Universidad Nacional de Córdoba
FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

PROGRAMA DE ASIGNATURA

ASIGNATURA: TEORIA DE GALOIS CON APLICACIONES DE CUERPOS FINITOS	**AÑO:** 2008
DOCENTE ENCARGADO: PODESTÁ, RICARDO ALBERTO.	

CONTENIDOS

Unidad I: Anillos de polinomios sobre dominios íntegros.

Generalidades sobre anillos. Anillos de polinomios sobre dominios integros. Algoritmo de Euclides y consecuencias. Factorización única en $K[x]$, con K cuerpo. Raíces. Derivada formal y raíces múltiples. Soluciones de las ecuaciones cuadrática, cúbica y cuártica. Polinomios simétricos. Discriminante y resolvente. Contenido de un polinomio. Polinomios primitivos. Polinomios irreducibles sobre dominios integros y sobre sus cuerpos de fracciones. Criterios de irreducibilidad (Eisenstein, reducción módulo p).

Unidad II: Extensiones de cuerpos.

Cuerpos y característica. Cuerpos primos. Elementos algebraicos y trascendentes. Extensiones finitas, finitamente generadas y algebraicas. Polinoios minimales. Cuerpos de adjunción. Cuerpos compuestos. Familias distinguidas. Morfismos de cuerpos. Grupos de automorfismos. Existencia y unicidad de la clausura algebraica. Cuerpos de descomposición de polinomios. Extensiones normales. Extensiones separables. Grado de separabilidad. Teorema del elemento primitivo. Extensiones inseparables. Grado de inseparabilidad. Aplicación geométrica: números euclídeos y construcciones con regla y compás (insolubilidad de los 3 problemas clásicos de la geometría griega).

Unidad III: Cuerpos de funciones algebraicas.

Cuerpos de funciones algebraicas. Anillos de valuación y lugares. Valuaciones discretas. Cuerpo residual. Grado de un lugar. Ceros y polos. El grupo de divisores. Espacio de Riemann-Roch de un divisor. Propiedades. El género de un cuerpo de funciones. Enunciados del Teorema de Riemann y de Riemann-Roch. Caracterización de los cuerpos de funciones de género de 0.

Unidad IV: Cuerpos finitos y polinomios.

Existencia y unicidad de cuerpos finitos. Caracterización. El grupo multiplicativo. Elementos primitivos. Estructura de los cuerpos finitos. Subcuerpos. Extensiones. Clausura algebraica. Distintas construcciones de cuerpos finitos. Automorfismo de Frobenius y grupo de automorfismos. Raices cuadradas y raìces p-ésimas. Norma y Traza. Resolución de ecuaciones cuadráticas en característica 2. Grupos de Galois de cuerpos finitos. Polinomios irreducibles. Polinomios primitivos. Bases normales. Orden de un polinomio irreducible. Función de Möbius y número de polinomios irreducibles. Polinomios linealizados. Número de bases normales. Elementos conjugados. Conjuntos ciclotómicos y factorización de $x^n - 1$. Criterio de irreducibilidad de polinomios ciclotómicos sobre cuerpos finitos.

Unidad V: Teoría de Galois.

Extensiones de Galois. Grupo de Galois de una extensión. Cuerpo fijo. Teorema de Artin y correspondencia de Galois. El grupo de Galois de un cuerpo compuesto. Ejemplos. El grupos simétrico $\mathbb{S}_n$ y los subgrupos alternante $\mathbb{A}_n$ y dihedral $\mathbb{D}_n$. El grupo de Galois G_f de un polinomio f. Determinación de grupos de Galois de polinomios de grado 2,3 y 4 (criterio del discriminante, teorema de Kaplansky, la resolvente cúbica). Uso del teorema de Dedekind para encontrar orbitas de G_f. El problema inverso de Galois. Polinomios con grupo de Galois $\mathbb{S}_n$. El polinomio general de grado n. Funciones simétricas. Uso del teorema de densidad de Chebotareff para determinar el orden de G_f.

Unidad VI: Extensiones cíclicas.

Raíces de la unidad. Extensiones ciclotómicas y polinomios ciclotómicos. Propiedades de los polinomios ciclotómicos. Norma y Traza. Independencia de los caracteres y Teorema 90 de Hilbert. Extensiones cíclicas. Extensiones de Artin-Schreier. Extensiones solubles y radicales. Irresolubilidad de la quíntica.

Unidad VII: Teoría de Galois infinita.

Anillo de enteros p-ádicos $\mathbb{Z}_p$ y cuerpos de números p-ádicos $\mathbb{Q}_p$. Familias inversas y límite proyectivo. Grupos topológicos. Grupos profinitos. Extensiones de Galois infinitas. Topología de Krull. Correspondencia de Galois general. El grupo de Galois $G(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. Ejemplos. Límite directo. Relación entre $\mathbb{Z}_p$ y $\mathbb{Z}_{p^\infty}$.

BIBLIOGRAFÍA

- *Serge Lang*, "Algebra", Addison-Wesley.
- *Thomas Hungerford*, "Algebra", Springer.
- *Ian Stewart*, "Galois Theory", Chapman & Hall.
- *Steven Roman*, "Coding and Information Theory", Springer.
- *Lidl-Niederreiter*, "Introduction to finite fields and their applications", Cambridge.
- *Zhe-Zian Wan*, "Lectures on finite fields and Galois rings", World Scientific.
- *Henning Stichtenoth*, "Algebraic function fields and codes", Springer.

EVALUACIÓN

FORMAS DE EVALUACIÓN

- El alumno deberá entregar ejercicios específicos de los prácticos resueltos.
- En principio sin evaluaciones parciales, se contempla la posibilidad de tomar 2 parciales
- El examen final contará de una evaluación escrita sobre contenidos teórico-prácticos (se permite la modalidad “take-home”), y una exposición oral sobre los contenidos teóricos del curso.
- La materia no es promocionable.

CONDICIONES PARA OBTENER LA REGULARIDAD

1. Asistencia regular a clases.
2. Entrega de algunos ejercicios específicos resueltos.
3. Aprobar 1 de los 2 parciales, si los hubiere.