Propuesta de Trabajos Fin de Grado, curso académico 2018-19

PROFESOR: Yago Antolín

1.- **TÍTULO**: Grupos libres y el ping-pong

Resumen/contenido: En este trabajo se trata de entender los grupos libres y utilizar una técnica llamada "ping-pong" para encontrar grupos libres como subgrupos de otros grupos. Usaremos estas representaciones para obtener propiedades de los grupos libres.

Bibliografía/referencias:

[1] O. Bogopolski. Introduction to Group Theory. EMS Textbooks in Mathematics.

[2] B. Deroin, A. Navas, C. Rivas., Groups, Orders and dynamics

https://arxiv.org/abs/1408.5805

[3] P. de La Harpe. Topics in geometric group theory. University of Chicago Press.

[4] J. Rotman. An introduction to the theory of groups. Graduate text in Mathematics 148, Springer Verlag.

2.- **TÍTULO**: Espacios topológicos de dimensión 1 y el pendiente Hawaiano.

Resumen/contenido: En este trabajo se estudiará grupos fundamentales de espacios topológicos de dimensión 1. En general estos grupos fundamentales son libres, sin embargo, esto no es cierto para ciertos espacios topólogicos exóticos, como el pendiente Hawaiano.

Bibliografía/referencias:

[1] J. Cannon, G. Conner, The combinatorial structure of the Hawaiian earring group, Top. Appl. 106 (2000) 225-271.

[2] J. R. Munkres, Topology,Prentice Hall, Incorporated, 2000

3.- **TÍTULO**: Grupos Nilpotentes

Resumen/contenido: En este trabajo se estudiarán generalidades de grupos nilpotentes. Se verán que aparecen de forma natural en en el teorema de estabilización de cadenas y se estudiará un reciente resultado de Shalev que sobre la probabilidad de que cierta ecuación de nilpotencia se cumpla.

Bibliografía/referencias:

[1] Hall, P. Some sufficient conditions for a group to be nilpotent. *Illinois J. Math.* **2** 1958 787–801.

[2] J. Rotman. An introduction to the theory of groups. Graduate text in Mathematics 148, Springer Verlag.

[3] A. Shalev, Probabilistically nilpotent groups. Proc. Amer. Math. Soc. 146 (2018), no. 4, 1529-1536.

4.- **TÍTULO**: Construcciones de objetos pseudo-aleatorios.

Resumen/contenido: En este trabajo se trata de dar una demostración del teorema (que no se prueba durante el curso de códigos y criptografía) que dice que son equivalentes (1) los generadores de números pseudo-aleatorios, (2) las funciones pseudo-aleatorias y (3) las funciones de un sólo sentido.

Bibliografía/referencias:

[1] J. Katz y Y. Lindell. Introduction to modern criptography, 2nd ed., CRC Press (2014).

5. **TITULO**: P vs NP y problemas criptográficos

Resumen/contenido: En este trabajo se estudiarán las clases P, NP y NP-completo. Se pondrá énfasis en problemas criptográficos, estudiando, por ejemplo, el algoritmo AKS que demuestra que la factorización de primos está en la clase P, o el criptosistema de Merkle-Hellman basado en Knapsac, que es un problema NP-completo.

Bibliografía/referencias:

[1] Agrawal, M., Kayal, N., & Saxena, N. (2004). PRIMES is in P. *Annals of mathematics*, 781-793.

[2] Shamir A. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. InFoundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on 1982 Nov 3 (pp. 145-152). IEEE.

[3] Avi Wigderson, Mathematics and Computation,
https://www.math.ias.edu/avi/book