SEMINARIOS JÓVENES

ORGANIZADORES: J. ÁNGEL GONZÁLEZ, CRISTÓBAL MEROÑO, DIEGO SOLER

- *H-Cobord (Teorema del H-Cobordismo)*: J. Ángel González.
- *DistPrimos (Distribución de Primos)*: Diego Soler.
- *FisMat (Física-Matemática)*: Cristóbal Meroño, Diego Soler.
- *Schrö (Convergencia al dato inicial en la ecuación de Schrödinger)*: Cristóbal Meroño.
- *FuncDer (Functores Derivados y Cohomología de Haces)*: J. Ángel González.
- *T. Hodge (Introducción a Teoría Hodge)*: J. Ángel González.
- *Fractales (Medidas de Hausdorff y Fractales)*: Samuel Ranz.
- *CurElip (Curvas Elípticas y Criptografía)*: María Inés de Frutos.
- *IntSimb (Integración simbólica)*: Antonio Jiménez.

Semana del 23 al 27 de Junio

Horas	**Lunes**	**Martes**	**Miércoles**	**Jueves**	**Viernes**
10:00-11:00					IntSimb
11:00-12:00	H-Cobord	DistPrimos	DistPrimos	DistPrimos	IntSimb
12:15-13:30	FisMat	H-Cobord	H-Cobord	H-Cobord	H-Cobord
15:00-16:00	FuncDer	FuncDer	FuncDer	Fractales	Schrö
16:15-17:30	CurElip	FisMat	FisMat	T. Hodge	T. Hodge
17:30-18:30		CurElip	CurElip		

Lugar: ICMAT. Sala Gris 1.

Abstracts

0.1. H-Cobordismo. Dadas dos variedades diferenciales cerradas M_0 y M_1, se dice que son cobordantes si existe una variedad compacta W tal que $\partial W = M_0 \sqcup M_1$. El teorema del h-cobordismo, justamente, da condiciones muy débiles para asegurar que un cobordismo sea trivial, esto es, difeomorfo a $M_0 \times [0,1]$. A partir de este resultado, pueden resolverse problemas de gran profundidad, como la conjetura de Poincaré generalizada para dimensiones altas, que afirma que toda variedad diferenciable con los mismos grupos de homología que una esfera es homeomorfa a una esfera.

En esta serie de seminarios abordaremos la demostración del teorema del h-cobordismo, desarrollando para ello las herramientas técnicas necesarias. Así, analizaremos la relación entre la adjunción de asas y la cirugía, y cómo mediante teoría Morse es posible descomponer un cobordismo en una descomposición por asas. A partir de esta descomposición, invertigaremos cómo, utilizando técnicas de topología algebraica, estas asas pueden ser canceladas unas con otras hasta alcanzar la trivialidad del cobordismo. En este proceso, descubriremos la necesidad de un teorema técnico de gran importancia, conocido como el truco de Whitney y cómo se halla en el corazón de la prueba y condiciona las hipótesis del teorema del h-cobordismo.

0.2. Distribución de primos. En estos seminarios, analizaremos algunos teoremas sobre la distribución de los números primos. En particular, nos centraremos en mostrar cómo la precisión con la que se puede estimar el error de $\pi(x)$ por el logaritmo integral depende de fuertemente de la hipótesis de Riemann y las consecuencias que de ello se derivan.

0.3. Física-Matemática. En estos seminarios se realizará una pequeña introducción a la física matemática, con especial atención a la formulación matemática de la mecánica cuántica. Se estudiará, así, los orígenes físicos de la teoría y su formalización en términos de espacios de Hilbert.

0.4. Convergencia al dato inicial en la ecuación de Schrödinger. La ecuación de Schrödinger es una ecuación en derivadas parciales lineal. El interes de su estudio proviene originariamente de la física, como ocurre con otras muchas EDP's de importancia como la ecuación del calor, la de ondas o la de Poisson; aunque en este caso sea la primera ecuación que proviene del mundo cuántico.

En este seminario concentraremos nuestra atención en la ecuación libre de Schrödinger formulada en $\mathbb{R}^n$, esto es, sin ningún término de potencial. Usando la transformada de Fourier, es fácil intuir una solución formal para este problema. Más aún, es un ejercicio sencillo observar que esta solución formal converge en L^2 al dato inicial. El propósito de esta charla, es probar que, de hecho, se tiene convergencia en casi todo punto al dato inicial, hecho altamente no trivial que fue probado por Carleson en 1966.

0.5. Fractales. En este seminario se estudiarán los conjuntos autosemejantes como caso particular de los fractales. Se calculará la dimensión de Hausdorff de estos conjuntos y se mencionarán algunas aplicaciones importantes de los fractales.

0.6. Functores derivados y Cohomología de Haces. La cohomología de haces es uno de los artilugios algebraicos más potentes de los que dispone la geometría algebraica. Tanto es así que distintas teoría cohomológicas como la cohomología de de Rham o la de Čech pueden ser vistas como ejemplos sencillos de cohomología de haces.

En estas charlas analizaremos la noción de functores derivados y cómo estos pueden ser utilizados para definir la cohomología de haces. En particular, nos centraremos en los conceptos de objetos inyectivos y proyectivos, así como la existencia de estos en la categoría de módulos y haces. Finalmente veremos cómo es posible utilizar resoluciones de estos objetos para construir los functores derivados. Para finalizar, si el tiempo lo permite, realizaremos una pequeña incursión a la noción de categoría derivada.

0.7. Introducción a Teoría Hodge. En estos cursos estudiaremos cómo se puede generalizar el concepto de función armónica a formas y su extensión a variedades. Para ello, trataremos temas como la métrica L^2 en el espacio de formas, la estrella de Hodge o el operador autoadjunto asociado a la diferencial exterior, para a partir de ellos definir el operador de Laplace-Beltrami.

Una vez comprendidos estos conceptos, analizaremos el teorema de descomposición de Hodge del espacio de formas y sus repercusiones en la cohomología de de Rham. Finalmente, estudiaremos la descomposición de Hodge en el caso Kähler.

0.8. Curvas Elípticas y Criptografía. En estos seminarios se introducirá el concepto de curva elíptica, así como un modelo para dicho tipo de curvas, la ecuación de Weierstrass. Se definirá una operación suma sobre los puntos de una curva elíptica y se demostrará que dicha operación dota a los puntos de la curva de estructura de grupo abeliano.

A continuación, se definirá el problema del logaritmo discreto sobre grupos cíclicos finitos, y se presentarán algunas aplicaciones criptográficas de dicho problema (como por ejemplo el intercambio de claves de Diffie-Hellman, el esquema de firma digital de Elgamal, o el esquema de cifrado integrado en curvas elípticas), adaptándolas especialmente para operar sobre curvas elípticas.

Por último, se describirá el funcionamiento de algunos ataques al problema del logaritmo discreto, tanto generales, es decir, que no dependen del grupo finito empleado

(Baby-Step Giant-Step, el método rho de Pollard y el algoritmo de Pohlig-Hellman), como específicos (Index Calculus y Xedni Calculus), y se compararán los rendimientos teóricos de los distintos ataques.

0.9. Integración Simbólica. Primero, daré una breve introducción al álgebra diferencial, introduciendo el concepto de derivación como operador abstracto y viendo el comportamiento en los cuerpos diferenciales (en las extensiones algebraicas y trascendentes simples). Luego, hablaré de las extensiones monomiales, su importancia y sus propiedades (polinomios especiales y normales, representación canónica, órdenes y residuos). Por último, plantearé y explicaré la Ecuación Diferencial de Risch, acompañándola con un ejemplo llamativo.