UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE CIENCIAS MATEMÁTICAS

SÍLABO

1. INFORMACIÓN GENERAL

1.1 Curso	:	Estructuras Algebraicas
1.2 Código	:	MA381
1.3 Programa Académico	:	Computación Científica
1.4 Créditos	:	4
1.5 Prerrequisitos	:	MA281. Teoría de números. (5^{to} Sem)
1.6 Tipo de curso	:	Electivo
1.7 Área de Estudios	:	Estudios Generales
1.8 Número de Semanas	:	16
1.9 Horas por semana	:	2 HT; 4 HP;
1.10 Ciclo	:	I
1.11 Modalidad de aprendizaje	:	Presencial
1.12 Periodo Académico	:	2026-I
1.13 Inicio del semestre	:	
1.14 Fin del semestre	:	

2. PROFESORES

Atención previa coordinación con el profesor

3. INTRODUCCIÓN AL CURSO

El curso de Estructuras Algebraicas proporciona la base formal y abstracta esencial para las matemáticas avanzadas y sus aplicaciones computacionales. Este curso introduce las estructuras fundamentales del álgebra moderna —grupos, anillos y campos— desarrollando la capacidad de pensar en términos de axiomas, homomorfismos e invariantes. El dominio de estos conceptos es crucial para comprender los fundamentos teóricos de áreas como la teoría de códigos, la criptografía, el diseño de algoritmos y la geometría algebraica. El curso enfatiza la interacción entre la teoría abstracta y los ejemplos concretos, particularmente aquellos que surgen en matemáticas discretas y computacionales.

4. OBJETIVOS

- Dominar las definiciones axiomáticas y las propiedades básicas de grupos, anillos y campos.
- Comprender y aplicar los conceptos de subgrupos, subgrupos normales, grupos cociente y los teoremas fundamentales de homomorfismos para grupos.
- Analizar la estructura de los anillos, incluyendo ideales, anillos cociente, dominios de integridad y campos.
- Aplicar la teoría de campos finitos a problemas prácticos en teoría de códigos y criptografía.
- Desarrollar la capacidad de construir demostraciones rigurosas y reconocer estructuras algebraicas en diversos contextos matemáticos y computacionales.

5. RESULTADOS DEL ESTUDIANTE

ABET-1) Habilidad para identificar, formular y resolver problemas técnicos o científicos ampliamente definidos mediante la aplicación de conocimientos de matemáticas y ciencias y/o temas técnicos en áreas relevantes para la disciplina. (Usage)

ABET-3) Habilidad para desarrollar y llevar a cabo experimentos o probar hipótesis, analizar e interpretar datos y utilizar el juicio científico para obtener conclusiones. (Usage)

6. TEMAS

Unidad 1: Grupos y Subgrupos (16 horas)	
Resultados esperados: ABET-1,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Operaciones binarias y definición de grupo. Ejemplos básicos: grupos cíclicos, simétricos, diédricos y de matrices. ▪ Propiedades elementales de grupos: unicidad del elemento neutro y de los inversos, leyes de cancelación. ▪ Subgrupos y pruebas de subgrupo. Centralizador, normalizador y centro de un grupo. ▪ Grupos cíclicos: clasificación, estructura y subgrupos. ▪ Grupos de permutaciones: notación cíclica, transposiciones y paridad.	▪ Enunciar los axiomas de grupo y verificar si un conjunto dado con una operación forma un grupo [Familiarizarse]. ▪ Aplicar las pruebas de subgrupo y generar subgrupos, incluyendo los subgrupos cíclicos generados por un elemento [Usar]. ▪ Analizar la estructura de grupos cíclicos finitos y descomponer permutaciones en ciclos disjuntos [Evaluar].
Lecturas : [**Dummit2004**], [**Gallian2021**]	

Unidad 2: Clases Laterales, Subgrupos Normales y Homomorfismos (16 horas)	
Resultados esperados: ABET-1,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Clases laterales y Teorema de Lagrange. Aplicaciones al orden de los elementos. ▪ Subgrupos normales y su caracterización. Grupos cociente (o factores). ▪ Homomorfismos e isomorfismos de grupos: definiciones, propiedades y ejemplos. ▪ Teorema Fundamental del Homomorfismo (Primer Teorema de Isomorfía) para grupos. ▪ Introducción a las acciones de grupo: definición y ejemplos básicos (órbita-estabilizador).	▪ Calcular clases laterales y usar el Teorema de Lagrange para deducir propiedades de grupos finitos [Familiarizarse]. ▪ Determinar si un subgrupo es normal y construir el correspondiente grupo cociente [Usar]. ▪ Utilizar el Teorema Fundamental del Homomorfismo para establecer isomorfismos entre grupos cociente y grupos conocidos [Evaluar].
Lecturas : [**Dummit2004**], [**Judson2021**]	

Unidad 3: Anillos, Ideales y Dominios de Integridad (16 horas)	
Resultados esperados: ABET-1,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Definición y ejemplos básicos de anillos, anillos conmutativos y anillos con unidad. ▪ Homomorfismos e isomorfismos de anillos, propiedades básicas. ▪ Ideales y anillos cociente. Teorema Fundamental del Homomorfismo para anillos. ▪ Operaciones con ideales: suma, producto e intersección. ▪ Dominios de integridad, campos y característica de un anillo. Los dominios de integridad finitos son campos.	▪ Identificar las propiedades definitorias de anillos, dominios de integridad y campos a partir de ejemplos dados [Familiarizarse]. ▪ Verificar si un subconjunto de un anillo es un ideal y construir el correspondiente anillo cociente [Usar]. ▪ Aplicar los teoremas de homomorfismo de anillos para analizar estructuras y demostrar resultados básicos sobre dominios de integridad [Evaluar].
Lecturas : [**Dummit2004**], [**Hungerford2014**]	

Unidad 4: Campos y Aplicaciones (16 horas)	
Resultados esperados: ABET-1,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Extensiones de campos: elementos algebraicos y trascendentes. Grado de una extensión. ▪ Campos finitos (campos de Galois): existencia, unicidad y estructura. El campo $GF(p^n)$. ▪ Anillos de polinomios sobre un campo. Polinomios irreducibles y construcción de campos finitos. ▪ Elementos primitivos en campos finitos y su aplicación en criptografía (ej: Diffie-Hellman, AES). ▪ Breve introducción a códigos correctores de errores: distancia de Hamming y códigos lineales como espacios vectoriales sobre campos finitos.	▪ Describir la clasificación y propiedades básicas de los campos finitos [Familiarizarse]. ▪ Construir campos finitos pequeños utilizando polinomios irreducibles sobre $\mathbb{Z}_p$ [Usar]. ▪ Explicar cómo la estructura de los campos finitos sustenta protocolos criptográficos modernos y la teoría de códigos [Evaluar].
Lecturas : [**Gallian2021**], [**Lidl1994**]	

7. PLAN DE TRABAJO

7.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

7.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

7.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

8. SISTEMA DE EVALUACIÓN

********* EVALUATION MISSING ********

9. BIBLIOGRAFÍA BÁSICA