$, entonces la topología inducida por esos cerrados en M^n es noetheriana y además M es una geometría de Zariski.*

En general, las geometrías de Zariski vistas como estructuras no eliminan imaginarios, sin embargo es posible dar condiciones necesarias y suficientes en términos de la dimensión para que sí lo hagan.

6.3. Conjetura de tricotomía para las geometrías de Zariski. Como ya dijimos anteriormente, una geometría de Zariski es fuertemente minimal. A continuación daré ejemplos de geometrías de Zariski que son triviales y modulares (en particular localmente modulares).

Sea D un conjunto infinito, consideremos al conjunto de cerrados básicos en D^n como combinaciones booleanas de fórmulas como las siguientes: $x_i = x_j$ ó $x_i = a$ con $a \in D$, entonces D es una geometría de Zariski. Vista como una geometría (en el sentido de las pregeometrías) es trivial.

Para un ejemplo de una geometría de Zariski que sea localmente modular consideremos un espacio vectorial D sobre un anillo con división R. Si consideramos a los conjuntos cerrados básicos en D^n como uniones finitas de trasladados de subespacios vectoriales en D^n, entonces D es modular (en particular es localmente modular cuando se localiza por $\emptyset$).

Antes de hablar de del caso no localmente modular voy a dar una condición geométrica que equivale a ser localmente modular para las geometrías de Zariski. Antes necesitamos algunas definiciones, las cuáles espero sean lo suficientemente geométricas para no necesitar ejemplos que nos den una idea de lo que significan (de ser necesario sugiero consultar [46]). Para los últimos dos incisos recomiendo pensar en divisores.

Definición 6.13. 1. *Supongamos que D es una geometría de Zariski. Sea $C \subseteq D^n$ cerrado e irreducible, decimos que $a \in C$ es* ***genérico*** cuando $a \notin F$ para todo $F \subseteq C$ cerrado.

2. Una **curva plana** es un $C \subseteq D^2$ que cumple con ser irreducible, $dim\,(C) = 1$ y ser cerrado.
3. Una **familia de curvas planas** está dada por $C \subseteq E \times D^2$, donde $E \subseteq D$ es irreducible cerrado (de hecho cumple algunas otras propiedades pero las evitaré) de tal forma que para cada $e \in E$ genérico: la fibra $C\,(e)$ es una curva plana.
4. Decimos que D es **amplia** cuando existe una familia de curvas planas C de tal forma que para cualesquiera dos $p, q \in D^2$ genéricos e independientes (en el sentido de pregeometrías, si se quiere), entonces existe una curva plana $C\,(e)$ de tal forma que $p, q \in C\,(e)$.
5. Decimos que D es **muy amplia** cuando para cualesquiera $p, q \in D^2$ (no necesariamente independientes esta vez), existe una familia de curvas planas C de tal forma que haya una curva plana $C\,(e)$ con $p \in C\,(e)$ pero $q \notin C\,(e)$.

En el caso de una curva algebraica D sobre un campo algebraicamente cerrado se tiene que D es muy amplia como geometría de Zariski. El teorema que demostraron Hrushovski y Zilber sobre las geometrías de Zariski no solamente prueba la conjetura de tricotomía, sino también demuestra que el recíproco del enunciado anterior es cierto.

Hablar en abstracto de geometrías de Zariski que no sean localmente modulares es un poco difícil sin las definiciones anteriores. El siguiente lema nos dice por qué las geometrías no localmente modulares son considerablemente útiles:

Lema 6.14. *Si D es una geometría de Zariski, entonces D no es localmente modular si y sólo si D es amplia.*

Teorema 6.15. *Se D es una geometría de Zariski que no es localmente modular entonces*

- *D interpreta un campo algebraicamente cerrado K.*
- *Si D es muy amplia, entonces entonces existe una curva lisa cuasi-proyectiva definida sobre K y una biyección $f : D \longrightarrow C$ de tal forma que para cada n, la biyección de $D^n \longrightarrow C^n$ inducida por f es cerrada y continua.*

Ya vimos algunos ejemplos de geometrías de Zariski, pero será el siguiente el que utilizaremos en la demostración de Mordell-Lang.

Teorema 6.16. *Sea K un campo diferencialmente cerrado. Si $D \subseteq K^m$ es fuertemente minimal, entonces existe un número finito F de elementos en D, de tal forma que $D \backslash F$ es una geometría de Zariski.*

La demostración no es complicada, sin embargo sí un poco extensa y hace uso de más cosas del álgebra diferencial. Se puede encontrar en [18].

7. DE LA CONJETURA DE MORDELL-LANG AL TEOREMA DE HRUSHOVSKI

Esta sección se divide en 3 subsecciones. La primera consiste en enunciar teoremas importantes que se utilizarán en la demostración de Mordell-Lang cuya demostración es muy extensa y excede los propósitos de esta tesis. Es importante mencionar que ninguno de estos teoremas fue demostrado por Hrushovski cuando demostró Mordell-Lang. Los teoremas hablan sobre campos diferencialmente cerrados.

En la segunda sección incluyo por primera vez el enunciado formal de Mordell-Lang así como una motivación de su formulación.

La tercera sección incluye una traducción en términos de geometría algebraica de ser uno-basado. Es notable que esta traducción coincide fielmente con una de las posibles conclusiones de Mordell-Lang.

7.1. Teoremas importantes sobre campos diferencialmente cerrados. La maquinaria desarrollada en las seccioness anteriores nos permitirá demostrar resultados que serán fundamentales para la demostración de Mordell-Lang. Todos los resultados a continuación involucran DCF_0.

Teorema 7.1. *Sea H un grupo de K que es δ-definible, $H \subseteq K_C^n$ y sea g un mapeo que va de H a K^m. Entonces:*

1. *Existe un grupo algebraico G definido sobre K_C de tal forma que $H = G(K_C)$.*
2. *Sea $D \subseteq K$ finito de tal forma que g está definido sobre D. Entonces $H = E_1 \cup \ldots \cup E_m$ es una partición finita de H de tal forma que cada E_i es un subconjunto de K_C^n, K_C-definible y para cada i, g_{E_i} es una función racional definida sobre $D \subseteq D'$*

Para una demostración de este corolario ver [18].

Los siguientes teoremas se utilizarán directamente en la demostración de Mordell-Lang, sus demostraciones se pueden encontrar en [11].

Teorema 7.2. *Un campo infinito F con rango de Morley Finito y que sea δ-definible en un campo diferencialmente cerrado K, es δ-isomorfo al subcampo de constantes de K.*

Teorema 7.3. *Sea A una variedad abeliana definida sobre un campo diferencialmente cerrado K respecto a una diferencial δ con $\Gamma \subset A(K)$ con rango finito. Entonces existe un grupo $H \subset A(K)$ de tal forma que $\Gamma \subset H$, H es δ-definible y además H tiene rango de Morley finito.*

7.2. Motivación histórica para el enunciado de Mordell Lang. La conjetura de Mordell-Lang se fórmula sobre campos de funciones, pero tiene su origen histórico formulado sobre campos numéricos.

Definición 7.4. *Un campo K es un **campo numérico*** cuando es una extensión algebraica de $\mathbb{Q}$

El problema que dio origen a la Conjetura de ML es el siguiente, considérese $f(x, y) \in \mathbb{Q}[x, y]$, este polinomio define una curva X. Si queremos estudiar el conjunto de soluciones $X(\mathbb{Q}) = \{a, b \in \mathbb{Q}^2 | f(a, b) = 0\}$, podemos dividirlo en tres casos:

Caso 1. *Cuando el género de la curva es cero, entonces si la curva no es vacía, se puede hacer isomorfa al plano proyectivo al agregar una cantidad finita de puntos.*

Caso 2. *Cuando el género de la curva X es 1, entonces: $X(\mathbb{Q}) = \emptyset$ o $X(\mathbb{Q})$ es una curva elíptica.*

Caso 3. *El caso que más nos interesa es cuando el género de X es mayor o igual a 2, pues Mordell conjeturó lo siguiente:*

Conjectura de Mordell (primera version). *Si X es una curva con género $\geq 2 \Rightarrow X(\mathbb{Q})$ es finito.*

Años después, Faltings demostró un caso aún más general, pero veamos una reformulación de la Conjetura de Mordell. Notemos que es suficiente con demostrar que si tenemos una curva X con género mayor o igual a 2 y llamamos J_X a su Jacobiana, como $X \hookrightarrow J_X$, se tiene que $X(\mathbb{Q}) = X \cap (J_X(\mathbb{Q}))$. Pero como J_X es una variedad abeliana, resulta que $J_X(\mathbb{Q})$ es un subgrupo. Para poder generalizar la primera versión de la Conjetura de Mordell es necesario recordar el siguiente teorema de Mordell-Weil:

Teorema de Mordell Weil. *Si K es un campo de grado finito sobre $\mathbb{Q}$ y A es una variedad abeliana definida sobre K, entonces $A(K)$ es un subgrupo finitamente generado.*

Usando lo anterior, podemos escribir una versión más fuerte de la Conjetura de Mordell:

Conjectura de Mordell (segunda version). *Si X es una curva con género ≥ 2 y $\Gamma \subseteq J_X$ un subgrupo finitamente generado, entonces $X \cap \Gamma$ es finito.*

De manera aún más general:

Conjetura de Mordell (version final). *Si X es una curva con género ≥ 2 dentro de una variedad abeliana A, y $\Gamma \subseteq A$ un subgrupo finitamente generado, entonces $X \cap \Gamma$ es finito.*

Es inmediato que la versión final implica la segunda versión y que ella a su vez implica la primera. Más adelante veremos que nuestra generalización de la primera versión de la Conjetura de Mordell va por un camino distinto a la versión final de la Conjetura de Mordell, pues el enunciado general de Mordell-Lang mezcla la visión de la Conjetura de Mordell con la Conjetura de Lang, la cual veremos dentro de poco. Manin y Mumford se preguntaron (con otras motivaciones que las de Mordell), cuándo era cierto lo siguiente:

Conjetura de Manin Mumford. *Sea A una variedad abeliana definida sobre un campo numérico K, $X \subseteq A$ una subvariedad y A_{tors} el grupo de torsión de A entonces $X(K) \cap A_{tors}$ es finito.*

Es importante notar que a pesar de que A_{tors} si es un subgrupo de A, no siempre será finitamente generado como en el caso expuesto en [**?**]. Sin embargo, resulta que A_{tors} sí tiene rango finito en el siguiente sentido:

Definición 7.5. *Un grupo Γ tiene **rango finito*** si existe $\Gamma_0 \leq \Gamma$ finitamente generado de tal forma que $\forall \gamma \in \Gamma$, $\exists n \geq 1$ de tal forma que $n\gamma \in \Gamma_0$ (cuando hablemos de variedades abelianas definidas sobre un campo de característica p, la definición se modificará un poco).

Serge Lang se preguntó si el siguiente enunciado era cierto:

Conjetura de Lang (Campos Numericos). *Sea X una subvariedad de una variedad abeliana A, ambas definidas sobre un campo numérico K. Γ un subgrupo de $A(K)$ con rango finito, entonces existen $\gamma_1, \gamma_2, \ldots \gamma_n \in \Gamma$ y $B_1, \ldots B_n$ subvariedades abelianas de tal forma que $\gamma_i + B_i \subseteq X$ y*

$$X(K) \cap \Gamma = \bigcup \gamma_i + (B_i(K) \cap \Gamma)$$

Observacion. *Es cierto que:* $\bigcup(\gamma_i + (B_i(K) \cap \Gamma)) = \bigcup((\gamma_i + B_i(K)) \cap \Gamma)$.

Por doble contención: sea $\gamma_i + a \in \bigcup(\gamma_i + (B_i(K) \cap \Gamma))$ entonces $a \in B_i(K), \Gamma$. Es claro que $\gamma_i + a \in \gamma_i + B_i(K)$, pero como $\gamma_i \in \Gamma$, entonces $\gamma_i + a \in \Gamma$. Asi: $\bigcup(\gamma_i + (B_i(K) \cap \Gamma)) \subseteq \bigcup((\gamma_i + B_i(K)) \cap \Gamma)$. Para el otro lado, sea $\gamma_i + a \in \bigcup((\gamma_i + B_i(K)) \cap \Gamma)$ entonces $\gamma_i + a \in (\gamma_i + B_i(K)), \Gamma$. Eso significa que $\gamma_i + a \in \gamma_i + B_i(K)$, asi que $a \in B_i(K)$. Además, $\gamma_i + a \in \Gamma$ pero nuevamente usando que $\gamma_i \in \Gamma$ obtenemos que $a \in \Gamma$.

Nota. *Es muy importante mencionar que la Conjetura de Lang trata sobre una subvariedad X muy general, y no sólo una curva con género mayor o igual que 2, sin embargo:*

Proposición 7.6. *La Conjetura de Lang implica la primera versión de la Conjetura de Mordell.*

Demostración. Considérese $X = C$ una curva con género ≥ 2 definida sobre $\mathbb{Q}$. Sea $A = J_X$. Por el teorema de Mordell-Weil, $J_X(\mathbb{Q})$ es un subgrupo finitamente generado, en particular J_X tiene rango finito. Como ya anteriormente habíamos dicho, se tiene que $C(\mathbb{Q}) = C \cap J_X(\mathbb{Q})$, así que se cumplen las hipótesis de la conjetura de Lang. Entonces:

$$C(\mathbb{Q}) = C(\mathbb{Q}) \cap J_X(\mathbb{Q}) = \bigcup(\gamma_i + (B_i(\mathbb{Q}) \cap J_X(\mathbb{Q})))$$

Con $\gamma_i + B_i \subseteq C$, B_i subvariedades abelianas de J_X y $\gamma_i \in J_X(\mathbb{Q})$. Pero es claro que: $B_i(\mathbb{Q}) \cap J_X(\mathbb{Q}) = B_i(\mathbb{Q})$, así que: $C(\mathbb{Q}) = \bigcup(\gamma_i + B_i(\mathbb{Q}))$ Ahora hagamos dos casos:

Caso 1.

El primero es cuando B_i es el grupo trivial para toda i. Entonces $C(\mathbb{Q}) = \bigcup \gamma_i$, es decir, $C(\mathbb{Q})$ es finito.

Caso 2.

De otra manera existe algún i tal que B_i tiene dimensión mayor que cero. Como C es una subvariedad, entonces $C(\mathbb{Q})$ es cerrado, así que: $\overline{\bigcup(\gamma_i + B_i(\mathbb{Q}))} = \bigcup\left(\gamma_i + \overline{B_i(\mathbb{Q})}\right) = \overline{C(\mathbb{Q})} = C(\mathbb{Q})$. Pero C es irreducible y con $dim(C) = 1$, entonces $\gamma_i + \overline{B_i(\mathbb{Q})} = C(\mathbb{Q})$. Como B_i tiene dimensión mayor a cero y además $\gamma_i + B_i \subseteq C$, entonces $dim(B_i) = 1$. Pero la Conjetura de Lang dice que B_i es una subvariedad abeliana y las variedades abelianas de dimensión 1 son curvas elípticas. Además es cierto que toda curva elíptica tiene género 1. Pero la definición del género es independiente de los puntos $\mathbb{Q}$ racionales, así que C también tendría género 1 lo cual es una contradicción con nuestra elección de la curva C. □

Ahora haremos un par de reducciones para la demostración de la Conjetura de Lang:

Proposición 7.7. *La conjetura de Lang es equivalente a lo siguiente: Bajo las mismas hipótesis, si* $\overline{X \cap \Gamma(K)} = X(K) \Rightarrow X(K) = \gamma + B(K)$. *Con* $\gamma \in \Gamma$ *y* $B \subseteq A$ *es una subvariedad abeliana.*

Demostración. Primero demostraremos que Lang implica :$\overline{X \cap \Gamma(K)} = X(K) \Rightarrow X = \gamma + B(K)$. Suponemos $X(K) \cap \Gamma = \bigcup \gamma_i + (B_i(K) \cap \Gamma)$. Ademas supongamos que $\overline{X \cap \Gamma(K)} = X(K)$. Eso significa que $\bigcup \gamma_i + \overline{(B_i(K) \cap \Gamma)} = X(K)$. Pero al ser X una variedad, no se puede expresar como unión de 2 o más cerrados, así que $X(K) = \gamma_i + \overline{B_i(K) \cap \Gamma}$. Lo cual es nuestra conclusión.

Ahora demostremos que $\overline{X \cap \Gamma(K)} = X(K) \Rightarrow X(K) = \gamma + B(K)$ implica la Conjetura de Lang. La contrapuesta de nuestra hipótesis es: $X(K) \neq \gamma + B(K)$ para

cualquier subvariedad abeliana $B \Rightarrow \overline{X \cap \Gamma(K)} \subset X(K)$. Haré la demostración usando inducción sobre la dimensión de X.

Supongamos que $dim(X) = 1$. Si $X(K) = \gamma + B(K)$ entonces $X(K) \cap \Gamma = \gamma + B(K) \cap \Gamma$ lo cual es la conclusión de Lang. Si en cambio $X(K) \neq \gamma + B(K)$, usando nuestra hipótesis tenemos que $\overline{X \cap \Gamma(K)} \subset X(K)$. Pero como la contención es propia, entonces $dim\left(\overline{X \cap \Gamma}\right) = 0$, entonces $\overline{X \cap \Gamma(K)}$ es una cantidad finita de puntos. Así que $X \cap \Gamma(K)$ es a lo más una cantidad finita de puntos.

Supongamos que es cierto para toda subvariedad de dimensión menor o igual a n y lo queremos demostrar cuando $dim(X) = n + 1$. Nuevamente podemos suponer que $X(K) \neq \gamma + B(K)$, entonces $\overline{X \cap \Gamma(K)} \subset X(K)$. Como la contención es propia, $\overline{X \cap \Gamma}$ tiene dimensión menor o igual a n, así que Lang es cierta: $\overline{X \cap \Gamma}(K) \cap \Gamma = \bigcup \gamma_i + (B_i(K) \cap \Gamma)$.

Pero afirmo lo siguiente: $\overline{X \cap \Gamma}(K) \cap \Gamma = X(K) \cap \Gamma$. Lo haré por doble contención: Sea $a \in \overline{X \cap \Gamma}(K) \cap \Gamma$. Por demostrar: $a \in X$. Como X es variedad, entonces $\overline{X} = X$, así que basta demostrar que $a \in \overline{X}$. Pero $\overline{X \cap \Gamma} \subseteq \overline{X} \cap \overline{\Gamma}$. Así que $a \in \overline{X}$. Para la otra contención: Supongo $a \in X \cap \Gamma$. Falta por demostrar que $a \in \overline{X \cap \Gamma}$. Pero notemos que $X \cap \Gamma \subseteq \overline{X \cap \Gamma}$. Así que terminamos. □

Definimos $Stab_X = \{a \in A : a + X \subseteq X\}$. Sea X una subvariedad. En [47] se demuestra que $Stab_X$ es un subgrupo algebraico de A, mientras que en [1] se demostró que el grupo cociente de una variedad abeliana por un subgrupo algebraico, es una variedad abeliana, así que podemos hablar de la variedad abeliana $A/Stab_X$ y del morfismo canónico $\pi : A \to A/Stab_X$ como un morfismo de variedades abelianas. Denotemos $\pi(X) = X'$. Es claro que $Stab_{X'} = \{0\}$. Podemos reducir aún más la Conjetura de Lang.

Proposición 7.8. *Si la Conjetura de Lang es cierta para X de tal forma que $Stab_X = \{0\}$, entonces la Conjetura de Lang es cierta para X arbitraria.*

Demostración. El plan de la demostración es el siguiente: Usaremos el enunciado equivalente a Lang demostrado en la proposición anterior, es decir: supongamos que X no es el trasladado de una subvariedad abeliana y demostremos que $X \cap \Gamma$ no es Zariski denso en X. Para ello demostraremos dos cosas: Si X no es el trasladado de una subvariedad abeliana, entonces tampoco lo es X'. Como asumimos cierto Lang para X', entonces obtendremos que $X' \cap \pi(\Gamma)$ no es Zariski denso en X'. La segunda cosa que debemos demostrar es que si $X' \cap \pi(\Gamma)$ no es Zariski denso en X', entonces tampoco $X \cap \Gamma$ es Zariski denso en X. Empecemos con este último:

Afirmación 1. *Si $\overline{X' \cap \pi(\Gamma)} \subset X'$, vamos a demostrar que $\overline{X \cap \Gamma} \subset X$.*

Supongamos por contradicción que $\overline{X \cap \Gamma} = X$. Tenemos que $\pi(X \cap \Gamma) \subseteq X' \cap \pi(\Gamma)$, así que $\overline{\pi(X \cap \Gamma)} \subseteq \overline{X' \cap \pi(\Gamma)} \subset X'$. Pero porque π es continua, $\pi\left(\overline{X \cap \Gamma}\right) \subseteq \overline{\pi(X \cap \Gamma)}$. Así que $\pi\left(\overline{X \cap \Gamma}\right) \subset \pi(X)$. Pero habíamos supuesto que $\overline{X \cap \Gamma} = X$, entonces $\pi(X) \subset \pi(X)$, lo cual es una contradicción.

Lo que resta demostrar es que si X no es el trasladado de una subvariedad abeliana, entonces tampoco lo será X'. Antes de continuar, notemos lo siguiente:

Afirmación 2. *Si $X' = \{b\}$ entonces X es el trasladado de una subvariedad abeliana.*

En efecto, si lo vemos como clases laterales: $\pi(X) = b + Stab_X$. Pero en una variedad, los puntos siempre son cerrados, así que $\overline{X'} = X'$, eso significa que $\pi(X) = b + \overline{Stab_X}$. Luego: $X = b + \pi^{-1}\left(\overline{Stab_X}\right)$. Pero π es continua, así que $\pi^{-1}(0)$ es un cerrado, y como

la imagen inversa de un subgrupo es nuevamente un subgrupo, entonces $\pi^{-1}(0)$ es una subvariedad abeliana de A, lo cual significa que X es el trasladado de una subvariedad abeliana como se quería.

La contrapuesta de la afirmación anterior es: Si X no es el trasladado de una subvariedad abeliana, entonces X' no se reduce a un punto. Así que, si la única forma de que X' fuera el trasladado de una subvariedad abeliana es cuando X' es un punto, entonces ya habríamos acabado. De hecho sí es el caso: Supongamos que $X' = \gamma + B$ con $dim(B)$ mayor a cero. Eso quiere decir que hay una cantidad infinita de $b \in B$. Pero notemos que $b+(\gamma + B) = \gamma+B \; \forall b \in B$ pues B es un subgrupo. Así que tendríamos que $B \subseteq Stab_{X'}$, lo cual contradice el hecho de que $Stab_{X'}$ es finito. Eso termina nuestra demostración. □

Usando las proposiciones 7.8 y 7.7 podemos enunciar la conjetura de Lang de la siguiente forma: Sea X una subvariedad de una variedad abeliana A, ambas definidas sobre un campo numérico K. Γ un subgrupo de $A(K)$ con rango finito. Supongamos además que $Stab_X$ es finito y que $X \cap \Gamma$ es Zariski denso en X. Entonces X es el trasladado de una subvariedad abeliana.

Observacion. *Si además suponemos que $X(K)$ no es finita. Al asumir $Stab_X$ finito, se tiene inmediatamente que X no puede ser el trasladado de una subvariedad abeliana. Supongamos por contradicción que $X = \gamma + B$ con B una subvariedad abeliana. B debe ser infinita. Tómese un $b \in B$, afirmo que $b + X \subseteq X$ y de esa forma: $B \subseteq Stab_X$ así que tendríamos una contradicción. Sea $b + x \in b + X$. Como $X = \gamma + B$, se tiene que $x = \gamma + b_1$, $b_1 \in B$. Así que $b + x = b + \gamma + b_1$. Como la variedad es abeliana: $b+x = \gamma+(b + b_1) \in \gamma+B = X$, asi que $Stab_X$ es infinito, lo cual es una contradicción.*

Con la observación anterior, podemos simplificar aún más el enunciado de la Conjetura de Lang:

Primera reformulacion de la Conjetura de Lang (Campos Numericos). *Sea X una subvariedad de una variedad abeliana A con $X(K)$ infinito. Ambas variedades definidas sobre un campo numérico K. Γ un subgrupo de $A(K)$ con rango finito. Supongamos ademas que $Stab_X$ es finito, entonces $X \cap \Gamma$ no es es Zariski denso en X.*

La versión de la Conjetura de Mordell-Lang que demostró Hrushovski está enunciada sobre campos de funciones, mientras que todo lo anterior se hizo para campos numéricos. Veremos ahora los análogos de los teoremas anteriores para campos de funciones.

Definición 7.9. *Sea k un campo algebraicamente cerrado. Un* ***campo de funciones*** K (con grado de trascendencia 1) sobre k es el campo de funciones racionales de $V(k)$, con V una curva definida sobre k. Lo denotaremos por K/k.

La conjetura de Mordell enunciada exactamente igual que para campos numéricos no es cierta para campos de funciones. De alguna manera es normal que no lo sea, pues todo campo numérico es numerable, mientras que los campos de funciones son extensiones de campos algebraicamente cerrados arbitrarios. Así que la cantidad de soluciones podría ser mucho mayor como lo ilustra el siguiente ejemplo:

Ejemplo 7.10. *La curva de Fermat F definida por $x^n = y^n + z^n$ tiene género mayor que 1 cuando $n \geq 3$. Además tiene sentido preguntarnos por $F(\mathbb{C})$ y por $F(\mathbb{C}(t))$ pues su ecuación está definida sobre $\mathbb{C}$ y además $\mathbb{C} \hookrightarrow \mathbb{C}(t)$. Es claro que $F(\mathbb{C})$ es infinito y por la inclusión, también lo es $F(\mathbb{C}(t))$. Así que la Conjetura de Mordell no es cierta para el campo de funciones $\mathbb{C}(t)$. Sin embargo, en* [11] *se demuestra que $F(\mathbb{C}(t)) \setminus F(\mathbb{C})$ es finito, lo cual da esperanzas de que exista una formulación adecuada para campos de funciones. De hecho sí la hay cuando definimos una nueva noción de «finitud».*

Por el momento, trabajaremos sólo en característica 0. El equivalente a la primera versión de la Conjetura de Mordell para campos de funciones fue enunciada y demostrada por Manin en [48]. El enunciado dice lo siguiente:

Conjetura de Mordell (Campos de Funciones). *Sea C una curva con género ≥ 2 definida sobre un campo de funciones K/k. Entonces se cumple alguna de las siguientes conclusiones:*

1. *$C(K)$ es finito*
2. *Existe una curva C_0 definida sobre k que es birracionalmente equivalente sobre K a C, además cumple que $C_0(K) - C_0(k)$ es finito.*

Notemos que la curva de Fermat satisface la condición 2 del teorema anterior tomando $k = \mathbb{C}$.

Resulta que en característica cero y sobre campos de funciones, la conjetura de Lang (la versión que dimos para campos numéricos) sigue siendo cierta. Mc Quillen (en [**?**]) lo demostró cuando $k = \mathbb{C}$, pero en [31] se demuestra cómo ese resultado implica la conjetura de Lang para campos de funciones y campos numéricos de característica cero. A esta versión se le conoce como la versión global de la conjetura de Lang.

Para campos numéricos, demostramos que la conjetura de Lang implica la conjetura de Mordell. Mientras que para campos de funciones de característica cero, tanto la Conjetura de Lang como la adecuación de la Conjetura de Mordell son ciertas.

Cuando demostramos que Lang implica Mordell, utilizamos el teorema de Mordell Weil, el cual es cierto para campos numéricos, sin embargo, existe una adecuación de ese teorema para campos de funciones. Es útil conocer esa versión pues nos da una idea de porqué la versión que dimos para Mordell en campos de funciones sí es adecuada.

Definición 7.11. *Sea A una variedad abeliana definida sobre un campo de funciones K/k, entonces existe una subvariedad A_0 definida sobre k y un homomorfismo con kernel finito $\tau : A_0 \longrightarrow A$ con la siguiente propiedad universal: Si $\phi : B \longrightarrow A$ con B una variedad abeliana definida sobre k y ϕ un morfismo de variedades abelianas, entonces existe un morfismo $f : B \longrightarrow A_0$ que factoriza a τ. A_0. Recibe el nombre de la K/k* ***traza*** de A.

Teorema de Mordell Weil relativo. *Sea A una variedad abeliana definida sobre un campo de funciones K/k. Sea $\tau : A_0 \to A$ su K/k traza. Entonces $A(K)/\tau(A_0(k))$ es un grupo finitamente generado.*

No discutiré si la conjetura de Lang implica la de Mordell para campos de funciones en característica cero, pero el teorema anterior motiva a pensar que el enunciado de Mordell para campos de funciones es una buena formulación.

En característica p las cosas son aún más complicadas pues las versiones que hemos dado de Mordell y Lang no son ciertas.

El siguiente ejemplo muestra que la segunda afirmación de la Conjetura de Mordell para campos de funciones no es cierta en característica p.

Ejemplo 7.12. *Consideremos el campo de funciones $K = \overline{\mathbb{F}}_p(t)$ con p primo. Sea C una curva con género mayor o igual a 2 definida sobre $\mathbb{F}_p$, por ejemplo: $y^2 = x^5 - x - 1$ y α un elemento como $\alpha = \left(t^5 - t - 1\right)^{1/2}$.*

Afirmación. *$C\left(\overline{\mathbb{F}}_p(t)\right) \setminus C\left(\overline{\mathbb{F}}_p\right)$ es infinito.*

Claro que (t, α) es una solución que no está $\overline{\mathbb{F}}_p$. Pero además, para cada $n \in \mathbb{N}$, $\left(t^{p^n}, \alpha^{p^n}\right)$ también es una solución. Como $t \notin \overline{\mathbb{F}}_p$ entonces todos esos puntos son distintos y siguen sin estar en $\overline{\mathbb{F}}_p$ como se quería.

A pesar de que la versión que habíamos enunciado para característica cero no es cierta, nuevamente podemos adecuar la formulación. El siguiente teorema fue demostrado en [35] por Samuel:

Conjetura de Mordell (Campos de Funciones en caracteristica p). *Sea C una curva género mayor o igual a 2 y definida sobre un campo de funciones K/k. Entonces se cumple alguna de las dos condiciones:*

1. *$C(K)$ es finito.*
2. *Existe una variedad abeliana C_0 definida sobre k que es birracionalmente equivalente a C sobre alguna extensión finita de K.*

Resulta que la equivalencia birracional también está definida sobre K cuando la curva C no está definida sobre un campo finito.

Respecto a la Conjetura de Lang tenemos lo siguiente: En [3] se da un ejemplo cuando la Conjetura de Lang es falsa para característica p. Con ese ejemplo y el que hace falsa a la Conjetura de Mordell como evidencia, Voloch y Abramovich formularon la conjetura de Lang para campos de funciones en cualquier característica. Para ello introdujeron el siguiente concepto:

Definición 7.13. *Sea K/k . Una subvarierdad $X \subseteq A$ de una variedad abeliana A definida sobre K se dice que es* ***especial*** cuando existe una subvariedad abeliana $B \subseteq A$, una variedad abeliana S definida sobre k, X_0 una subvariedad de S también definida sobre k y un morfismo suprayectivo de variedades abelianas $h : B \to S$ de tal forma que $X = a_0 + h^{-1}(X_0)$.

Un ejemplo de una subvariedad especial es $X = a + C$ con C una subvariedad abeliana definida sobre K. En efecto, sea $B = C$, $S = X_0 = 0$ y $h = 0$.

Debido a que la Conjetura de Lang y la de Mordell han ido motivando nuestros enunciados, a partir de ahora la conjetura de Lang la llamaremos conjetura de Mordell-Lang. Con el objeto de utilizar la eliminación de cuantificadores para los campos algebraicamente cerrados supondremos que K lo es. El enunciado dice lo siguiente:

Conjetura de Mordell-Lang (Campos de Funciones). *Sean K/k un campo de funciones algebraicamente cerrado. A una variedad abeliana definida sobre K y X una subvariedad también definida sobre K. Γ un subgrupo de rango finito de $A(K)$. Supongamos que $Stab_X$ es finito. Entonces pasa alguna de las siguientes situaciones:*

1. *$X \cap \Gamma$ no es denso en $X(K)$.*
2. *X es especial.*

Notemos que en este caso la característica del campo no está restringida. Resulta que en característica cero, la Conjetura de Lang implica la Conjetura de Mordell-Lang, y lo anterior es inmediato pues ya dijimos que el trasladado de una subvariedad abeliana es especial.

De esta formulación, Voloch y Abramovich demostraron varios casos particulares, pero no fue sino Hrushovski quien la demostró en toda su generalidad. A esta versión también se le conoce como la Conjetura de Lang relativa.

Pero la conjetura relativa no es sólo un caso particular, sino que existe un caso en el que ambas conjeturas dicen lo mismo. Supongamos que la K/k traza de la variedad abeliana A es cero. La afirmación es que si X es especial entonces X es el trasladado de una subvariedad abeliana. Supongamos que X es especial. Consideremos la inclusión $i : B \hookrightarrow A$. Por la definición de traza, existe un morfismo $f : B \to 0$ de tal forma que $i = j \circ f$

donde $j : 0 \to A$. Entonces $Im\,(i) = Im\,(j \circ f)$. Pero $Im\,(j \circ f) = 0$. Así que $Im\,(i) = 0$, y como i es la inclusión, entonces $B = 0$. Eso quiere decir que en la definición de ser una variedad especial, $S = X_0 = 0$ (pues el morfismo h es suprayectivo). Así que $X = a_0$. Lo cual hace a X el trasladado de una subvariedad abeliana trivialmente.

Observacion. *Si suponemos que X es infinito, entonces la subvariedad S que hace a X especial no es trivial. Por contradicción supongamos que $S = \{0\}$, entonces $X_0 = S = \{0\}$. De esta forma: $h^{-1}[X_0] = h^{-1}[S] = B$. Así que $X = \gamma + B$, y por una observación anterior, eso supondría que $Stab_X$ es infinito, lo cual es una contradicción pues supusimos lo contrario.*

Con las observaciones anteriores, obtenemos la formulación del teorema que vamos a demostrar:

Conjetura de Mordell-Lang (Campos de Funciones). *Sean K/k un campo de funciones algebraicamente cerrado. A una variedad abeliana definida sobre K y X una subvariedad infinita también definida sobre K. Γ un subgrupo de rango finito de $A\,(K)$. Supongamos que $Stab_X$ es finito y que $X \cap \Gamma$ es denso en X. Entonces X es especial.*

7.3. teoría de modelos en la Conjetura de Mordell. La idea genuina de la conjetura de Mordell para campos numéricos es que la descomposición de $X \cap \Gamma$ es igual a la unión finita de trasladados de subgrupos en Γ. Resulta que esta condición ocurre si y sólo si Γ es un grupo uno-basado. La siguiente sección se dedica a demostrar un caso particular de esa equivalencia y a demostrar una consecuencia bastante técnica de ese hecho que se usará en la demostración de Mordell-Lang.

Definición 7.14. *Sea K un campo algebraicamente cerrado, A los puntos K racionales de un grupo algebraico conmutativo sobre K y Γ un subgrupo de A. Decimos que (K, A, Γ) es de **«tipo Lang»*** si para cada $n \in \mathbb{N}$ y cada subvariedad algebraica $X \subseteq A^n$ definida sobre K, $\Gamma^n \cap X$ es la unión finita de trasladados de subgrupos de Γ, i.e. $\Gamma^n \cap X = \cup_{i=1}^{n} (\gamma_i + \Gamma)$.

El teorema que queremos demostrar utiliza una definición para fórmulas del concepto de uno-basado. Recordemos que hasta ahora habíamos hablado de teorías uno-basadas.

Definición 7.15. *Sea T una teoría completa y estable y $\phi\,(x)$ una fórmula en el lenguaje L de T. Decimos que $\phi\,(\bar{x})$ es **uno-basado*** cuando siempre que $\bar{a}$ sea una realización de ϕ en un modelo M de T y $A \subseteq M$, entonces $Cb\,(tp\,(\bar{a}/A)) \subseteq acl^{eq}\,(\bar{a})$.

Nota. *Es inmediato que una teoría es uno-basada cuando todas sus fórmulas son uno-basadas.*

El teorema que utilizaremos para la demostración de Mordell-Lang es el siguiente:

Teorema 7.16. *Sea K un campo algebraicamente cerrado, A los K puntos de un grupo algebraico conmutativo sobre K y Γ un subgrupo de A. Entonces (K, A, Γ) es de «tipo Lang» si y sólo si $Th\,(K, +, \cdot, \Gamma, a)_{a \in K}$ es estable y además la fórmula $x \in \Gamma$ es uno-basado.*

La demostración de este hecho en toda su generalidad se puede encontar en [16]. Yo sólo demostraré la siguiente proposición, la cual establece una conexión entre ser uno-basado y algo un poco más débil que ser de Tipo Lang.

Proposición 7.17. *G es un grupo basado si y sólo si todo subconjunto definible de G^n es una combinación booleana de trasladados de subgrupos definibles de G.*

Por último utilizaremos el teorema anterior para demostrar un resultado sobre grupos que relaciona la ortogonalidad con el concepto de ser uno-basado:

Proposición 7.18. *Sea G un grupo uno-basado. Si $A, B \leq G$ son ortogonales y uno-basados, entonces $A + B$ es un grupo uno-basado.*

Demostración. No demostraré este teorema en toda su generalidad, en cambio demostraré que $A \times B \leq G \times G$ es uno-basado. De este hecho se sigue que $A + B$ es uno-basado, sin embargo se necesita bastante más trabajo. He decidido ahorrármelo porque considero que no aporta demasiado al texto, sin embargo estos detalles se pueden encontrar en [28].

Utilizando el teorema anterior, queremos demostrar que cualquier conjunto definible $C \subseteq A \times B$ es una combinación booleana de clases laterales de subgrupos de $A \times B$ definibles. Sea $C \subseteq A \times B$ como dijimos, ya que A, B son ortogonales, entonces todo subconjunto definible es de la forma $C = \cup_{i=1}^{n} A_i \times B_i$.

Como estamos suponiendo que A, B son uno-basados, entonces cada A_i y B_i es una combinación booleana (finita) de clases laterales de subgrupos definibles en A y en B respectivamente. Como el producto de subrupos definibles es definible, entonces C es una combinación booleana de clases laterales de subgrupos definibles como se quería. □

8. DEMOSTRACIÓN

El enunciado que vamos a demostrar es el siguiente:

Conjetura de Mordell-Lang (Campos de Funciones). *Sean K/k un campo de funciones algebraicamente cerrado. A una variedad abeliana definida sobre K y X una subvariedad infinita también definida sobre K. Γ un subgrupo de rango finito de $A(K)$. Supongamos que $Stab_X$ es finito y que $X \cap \Gamma$ es denso en X. Entonces X es especial.*

Notemos que mientras A y X sí están definidos sobre K, el grupo Γ no tiene porque ser definible. La primera parte consiste en hacer una adecuación a las hipótesis sobre los campos K y k_0 de modo que Γ sea definible y además mantenga una idea de «pequeño». Para hacer eso vamos a enriquecer el lenguaje de los campos algebraicamente cerrados.

Proposición 8.1.
1. *Es posible agregarle al lenguaje una símbolo de función 1-aria δ de tal forma que en el campo K se interprete como una diferencial, y además k_0 resulte ser su campo de constantes de la cerradura diferencial de K.*
2. *Si podemos demostrar la Conjetura de Mordell-Lang para una extensión $\aleph_0$-saturado de la cerradura diferencial L de K, entonces Mordell-Lang es cierta para K.*

Demostración.
1. Este hecho se puede encontrar en [4].
2. Primero veamos que no hay problema si demostramos Mordell-Lang para L. Sea L la cerradura diferencial de K respecto a δ. Supongamos ahora que podemos demostrar la conjetura de Mordell-Lang cuando la variedad abeliana A y su subvariedad X están definidos sobre L; Γ un subgrupo de rango finito de los puntos L racionales de A de tal forma que $X \cap \Gamma$ es denso en $X(L)$. Demostrar Mordell-Lang en este caso significaría que demostramos que X es especial sobre el campo de constantes de L, el cual ya dijimos que coincide con k_0. Así que demostrar Mordell-Lang en este caso no haría diferencia.

   Veamos qué pasa respecto a las extensiones $\aleph_0$-saturadas. En el enunciado de Mordell-Lang tenemos una variedad abeliana A, una subvariedad $X \subseteq A$, y un subgrupo de rango finito $\Gamma \subseteq A(L)$. Notemos que todos ellos son definibles sobre L (muy probablemente usando parámetros en K). Como la teoría de campos diferencialmente cerrados es ω-estable, entonces existe una extensión L' que es $\aleph_0$ saturada. Por definición de extensión elementariamente equivalente, si k_0' denota al campo de constantes de L, entonces $k_0 \subseteq k_0'$. Supongamos que podemos demostrar Mordell-Lang para L' y k_0', ahora queremos ver que aún es cierto para L y k_0.

   Si demostramos Mordell-Lang para k_0' y L' significa que existe una subvariedad abeliana $B \subseteq A$ definida sobre L' (con parámetros), una variedad abeliana S', una subvariedad $X' \subseteq B'$ y un morfismo biyectivo $h' : B' \longrightarrow S'$, todos ellos definidos (con parámetros) sobre k_0' (recordemos que k_0' es definible en L'). Lo que queremos es regresar el enunciado de la conclusión en Mordell-Lang a los campos L y k_0.

   Por la propiedad $P3$ en las primeras páginas, si tenemos que A es una variedad abeliana definida sobre L (algebraicamente cerrado) y B es una subvariedad abeliana (en particular un subgrupo cerrado), entonces B también está definida sobre L.

   Consideremos la fórmula en lenguaje de primer orden que expresa lo siguiente: «h' es un morfismo biyectivo que va de B (definida con parámetros en L) a una variedad abeliana S'; existe una subvariedad $X_0' \subseteq S'$ de tal forma que $X = a_0' + h'^{-1}(X_0')$». Los parámetros de esta fórmula vienen de L y esta fórmula no

es vacía L', pero como suponemos que $L \prec L'$, entonces (por Tarski-Vaught) esta fórmula también se satisface en L, lo cual es lo que queríamos.

□

Una vez hecho esto, recordemos el teorema 7.3, así que tenemos un grupo $H \subset A(K)$ de tal forma que $\Gamma \subset H$, H es δ-definible y además H tiene rango de Morley finito.

Notemos que como $X \cap \Gamma$ es Zariski denso, entonces $X \cap H$ también lo es. Queremos demostrar que X es especial, así que para ese fin, no es importante si consideramos al subgrupo H en la demostración. Gracias a las dos proposiciones anteriores, el teorema que queremos demostrar es el siguiente:

Teorema 8.2. *Sea L $\aleph_0$-saturado y diferencialmente cerrado respecto a δ con un campo de constantes k_0. A una variedad abeliana definida sobre L, X una subvariedad de A con estabilizador finito y definida sobre L. H un subgrupo de $A(L)$ que es δ-definible, con rango de Morley finito y $X \cap H$ es Zariski denso en X. Entonces X es especial.*

La parte más larga de la demostración consiste en probar que podemos reducir el teorema anterior al caso cuando $H \subseteq B$, donde B es un conjunto fuertemente minimal, H no es uno-basado, es δ-definible y conectable (en el sentido de la teoría de modelos). Esa reducción la haremos más adelante, por lo pronto supongamos que ya la hicimos. El siguiente teorema terminaría con la demostración de la conjetura de Mordell-Lang:

Proposición 8.3. *Sea L $\aleph_0$-saturado y diferencialmente cerrado con k_0 su campo de constantes. Sea A una variedad abeliana definida sobre L y sea H un subgrupo de $A(L)$ tal que existe B un conjunto fuertemente minimal con $H \subseteq acl(B)$. Además suponemos que H es conectable, δ-definible y no uno-basado. Entonces:*

- *Existe una variedad abeliana S definida sobre k_0 y un morfismo biyectivo*
$$f : \overline{H} \longrightarrow S$$
tal que $f(H) = S(k_0)$
- *Sea X una subvariedad de A definida sobre L, tal que $X \cap H$ es denso en X. $\Rightarrow$ $\exists X_0$ subvariedad de S, definida sobre k_0 de tal forma que $f^{-1}(X_0) = X$.*

Notemos que la cerradura de Zariski de un conjunto dentro de los L puntos de A es una variedad, así que en la primera parte del teorema estamos diciendo que existe un morfismo f entre variedades que en particular nos da una función entre los puntos k_0 racionales de esas variedades.

Demostración. La primera afirmación es que B no puede ser localmente modular: El teorema 5.78 dice que si B fuertemente minimal, entonces B no es localmente modular si y sólo si no es uno-basado. Así que basta con demostrar que B no es uno-basado. Pero como $H \subseteq acl(B)$ y H no es uno-basado entonces B tampoco lo es (ver contrapuesta al lema 5.81). Así que B es un conjunto fuertemente minimal que no es localmente modular.

Pero en la sección de Geometrías de Zariski se demostró (6.16) que: todo conjunto fuertemente minimal sobre un campo diferencialmente cerrado es una geometría de Zariski, y la conjetura de tricotomía de Zilber es cierta para las Geometrías de Zariski(Teorema 6.15). Así que B interpreta un campo algebraicamente cerrado. Eso quiere decir que existe un campo F' el cual es definible en B^{eq}. Pero B esta contenido en los puntos L racionales de la variedad A, y usando nuevamente que los campos diferencialmente cerrados tienen eliminación de imaginarios: existe un campo F que es δ-definible en $B \subseteq L$. Además, afirmo que F tiene rango de Morley finito. Esto es porque F se definió (eliminación de imaginarios) en B, el cual es un conjunto fuertemente minimal, eso quiere decir que su

rango de Morley es igual a uno. Así que F tiene rango de Morley menor o igual a 1 pues el rango de Morley es monótono (de hecho es uno, porque F es un campo algebraicamente cerrado, entonces es infinito). En particular, F tiene rango de Morley finito.

Ahora podemos usar el teorema de Cassidi-Sokolovic(7.2) que enunciamos en la sección. La conclusión de este resultado dice que F es δ-definiblemente isomorfo (quiero decir que el morfismo que los hace isomorfos es δ-definible) al campo de constantes de L, es decir: $F \cong_\delta k_0$

En este momento afirmo que B y k_0 no pueden ser ortogonales. Como k_0 es algebraicamente cerrado, entonces es fuertemente minimal, por otro lado: B y k_0 no son ortogonales si y sólo si $k_0 \subseteq acl(A \cup B)$ para un conjunto finito de parámetros A (lema 5.85). Pero como k_0 es definible en B, entonces $k_0 \subseteq acl(\emptyset \cup B)$. Así que k_0 y B no son ortogonales, $k_0 \not\perp B$.

Ahora diré porqué H y k_0 tampoco pueden ser ortogonales. Usaré la contrapuesta del lema 5.88. Primero notemos que por la eliminación de imaginarios $acl^{eq} = acl$ entonces a pesar de que el lema está enunciado para acl^{eq}, usaré libremente acl. Además es cierto que $k_0 \subseteq acl(k_0)$, y como estamos suponiendo que $k_0 \not\perp B$ y $H \subseteq acl(B)$ con B fuertemente minimal y H grupo abeliano, entonces se cumplen las hipótesis de la contrapuesta del lema 5.88 haciendo $k_0 = E = G$, $H = H$ y $B = B$. Concluimos que $H \not\perp k_0$.

Por el teorema 5.87 aplicado a H y k_0, existe un grupo δ-definible G con parámetros en k_0, $G \subseteq k_0^n$ y un morfismo δ-definible $h : H \to G$ con kernel finito (recordemos que este teorema esta enunciado sobre T^{eq} para alguna teoría T, pero nuevamente usamos eliminación de imaginarios).

Este grupo G lo utilizaremos para definir a la variedad abeliana S definida sobre k_0 de la conclusión del teorema, pero necesitamos un poco más de esfuerzo para convertirlo en variedad abeliana:

Primero afirmo que G es conectable (teoría de modelos). Como h, H, G son δ-definibles, y el morfismo h es finito a uno (pues su kernel es finito), entonces por la proposición 5.30, se tiene que $gr_M(H) = gr_M(G)$. Pero ya habíamos visto en el lema 5.93 que un grupo (por ejemplo H) es conectable si y sólo si $gr_M(H) = 1$, así que G también será conectable.

Lo primero que haré es demostrar que existe un morfismo suprayectivo y con kernel finito $g_0 : G \longrightarrow H$:

Sea $y \in G$. Quiero definir quién es $g_0(y)$. Como $ker(h)$ es finito, supongamos que tiene $n \in \mathbb{N}$ elementos. Además sabemos que h es suprayectivo, entonces para todo $y \in G$, existe un $x \in H$ de tal forma que $h(x) = y$. Defino $g_0(y) = nx$. No es inmediato que esto sea una función: Supongamos que $y = h(x) = h(x')$. Quiero demostrar que $nx = nx'$. Como $h(x) = h(x')$, entonces $h(x - x') = 0$. Pero por la definición de g_0, $g_0(0) = n(x - x') = nx - nx'$, mientras que por otro lado: $g_0(0) = 0$, así que $nx = nx'$ como queríamos.

Además afirmo que g_0 tiene kernel finito: Supongamos que $g_0(y_1) = g_0(y_2) = \ldots = 0$ con los $y_1, \ldots$ distintos. Como h es una función (y además ya dijimos que es suprayectiva), entonces existe una cantidad infinita $x_1, \ldots$ de tal forma que $h(x_i) = y_i, \forall i \in \mathbb{N}$. Pero por la definición de g_0, tenemos que $nx_i = 0, \forall i \in \mathbb{N}$. Pero en el apéndice, enunciamos un importante hecho de las variedades abelianas: El subgrupo de n-torsión de una variedad abeliana es finito para cualquier $n \in \mathbb{N}$. En particular lo será para aquella n que usamos para definir a g_0 y como el grupo H es subgrupo de una variedad abeliana A, tendríamos una contradicción.

El morfismo g_0 es suprayectivo. Afirmo que sería suficiente con demostrar que $nH = H$: Para demostrar que g_0 es suprayectiva habría que probar que $H = im\,(g_0)$, por otro lado, $im\,(g_0) \subseteq nH$. Pero yo digo que incluso tenemos $nH = im\,(g_0)$: sea $na \in nH$, defino $y = h\,(a)$, por la definición de g_0 tenemos que $g_0\,(y) = na$, así que en efecto es suficiente con demostrar que $nH = H$. Ahora demostraré que $RM\,(nH) = RM\,(H)$: Consideremos la función $t : H \longrightarrow nH$ definida por $a \longmapsto na$, esta función es suprayectiva, y por la observación anterior (el subgrupo de n torsión es finito) entonces la función que definimos es finito a uno. Por el teorema 5.30, tenemos que $RM\,(nH) = RM\,(H)$. Sin embargo, el lema 5.90 nos dice que el índice de H' en H debe ser finito. Como el grupo H es conectable, no podríamos tener una contención propia. Entonces $nH = H$. Así que $g_0 : G \longrightarrow H$ es un morfismo suprayectivo con kernel finito.

Defino a $G_1 = G/ker\,(g_0)$ y a g como el isomorfismo inducido por g_0 de G_1 en H. Por el teorema 7.1 existe un grupo algebraico G_2 que esta definido sobre k_0 y además $G_1 = G_2\,(k_0)$. Este corolario también asegura que $g : G_1 = G_2\,(k_0) \longrightarrow H$ es racional.

Afirmo que existe una extensión suprayectiva del morfismo g, que llamaremos $\overline{g}$: $\overline{G_2\,(k_0)} = G_2\,(L) \longrightarrow \overline{H}$. Lo anterior es porque ..... Notemos que $\overline{H}$ es una variedad abeliana porque es un subgrupo cerrado en A.

Ahora afirmo que el kernel de $\overline{g}$ es trivial, la razón es la siguiente: por el teorema de Chevalley (9.34) aplicado al grupo algebraico G_2, existe un subgrupo $M \subseteq G_2$ que es minimal, cerrado y k_0 definible de tal forma que G_2/M es una variedad abeliana. Por otro lado, $G_2\,(L)\,/ker\,(\bar{g})$ es isomorfo a $\bar{H}$, el cual ya dijimos que es una variedad abeliana, así que $G_2\,(L)\,/ker\,(\bar{g})$ es una variedad abeliana. Como M es minimal, entonces $M \subseteq ker\,(\bar{g})$, así que $M\,(k_0) \subseteq ker\,(\bar{g})\,(k_0)$, pero $\bar{g}$ restringido a k_0 es inyectivo (porque g es un isomorfismo), así que $M\,(k_0) \subseteq ker\,(\bar{g})\,(k_0) = \{0\}$, entonces $M\,(k_0) = \{0\}$. Además recordemos que M está definido sobre k_0, eso significa que M es trivial, entonces G_2 ya era una variedad abeliana. Ahora usaremos la propiedad (P3) para demostrar que el subgrupo $ker\,(\bar{g}) \subseteq G_2$ también esta definido sobre k_0. Eso significaría que $ker\,(\bar{g})$ es trivial (pues $ker\,(\bar{g})\,(k_0) = \{0\}$). Como $ker\,(\bar{g})$ es un subgrupo cerrado de una variedad abeliana definida sobre k_0, entonces también $ker\,(\bar{g})$ está definido sobre k_0.

Ya que $\overline{g}$ es biyectiva, entonces existe una inversa a la que llamaremos $f : \overline{H} \longrightarrow G_2\,(L)$. Donde $\overline{H}$ es una subvariedad abeliana de A y $G_2 = S$ es una variedad abeliana definida sobre k_0. Es inmediato que $f\,(H) = G_2\,(k_0)$ pues $\overline{g}$ extiende a g. Así hemos demostrado la primera parte del teorema.

Para la segunda, defino $X_0 = f(X)$. Como X es cerrado, irreducible y $\overline{X \cap H} = X$ entonces $f(X) = X_0$ es cerrado, irreducible y $\overline{f(X \cap H)} = f(X)$. Pero $f(X \cap H) \subseteq f(H)$, así que $f(X \cap H)$ está contenido en k_0 (pues $f\,(H)$ lo está). Y por un teorema antes demostrado, $\overline{f(X \cap H)} = f(X)$ también está definida sobre k_0. Así que $X_0 = f(X) = \overline{f(X \cap H)}$ también está definido sobre k_0. Lo cual termina la demostración. □

El resto de la demostración, consiste en reducir el teorema 8.2 a la proposición anterior. Lo que haremos es demostrar que dadas las condiciones del teorema 8.2 entonces existe un subgrupo G_1 de H, de tal forma que $\overline{G_1 \cap X} = X$ con G_1 casi fuertemente minimal, δ definible, conectable y no uno-basado. Lo anterior es suficiente porque la hipótesis más importante sobre el grupo H, es que su intersección con X es densa en X, pues si recordamos las motivaciones del enunciado de Mordell-Lang, cuando lo anterior sucede, lo que tenemos es información sobre la variedad X.

Por el teorema 5.97 Existe un subgrupo $G \subseteq H$ de tal forma que:

- G es conectable, existe un F finito de tal forma que $G \subseteq acl\left(F \cup Y_1 \cup \ldots \cup Y_n\right)$ con Y_i fuertemente minimal, δ-definible y G es máximo con esas propiedades.
- $G = G_1 + \ldots + G_k$ donde cada G_i es casi fuertemente minimal, conectable, δ-definible subgrupo de G y los $G_{i's}$ son ortogonales en parejas.

Sea $F \subseteq F_0$ un conjunto finito de L de tal forma que A, X, H, G y los $G_{i's}$ son definibles sobre F_0.

Definición 8.4. *Sea G un grupo δ-definible definido sobre F_0. Decimos que G es **rígido*** si para todos los subgrupos de G que sean δ-definibles y conectados, son δ-definibles sobre $acl\left(F_0\right)$.

Ser rígido tiene una equivalencia que nos será útil, los detalles se puede buscar en [11].

Lema 8.5. *G es rígido si y sólo si no existe una familia infinita de subgrupos de G que sean uniformemente δ-definibles.*

Lema 8.6. *El grupo G dado por el teorema 5.97 es rígido.*

Demostración. Primero notemos que es suficiente con demostrar que cada G_i es rígido: Demostraré que si G_1, G_2 son rígidos, entonces $G_1 + G_2$ también lo es, y eso será suficiente: Notemos que cualquier subgrupo definible en $G_1 + G_2$ es la imagen de un subgrupo definible en $G_1 \times G_2$ bajo la función definible $+ : G_1 \times G_2 \longrightarrow G_1 + G_2$. Así que es suficiente con estudiar los subgrupos definibles en $G_1 \times G_2$. Recordemos que $G_1 \perp G_2$, entonces cualquier subgrupo definible en $G_1 \times G_2$ es de la forma $H_1 \times H_2$ con H_i subgrupos definibles. Como cada G_i es rígido, entonces H_i está definido sobre F_0, así que $H_1 \times H_2$ también está definido sobre F_0. Ahora, haremos dos casos:

- Si G_i es uno-basado, entonces por el teorema 5.82 G_i es rígido.
- Si G_i no es uno-basado, entonces se cumple las hipótesis de la proposición 8.3, así que por el primer inciso, existe una variedad abeliana S, definida sobre k_0, un morfismo biyectivo y definible $h : \overline{G_i} \longrightarrow S$, de tal forma que $h\left(G_i\right) = S\left(k_0\right)$. Como $S\left(k_0\right)$ es una variedad abeliana definida sobre k_0, usando la propiedad $P3$, entonces todo subgrupo cerrado de $S\left(k_0\right)$ está definido sobre k_0 (pues ya es algebraicamente cerrado). En particular, no existe una familia uniformemente definible de subgrupos cerrados en $S\left(k_0\right)$. Pero como ya habíamos visto en **??**, todos los grupos definibles son cerrados (nuevamente estamos usando que k_0 es algebraicamente cerrado), así que no hay familia uniforme de subgrupos definibles en $S\left(k_0\right)$. Por la nota 8.5, tenemos que $S\left(k_0\right)$ es rígido. Pero es claro que la rigidez es un concepto preservado por isomorfismos definibles, así que G_i también es rígido.

□

Ahora definimos el estabilizador de un tipo estacionario:

Definición 8.7. *Sea q un tipo completo y estacionario y Y el conjunto de sus realizaciones. Supongamos que además $Y \subseteq H$ para un grupo H. Defino al **estabilizador*** de Y en términos de la teoría de modelos de la siguiente forma:

$$StabTM\left(Y\right) = \{h \in H : RM\left(\left(h + Y\right) \cap Y\right) = RM\left(Y\right)\}$$

En el caso de las variedades algebraicas, este estabilizador coincide con un viejo conocido:

Proposición 8.8. *Sea H un grupo contenido en una variedad algebraica y $q\left(L\right) = Y \subseteq H$ con un tipo estacionario q, entonces:*

$$Stab\left(Y\right) = StabTM\left(Y\right)$$

La demostración de este hecho se puede encontrar en[20].

Los siguientes dos lemas implicarán el corolario 8.11.

Lema 8.9. *Existe un tipo estacionario q (sobre un $F_0 \subseteq E$ finito) en $X \cap H$ (es decir que el conjunto de sus realizaciones está contenido en $X \cap H$) de tal forma que $Y = q(L)$ es denso en X y $StabTM(Y)$ en H es finito.*

Demostración. Primero vamos a enunciar la siguiente afirmación, cuya demostración se puede encontrar [28] y no incluimos aquí.

Afirmación. *Sea A un espacio topológico, $D \subseteq A$ cualquier conjunto y $W \subseteq A$ denso en A. Entonces $W \cap D$ o $W \backslash D$ es denso en A.*

Ahora construiremos al tipo q. Como queremos que esté contenido en $X \cap H$. Consideramos al tipo (no completo) q_0 que contiene a todas las fórmulas $x \in X \cap H$, así que en particular $q_0(L) \subseteq X \cap H$; también por lo anterior $q_0(L)$ es denso en $X \cap H$. Ahora el trabajo es encontrar un tipo completo que extienda a q_0 y que sea estacionario. Sea F_0 el conjunto que ya habíamos mencionado antes sobre el cual X y H se definen.

Enumeremos a todas las fórmulas con parámetros en $acl(F_0)$ (así el conjunto de parámetros es acl-cerrado): $\phi_1, \phi_2, \ldots$. Construiuré una cadena de tipos $q_0 \subseteq q_1 \subseteq \ldots$ de manera inductiva: En el paso i, supongamos que $q_i(L)$ es denso en $X \cap H$. Por la afirmación anterior, $q_i \cup \phi_{i+1}(L)$ o $q_i \cup \neg\phi_{i+1}(L)$ es denso en $X \cup H$. Así que construyamos q_{i+1} igual a $q_i \cup \phi_{i+1}$ o $q_i \cup \neg\phi_{i+1}$ de acuerdo al caso. Ahora consideremos el tipo $\cup_{i=1}^{\infty} q_i$ el cual es completo.

Por el teorema 5.40 este tipo es estacionario, pues L tiene eliminación de imaginarios. Denotemos $q(L) = Y$.

Ahora resta probar que este tipo tiene estabilizador finito. Como estamos trabajando en una teoría ω-estable entonces $RM(Y)$ existe, así que es posible considerar a Y con rango de Morley mínimo. Por otro lado, como X es infinito y $\bar{Y} = X$, entonces $RM(Y) = \alpha > 0$.

Sea $h \in StabTM(Y)$, la idea es demostrar que $h \in Stab(Y)$ y como es finito entonces habríamos terminado. Lo primero que haré es demostrar que $(h + Y) \cap Y$ es Zariski denso en X. Sea $U \subseteq X$ cualquier abierto definido sobre un conjunto de parámetros D, quiero demostrar que $((h + Y) \cap Y) \cap Y \neq \emptyset$. Por la suposición de minimalidad de $RM(Y)$ y porque el Rango de Morley respeta contenciones: $RM(Y \cap U) = \alpha$. Por otro lado, el lema nos dice que $RM(Y \cap U)$ es igual al supremo de los $RM(a/F)$ sobre $a \in Y \cap U$ y F cualquier conjunto de parámetros sobre el que se defina $Y \cap U$, y como el supremo se alcanza podemos tomar $a \in Y \cap U$ de tal forma que $RM(a/D \cup acl(F_0))$.

La proposición 8.8 nos dice que $h \in Stab(Y)$, así que $h + a \in Y$. Así que $h + a \in (h + Y) \cap Y$ y por la definción de $StabTM(Y)$: $RM(h + a/D \cup acl(F_0)) = RM(a/D \cup acl(F_0))$.

Además sabemos que q es estacionario y $a \in q(L) = Y$, así que $tp(a/D \cup acl(F_0))$ extiende a q. Entonces cualquier otra extensión de q que no separe será igual a $tp(a/D \cup acl(F_0))$, en particular $tp(a/D \cup acl(F_0)) = tp(h + a/D \cup acl(F_0))$. En particular $h+a \in Y \cap U$, lo cual significa que $((h + Y) \cap Y) \cap Y \neq \emptyset$. Por tanto $(h + Y) \cap Y$ es denso en X.

Sabemos por otro lado que $\overline{(h + Y) \cap Y} \subseteq (h + X) \cap X \subseteq X$, en particular $(h + X) \cap X = X$. Así que $h \in Stab(X)$, el cuál es finito. En particular $StabTM(Y)$ es finito.

□

Lema 8.10. *Dadas todas las condiciones anteriores, supongamos el tipo estacionario q dado por el último lema. Entonces $q(L)$ está contenido en una única clase lateral de G.*

Corolario 8.11. *$X \cap G$ es Zariski denso en X.*

Demostración. Como la conclusión del teorema 8 habla de que X es un trasladado de la imagen inversa de una variedad definida sobre k_0, podemos reemplazar libremente a X por un trasladado de ella. Así que, utilizando los lemas anteriores, podemos suponer que $Y \subseteq G$ (pues ya estaba contenido en una clase lateral de G). Como $\overline{Y} = X$, entonces $\overline{X \cap G} = X$ que es la conclusión de la proposición que estamos demostrando. □

Ahora afirmo que G no es uno-basado. Si lo fuera, por el teorema 7.16 tendríamos que $G \cap X = \cup_{i=0}^{n} (g_i + G_i)$ y como $G \cap X$ es denso en X, entonces $X = \cup_{i=0}^{n} \overline{(g_i + G_i)}$. Pero X es irreducible, así que $X = g_0 + \overline{G_0}$, es decir: una variedad abeliana. Por otro lado recordemos que $Stab_X$ es finito, y como estamos suponiendo que X no es finita, entonces $\overline{G_0}$ tampoco lo es. Pero $\overline{G_0}$ tiene estructura de grupo, así que $g_0 + g' + g \in \overline{G_0}, \forall g, g' \in \overline{G_0}$, lo cual contradice que $Stab_X$ es finito. Así que G no es uno-basado. Como sus subgrupos son ortogonales sabemos por la proposición 7.18 que uno de ellos no es uno-basado, llamémosle G_i.

De hecho podemos decir más sobre ese grupo G_i que existe y no es uno-basado:

Proposición 8.12. *Existe un único sumando en la descomposición de G que no es uno-basado. Digamos G_1.*

Demostración. Sea G_1 alguno de «esos» grupos que no son uno-basados. Si Y_1 es el conjunto fuertemente minimal tal que $G_1 \subseteq acl\,(Y_1)$. Ya habíamos dicho (teorema 6.16) que los conjuntos fuertemente minimales sobre campos diferencialmente cerrados son geometrías de Zariski. Así que como la conjetura de Zilber es cierta para las geometrías de Zariski 6.15, entonces k_0 es definible en Y_1, y como ellos son fuertemente minimales, entonces Y_1 y k_0 no son ortogonales (ver lo hecho en el segundo párrafo de la proposición 8.3). Si suponemos que existe otro conjunto fuertemente minimal Y_2 (que corresponda a un sumando G_2 en la descomposición de G), entonces también k_0 y Y_0 serían no-ortogonales. Pero la no-ortogonalidad es una relación de equivalencia para los conjuntos fuertemente minimales (lema 5.86), y como k_0 es un campo algebraicamente cerrado, entonces también es fuertemente minimal, así que (transitividad) Y_1 y Y_2 son no-ortogonales. Pero se había supuesto que en la descomposición de G, los conjuntos fuertemente minimales fueran ortogonales a pares. Así que sólo puede existir un G_i que no sea uno-basado, llamémosle G_1. □

Ahora queremos demostrar que $G_1 \cap X$ es denso en X, para ello utilizaremos el siguiente lema:

Lema 8.13. *Existe una única clase lateral de G_1 que contiene a Y.*

Corolario 8.14. *$X \cap G_1$ es Zariski denso en X.*

Demostración. Como $Y \subseteq g_1 + G_1$ (una clase lateral vista como conjunto), entonces podemos trasladar nuevamente (pues X será un trasladado) y obtenemos que $Y \subseteq G_1$. Entonces $\overline{Y} = \overline{X \cap G_1} = X$. □

Así tenemos que G_1 no es uno-basado, es casi fuertemente minimal y además es δ-definible. Pero lo más importante: $G_1 \cap X$ es Zariski denso en X. Así que demostrar Mordell-Lang para este G_1 sería suficiente. Ahora sólo apliquemos la proposición 8.3 y hemos terminado.

9. APÉNDICE: GEOMETRÍA ALGEBRAICA Y VARIEDADES ABELIANAS

El objetivo de esta sección es introducir los conceptos de geometría algebraica necesarios para entender el enunciado y la demostración de la conjetura de Mordell-Lang. No pretendo ser exhaustivo ni mucho menos simplificar la geometría algebraica utilizada para describir las variedades abelianas, sin embargo pretendo que un lector no familiarizado con el tema conozca todas las definiciones que serán utilizadas en el texto. Para aquellos que después de leer esta invitación a las variedades abelianas deseen profundizar les recomiendo ampliamente las siguientes referencias [8], [7] y [9].

Hablaremos sobre geometría algebraica en el lenguaje de las variedades algebraicas y no desde el punto de vista de los esquemas. La demostración original de Hrushovski usa el lenguaje de los esquemas, y aunque ese hecho hace que su demostración sea aún más general, trabajar con esquemas no aporta nada a las ideas que pretendo exponer en esta tesis. A pesar de que es posible hablar de variedades en general, en este apéndice sólo incluiré variedades afines y proyectivas.

Sea k un campo y $\bar{k}$ su cerradura algebraica.

Definición 9.1.

- *El **espacio afín de dimensión** n **sobre** k* denotado por $\mathbb{A}_k^n$ o símplemente $\mathbb{A}^n$ es el conjunto:
$$\mathbb{A}^n = \left\{(x_1, \ldots, x_n) : x_i \in \bar{k}\right\}$$
- Si $k \subseteq l \subseteq \bar{k}$ es un campo, definimos al **conjunto de l-puntos racionales** de $\mathbb{A}^n$ como el conjunto:
$$\mathbb{A}^n(l) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n : x_i \in l\}$$

Existe una manera alternativa de caracterizar a los puntos l-racionales del espacio afín cuando el campo l es perfecto:

$\mathbb{A}^n(l) = \left\{(x_1, \ldots, x_n) \in \mathbb{A}^n : \sigma(x_i) = x_i \forall \sigma \in G\left(\bar{k}/l\right)\right\}$ donde $G\left(\bar{k}/l\right)$ es el grupo de Galois. La notación $\mathbb{A}^n(-)$ es la de un funtor que a cada campo perfecto l le asigna el conjunto $\mathbb{A}^n(l)$.

Definición 9.2. *Sea $I \subseteq \bar{k}[x_1, \ldots, x_n] = \bar{k}[x]$ un ideal, a I le asociamos su **conjunto de ceros:***
$$Z(I) = \left\{x \in \mathbb{A}^n : P(x) = 0 \forall P \in \bar{k}[x]\right\}$$

La observación importante es que si $H \subseteq \bar{k}[x]$ es un conjunto cualquiera entonces $Z(H) = Z(\langle H\rangle)$ donde $\langle H\rangle$ denota el ideal generado por H. Así que es suficiente con restringir nuestro estudio a los ideales. De manera análoga:

Definición 9.3. *Sea $S \subseteq \mathbb{A}^n$, definimos el **ideal generado** por S como:*
$$I_S = \left\{P[x] \in \bar{k}[x] : P(s) = 0 \forall s \in S\right\}$$

Definición 9.4. *$A \subseteq \bar{k}^n$ es un **conjunto algebraico afín*** cuando $A = Z(I)$ para algún ideal I. Sea $k \subseteq l \subseteq \bar{k}$, si suponemos que I es un ideal generado por polinomios en $l[x]$ entonces diremos que el conjunto algebraico afín A está definido sobre l.

Uno de los tres pilares de la geometría algebráica es el siguiente teorema:

Teorema 9.5. ***Teorema de la base de Hilbert.*** Cualquier ideal en $\bar{k}[x]$ es finitamente generado.

Este teorema nos dice que no sólo es suficiente con estudiar ideales para conocer todos los conjuntos algebraicos afínes sino incluso podemos restringir nuestro estudio a conjuntos finitos de polinomios.

Definición 9.6. *Sea $k \subseteq l \subseteq \bar{k}$ un campo y $Z(I) = V \subseteq \mathbb{A}^n$ un conjunto algebráico afín definido sobre k, definimos el* ***conjunto puntos l-racionales*** de V como:

$$V(l) = V \cap \mathbb{A}^n(l) = \left\{ v \in V : \sigma(v) = v \forall \sigma \in G\left(\bar{k}/l\right) \right\}$$

Ahora enunciamos propiedades fundamentales de los conjuntos algebraicos afínes, la idea principal es demostrar que mediante las operaciones $Z(-)$ e I_- es posible establecer una correspondencia entre ideales y conjuntos algebraicos afines:

Proposición 9.7. *Si $\{V_i\}_{i \in I}$ son conjuntos algebraicos afínes entonces:*

- *$\cap_{i \in I} V_i$ es un conjunto algebraico afín.*
- *$V_1 \cup V_2 \cup \ldots \cup V_n$ es un conjunto algebraico afín para todo $n \in \mathbb{N}$.*
- *Si $S_1 \subseteq S_2 \subseteq \mathbb{A}^n$ entonces $I_{S_2} \subseteq I_{S_1}$.*
- *Si $I_1 \subseteq I_2 \subseteq \bar{k}[x]$ entonces $Z(I_2) \subseteq Z(I_1)$.*
- *Si V es un conjunto algebraico afín entonces $Z(I_V) = V$*

Para tener una correspondencia completa entre ideales y conjuntos alegbraicos necesitamos el siguiente teorema el cual es considerado otro pilar dentro de la geometría algebráica:

Teorema 9.8. ***Nullstellensatz*** Sea $I \subseteq \bar{k}[x]$ un ideal entonces $I_{Z(J)} = \sqrt{J}$.

Notemos además que:

$$\mathbb{A}^n = Z(\{0\}), \emptyset = Z\left(\bar{k}[x]\right)$$

Así que es posible definir una topología:

Definición 9.9. *Para cada n definimos una topología en $\mathbb{A}^n$ como la generada por los conjuntos algebraicos afínes vistos como cerrados. A esta topología se le llama* ***topología de Zariski*** . La topología de Zariski para un conjunto algebraico A es la topología inducida por la inclusión $A \longrightarrow \mathbb{A}^n$.

De esta forma, aquellos subconjuntos B en $\mathbb{A}^n$ tales que para cada n-ada en B existe una cantidad finita de polinomios con la propiedad que alguno de esos polinomios no se hace cero al evaluar en esa n-ada, son considerados como abiertos en la topología de Zariski.

Cuando hablemos de cerradura de Zariski, de Zariski denso, de Zariski irreducible[12] o cualquier otro concepto topológico, nos referimos al concepto pertinente dentro de la topología de Zariski.

Definición 9.10. *Una* ***variedad algebraica afín*** es un conjunto algebraico afín $V \subseteq \mathbb{A}^n$ irreducible.

Proposición 9.11. *Un conjunto algebraico afín V es una variedad algebraica afín si y sólo si I_V es un ideal primo.*

Es un cambio sustancial de la geometría algebraica moderna considerar a una variedad algebraica como el conjunto de polinomios que la definen y no como los ceros de esos polinomios (sus puntos $\bar{k}$ racionales cuando los polinomios tienen coeficientes en $\bar{k}$).

Cuando no especifiquemos el campo, por una variedad nos referiremos a sus puntos $\bar{k}$ racionales. Las siguientes propiedades son de suma importancia. La primera para la geometría algebraica en general, y la segunda se utilizará en el texto.

[12]Si X es un espacio topológico y $Y \subseteq X$ decimos que Y es irreducible si no es posible expresar $Y = S_1 \cup S_2$ con S_i cerrados en X y propios en Y.

Proposición 9.12. *Supongamos $k \subseteq l \subseteq \bar{k}$ y $W \subseteq \mathbb{A}^n(l)$ entonces su cerradura de Zariski $\overline{W}$ en $\mathbb{A}^n$ está definida sobre l.*

Proposición 9.13. *Supongamos $k \subseteq l \subseteq \bar{k}$ y $W \subseteq \mathbb{A}^n(l)$ entonces la cerradura de Zariski $\overline{W}$ en $\mathbb{A}^n$ es una variedad algebraica afín.*

Antes de hablar de los que serán los morfismos en la categoría de variedades algebraicas necesitaremos el siguiente concepto:

Definición 9.14. *Sea V una variedad algebraica afín, definimos el **anillo de cordenadas afínes*** de la variedad V como $\bar{k}[x]/I_V$.

Es posible definir variedades algebraicas en general sin embargo considero que para este apéndice es suficiente si nos concentramos en las variedades algebraicas afínes y en las variedades algebraicas proyectivas. Para un tratamiento en general de las variedades algebraicas es necesario usar trucos como los de geometría diferencial: una variedad algebráica es un espacio topológico que tiene una cubierta de variedades algebraicas afines. El principal problema de esta definición es que el tratamiento de los puntos l-racionales puede ser un poco complicado.

Ahora definiremos las variedades proyectivas:

Definición 9.15. *El **espacio proyectivo*** $\mathbb{P}^n$ de dimensión n es el conjunto líneas de $\mathbb{A}^{n+1}$ que pasan por el orígen. A cada una de esas líneas las llamaremos puntos del espacio proyectivo.

Es posible identificar cualquiera de esas líneas con una clase de equivalencia en $\mathbb{A}^{n+1}$ módulo la relación de equivalencia que identifica dos puntos cuando estén en la misma línea que pase por el orígen.

Sea $p \in \mathbb{P}^n$, es posible asignarle coordenadadas a p a las que llamaremos **coordenadas homogéneas** de p: $(x_0 : x_1 : \ldots : x_n)$ con $x_i \in \bar{k}$ cuando p represente la clase de equivalencia del punto $(x_0, x_1, \ldots, x_n)$.

Definición 9.16. *Sea $k \subseteq l \subseteq \bar{k}$ definimos el conjunto de **puntos l-racionales*** de $\mathbb{P}^n$ como el conjunto de líneas de $\mathbb{A}^{n+1}$ que está definidas sobre l. Lo denotaremos por $\mathbb{P}^n(l)$.

Existen varias maneras distintas de ver a $\mathbb{P}^n(l)$:

- $\mathbb{P}^n(l)$ coíncide con el conjunto de puntos en $\mathbb{P}^n$ para los que es posible encontrar coordenadas homogéneas en $\mathbb{A}^{n+1}(l)$.
- $\mathbb{P}^n(l)$ coíncide con el conjunto de puntos con coordenadas homogéneas $(x_0 : x_1 : \ldots : x_n)$ de tal forma que para toda $x_j \neq 0$ todos los $x_i/x_j \in l$.
- $\mathbb{P}^n(l)$ coíncide con el conjunto de puntos cuyas coordenadas homogéneas quedan fijas por el grupo de Galois $G\left(\bar{k}/l\right)$.

Definición 9.17. *Sea $p \in \mathbb{P}^n$, el **campo de definición*** de P es la extensión l más pequeña de k de tal forma que $G\left(\bar{k}/l\right) = \left\{\sigma \in G\left(\bar{k}/k\right) : \sigma(P) = P\right\}$

Ahora vamos a definir los conjuntos algebraicos proyectivos:

Definición 9.18. *$S \subseteq \mathbb{P}^n$ es con conjunto algebraico proyectivo si $S = Z(J)$ donde $J \subseteq \bar{k}[x]$ es un ideal de polinomios homogéneos.*

La topología de Zariski para $\mathbb{P}^n$ se define de la misma manera que para el espacio afín, así mismo las **variedades proyectivas** .

La correspondencia entre ideales y conjuntos algebraicos proyectivos es casi la misma salvo un pequeño error, mientras que nuevamente es cierto que un conjunto S es una variedad proyectiva si y sólo si I_S es un ideal primo.

También el anillo de coordenadas homogéneas se define de la misma manera para las variedades proyectivas.

Nuestra meta es definir la idea adecuada de morfismo entre variedades, como queremos que un morfismo no dependa de la inclusión de una variedad en el espacio afín o en el proyectivo consideraremos una variedad algebraica en abstracto como un espacio topológico que se puede cubrir con espacios afines. Una **subvariedad algebraica** es un cerrado que es una variedad algebraica con la topología inducida .

Definición 9.19. *Sea X una variedad algebraica y $s \in X$. Una función $f : X \longrightarrow \bar{k}$ es **regular** en s* cuando existe una vecindad abierta de s $U \subseteq X$ que sea homeomorfa a un espacio afín y dos polinomios $p, q \in \bar{k}[x]$ de tal forma que $q(s) \neq 0$ y además $f(r) = p(r)/q(r)\ \forall r \in U$. La función f es regular en X cuando lo sea para cada punto de X. El anillo de funciones regulares en X se denota por $O(X)$.

Definición 9.20. *Sea $x \in X$ con X una variedad algebraica. Definimos el anillo local de X en x como el **anillo de funciones regulares en** x* al identificar funciones regulares cuando coíncidan en una vecindad abierta de x. A este anillo lo denotaremos por $O_{x,X}$.

Definición 9.21. *Sean $Y \subseteq X$ una subvariedad algebraica y una variedad algebraica respectivamente. Definimos el **anillo local de X a lo largo de Y*** como el conjunto de parejas ordenadas (U, f) donde $U \subseteq Y$ es un abierto de X con $U \cap Y \neq \emptyset$ y $f \in O(U)$ es una función regular y donde identificamos dos parejas (U, f) y (V, g) cuando $f = g$ en $U \cap V$. A este anillo lo denotamos por $O_{Y,X}$.

En la definición anterior, cuando $Y = X$ entonces $O_{Y,X}$ no sólo es un anillo sino también un campo. Así llegamos a la definición de campo de funcione:

Definición 9.22. *Sea X una variedad algebraica, definimos al **campo de funciones*** de X como $O_{X,X}$ al que denotaremos por $\bar{k}(X)$.

Ahora enunciamos unas primeras propiedades de los campos de funciones:

- $\bar{k}(\mathbb{P}^n) = \bar{k}(x)$.
- $\bar{k}(X)$ es isomorfo al campo de fracciones del anillo de coordenadas locales $\bar{k}[X]$.

Gracias al campo de funciones es posible definir una dimensión para las variedades algebraicas.

Definición 9.23. *Sea X una variedad algebraica, definimos la **dimensión*** de X como el grado de trascendencia de $\bar{k}(X)$ sobre $\bar{k}$.

Ahora por fin lleamos al concepto de morfismo:

Definición 9.24. *Sean X, Y dos variedades algebraicas, un mapeo $\phi : X \longrightarrow Y$ es un **morfismo*** cuando sea continuo y para todo abierto $U \subseteq Y$ y toda $f \in O(U)$, la función $f \circ \phi$ es regular en $\phi^{-1}(U)$.

Los «morfismos» anteriores serán de utilidad, sin embargo son las funciones racionales las que tendrán las mejores propiedades:

Definición 9.25. *Sean X, Y dos variedades algebraicas, a una función $\phi : X \longrightarrow Y$ se le llama **mapeo racional*** cuando existe un $U \subseteq X$ donde ϕ es un morfismo.

Definición 9.26. *Un **mapeo birracional*** entre dos variedades algebraicas X, Y es un mapeo racional ϕ con inverso racional.

Diremos que un morfismo entre variedades está **definido sobre** l cuando los polinomios que las hacen una función regular tienen coeficientes en l.

Nos interesarán aquellas variedades algebraicas con más estructura:

Definición 9.27. *Sea V una variedad algebraica, diremos que V es un **grupo algebraico*** cuando existan dos morfismos $f : V \times V \longrightarrow V$, $g : V \longrightarrow V$ y un $e \in V\left(\bar{k}\right)$ de tal forma que tomando a f como la operación dentro del grupo, a g como la función que a cada elemento lo manda a su inverso y a e como al elemento identidad V tiene estructura de grupo.

Definición 9.28. *Una variedad algebraica V se dirá que es **completa*** cuando la proyección $p : V \times W \longrightarrow W$ es cerrada (manda cerrados en cerrados) para toda variedad W.

Todas las variedades proyectivas son completas.

Definición 9.29. *Una **variedad abeliana** A* es un grupo algebraico que además es completo. Una **subvariedad abeliana** de V es un subgrupo de A que además es cerrado.

En el caso de curvas algebraicas (i.e. variedades algebraicas de dimensión 1) siempre es posible construir una variedad abeliana que contenga una copia isomorfa de la curva:

Teorema 9.30. *Dada una curva algebraica C con género mayor o igual a 1, es posible construir una variedad abeliana $J(C)$ de tal forma que $C \hookrightarrow J(X)$. A $J(C)$ le llamaremos la **jacobiana*** de la curva C.

Ahora enunciaremos propiedades importantes sobre las variedades abelianas.

Proposición 9.31. *Sea A una variedad abeliana, si G es un subgrupo de $A(l)$ con $k \subseteq l \subseteq \bar{k}$, entonces la cerradura de Zariski de G en $\bar{k}$ es una variedad abeliana.*

Proposición 9.32. *Si A es una variedad abeliana, entonces $A(l)$ es un grupo abeliano para todo $k \subseteq l \subseteq \bar{k}$.*

Lema 9.33. *Supongamos que tenemos una extensión de campos $k \subseteq K$. Sea $A \subseteq k^n$. Si V es la cerradura de Zariski de A en K, entonces V es k cerrado.*

Un teorema fundamental en la teoría de variedades abelianas es el siguiente:

Teorema 9.34. ***[Teorema de Chevalley.]*** Si G es un grupo algebraico definido sobre un campo algebraicamente cerrado K, entonces existe un subgrupo cerrado M que además es minimal y definido sobre K, de tal forma que G/M es una variedad abeliana.

Por último enunciaremos algunas propiedades de las variedades abelianas que utilizaremos en la demostración de Mordell-Lang. Las demostraciones las pueden encontrar en [28]. En el resto del documento, nos referiremos a ellas como P seguida del número que representan.

Propiedades. Sea A una variedad abeliana definida sobre un campo algebraicamente cerrado K de característica cero.

1. A es un grupo conmutativo algebraico y que está conectado.
2. El subgrupo de n-torsión (con $n \in \mathbb{N}$) de A es finito, mientras que el subgrupo de torsión es infinito.
3. Si A estuviera definida sobre un campo $k < K$, y G es un subgrupo cerrado en A, entonces G está definido sobre la cerradura algebraica de k.

REFERENCIAS

[1] Wei Liang Chow. On the quotient variety of an Abelian Variety. 1952
[2] David, Zywina. Abelian Varieties over large algebraic fields with infinite torsion.
[3] Deirdre Haskell, Anand Pillay and Charles Steinhorn. Model Theory, Algebra and Geometry. Mathematical Sciences Research Institute. 2000
[4] David Marker. Model Theory, an introduction. Springer. 2002
[5] Marcja. A guide to Classical and Modern Model Theory. Kluwer Academic Publishers. 2003
[6] Boris Zilber. Zariski Geometries. Cambridge University Press. 2010
[7] Robin Hartshorne. Algebraic Geometry. Springer. 1977
[8] Marc Hindry. Diophantine geometry. Springer. 2000
[9] I. R. Shafarevich. Algebraic Geometry. Springer. 1994
[10] Bruno Poizat. A Course in Model Theory. Springer. 2000
[11] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Springer. 1998
[12] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 1 - Introduction to model theory. Springer. 1998
[13] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 2 - Introduction to stability theory and Morley. Springer. 1998
[14] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 3 - Omega-stable groups. Springer. 1998
[15] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 4 - Model theory of algebraically closed fields. Springer. 1998
[16] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 5 - Introduccion to abelian varieties. Springer. 1998
[17] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 6 - The model theoretic content of lang conjucture. Springer. 1998
[18] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 7 - Zarisky geometries. Springer. 1998
[19] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 9 - Separable closed fields. Springer. 1998
[20] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 10 - Proof of mordel lang conjecture. Springer. 1998
[21] Elisabeth Bouscaren. Model theory and Algebraic Geometry. Chapter 11 - Proof of mains theorem by reduction to positive characteristic. Springer. 1998
[22] Joris Potier. ACF not locally modular. Pdf. 2007
[23] Anand Pillay. Lecture notes - Applied Stability Theory. Differential fields. Pdf. 2003
[24] Anand Pillay. Lecture notes - Model Theory. Pdf. 2002
[25] Anand Pillay. Lecture notes-Stability Theory. Pdf. 2003
[26] David Marker. Model Theory of Differential Fields. Pdf.
[27] Robert Lakatos. Model Theory and the Mordell-Lang conjecture. Pdf. 2001
[28] Christopher Eagle. The Mordell-Lang Theorem from the Zilber Dichotomy. Pdf. 2010
[29] Geometry of Strongly Minimal Sets. Pdf.
[30] Ehud Hrushovski. The Mordell-Lang conjucture for function fields. Pdf. 1996
[31] Michael McQuillan. Division points on semi-abelian varieties. Pdf. 1995
[32] Pete L. Clark. Curves over global fields violating the hasse principle. Pdf.
[33] John B. Goode. H. L. M. (Hrushovski-Lang-Mordell). Pdf. 1996
[34] Serge Lang. Integral points on curve. Pdf. 1960
[35] P. Samuel. Lectures on old and new results on algebraic curves. Pdf. 1966
[36] Megumu Miwa. On Mordell's conjecture for the curve over function field with arbitrary constant field. Pdf. 1968
[37] Kazuhisa Maehara. On the higher dimensional mordell conjecture over function fields. Pdf. 1989
[38] Pierre Samuel. Compléments à un article de Hans Grauert sur la conjecture de Mordell. Pdf. 1966
[39] Dragos Ghioca. The isotrivial case in the Mordell-Lang Theorem. Pdf.
[40] Dan Abramovich y Jose Felipe Voloch. Toward a proof of the Mordell-Lang conjecture in characteristic. Pdf. 1995
[41] T. M. Gendron. Introducción rápida a la teoría de modelos. Pdf. 2010
[42] T. M. Gendron. Introducción rápida a la teoría de modelos. Pdf. 2010
[43] A. Buium, Intersections in jet spaces and a conjecture of S. Lang, Ann. of Math. 1992
[44] Anand Pillay. Geometric Stability Theory (Oxford Logic Guides)

[45] Zoé Chatzidakis, Dugald Macpherson, Anand Pillay and Alex Wilkie. Model Theory with Applications to Algebra and Analysis: Volume 1 (London Mathematical Society Lecture Note Series).
[46] Ehud Hrushovski and Boris Zilber, Zariski geometries. J. Amer. Math. Soc. 9, 1996
[47] Grothendieck, Alexandre; Dieudonné, Jean (1961). Éléments de géométrie algébrique II. Étude globale élémentaire de quelques classes de morphismes.
[48] Yu. Manin. Rational points on an algebraic curve over function fields. Trans American Mathematical Society.
[49] K. Tent and Martin Ziegler. A course in Model Theory.