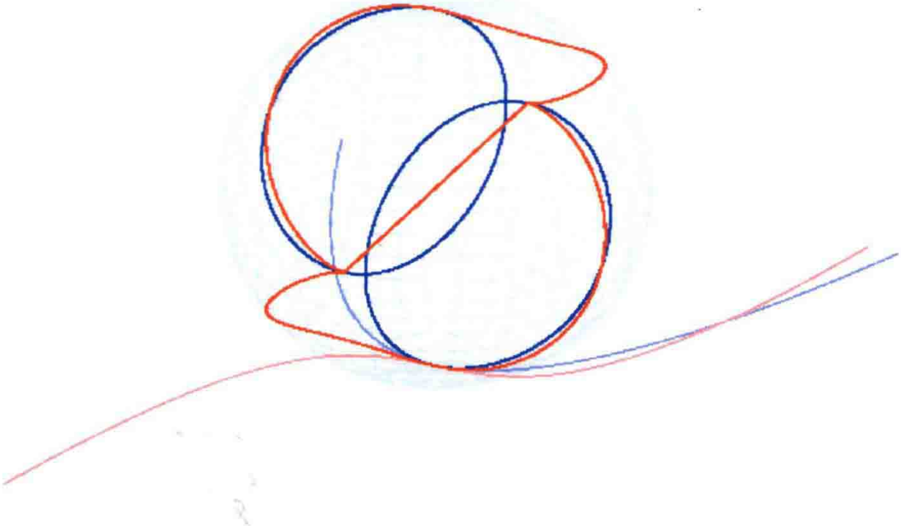
DE GRUYTER
OPEN

Alvanos Paraskevas

RIEMANN-ROCH SPACES AND COMPUTATION



DE
G

Paraskevas Alvanos

Riemann-Roch Spaces and Computation

Managing Ediror: Aleksandra Nowacka-Leverton

Associate Editor: Dimitris Poulakis

Language Editor: Nick Rogers

DE GRUYTER
OPEN

Published by De Gruyter Open Ltd, Warsaw/Berlin
Part of Walter de Gruyter GmbH, Berlin/Munich/Boston

ISBN 978-3-11-042613-7
e-ISBN 978-3-11-042612-0

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.dnb.de.

Managing Editor: Aleksandra Nowacka-Leverton
Associate Editor: Dimitris Poulakis
Language Editor: Nick Rogers

www.degruyteropen.com

Cover illustration: © Paraskevas Alvanos

Paraskevas Alvanos

Riemann-Roch Spaces and Computation

To my "*Flower*"
Στο "*Τζατζούρι*" μου

Preface

Riemann-Roch space is a field of functions with applications in algebraic geometry and coding theory. This textbook is focused on theory and on computations that are relevant to Riemann-Roch spaces. It is noted that for the computation of integral points on curves, the study of a Riemann-Roch space is necessary (Alvanos et al., 2011; Poulakis et al., 2000; Poulakis et al., 2002). Besides the computation of integral points on curves, computation of Riemann-Roch spaces are used for the construction of Goppa codes (Goppa, 1981; Goppa, 1988), symbolic parametrizations of curves (Van Hoeij, 1995; Van Hoeij, 1997), integration of algebraic functions (Davenport, 1981) and a lot more (Hiren et.al, 2005).

Riemann-Roch space arises from the classical Riemann-Roch theorem which computes the dimension of the field of functions with specific zeros and poles

$$\dim D = \deg D - g + 1 + i(D).$$

Here D is a divisor, g is the genus of the function field and $i(D)$ an invariant of the function field. The inequality

$$\dim D \geq \deg D - g + 1$$

was initially proved by Riemann (1857) and was upgraded to equality by Roch (1865).

The scope of the textbook is not to add original research to the literature but to give an educational perspective on Riemann-Roch spaces and the computation of algebraic structures connected to Riemann-Roch theorem. The proofs of theorems that use stiff techniques are avoided, and proofs with educational value (according to the author's opinion) are presented, allowing the reader to follow the book without many difficult computation. In order to follow the textbook, the reader should be aware of the basic algebraic structures such as group, ring, prime ideal, maximal ideal, number field, modules, vector spaces and the basics of linear algebra, matrix theory and polynomial theory.

The first part of the textbook consists of four chapters where algebraic structures and some of their properties are analysed. The second part of the textbook consists of four more chapters where algorithms and examples connected to Riemann-Roch spaces are presented. Throughout the textbook a variety of examples cover the majority of the cases.

This textbook is a résumé of the author's work and his research the last 15 years. Therefore, the author would like to thank all of his colleagues and friends that helped him in every way during those years. Especially, the author would like to express his deep gratitude to his beloved wife, K. Roditou, for her comments and her support during the writing of this textbook. The author would also like to thank very much the referees for their corrections and their very thoughtful and useful comments and K. Chatzinikolaou for his suggestions about the design of the cover. Last but not least, the author would like to express his ultimate respect to his former supervisor and current mathematical mentor prof. D. Poulakis.

Contents

Preface —— VIII

Part I: Riemann-Roch Spaces

1 Elements of Algebra —— 2
1.1 Domains —— 2
1.2 Rings and Fields —— 9
1.3 Norm and Trace —— 13
1.4 Group of Units —— 15

2 Function Fields and Curves —— 17
2.1 Algebraic Function Fields —— 17
2.2 Affine Curves —— 19
2.3 Projective Curves —— 23
2.4 Genus of a Curve —— 27

3 Riemann-Roch Spaces —— 32
3.1 Valuation Rings —— 32
3.2 Places and Divisors —— 36
3.3 Riemann-Roch Space —— 39
3.4 Holomorphy Rings —— 41

4 Integral Domains —— 44
4.1 Fractional Ideals —— 44
4.2 Localization —— 46
4.3 R-module V —— 50

Part II: Computation

5 Computing Integral Bases —— 54
5.1 Discriminant —— 54
5.2 Ideal Basis —— 56
5.3 Idealizer —— 58
5.4 Radical —— 60
5.5 Computing the Discriminants Ideal Radical —— 61
5.6 Computing Idealizers and Inverse Ideals —— 64
5.7 Trager's Algorithm —— 66
5.8 Examples —— 67

6 Computing Riemann-Roch Spaces —— 73

6.1 Reduced Basis Algorithms — 73
6.2 The Dimension of L(D) — 79
6.3 Computing L(D) — 81

7 Computing Resultant and Norm Form Equations — 85
7.1 Resultant — 85
7.2 Computing $N_{L/K}(x_1 a_1 + \cdots + x_n a_n) = k$ — 90
7.3 Examples — 92

8 Computing Integral Points on Rational Curves — 98
8.1 Integral Points on Curves — 98
8.2 Integral Points on Curves with $|\Sigma_\infty(C)| \geq 3$ — 99
8.3 Integral Points on Curves with $|\Sigma_\infty(C)| = 2$ (i) — 106
8.4 Integral Points on Curves with $|\Sigma_\infty(C)| = 2$ (ii) — 109
8.5 Integral Points on Curves with $|\Sigma_\infty(C)| = 1$ — 112

Appendices — 115

A Unimodular Matrices — 115
A.1 Transformation Matrix — 115
A.2 Unimodular Transformations — 116

B Algorithm's Codes — 118
B.1 Integral Points 3 Algorithm's Code — 118
B.2 Integral Points 2i Algorithm's Code — 126
B.3 Integral Points 2ii Algorithm's Code — 129
B.4 Integral Points 1 Algorithm's Code — 133

Bibliography — 136

Index — 139

Index of Algorithms — 141

Part I: **Riemann-Roch Spaces**

1 Elements of Algebra

In this first chapter we introduce the algebraic structures that will be used in the following chapters. Definitions are enriched with lots of examples and figures for better understanding. We will only deal with commutative rings and number fields and therefore every reference to a ring or a field implies a commutative ring and a number field respectively.

1.1 Domains

In this section we investigate some basic properties of domains that are used throughout the textbook. Starting with the algebraic structure of the commutative ring and adding properties to it, we establish the algebraic structure of the field.

Definition A commutative ring R is called an *integral domain* if for any two elements $a, b \in R$, $a \cdot b = 0$ implies that $a = 0$ or $b = 0$.

The definition of integral domain is necessary in order to have a domain where divisibility can occur. As we know the set of $n \times n$ invertible matrices, where the identity element of the ring is the identity matrix and the zero element of the ring is the zero matrix, form a commutative ring. The product of two matrices A, B might be the zero matrix while neither of A and B are zero matrices. For instance

$$\begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus, the ring of $n \times n$ diagonal matrices is not an integral domain, even though it is a commutative ring. All fields, the ring of rational integers $\mathbb{Z}$ and all the subrings of integral domains are integral domains.

Proposition 1.1.1. *If R is an integral domain then $R[x]$ is also an integral domain.*

Proof. In order to prove that $R[x]$ is an integral domain it is equivalent to prove that for any two elements

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \ a_n \neq 0$$

and

$$g(x) = b_m x^m + \cdots + b_1 x + b_0, \ b_m \neq 0$$

if $f(x)g(x) = 0$ then $f(x) = 0$ or $g(x) = 0$. The product $f(x)g(x)$ is

$$f(x)g(x) = a_n b_m x^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0 = 0.$$

Thus $a_n b_m = 0$, which is a contradiction. □

Divisibility in commutative rings give rise to interesting properties for the elements of those rings. Those properties inspire the following definitions. Let R be an integral domain. An element $u \in R$ is called *unit* if there is $u^{-1} \in R$ such that $u \cdot u^{-1} = 1$ and is called *n-th root of unity* if $u^n = 1$ for some n positive integer. The element u^{-1} is called an *invertible element* of u. An element $r \in R$ is called *irreducible* if there are no non-unit elements a, b of R such that $a \cdot b = r$. An element $p \in R$ is called *prime* if for any a, b of R such that $p|ab$, then $p|a$ or $p|b$. The definition of the prime element is equivalent to the condition that p is prime if the principal ideal (p) is a prime ideal. Two elements r_1 and r_2 of R are called *associates* if there is a unit $u \in R$ such that $r_1 = ur_2$.

Proposition 1.1.2. *The prime elements of an integral domain are irreducible.*

Proof. Let p be a prime element of an integral domain R. Then, for any $a, b \in R$ such that $p = ab$ we have that $p|a$ or $p|b$. Assume, without loss of generality, that $p|a$. Then there is $c \in R$ such that $a = pc$. Hence,

$$p = ab \Rightarrow p = pcb \Rightarrow cb = 1 \Rightarrow b \text{ is a unit}$$

and therefore p is irreducible. □

Definition An integral domain R in which every non-zero element a can be written uniquely with respect to a unit as a product of irreducible elements of R is called a *unique factorization domain.*

This means that if we have an element a of a unique factorization domain R that can be factorized in two ways, for instance

$$a = b_1^{q_1} \cdots b_n^{q_n} = c_1^{r_1} \cdots c_m^{r_m}$$

where b_i and c_j are irreducible elements of R and q_i and r_j are rational integers, then necessarily $n = m$ and each irreducible factor b_i is equal up to a unit to exactly one irreducible factor c_j. The definition of the unique factorization domain arises from the generalization of the *Fundamental Theorem of Arithmetic* which states that every positive integer except 1 is either a prime or it can be written uniquely as a product of prime elements. A historical survey of the Fundamental Theorem of Arithmetic can be found in (Agargün et al., 2001).

Now, let R be the polynomial ring $\mathbb{Z}[\sqrt{-5}]$ which is the ring that consists of the elements $a + b\sqrt{-5}$ for any $a, b \in \mathbb{Z}$. The element $9 \in \mathbb{Z}[\sqrt{-5}]$ can be written in two ways. That is

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Since 3 does not differ from either $(2 + \sqrt{-5})$ or $(2 - \sqrt{-5})$ by more than a unit, we conclude that 9 has two representations with irreducible elements and therefore $\mathbb{Z}[\sqrt{-5}]$

is not a unique factorization domain. On the other hand the set of the *Gaussian integers* $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ is a unique factorization domain and the irreducible Gaussian integers are exactly the rational integer primes which are not a sum of two rational integers and the elements of the form $a \pm bi$ such that $a^2 + b^2$ is prime. In addition if R is a unique factorization domain then so is $R[x]$.

Proposition 1.1.3. *Every irreducible element of a unique factorization domain is prime.*

Proof. Let r be an irreducible element of the unique factorization domain R. Assume that $r|ab$ for some $a, b \in R$. Then there is a $c \in R$ such that $ab = cr$. Since R is a unique factorization domain, a and b can be factorized uniquely into irreducible elements as follows

$$a_1 \cdots a_n b_1 \cdots b_m = cr.$$

Thus r must be associate to a factor of either a or b. Therefore $r|a$ or $r|b$ which implies that r is prime. □

Definition An integral domain in which every ideal is principal is called a *principal ideal domain.*

This means that every ideal of R can be generated by a single element. If a and b are elements of the same principal ideal domain then there is a d such that the principal ideal (d) generated by d is equal to the ideal (a, b) generated by a and b. If a and b have no common divisors then every element of the R can be represented as $ar_1 + br_2$ for some r_1 and r_2 of R.

Every field K is a principal ideal domain since its trivial ideal (0) is unique and therefore at the same time maximal. Next we will show that the ring of integers $\mathbb{Z}$ and the polynomial ring $K[x]$ are also principal ideal domains.

Proposition 1.1.4. *The ring of integers $\mathbb{Z}$ is a principal ideal domain.*

Proof. Let I be a non zero ideal of $\mathbb{Z}$ and a the smallest positive integer of I. According to the euclidean division for any element $b \in I$ it holds that

$$b = \pi a + \upsilon$$

where $0 \leq \upsilon < a$. Since $b, \pi a$ are elements of I it implies that $\upsilon \in I$ but since $\upsilon < a$ and a is the smallest positive integer of I we deduce that $\upsilon = 0$. Thus, $b = \pi a$ and therefore I is equal to the principal ideal (a). □

Proposition 1.1.5. *For any field K, the polynomial ring $K[x]$ is a principal ideal domain.*

Proof. Let I be a non-zero ideal of $K[x]$ and $f(x)$ an element of I having the minimal degree of all elements of $K[x]$. Assume that there is a $g(x) \in I$ and that

$$g(x) = \pi(x)f(x) + \upsilon(x)$$

where $0 \leq \deg \upsilon(x) < \deg f$. Since $g(x)$ and $\pi(x)f(x)$ are elements of I we deduce that $\upsilon(x)$ is also an element of I. But $f(x)$ is an element of minimum degree and $0 \leq \deg \upsilon(x) < \deg f$, so $\upsilon(x) = 0$, $g(x) = \pi(x)f(x)$ and therefore $I = (f(x))$. □

Examples of domains that are not principal ideal domains are the bivariate ring $K[x, y]$ and the polynomial ring $\mathbb{Z}[x]$. For example the ideal generated by (x, y) is not a principal ideal of $K[x, y]$ and the ideal (x, n) generated by the two elements x and $n \in \mathbb{Z}$ where $n \geq 2$ is not a principal ideal of $\mathbb{Z}[x]$.

Proposition 1.1.6. *If R is a principal ideal domain, then every prime ideal of R is maximal.*

Proof. Assume that (a) is a non-maximal prime ideal of R. Then there is a principal ideal (b) such that $(a) \subsetneq (b) \subsetneq R$. Thus, $a \in (b)$ and there is $c \in R$ such that $a = bc$. Since $b \notin (a)$ it implies that $c \in (a)$. Thus there is $d \in R$ such that $c = da$ and therefore

$$a = bc \Rightarrow a = bda \Rightarrow bd = 1.$$

Hence, 1 belongs to (b) which means that $(b) = R$. This is a contradiction since we assumed that $(b) \subsetneq R$. □

Proposition 1.1.7. *Every principal ideal domain is a unique factorization domain.*

Proof. In order to prove that a principal ideal domain R is a unique factorization domain it is equivalent to show that every non-unit element a of R has a factorization into irreducible factors with respect to a unit. Initially assume that none of the factors of a is irreducible. Let $a_1 \in R$ such that $a_1|a$. Then a_1 does not have any irreducible factors. Inductively, we can create an infinite sequence of non-irreducible factors $\cdots a_2|a_1, a_1|a$ such that

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots .$$

Now, assume that I is generated by $a, a_1, a_2, \ldots$. Since R is a principal ideal domain, there is a $b \in R$ such that

$$b = \sum_{i=0}^{n} r_i a_i, \quad r_i \in R, \; a_0 = a.$$

Thus $b \in (a_n)$ and $(b) \subset (a_n)$. On the other hand we have that

$$(a_n) \subsetneq (a, a_1, a_2, \ldots) = I.$$

This is a contradiction with the assumption that a was irreducible, and therefore we have proved that every element a of R has at least one irreducible factor.

Suppose now that $a = a_1 r_1$ where r_1 is the irreducible factor of a. If a_1 is a unit then a is irreducible. If a_1 is not a unit then there is an irreducible factor r_2 and some $a_2 \in R$ such that $a_1 = a_2 r_2$. If a_2 is a unit then $a = a_2 r_1 r_2$ is a factorization of a into irreducible factors. This procedure could be continued indefinitely, and therefore a has an irreducible factor. □

The following theorem is very enlightening since it provide us a sufficient and necessary condition for a unique factorization theorem to be a principal ideal domain

Theorem 1.1.8. *A unique factorization domain R is a principal ideal domain if and only if every prime ideal of R is maximal.*

Proof. We will show that if every prime ideal of R is maximal then R is a principal ideal domain, since the converse is obvious by 1.1.7.

Let I be a non-trivial ideal of R and $a, b \in R$ where

$$a = a_1 \cdots a_n$$

and

$$b = b_1 \cdots b_m$$

are the decompositions of a and b respectively into irreducible elements such that $a_i \neq b_j$ for any i and j with respect to the units of R. Since I is prime, at least one factor from p_i and b_j belong to I. Without loss of generality suppose that $p_1, q_1 \in I$. Since p_1, q_1 are irreducibles, by 1.1.3 we get that (p_1) and (q_1) are primes and maximal by our assumption. This is a contradiction since $p_1 \neq q_1$ and therefore it holds that

$$(p_1) \subsetneq (p_1, q_1) \subset I \subsetneq R$$

and

$$(q_1) \subsetneq (p_1, q_1) \subset I \subsetneq R.$$

Now let $\mathcal{I}$ be the set of non-principal ideals of R and assume that $\mathcal{I}$ is not an empty set. Let

$$I_1 \subset I_2 \subset \cdots$$

and

$$I = \bigcup (I_i).$$

If I is a principal ideal (a), then $a \in I_i$ for some i and therefore $I_i = (a)$. This is a contradiction and therefore $I \in \mathcal{I}$. By Zorn's lemma (see (Vereshchagin and Shen, 2002) or (Komjáth and Totik, 2006)), we get that there is I a maximal ideal of $\mathcal{I}$. If I is not a prime ideal, then there exist $a, b \in R$ such that $ab \in I$ and $a, b \notin I$. Then

$$I \subsetneq (I, a) = (c)$$