Facultad de Ciencias Naturales, Exactas y de la Educación

Departamento: Matemáticas

Tipo de Actividad: Asignatura

Créditos: 5 por semestre

Nombre: Campos Finitos I (Mat 528)

Intensidad Horaria: 4 H.S.

Requisitos: Álgebra (Mat 520)

INTRODUCCIÓN

Un campo finito es una estructura matemática discreta que satisface todos los axiomas de un campo, muy similar al campo de los números reales o complejos, excepto por su finitud. Es relativamente fácil demostrar que tales estructuras existen únicamente cuando el número de sus elementos es una potencia de un primo y que cualquier dos campos finitos con el mismo número de elementos son isomorfos.
Las propiedades de los campos finitos son de interés por derecho propio ya que tienen papel central en muchas áreas de las matemáticas, además del álgebra moderna, se relacionan, por ejemplo, con combinatoria y teoría de diseños, con teoría de códigos y teoría grafos, con geometría algebraica y teoría de números. Sin embargo, quizás sea el papel fundamental que tienen los campos finitos en muchas aplicaciones el que los hace merecedores de varios congresos especializados y de varias revistad dedicadas a la teoría de campos finitos y sus aplicaciones.
Sus orígenes pueden ubicarse en los siglos 17 y 18, con el trabajo de eminentes matemáticos tales como: Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) y Adrien-Marie Legendre (1752-1833), quienes contribuyeron a estructurar la teoría de campos finitos primos. Puede decirse que la teoría general de campos finitos comenzó con el trabajo de Carl Friedrich Gauss (1777-1855) y Evaristo Galois (1811-1832), pero para las matemáticas aplicadas vino a ser de interés únicamente en décadas recientes con la emergencia de las matemáticas discretas.

DESCRIPCIÓN DEL CURSO

El texto guía es: Rudolf Lidl and Hararald Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1997.

Se selecciona este libro porque es el primero dedicado completamente a campos finitos y porque presenta tanto los aspectos clásicos como aquellos orientados a las aplicaciones. Además de la teoría esencial, incluye resultados y técnicas de importancia en las aplicaciones.
Este primer curso de campos finitos (como el texto guía) supone como prerrequisitos los siguientes: fundamentos de álgebra lineal, algunos temas de álgebra abstracta, un poco de análisis básico y de teoría de números elemental.

CAPÍTULO I: FUNDAMENTOS ALGEBRAICOS

En este capítulo se resume toda la información básica. Únicamente se introducen las definiciones y propiedades más fundamentales de los sistemas algebraicos, y la teoría se discute en la extensión necesaria para el estudio de los campos finitos

1.1. Grupos, Anillos y Campos.
1.2. Polinomios.
1.3. Extensiones de Campos.

CAPÍTULO II: ESTRUCTURA DE LOS CAMPOS FINITOS

Contiene la teoría estructural general de los campos finitos como también la discusión de conceptos que se utilizan a través del contenido siguiente. Incluye varias propiedades fundamentales de los campos finitos y una descripción de métodos para construirlos. Se prueba, por ejemplo, que todo campo finito es de orden potencia prima y que, recíprocamente, para toda potencia prima existe un campo finito cuyo número de elementos es exactamente esa potencia prima. También, se interpreta un campo finito como campo descomposición de polinomios irreducibles y se muestran otras formas de representar los elementos de un campo finito. Muchos de los temas en este capítulo se generalizan parcialmente en capítulos posteriores.

2.1. Caracterización de los Campos Finitos
2.2. Raíces de Polinomios Irreducibles
2.3. Trazas, Normas y Bases
2.4 Raíces de la Unidad y Polinomios Ciclotómicos
2.5 Representación de Elementos de Campos Finitos

CAPÍTULO III: POLINOMIOS SOBRE CAMPOS FINITOS

La teoría de polinomios sobre campos finitos es importante tanto para investigar la estructura algebraica de los campos finitos como para muchas aplicaciones. Sobre todo los polinomios irreducibles son indispensables para construir campos finitos y para computar con los elementos de un campo finito. Este capítulo constituye una unidad con el Capítulo IV.

3.1. Orden de un Polinomio y Polinomios Primitivos
3.2. Polinomios Irreducibles
3.3. Construcción de Polinomios Irreducibles
3.4. Polinomios Linealizados
3.5. Binomios y Trinomios

CAPÍTULO IV: FACTORIZACIÓN DE POLINOMIOS

Todo polinomio sobre un campo finito puede expresarse como un producto de polinomios irreducibles y, en el caso de campos finitos, existen algoritmos razonablemente eficientes para calcular dichos factores irreducibles. Esto es importante para teoría de códigos y para el estudio de recurrencias lineales en campos finitos. Algunos de los algoritmos reducen el problema de factorizar polinomios al de encontrar las raíces de otros polinomios, razón por la cual se discute este último problema.

4.1. Factorización sobre Campos Finitos Pequeños
4.2. Factorización sobre Campos Finitos Grandes
4.3. Cálculo de raíces de Polinomios

BIBLIOGRAFIA

1. Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1997.
2. Revista Especializada: *Finite Fields and Their Applications*. http://www.elsevier.com/locate/ffa
3. Steven Roman. *Field Theory*. Graduate Texts in Mathematics, Springer-Verlag, 1995.
4. Thomas W. Hungerford. *Algebra*. Graduate Texts in Mathematics, Springer-Verlag, 1974.
5. David S. Dummit and Richard M. Foote. *Abstract Algebra*. Third Edition, John Wiley & Sons, Inc., 2004.

Nota: Este curso es ofrecido por el Grupo de Investigación ALTENUA ("Álgebra, Teoría de Números y Aplicaciones: ERM").