Universidad del Cauca

Facultad de Ciencias Naturales, Exactas y de la Educación

Departamento de Matemáticas

Tipo de actividad: Asignatura(MAT626)	Créditos: 5
Nombre: Campos Finitos II .	Intensidad Horaria: 4 Horas semanales.
Requisitos: MAT528	Correquisitos:

Introducción

Como se mencionó en el programa de Campos Finitos I, las propiedades de los campos finitos son de interés por derecho propio ya que tienen papel central en muchas áreas de las matemáticas; se relacionan, por ejemplo, con combinatoria y teoría de diseños, con teoría de códigos y teoría grafos, con geometría algebraica y teoría de números. Esta rama del álgebra moderna ha tomado fuerza en los últimos 50 años debido a sus diversas aplicaciones, entre las cuales destacamos las siguientes.

Los Códigos Correctores de Errores, fundamentales en comunicación digital y sistemas de almacenamiento de datos, para mejorar el manejo del error sobre canales ruidosos. Hoy en día se incluyen en sistemas electrónicos comerciales tales como discos compactos. Estos códigos y sus algoritmos de decodificación dependen de la estructura y las propiedades de los campos finitos y de polinomios sobre ellos.

La aparición de la Criptografía de Clave Pública en los años 1970 ha generado innumerables protocolos de seguridad que encuentran aplicaciones en comunicación digital, en transacciones electrónicas, y en aspectos similares. La mayoría de esos esquemas utilizan o enteros o campos finitos como dominio de computación para lograr sus metas.

Secuencias seudoaleatorias, es decir secuencias deterministas con propiedades semi-aleatorias, se requieren en varias aplicaciones, tales como criptografía donde se requieren semillas semi-aleatorias. Además, el diseño de secuencias, principalmente binarias, para correlación es central en la tecnología de teléfonos celulares. Muchos de tales sistemas requieren la aplicación de varias propiedades de los campos finitos.

Contenido

CAPÍTULO I SUMAS EXPONENCIALES

Sumas exponenciales son herramientas importantes en teoría de números para resolver problemas que involucran enteros y que son intratables por otros medios. Sumas análogas pueden considerarse en campos finitos y resultan útiles cuando se estudia el número de soluciones de ecuaciones sobre campos finitos.

1.1. Caracteres.
1.2. Sumas de Gauss y Sumas de Jacobi.
1.3. Sumas de Caracteres con Argumentos Polinomiales
1.4. Resultados Adicionales sobre Sumas de Caracteres.

CAPÍTULO II ECUACIONES SOBRE CAMPOS FINITOS

En casos especiales es posible dar fórmulas explícitas para el número de soluciones de ecuaciones sobre campos finitos, pero en general debemos estar satisfechos con estimaciones. En este capítulo se presentan ejemplos específicos de cada tipo. Mucha información sobre el número de soluciones de ecuaciones depende de estimar sumas de caracteres, los métodos que se presentan son elementales, no dependen ni de geometría algebraica ni del conocimiento detallado de campos de funciones algebraicas.

2.1. Resultados Básicos sobre el Número de Soluciones
2.2. Formas Cuadráticas
2.3. Ecuaciones Diagonales
2.4 El Método de Stepanov-Schmidt

CAPÍTULO III: POLINOMIOS PERMUTACIÓN

Se presenta un resumen de resultados sobre polinomios para los cuales las funciones asociadas son permutaciones de un campo finito. Polinomios de este tipo se llaman polinomios permutación y existen para todo campo finito ya que, en general, toda aplicación de un campo finito en si mismo puede expresarse como un polinomio. Aparecen preguntas naturales en conexión con este tipo de polinomios y, en consecuencia se presentan varios resultados para tipos especiales de tales polinomios.

3.1. Criterios para Polinomios Permutación
3.2. Tipos Especiales de Polinomios Permutación
3.3. Grupos de Polinomios Permutación
3.4. Polinomios Excepcionales
3.5. Polinomios Permutación en Varias Variables

CAPÍTULO IV: ALGUNAS APLICACIONES DE CAMPOS FINITOS

En este capítulo se describen algunas aplicaciones para dar ejemplos del uso de varias propiedades de los campos finitos. Una de las aplicaciones fundamentales de los campos finitos es la teoría de códigos. Esta teoría tiene sus orígenes en un famoso teorema de Shannon que garantiza la existencia de códigos que pueden transmitir información a razones cercanas a la capacidad con una probabilidad de error arbitrariamente pequeña. Un propósito de la teoría algebraica de códigos es diseñar métodos para la construcción de tales códigos, aquí los campos finitos y polinomios sobre ellos son fundamentales. También, se muestran algunos resultados sobre el uso de los campos finitos en: planos afines y proyectivos con un número finito de puntos y líneas (geometría finita), en problemas de diseños de experimentos, y en sistemas modulares lineales.

4.1. Códigos Lineales y Códigos Cíclicos
4.2. Geometrías Finitas
4.3. Combinatoria
4.4. Sistemas Modulares Lineales

CAPÍTULO V: SECUENCIAS RECURRENTES LINEALES

Secuencias en campos finitos cuyos términos dependen de manera simple de sus antecesores son importantes para varias aplicaciones. Tales secuencias son fáciles de generar mediante procedimientos recursivos, esto es ventajoso desde el punto de vista computacional, y tienden a tener propiedades estructurales útiles. De interés especial es el caso cuando los términos dependen linealmente de un número fijo de antecesores, resultando las secuencias recurrentes lineales empleadas en teoría de códigos y en otras ramas de ingeniería electrónica.

5.1. Registros. Propiedades de Periodicidad
5.2. Secuencias Impulso Respuesta. Polinomios Característicos
5.3. Funciones Generadoras
5.4. Polinomio Minimal
5.5. Familias de Secuencias Recurrentes Lineales
5.6. Caracterización de Secuencias Recurrentes Lineales.

Bibliografía

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.