Programa del Seminario de Álgebra, Geometría algebraica y Singularidades 2018

Se detalla a continuación los resúmenes de todas la charlas impartidas en el Seminario de Álgebra, Geometría algebraica y Singularidades, durante el año 2018.

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 31 de enero de 2018, 16:00 a 17:00 horas.

Elementos con factorizaciones de igual longitud en semigrupos numéricos

M. A. Moreno-Frías [**]
Universidad de Cádiz[1]

Denotemos por $\mathbb{N}$ el conjunto de los enteros no negativos. Un *semigrupo numérico* S es un subconjunto no vacío de $\mathbb{N}$ que es cerrado bajo la suma, contiene el elemento nulo y tiene complemento finito en $\mathbb{N}$. Si $A = \{a_1, \ldots, a_p\}$ es un subconjunto de $\mathbb{N}$ tal que $\gcd(a_1, \ldots, a_p) = 1$, entonces se verifica (ver [6]) que el conjunto $\langle A\rangle = \{\sum_{i=1}^{p} x_i a_i : x_i \in \mathbb{N}, a_i \in A, 1 \leq i \leq p\}$ es un semigrupo numérico. También puede verse en [6], que todo semigrupo numérico es de esta forma. Si $S = \langle A\rangle$, diremos que A es un *sistema generador* del semigrupo S. Todo semigrupo numérico posee un único sistema minimal de generadores (respecto de la cardinalidad y relación de inclusión). Llamaremos *dimensión de inmersión*, al cardinal del sistema minimal de generadores del semigrupo. Dado $S = \langle a_1, \ldots, a_p\rangle$, si $s \in S$ entonces se tiene que $s = x_1a_1 + \ldots + x_pa_p$. Diremos, en este caso que $(x_1, \ldots, x_p)$ es una *factorización* del elemento s. Llamaremos *longitud* de s al número entero no negativo $x_1 + \ldots + x_p$. El estudio de las longitudes de las factorizaciones de un elemento en un semigrupo es un tópico de gran interés en la teoría de factorización no única para semigrupos, como así lo atestiguan el gran número de publicaciones recientes (ver [3], [2] y [1]), siendo [5] un manual de referencia

En [4], los autores proporcionan una fórmula para calcular en un semigrupo de dimensión de inmersión 3, el elemento más pequeño tal que a partir de él todos los elementos tienen dos factorizaciones de igual longitud. Ellos también muestran que esta fórmula no es válida para dimensiones superiores a 3.

Nuestro objetivo en esta charla es calcular una cota a partir de la cual todos los elementos del semigrupo S con dimensión de inmersion p, siendo $p \geq 3$, tienen m factorizaciones de igual longitud.

Referencias

[1] F. Aguiló-Gost, D. Llena, *Computing denumerants in numerical 3-semigroups,* arXiv:1706.08768, 2017.

[**]Supported by FQM-298 (Junta de Andalucía).

[2] A. Assi, P. A. García-Sánchez, *Nunerical Semigroups and Applications,* Springer, New York, 2016.

[3] S. Colton, N. Kaplan, *The realization problem for delta sets of numerical semigroups,* arxiv.org/pdf/1503.08496 (2016).

[4] S. T. Chapman, P. A. García, D. Llena and A. Marshall, *Elements in a numerical semigroup with factorizations of the same length,* Canad. Math. Bull. 54 (2011), no. 1, 39–43

[5] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory,* Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, 2006.

[6] J. C. Rosales, and P. A. García-Sánchez, *Numerical semigroups,* Developments in Mathematics, 20. Springer, New York, 2009.

[1]Departamento de Matemáticas
Universidad de Cádiz
mariangeles.moreno@uca.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 31 de enero de 2018, 17:00 a 18:00 horas.

El juego de la mordida en semigrupos numéricos

Ignacio García Marco
Universidad de La Laguna[1]

Sea P un conjunto parcialmente ordenado (poset) con un elemento mínimo que llamaremos 0. Una mordida consiste en elegir un elemento x de P y eliminar todos los elementos que son mayores o iguales que x. En el juego de la mordida, dos jugadores muerden el poset alternativamente y pierde el jugador que se vea obligado a morder el elemento 0. Este juego generaliza varios juegos clásicos como el NIM, Divisores o el juego de la tableta de chocolate.

El tipo de preguntas que uno busca resolver es: Dado P un poset, ¿ cuál de los dos jugadores tiene una estrategia ganadora? o ¿ cuál es la estrategia ganadora? En esta charla buscaremos darle respuesta a estas preguntas cuando el poset proviene de un semigrupo numérico.

Esta charla estś basada en un trabajo conjunto con Kolja Knauer.

[1]Departamento de Matemáticas, Estadística e I.O.
Universidad de La Laguna
iggarcia@ull.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 15 de febrero de 2018, 16:00 a 17:00 horas.

Estudio y cálculo de la regularidad de Castelnuovo-Mumford y otros invariantes de álgebras graduadas de dimensión dos

Eva García Llorente
Universidad de La Laguna[1]

Dado un ideal homogéneo pesado I del anillo de polinomios $R := K[x_1, \ldots, x_n]$ sobre un cuerpo K, estudiamos distintos invariantes del anillo cociente R/I. Veremos métodos efectivos para calcular distintos invariantes, como la regularidad de Castelnuovo-Mumford, y propiedades del mismo (por ejemplo, Cohen-Macaulay o Gorenstein), haciendo especial énfasis en dimensión 2. Además especializaremos los resultados para anillos de semigrupo simpliciales y distintas familias de curvas monomiales proyectivas.

[1]Departamento de Matemáticas, Estadística e I.O.
Universidad de La Laguna
evgarcia@ull.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 3 de abril de 2018, 18:30-19:30

El criptosistema DME

Miguel Ángel Marco Buzunáriz
Universidad de Zaragoza[1]

Los criptosistemas de clave pública que se usan habitualmente (RSA, El Gamal, ECDH...) se basan en el problema de la factorización de enteros o del cálculo del logaritmo discreto en grupos cíclicos.

Desgraciadamente, ambos problemas son vulnerables al algoritmo de Schor, que puede ejecutarse en tiempo polinomial en ordenadores cuánticos. Por lo tanto, se hace necesario proponer alternativas que sean resistentes a este tipo de ataques. Hasta ahora se han planteado posibles alternativas basadas en distintas teorías: retículos, códigos correctores de errores, funciones hash ...

Una de estas familias es la de los sistemas multivariantes, consistentes en aplicaciones polinómicas de varias variables. En esta charla presentamos un nuevo criptosistema de esta familia, llamado DME (double matrix exponentiation).

[1]Universidad de Zaragoza
mmarco@unizar.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 18 de abril de 2018, 16:00 a 17:00 horas.

Semigrupos numéricos y sus interacciones con ideales tóricos y estructuras discretas.
Semigrupos numéricos

Ignacio García Marco
Universidad de La Laguna[1]

Los semigrupos numéricos son submonoides de los números naturales con la suma usual. A todo semigrupo numérico se le puede dotar de una estructura de conjunto parcialmente ordenado (poset) de una forma natural.

Esta primera parte está dedicada al estudio de los semigrupos numéricos. Introduciremos conceptos como el número de Frobenius, los números de pseudo-Frobenius, el tipo del semigrupo y los conjuntos de Apéry del semigrupo. Estudiaremos cómo estos conceptos se interrelacionan y cómo la estructura de poset asociada puede ayudar a entender estos conceptos.

[1]Departamento de Matemáticas, Estadística e I.O.
Universidad de La Laguna
iggarcia@ull.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 25 de abril de 2018, 15:15 a 16:15 horas.

Semigrupos numéricos y sus interacciones con ideales tóricos y estructuras discretas.
Cálculos en semigrupos numéricos por medio del ideal tórico asociado.

Ignacio García Marco
Universidad de La Laguna[1]

En esta segunda parte introduciremos el concepto de ideal tórico asociado a un semigrupo numérico. Estudiaremos cómo se pueden traducir y resolver problemas de semigrupos numéricos en términos del ideal tórico asociado. La herramienta para resolver estos problemas serán típicamente las bases de Gröbner, es por ello que esta charla comenzará con una corta introducción a las bases de Gröbner.

[1]Departamento de Matemáticas, Estadística e I.O.
Universidad de La Laguna
iggarcia@ull.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 2 de mayo de 2018, 16:00 a 17:00 horas.

Semigrupos numéricos y sus interacciones con ideales tóricos y estructuras discretas.
La resolución libre minimal graduada de un ideal tórico unidimensional

Ignacio García Marco
Universidad de La Laguna[1]

Introduciremos con ejemplos el concepto de resolución libre minimal graduada de un ideal y nos centraremos en el estudio de estas resoluciones para ideales tóricos unidimensionales. Veremos cómo el semigrupo numérico asociado (y los conceptos introducidos en la Parte 1) nos pueden dar mucha información relevante sobre esta resolución.

[1]Departamento de Matemáticas, Estadística e I.O.
Universidad de La Laguna
iggarcia@ull.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 8 de mayo de 2018, 17:15 a 18:15 horas.

On some properties of resolutions of surface singularities

Meral Tosun
Galatasaray University[1]

In this introductory talk we will present some examples of surfaces with a singular point and, their resolutions. We aim to relate geometry, algebra and combinatorics.

[1]Galatasaray University
Estambul, Turquía
mtosun@gsu.edu.tr

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 16 de mayo de 2018, 16:00 a 17:00 horas.

Tangentes en puntos singulares de espacios analíticos complejos

Jawad Snoussi
UNAM[1]

Un punto singular de un espacio analítico o algebraico es precisamente un punto donde el espacio tangente no está claramente definido. En la literatura, se encuentran varias nociones que pueden sustituir la idea de tangencia en los puntos singulares. Presentaremos algunos de estos conceptos y mostraremos relaciones entre ellos. Trataremos los casos de curvas y superficies.

[1]Instituto de Matemáticas,
UNAM, Cuernavaca, México
jsnoussi@im.unam.mx

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 4 de junio de 2018, 16:30 a 17:30 horas.

Esquemas de compartición de secretos en rampa

Diego Ruano
Universidad de Valladolid[1]

La compartición de secretos (secret sharing) es un método criptográfico para distribuir un secreto entre un grupo de participantes. Cada participante recibe una participación del secreto de forma que éste sólo se puede recuperar cuando un número suficiente de participaciones son combinadas. Los métodos matemáticos incluyen la teoría de códigos lineales y métodos algebraicos. Trabajaremos con esquemas en rampa que permiten reducir el tamaño de las participaciones y veremos su seguridad, sus limitaciones y algunas construcciones.

[1]Departamento de Álgebra, Análisis, Geometría y Topología
Universidad Valladolid, España
diego.ruano@uva.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 11 de junio de 2018, 17:30 a 18:30 horas

Resolución de curvas planas

Ana Belén de Felipe Paramio
Universitat de Barcelona[1]

La existencia de resolución de singularidades es uno de los grandes problemas abiertos de la Geometría Algebraica. En esta charla nos concentraremos en el caso de dimensión uno, cuya solución se remonta a Noether. Introduciremos las ideas y técnicas fundamentales utilizando ejemplos y presentaremos brevemente un punto de vista más reciente: *the confortable embedding*. Esta última parte es un trabajo en curso con P. González Pérez y H. Mourtada.

[1]Departament de Matemàtiques i Informàtica
Universitat de Barcelona
adefelipe@ub.edu

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 11 de junio de 2018, 16:00 a 17:30 horas

Semigrupos métricos, semigrupos fractales y su relación con el número áureo y justificación matemática de la división de la octava musical en 12 partes en el temperamento igual

Maria Bras Amorós
Universitat Rovira i Virgili[1]

Los R-moldes de semigrupos numéricos se definen como secuencias crecientes de números reales cuya discretización puede dar semigrupos numéricos. La secuencia ideal de armónicos musicales es un R-molde y su discretización equivale a definir temperamentos iguales. El número de partes iguales de la octava en un temperamento igual corresponde a la multiplicidad del semigrupo numérico relacionado.

Analizando la secuencia de armónicos musicales se derivan dos propiedades importantes de los moldes, las de ser métrico y la de ser fractal. Se demuestra que, salvo normalización, solamente hay un molde métrico y solamente hay un molde fractal no biseccional. Además, se muestra que el único molde fractal no biseccional viene dado por la proporción áurea.

El caso de tubos cilíndricos semicerrados impone a la secuencia de armónicos musicales una tercera propiedad, la llamada propiedad de ser filtrable por términos alternos.

Vamos a demostrar que el número máximo de divisiones iguales de la octava de modo que las discretizaciones del molde métrico y el molde fractal no biseccional coincidan, y de tal manera que la discretización sea filtrable por términos alternos es 12.

Este resultado proporciona una justificación matemática alternativa a las ya conocidas para la elección de 12 como máximo número de divisiones iguales de la octava en temperamentos iguales.

[1]Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili
maria.bras@urv.cat

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 25 de junio de 2018, 16:30 a 17:30 horas.

Code-based cryptography with error-correcting pairs

Ruud Pellikaan
Eindhoven University of Technology[1]

First we will review elementary facts of error-correcting codes and their decoding. Then we will explain how to decode efficiently those codes that have an error-correcting pair [3, 4]. Generalities of one-way functions and public key crypto systems will be given. The McEliece public crypto system is based on the hardness of decoding a general code [2]. Finally we consider the question of the one-way-ness of error-correcting pair function [1, 5].

Keywords: McEliece public crypto system, error-correcting pair.

References:

[1] I. Márquez-Corbella and R. Pellikaan. *Error-correcting pairs for a public-key cryptosystem.* Preprint arXiv:1205.3647 (2012).

[2] R. A. McEliece. *A public-key cryptosystem based on algebraic coding theory.* DSN Progress Report 4244, 114-116 (1978).

[3] R. Pellikaan. *On decoding by error location and dependent sets of error positions.* Discrete Math. 106107, 369-381 (1992).

[4] R. Pellikaan. *On the existence of error-correcting pairs.* Statistical Planning and Inference 51, 229-242 (1996).

[5] R. Pellikaan and I. Márquez-Corbella. *Error-correcting pairs for a public-key cryptosystem.* J. Phys.: Conf. Ser. 855, 012032 (2017).

[1]Department of Mathematics and Computing Science
Eindhoven University of Technology, Netherlands
G.R.Pellikaan@tue.nl

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 2 de julio de 2018, 16:30 a 17:30 horas.

Introducción a la Geometría tropical

Patrick Popescu-Pampu
Université Lille[1]

Mediante ejemplos, haré una introducción a la Geometría tropical, una rama reciente de la Geometría algebraica que trata de unificar varios puntos de vista sobre aspectos combinatorios de la Geometría algebraica.

[1]Département de Maths
Université Lille, France
Patrick.Popescu@math.univ-lille1.fr

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 11 de julio de 2018, 16:30 a 17:30 horas.

Introducción a las bases de Gröbner

Alberto Vigneron Tenorio
Universidad de Cádiz[1]

Las bases de Gröbner fueron introducidas en 1965 por Bruno Buchberger en su tesis doctoral *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, University of Innsbruck, 1965. Desde ese momento, y a pesar de que su obtención conlleva una alta complejidad ($\mathcal{NP}$-completo), el cálculo de las bases de Gröbner de un ideal en un anillo de polinomios se convirtió en una de las principales herramientas del Álgebra Computacional. Gracias a ellas se puede abordar la resolución de problemas matemáticos básicos como la resolución de sistemas polinomiales, el problema de pertenencia a un ideal, etc.

En la exposición mostraremos los elementos básicos necesarios para poder definir las bases de Gröbner, así como un algoritmo que permita su cálculo.

[1]Departamento de Matemáticas
Universidad de Cádiz
alberto.vigneron@uca.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 11 de julio de 2018, 17:30 a 18:30 horas.

Semigrupos numéricos: tipos, elementos notables y cálculo de sus propiedades

Juan Ignacio García García
Universidad de Cádiz[1]

En esta charla veremos algunos tipos de semigrupos numéricos y sus propiedades más importantes. Además mostraremos cómo calcular estas propiedades utilizando algunos paquetes de cálculo simbólico.

[1]Departamento de Matemáticas
Universidad de Cádiz
ignacio.garcia@uca.es

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 16 de julio de 2018, 16:30 a 17:30 horas.

Foliaciones holomorfas singulares sobre $(\mathbb{C}^2, \mathbf{0})$: Reducción de singularidades y existencia de separatriz

Hernán Neciosup Puicán
Pontificia Universidad Católica del Perú[1]

Presentaremos, de forma breve y mediante ejemplos, el proceso de reducción de singularidades de ecuaciones diferenciales analíticas o más precisamente de foliaciones analíticas sobre $(\mathbb{C}^2, \mathbf{0})$. Esencialmente se trata de la sustitución del análisis local por el estudio global de una foliación con singularidades lineales. Luego presentaremos la existencia de curvas integrales (Separatriz) entorno de una singularidad y su vínculo entre su reducción de singularidades con la reducción de singularidades de la foliación.

[1]Departamento Académico de Ciencias
Sección Matemáticas
Pontificia Universidad Católica del Perú
hneciosup@pucp.pe

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 16 de julio de 2018, 17:30 a 18:30 horas.

Caracterización de foliaciones de segundo tipo usando polígono de Newton

Nancy Edith Saravia Molina
Pontificia Universidad Católica del Perú[1]

Estudiaremos las foliaciones no dicríticas de segundo tipo, estas foliaciones fueron introducidas por Mattei-Salem, donde dan una caracterización de este tipo de foliaciones en término de la multiplicidad de su unión de separatrices formales. En esta charla daremos otra caracterización de las foliaciones de segundo tipo en término del polígono de Newton de la foliación y el de su unión de separatrices. Además indicaremos cuando la familia de foliaciones cuspidales son de segundo tipo y cuando son curvas generalizadas.

[1]Departamento Académico de Ciencias
Sección Matemáticas
Pontificia Universidad Católica del Perú
nsaraviam@pucp.edu.pe

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 24 de julio de 2018, 16:30 horas.

On the Milnor number of plane curve singularities

Arkadiusz Płoski
Kielce University of Technology[1]

Let $f = f(x, y)$ be a complex polynomial in two variables x, y without multiple factors. Suppose that $O = (0, 0)$ is a singular point of the curve $f(x, y) = 0$. The Milnor number $\mu_O(f)$ is by definition the number of intersection at O of polar curves $\frac{\partial f}{\partial x} = 0$ and $\frac{\partial f}{\partial y} = 0$. It can be considered as *the degree* of the singular point. Our goal is the following problem. Given the degree d of the curve $f(x, y) = 0$ estimate the possible values of $\mu_O(f)$. For example, if $f(x, y) = 0$ is a pencil of lines throught the origin then $\mu_O(f) = (d-1)^2$. Apart of this case $\mu_O(f) < (d-1)^2$ and it is a natural to ask about the best bound of $\mu_O(f)$ in the class of polynomials f for which $\mu_O(f) < (d-1)^2$.

All notions which will appear in the lecture (algebraic curve, singular point, intersection multiplicity) will be explain in details.

[1]Kielce University of Technology
Kielce, Polonia
matap@tu.kielce.pl

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 23 de octubre de 2018, 16:00 horas.

Geometry of real hypersurfaces meets Subelliptic PDEs

Dmitri Zaitsev
School of Mathematics
Trinity College Dublin[1]

In his seminal work from 1979, Joseph J. Kohn invented his theory of multiplier ideal sheaves connecting a priori estimates for the d-bar problem with local boundary invariants constructed in purely algebraic way.

I will explain the origin and motivation of the problem, and how Kohn's algorithm reduces it to a problem in local geometry of the boundary of a domain.

I then present my recent work with Sung Yeon Kim based on the technique of jet vanishing orders, and show how it can be used to control the effectivity of multipliers in Kohn's algorithm, subsequently leading to precise a priori estimates.

[1]School of Mathematics
Trinity Collegue Dublin, Irlanda
zaitsev@maths.tcd.ie

Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 6 de noviembre de 2018, 16:00 horas.

Fitting ideals and geometry

Bernard Teissier
Institut de Mathématiques de Jussieu - Paris Rive Gauche[1]

Given a module M of finite presentation over a commutative ring R, say corresponding to an affine algebraic variety X, there exists a sequence of ideals of R depending only on M which provide a structure to the sets of points x of X where the dimension of the fiber $M \otimes_R (R/m_x)$ is greater than or equal to some integer. Applications to the definition of critical loci of maps and images of finite maps will be presented. All necessary definitions will be explained if needed.

[1]Equipe Géométrie et Dynamique
Bureau 702
Institut de Mathématiques de Jussieu - Paris Rive Gauche
París, Francia
bernard.teissier@imj-prg.fr