

# TEORÍA DE GALOIS CON APLICACIONES DE CUERPOS FINITOS

RICARDO A. PODESTÁ

## PROGRAMA

### **Preliminares.**

*Anillos de polinomios sobre dominios íntegros.* Algoritmo de Euclides y consecuencias. Factorización única sobre cuerpos. Criterios de irreducibilidad (Gauss, Eisenstein, reducción módulo  $p$ ). Raíces. Derivada formal y raíces múltiples. Soluciones de las ecuaciones cuadrática, cúbica y cuártica. Resultante y discriminante de polinomios.

### **Parte I: Teoría de Cuerpos.**

*Capítulo 1. Extensiones de Cuerpos.* Cuerpos y característica. Extensiones algebraicas. Embeddings y clausura algebraica. Cuerpos de descomposición de polinomios. Extensiones normales. Extensiones separables. Grado de separabilidad. Teorema del elemento primitivo. Extensiones inseparables. Aplicación algebraica: el teorema fundamental del algebra. Aplicación geométrica: números euclídeos y construcciones con regla y compás (los 3 problemas clásicos de la geometría griega)

*Capítulo 2. Teoría de Galois.* Extensiones de Galois. Teorema de Artin y correspondencia de Galois. Ejemplos. El grupo de Galois de un polinomio. Polinomios de grado a los sumo 4. Polinomios de grado  $n$ . Funciones simétricas. Topología de Krull. Extensiones de Galois infinitas. Ejemplos. Raíces de la unidad y polinomios ciclotómicos. Norma y Traza. Extensiones cíclicas. Teorema 90 de Hilbert y extensiones de Artin-Schreier. Extensiones solubles y radicales. Aplicación algebraica: solubilidad de las ecuaciones de grado menores que 5 e irresolubilidad de la quintica. Aplicación geométrica: polígonos construibles.

### **Parte II: Cuerpos finitos y polinomios.**

*Capítulo 3. Cuerpos finitos.* Existencia y unicidad de cuerpos finitos. Caracterización. El grupo multiplicativo. Estructura de los cuerpos finitos. Extensiones. Construcción de cuerpos finitos y representación de elementos. Automorfismo de Frobenius y grupo de automorfismos. Norma y Traza. Ecuaciones cuadráticas en característica 2. Clausura algebraica y grupos de Galois de cuerpos finitos. Caracteres y sumas de Gauss. El teorema de Davenport-Hasse. El Teorema de Stickelberger. Reciprocidad cuadrática

*Capítulo 4. Polinomios sobre cuerpos finitos.* (a) *Polinomios irreducibles:* Polinomios primitivos. Orden de un polinomio irreducible. Función de Möbius y número de polinomios irreducibles. Construcción de polinomios irreducibles. Polinomios “linealizados”. Binomios y trinomios. (b) *Factorización de polinomios:* El algoritmo de Berlekamp. Cálculo de raíces. Conjuntos ciclotómicos y factorización de  $x^n - 1$ . Factorización de polinomios ciclotómicos sobre cuerpos finitos. El método de levantamiento de Henssel.

### Parte III: Aplicaciones de cuerpos finitos.

*Capítulo 5. Códigos cíclicos.* Códigos sobre cuerpos finitos. Códigos lineales. Codificación y decodificación. Cotas de Singleton, de Hamming y de Gilbert-Varshamov. Enumeradores de peso. Códigos cíclicos. Polinomios generador y de control. Polinomios de Mattson-Solomon y la cota de BCH. Códigos BCH y de Reed-Solomon generalizados. Códigos alternantes y códigos algebraicos de Goppa.

*Capítulo 6. Curvas elípticas sobre cuerpos finitos.* Generalidades sobre curvas elípticas. La ley de grupo. Teoremas de Mordell-Weil, Mazur, Nagell-Lutz. Puntos racionales. Curvas sobre cuerpos finitos. El Teorema de Hasse-Weil. La función zeta asociada a una curva elíptica. Ecuación funcional y producto de Euler. La hipótesis de Riemann en este contexto. Aplicaciones: criptografía, algoritmo de factorización de Lenstra, tests de primalidad, códigos de Melas.

### BIBLIOGRAFÍA

#### *Algebra general*

- ★ *Serge Lang*, “Algebra”, Addison-Wesley.
- ★ *Thomas Hungerford*, “Algebra”, Springer.
- ★ *Henri Cohen*, “A course in computational algebraic number theory”, Springer.

#### *Teoría de Galois*

- ★ *Ian Stewart*, “Galois Theory”, Chapman & Hall.

#### *Cuerpos Finitos*

- ★ *Lidl & Niederreiter*, “Introduction to finite fields and their applications”, Cambridge.
- ★ *Zhe-Zian Wan*, “Lectures on finite fields and Galois rings”, World Scientific.

#### *Teoría de Códigos*

- ★ *Steven Roman*, “Coding and Information Theory”, Springer.
- ★ *Hiramatsu & Köhler*, “Coding theory and number theory”, Kluwer.
- ★ *Huffman & Pless*, “Fundamentals of error-correcting codes”, Cambridge.

#### *Curvas Elípticas*

- ★ *Silverman & Tate*, “Rational points on elliptic curves”, Springer.
- ★ *Lawrence Washington*, “Elliptic curves”, Chapman & Hall.
- ★ *Joseph Silverman*, “The arithmetic of elliptic curves”, Springer.
- ★ *Dale Husemöller*, “Elliptic curves”, Springer.

#### *Criptografía*

- ★ *Richard Mollin*, “An introduction to cryptography”, Chapman & Hall.

UNIVERSIDAD NACIONAL DE CÓRDOBA, ARGENTINA, 18 DE JUNIO DE 2008.

*E-mail address:* `podesta@mate.uncor.edu`