

Gabriel Daniel Villa Salvador

Topics in the Theory of  
Algebraic Function Fields

Birkhäuser  
Boston • Basel • Berlin

Gabriel Daniel Villa Salvador  
Centro de Investigación y de Estudios Avanzados del I.P.N.  
Departamento de Control Automático  
Col. Zacatenco, C.P. 07340  
México, D.F.  
México

Mathematics Subject Classification (2000): 11R58, 11R60, 14H05, 11G09, 11R32, 12F05, 12F10, 12F15, 11S20, 14H55, 11R37, 11R29, 14G10, 14G15, 14G50, 11S31, 11S20, 14H25, 12G05

Library of Congress Control Number: 2006927769

ISBN-10 0-8176-4480-6 e-ISBN 0-8176-4515-2  
ISBN-13 978-0-8176-4480-2

Printed on acid-free paper.

©2006 Birkhäuser Boston

*Birkhäuser*



Based on the original Spanish edition, *Introducción a la Teoría de las Funciones Algebraicas*, Fondo de Cultura Económica, México, 2003

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Birkhäuser Boston, c/o Springer Science+Business Media LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America. (TXQ/MP)

9 8 7 6 5 4 3 2 1

[www.birkhauser.com](http://www.birkhauser.com)

---

# Contents

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| <b>Preface</b> .....                                                  | vii |
| <b>1 Algebraic and Numerical Antecedents</b> .....                    | 1   |
| 1.1 Algebraic and Transcendental Extensions .....                     | 1   |
| 1.2 Absolute Values over $\mathbb{Q}$ .....                           | 3   |
| 1.3 Riemann Surfaces .....                                            | 8   |
| 1.4 Exercises .....                                                   | 11  |
| <b>2 Algebraic Function Fields of One Variable</b> .....              | 13  |
| 2.1 The Field of Constants .....                                      | 14  |
| 2.2 Valuations, Places, and Valuation Rings .....                     | 16  |
| 2.3 Absolute Values and Completions .....                             | 26  |
| 2.4 Valuations in Rational Function Fields .....                      | 36  |
| 2.5 Artin's Approximation Theorem .....                               | 43  |
| 2.6 Exercises .....                                                   | 52  |
| <b>3 The Riemann–Roch Theorem</b> .....                               | 55  |
| 3.1 Divisors .....                                                    | 55  |
| 3.2 Principal Divisors and Class Groups .....                         | 61  |
| 3.3 Repartitions or Adeles .....                                      | 67  |
| 3.4 Differentials .....                                               | 72  |
| 3.5 The Riemann–Roch Theorem and Its Applications .....               | 81  |
| 3.6 Exercises .....                                                   | 88  |
| <b>4 Examples</b> .....                                               | 93  |
| 4.1 Fields of Rational Functions and Function Fields of Genus 0 ..... | 93  |
| 4.2 Elliptic Function Fields and Function Fields of Genus 1 .....     | 101 |
| 4.3 Quadratic Extensions of $k(x)$ and Computation of the Genus ..... | 105 |
| 4.4 Exercises .....                                                   | 111 |

|          |                                                                     |     |
|----------|---------------------------------------------------------------------|-----|
| <b>5</b> | <b>Extensions and Galois Theory</b> . . . . .                       | 113 |
| 5.1      | Extensions of Function Fields . . . . .                             | 113 |
| 5.2      | Galois Extensions of Function Fields . . . . .                      | 118 |
| 5.3      | Divisors in an Extension . . . . .                                  | 128 |
| 5.4      | Completions and Galois Theory . . . . .                             | 132 |
| 5.5      | Integral Bases . . . . .                                            | 138 |
| 5.6      | Different and Discriminant . . . . .                                | 147 |
| 5.7      | Dedekind Domains . . . . .                                          | 150 |
| 5.7.1    | Different and Discriminant in Dedekind Domains . . . . .            | 154 |
| 5.7.2    | Discrete Valuation Rings and Computation of the Different . . . . . | 158 |
| 5.8      | Ramification in Artin–Schreier and Kummer Extensions . . . . .      | 164 |
| 5.9      | Ramification Groups . . . . .                                       | 180 |
| 5.10     | Exercises . . . . .                                                 | 186 |
| <br>     |                                                                     |     |
| <b>6</b> | <b>Congruence Function Fields</b> . . . . .                         | 191 |
| 6.1      | Constant Extensions . . . . .                                       | 191 |
| 6.2      | Prime Divisors in Constant Extensions . . . . .                     | 193 |
| 6.3      | Zeta Functions and $L$ -Series . . . . .                            | 195 |
| 6.4      | Functional Equations . . . . .                                      | 200 |
| 6.5      | Exercises . . . . .                                                 | 207 |
| <br>     |                                                                     |     |
| <b>7</b> | <b>The Riemann Hypothesis</b> . . . . .                             | 209 |
| 7.1      | The Number of Prime Divisors of Degree 1 . . . . .                  | 209 |
| 7.2      | Proof of the Riemann hypothesis . . . . .                           | 215 |
| 7.3      | Consequences of the Riemann Hypothesis . . . . .                    | 222 |
| 7.4      | Function Fields with Small Class Number . . . . .                   | 227 |
| 7.5      | The Class Numbers of Congruence Function Fields . . . . .           | 231 |
| 7.6      | The Analogue of the Brauer–Siegel Theorem . . . . .                 | 234 |
| 7.7      | Exercises . . . . .                                                 | 237 |
| <br>     |                                                                     |     |
| <b>8</b> | <b>Constant and Separable Extensions</b> . . . . .                  | 239 |
| 8.1      | Linearly Disjoint Extensions . . . . .                              | 239 |
| 8.2      | Separable and Separably Generated Extensions . . . . .              | 244 |
| 8.3      | Regular Extensions . . . . .                                        | 250 |
| 8.4      | Constant Extensions . . . . .                                       | 253 |
| 8.5      | Genus Change in Constant Extensions . . . . .                       | 265 |
| 8.6      | Inseparable Function Fields . . . . .                               | 276 |
| 8.7      | Exercises . . . . .                                                 | 281 |
| <br>     |                                                                     |     |
| <b>9</b> | <b>The Riemann–Hurwitz Formula</b> . . . . .                        | 283 |
| 9.1      | The Differential $dx$ in $k(x)$ . . . . .                           | 283 |
| 9.2      | Trace and Cotrace of Differentials . . . . .                        | 289 |
| 9.3      | Hasse Differentials and Residues . . . . .                          | 292 |
| 9.4      | The Genus Formula . . . . .                                         | 307 |
| 9.5      | Genus Change in Inseparable Extensions . . . . .                    | 311 |

|           |                                                                                  |            |
|-----------|----------------------------------------------------------------------------------|------------|
| 9.6       | Examples                                                                         | 325        |
| 9.6.1     | Function Fields of Genus 0                                                       | 325        |
| 9.6.2     | Function Fields of Genus 1                                                       | 330        |
| 9.6.3     | The Automorphism Group of an Elliptic Function Field                             | 337        |
| 9.6.4     | Hyperelliptic Function Fields                                                    | 344        |
| 9.7       | Exercises                                                                        | 351        |
| <b>10</b> | <b>Cryptography and Function Fields</b>                                          | <b>353</b> |
| 10.1      | Introduction                                                                     | 353        |
| 10.2      | Symmetric and Asymmetric Cryptosystems                                           | 354        |
| 10.3      | Finite Field Cryptosystems                                                       | 356        |
| 10.3.1    | The Discrete Logarithm Problem                                                   | 357        |
| 10.3.2    | The Diffie–Hellman Key Exchange Method and the Digital Signature Algorithm (DSA) | 357        |
| 10.4      | Elliptic Function Fields Cryptosystems                                           | 358        |
| 10.4.1    | Key Exchange Elliptic Cryptosystems                                              | 359        |
| 10.5      | The ElGamal Cryptosystem                                                         | 360        |
| 10.5.1    | Digital Signatures                                                               | 361        |
| 10.6      | Hyperelliptic Cryptosystems                                                      | 363        |
| 10.7      | Reduced Divisors over Finite Fields                                              | 367        |
| 10.8      | Implementation of Hyperelliptic Cryptosystems                                    | 370        |
| 10.9      | Exercises                                                                        | 374        |
| <b>11</b> | <b>Introduction to Class Field Theory</b>                                        | <b>377</b> |
| 11.1      | Introduction                                                                     | 377        |
| 11.2      | Čebotarev’s Density Theorem                                                      | 378        |
| 11.3      | Inverse Limits and Profinite Groups                                              | 388        |
| 11.4      | Infinite Galois Theory                                                           | 400        |
| 11.5      | Results on Global Class Field Theory                                             | 409        |
| 11.6      | Results on Local Class Field Theory                                              | 411        |
| 11.7      | Exercises                                                                        | 411        |
| <b>12</b> | <b>Cyclotomic Function Fields</b>                                                | <b>415</b> |
| 12.1      | Introduction                                                                     | 415        |
| 12.2      | Basic Facts                                                                      | 416        |
| 12.3      | Cyclotomic Function Fields                                                       | 422        |
| 12.4      | Arithmetic of Cyclotomic Function Fields                                         | 429        |
| 12.4.1    | Newton Polygons                                                                  | 430        |
| 12.4.2    | Abhyankar’s Lemma                                                                | 433        |
| 12.4.3    | Ramification at $p_\infty$                                                       | 435        |
| 12.5      | The Artin Symbol in Cyclotomic Function Fields                                   | 438        |
| 12.6      | Dirichlet Characters                                                             | 448        |
| 12.7      | Different and Genus                                                              | 461        |
| 12.8      | The Maximal Abelian Extension of $K$                                             | 463        |
| 12.8.1    | $E/K$                                                                            | 463        |

|           |                                                                  |     |
|-----------|------------------------------------------------------------------|-----|
| 12.8.2    | $K_T/K$ .....                                                    | 464 |
| 12.8.3    | $L_\infty/K$ .....                                               | 469 |
| 12.8.4    | $A = EK_TL_\infty$ .....                                         | 470 |
| 12.9      | The Analogue of the Brauer–Siegel Theorem .....                  | 478 |
| 12.10     | Exercises .....                                                  | 480 |
| <b>13</b> | <b>Drinfeld Modules</b> .....                                    | 487 |
| 13.1      | Introduction .....                                               | 487 |
| 13.2      | Additive Polynomials and the Carlitz Module .....                | 488 |
| 13.3      | Characteristic, Rank, and Height of Drinfeld Modules .....       | 490 |
| 13.4      | Existence of Drinfeld Modules. Lattices .....                    | 496 |
| 13.5      | Explicit Class Field Theory .....                                | 504 |
| 13.5.1    | Class Number One Case .....                                      | 505 |
| 13.5.2    | General Class Number Case .....                                  | 507 |
| 13.5.3    | The Narrow Class Field $H_A^+$ .....                             | 512 |
| 13.5.4    | The Hilbert Class Field $H_A$ .....                              | 516 |
| 13.5.5    | Explicit Class Fields and Ray Class Fields .....                 | 518 |
| 13.6      | Drinfeld Modules and Cryptography .....                          | 521 |
| 13.6.1    | Drinfeld Module Version of the Diffie–Hellman Cryptosystem ..... | 522 |
| 13.6.2    | The Gillard et al. Drinfeld Cryptosystem .....                   | 522 |
| 13.7      | Exercises .....                                                  | 523 |
| <b>14</b> | <b>Automorphisms and Galois Theory</b> .....                     | 527 |
| 14.1      | The Castelnuovo–Severi Inequality .....                          | 527 |
| 14.2      | Weierstrass Points .....                                         | 532 |
| 14.2.1    | Hasse–Schmidt Differentials .....                                | 534 |
| 14.2.2    | The Wronskian .....                                              | 542 |
| 14.2.3    | Arithmetic Theory of Weierstrass Points .....                    | 551 |
| 14.2.4    | Gap Sequences of Hyperelliptic Function Fields .....             | 561 |
| 14.2.5    | Fields with Nonclassical Gap Sequence .....                      | 566 |
| 14.3      | Automorphism Groups of Algebraic Function Fields .....           | 570 |
| 14.4      | Properties of Automorphisms of Function Fields .....             | 583 |
| 14.5      | Exercises .....                                                  | 593 |
| <b>A</b>  | <b>Cohomology of Groups</b> .....                                | 597 |
| A.1       | Definitions and Basic Results .....                              | 597 |
| A.2       | Homology and Cohomology in Low Dimensions .....                  | 615 |
| A.3       | Tate Cohomology Groups .....                                     | 624 |
| A.4       | Cohomology of Cyclic Groups .....                                | 627 |
| A.5       | Exercises .....                                                  | 631 |
|           | <b>Notations</b> .....                                           | 635 |
|           | <b>References</b> .....                                          | 639 |
|           | <b>Index</b> .....                                               | 647 |