# Graduate Texts in Mathematics

Serge Lang

# Introduction to Algebraic and Abelian Functions

## Second Edition

代数函数与Abelian函数 第2版

Springer

世界图书出版公司
www.wpcbj.com.cn

Serge Lang

# Introduction to Algebraic and Abelian Functions

Second Edition

Springer-Verlag
New York Berlin Heidelberg London Paris
Tokyo Hong Kong Barcelona Budapest

**图书在版编目（CIP）数据**

代数函数与 Abelian 函数导论：英文/（美）莱恩（Lang，S.）著．—2 版．—北京：世界图书出版公司北京公司，2009.8

书名原文：Introduction to Algebraic and Abelian Functions

ISBN 978-7-5100-0487-2

Ⅰ. 代… Ⅱ. 莱… Ⅲ. 函数—研究生—教材—英文 Ⅳ. 0174

中国版本图书馆 CIP 数据核字（2009）第 107714 号

| | |
|---|---|
| 书　　名： | Introduction to Algebraic and Abelian Functions 2nd Edition |
| 作　　者： | Serge Lang |
| 中 译 名： | 代数函数与 Abelian 函数导论 第 2 版 |
| 责任编辑： | 高蓉 |
| 出 版 者： | 世界图书出版公司北京公司 |
| 印 刷 者： | 三河国英印务有限公司 |
| 发　　行： | 世界图书出版公司北京公司（北京朝内大街 137 号　100010） |
| 联系电话： | 010-64021602，010-64015659 |
| 电子信箱： | kjb@ wpcbj. com. cn |
| 开　　本： | 24 开 |
| 印　　张： | 7.5 |
| 版　　次： | 2009 年 08 月 |
| 版权登记： | 图字：01-2009-1088 |
| 书　　号： | 978-7-5100-0487-2/O · 702　　定　价：25.00 元 |

Serge Lang
Department of Mathematics
Yale University
New Haven, Connecticut 06520
USA



AMS Classifications: 14HOJ, 14K25

With 9 illustrations.

Library of Congress Cataloging in Publication Data
Lang, Serge, 1927–
Introduction to algebraic and abelian functions.
(Graduate texts in mathematics; 89) Bibliography: p. 165 Includes index.
1. Functions, Algebraic. 2. Functions, Abelian.
I. Title. II. Series. QA341.L32 1982 515.9'83 82-5733 AACR2

The first edition of *Introduction to Algebraic and Abelian Functions* was published in 1972 by Addison-Wesley Publishing Co., Inc.



9 8 7 6 5 4 3 2 (Second corrected printing, 1995)

ISBN 0-387-90710-6 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-90710-6 Springer-Verlag Berlin Heidelberg New York

Graduate Texts in Mathematics 89

## Books of Related Interest by Serge Lang

**Linear Algebra**, Third Edition
1987, ISBN 96412-6

**Undergraduate Algebra**, Second Edition
1990, ISBN 97279-X

**Complex Analysis**, Third Edition
1993, ISBN 97886-0

**Real and Functional Analysis**, Third Edition
1993, ISBN 94001-4

**Algebraic Number Theory**, Second Edition
1994, ISBN 94225-4

**Introduction to Complex Hyperbolic Spaces**
1987, ISBN 96447-9

## Other Books by Lang Published by Springer-Verlag

Introduction to Arakelov Theory • Riemann-Roch Algebra (with William Fulton) • Complex Multiplication • Introduction to Modular Forms • Modular Units (with Daniel Kubert) • Fundamentals of Diophantine Geometry • Elliptic Functions • Number Theory III • Cyclotomic Fields I and II • $SL_2(R)$ • Abelian Varieties • Differential and Riemannian Manifolds • Undergraduate Analysis • Elliptic Curves: Diophantine Analysis • Introduction to Linear Algebra • Calculus of Several Variables • First Course in Calculus • Basic Mathematics • Geometry: A High School Course (with Gene Murrow) • Math! Encounters with High School Students • The Beauty of Doing Mathematics • THE FILE

# Introduction

This short book gives an introduction to algebraic and abelian functions, with emphasis on the complex analytic point of view. It could be used for a course or seminar addressed to second year graduate students.

The goal is the same as that of the first edition, although I have made a number of additions. I have used the Weil proof of the Riemann-Roch theorem since it is efficient and acquaints the reader with adeles, which are a very useful tool pervading number theory.

The proof of the Abel-Jacobi theorem is that given by Artin in a seminar in 1948. As far as I know, the very simple proof for the Jacobi inversion theorem is due to him. The Riemann-Roch theorem and the Abel-Jacobi theorem could form a one semester course.

The Riemann relations which come at the end of the treatment of Jacobi's theorem form a bridge with the second part which deals with abelian functions and theta functions. In May 1949, Weil gave a boost to the basic theory of theta functions in a famous Bourbaki seminar talk. I have followed his exposition of a proof of Poincaré that to each divisor on a complex torus there corresponds a theta function on the universal covering space. However, the correspondence between divisors and theta functions is not needed for the linear theory of theta functions and the projective embedding of the torus when there exists a positive non-degenerate Riemann form. Therefore I have given the proof of existence of a theta function corresponding to a divisor only in the last chapter, so that it does not interfere with the self-contained treatment of the linear theory.

The linear theory gives a good introduction to abelian varieties, in an analytic setting. Algebraic treatments become more accessible to the reader who has gone through the easier proofs over the complex numbers. This includes the duality theory with the Picard, or dual, abelian manifold.

I have included enough material to give all the basic analytic facts necessary in the theory of complex multiplication in Shimura-Taniyama, or my more recent book on the subject, and have thus tried to make this topic accessible at a more elementary level, provided the reader is willing to assume some algebraic results.

I have also given the example of the Fermat curve, drawing on some recent results of Rohrlich. This curve is both of intrinsic interest, and gives a typical setting for the general theorems proved in the book. This example illustrates both the theory of periods and the theory of divisor classes. Again this example should make it easier for the reader to read more advanced books and papers listed in the bibliography.

*New Haven, Connecticut* SERGE LANG

# Contents

Chapter IV
## The Theorem of Abel-Jacobi



Chapter V
## Periods on the Fermat Curve



Chapter VI
## Linear Theory of Theta Functions



Chapter VII
## Homomorphisms and Duality



Chapter VIII
## Riemann Matrices and Classical Theta Functions

Chapter IX

## Involutions and Abelian Manifolds of Quaternion Type



Chapter X

## Theta Functions and Divisors

CHAPTER I

# The Riemann-Roch Theorem

## §1. Lemmas on Valuations

We recall that a **discrete valuation ring** $\mathfrak{o}$ is a principal ideal ring (and therefore a unique factorization ring) having only one prime. If $t$ is a generator of this prime, we call $t$ a **local parameter**. Every element $x \neq 0$ of such a ring can be expressed as a product

$$x = t^r y,$$

where $r$ is an integer $\geqq 0$, and $y$ is a unit. An element of the quotient field $K$ has therefore a similar expression, where $r$ may be an arbitrary integer, which is called the **order** or **value** of the element. If $r > 0$, we say that $x$ has a **zero** at the valuation, and if $r < 0$, we say that $x$ has a **pole**. We write

$$r = v_{\mathfrak{o}}(x), \qquad \text{or} \qquad v(x), \qquad \text{or} \qquad \operatorname{ord}_{\mathfrak{o}}(x).$$

Let $\mathfrak{p}$ be the maximal ideal of $\mathfrak{o}$. The map of $K$ which is the canonical map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p}$ on $\mathfrak{o}$, and sends an element $x \notin \mathfrak{o}$ to $\infty$, is called the **place** of the valuation.

We shall take for granted a few basic facts concerning valuations, all of which can be found in my *Algebra*. Especially, if $E$ is a finite extension of $K$ and $\mathfrak{o}$ is a discrete valuation ring in $K$ with maximal ideal $\mathfrak{p}$, then there exists a discrete valuation ring $\mathfrak{O}$ in $E$, with prime $\mathfrak{P}$, such that

$$\mathfrak{o} = \mathfrak{O} \cap K \qquad \text{and} \qquad \mathfrak{p} = \mathfrak{P} \cap K.$$

If $u$ is a prime element of $\mathfrak{O}$, then $t\mathfrak{O} = u^e \mathfrak{O}$, and $e$ is called the **ramifica-**

**tion index** of $\mathfrak{O}$ over $\mathfrak{o}$ (or of $\mathfrak{P}$ over $\mathfrak{p}$). If $\Gamma_{\mathfrak{O}}$ and $\Gamma_{\mathfrak{o}}$ are the value groups of these valuation rings, then $(\Gamma_{\mathfrak{O}} : \Gamma_{\mathfrak{o}}) = e$.

We say that the pair $(\mathfrak{O},\mathfrak{P})$ **lies above** $(\mathfrak{o},\mathfrak{p})$, or more briefly that $\mathfrak{P}$ **lies above** $\mathfrak{p}$. We say that $(\mathfrak{O},\mathfrak{P})$ is **unramified above** $(\mathfrak{o},\mathfrak{p})$, or that $\mathfrak{P}$ is **unramified** above $\mathfrak{p}$, if the ramification index is equal to 1, that is $e = 1$.

**Example.** Let $k$ be a field and $t$ transcendental over $k$. Let $a \in k$. Let $\mathfrak{o}$ be the set of rational functions

$$f(t)/g(t), \quad \text{with} \quad f(t), g(t) \in k[t] \quad \text{such that} \quad g(a) \neq 0.$$

Then $\mathfrak{o}$ is a discrete valuation ring, whose maximal ideal consists of all such quotients such that $f(a) = 0$. This is a typical situation. In fact, let $k$ be algebraically closed (for simplicity), and consider the extension $k(x)$ obtained with one transcendental element $x$ over $k$. Let $\mathfrak{o}$ be a discrete valuation ring in $k(x)$ containing $k$. Changing $x$ to $1/x$ if necessary, we may assume that $x \in \mathfrak{o}$. Then $\mathfrak{p} \cap k[x] \neq 0$, and $\mathfrak{p} \cap k[x]$ is therefore generated by an irreducible polynomial $p(x)$, which must be of degree 1 since we assumed $k$ algebraically closed. Thus $p(x) = x - a$ for some $a \in k$. Then it is clear that the canonical map

$$\mathfrak{o} \to \mathfrak{o}/\mathfrak{p}$$

induces the map

$$f(x) \mapsto f(a)$$

on polynomials, and it is then immediate that $\mathfrak{o}$ consists of all quotients $f(x)/g(x)$ such that $g(a) \neq 0$; in other words, we are back in the situation described at the beginning of the example.

Similarly, let $\mathfrak{o} = k[[t]]$ be the ring of formal power series in one variable. Then $\mathfrak{o}$ is a discrete valuation ring, and its maximal ideal is generated by $t$. Every element of the quotient field has a formal series expansion

$$x = a_{-m}t^{-m} + \cdots + a_{-1}t^{-1} + a_0 + a_1 t + a_2 t^2 + \cdots,$$

with coefficients $a_i \in k$. The place maps $x$ on the value $a_0$ if $x$ does not have a pole.

In the applications, we shall study a field $K$ which is a finite extension of a transcendental extension $k(x)$, where $k$ is algebraically closed, and $x$ is transcendental over $k$. Such a field is called a **function field in one variable**. If that is the case, then the residue class field of any discrete valuation ring $\mathfrak{o}$ containing $k$ is equal to $k$ itself, since we assumed $k$ algebraically closed.

**Proposition 1.1.** *Let $E$ be a finite extension of $K$. Let $(\mathfrak{O},\mathfrak{P})$ be a discrete* *valuation ring in E above* $(\mathfrak{o},\mathfrak{p})$ *in K. Suppose that* $E = K(y)$ *where y is the root of a polynomial* $f(Y) = 0$ *having coefficients in* $\mathfrak{o}$, *leading coefficient* 1, *such that*

$$f(y) = 0 \quad \textit{but} \quad f'(y) \not\equiv 0 \bmod \mathfrak{P}.$$

*Then* $\mathfrak{P}$ *is unramified over* $\mathfrak{p}$.

*Proof.* There exists a constant $y_0 \in k$ such that $y \equiv y_0 \bmod \mathfrak{P}$. By hypothesis, $f'(y_0) \not\equiv 0 \bmod \mathfrak{P}$. Let $\{y_n\}$ be the sequence defined recursively by

$$y_{n+1} = y_n - f'(y_n)^{-1}f(y_n).$$

Then we leave to the reader the verification that this sequence converges in the completion $K_{\mathfrak{p}}$ of $K$, and it is also easy to verify that it converges to the root $y$ since $y \equiv y_0 \bmod \mathfrak{P}$ but $y$ is not congruent to any other root of $f$ and $\mathfrak{P}$. Hence $y$ lies in this completion, so that the completion $E_{\mathfrak{P}}$ is embedded in $K_{\mathfrak{p}}$, and therefore $\mathfrak{P}$ is unramified.

We also recall some elementary approximation theorems.

**Chinese Remainder Theorem.** *Let R be a ring, and let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *be distinct maximal ideals in that ring. Given positive integers* $r_1, \ldots, r_n$ *and elements* $a_1, \ldots, a_n \in R$, *there exists* $x \in R$ *satisfying the congruences*

$$x \equiv a_i \bmod \mathfrak{p}_i^{r_i} \quad \textit{for all } i.$$

For the proof, cf. *Algebra*, Chapter II, §2. This theorem is applied to the integral closure of $k[x]$ in a finite extension.

We shall also deal with similar approximations in a slightly different context, namely a field $K$ and a finite set of discrete valuation rings $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ of $K$, as follows.

**Proposition 1.2.** *If* $\mathfrak{o}_1$ *and* $\mathfrak{o}_2$ *are two discrete valuation rings with quotient field K, such that* $\mathfrak{o}_1 \subset \mathfrak{o}_2$, *then* $\mathfrak{o}_1 = \mathfrak{o}_2$.

*Proof.* We shall first prove that if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are their maximal ideals, then $\mathfrak{p}_2 \subset \mathfrak{p}_1$. Let $y \in \mathfrak{p}_2$. If $y \notin \mathfrak{p}_1$, then $1/y \in \mathfrak{o}_1$, whence $1/y \in \mathfrak{p}_2$, a contradiction. Hence $\mathfrak{p}_2 \subset \mathfrak{p}_1$. Every unit of $\mathfrak{o}_1$ is *a fortiori* a unit of $\mathfrak{o}_2$. An element $y$ of $\mathfrak{p}_2$ can be written $y = \pi_1^{\nu_1}u$ where $u$ is a unit of $\mathfrak{o}_1$ and $\pi_1$ is an element of order 1 in $\mathfrak{p}_1$. If $\pi_1$ is not in $\mathfrak{p}_2$, it is a unit in $\mathfrak{o}_2$, a contradiction. Hence $\pi_1$ is in $\mathfrak{p}_2$, and hence so is $\mathfrak{p}_1 = \mathfrak{o}_1\pi_1$. This proves $\mathfrak{p}_2 = \mathfrak{p}_1$. Finally, if $u$ is a unit in $\mathfrak{o}_2$, and is not in $\mathfrak{o}_1$, then $1/u$ is $\mathfrak{p}_1$, and thus cannot be a unit in $\mathfrak{o}_2$. This proves our proposition.

From now on, we assume that *our valuation rings* $\mathfrak{o}_i$ $(i = 1, \ldots, n)$ *are distinct, and hence have no inclusion relations.*

**Proposition 1.3.** *There exists an element $y$ of $K$ having a zero at $\mathfrak{o}_1$ and a pole at $\mathfrak{o}_j$ $(j = 2, \ldots, n)$.*

*Proof.* This will be proved by induction. Suppose $n = 2$. Since there is no inclusion relation between $\mathfrak{o}_1$ and $\mathfrak{o}_2$, we can find $y \in \mathfrak{o}_2$ and $y \notin \mathfrak{o}_1$. Similarly, we can find $z \in \mathfrak{o}_1$ and $z \notin \mathfrak{o}_2$. Then $z/y$ has a zero at $\mathfrak{o}_1$ and a pole at $\mathfrak{o}_2$ as desired.

Now suppose we have found an element $y$ of $K$ having a zero at $\mathfrak{o}_1$ and a pole at $\mathfrak{o}_2, \ldots, \mathfrak{o}_{n-1}$. Let $z$ be such that $z$ has a zero at $\mathfrak{o}_1$ and a pole at $\mathfrak{o}_n$. Then for sufficiently large $r$, $y + z^r$ satisfies our requirements, because we have schematically zero plus zero = zero, zero plus pole = pole, and the sum of two elements of $K$ having poles of different order again has a pole.

A high power of the element $y$ of Proposition 1.3 has a high zero at $\mathfrak{o}_1$ and a high pole at $\mathfrak{o}_j$ $(j = 2, \ldots, n)$. Adding 1 to this high power, and considering $1/(1 + y^r)$ we get

**Corollary.** *There exists an element $z$ of $K$ such that $z - 1$ has a high zero at $\mathfrak{o}_1$, and such that $z$ has a high zero at $\mathfrak{o}_j$ $(j = 2, \ldots, n)$.*

Denote by $\text{ord}_i$ the order of an element of $K$ under the discrete valuation associated with $\mathfrak{o}_i$. We then have the following approximation theorem.

**Theorem 1.4.** *Given elements $a_1, \ldots, a_n$ of $K$, and an integer $N$, there exists an element $y \in K$ such that* $\text{ord}_i(y - a_i) > N$.

*Proof.* For each $i$, use the corollary to get $z_i$ close to 1 at $\mathfrak{o}_i$ and close to 0 at $\mathfrak{o}_j$ $(j \neq i)$, or rather at the valuations associated with these valuation rings. Then $z_1 a_1 + \cdots + z_n a_n$ has the required property.

In particular, we can find an element $y$ having given orders at the valuations arising from the $\mathfrak{o}_i$. This is used to prove the following inequality.

**Corollary.** *Let $E$ be a finite algebraic extension of $K$. Let $\Gamma$ be the value group of a discrete valuation of $K$, and $\Gamma_i$ the value groups of a finite number of inequivalent discrete valuations of $E$ extending that of $K$. Let $e_i$ be the index of $\Gamma$ in $\Gamma_i$. Then*

$$\sum e_i \leqq [E : K].$$

*Proof*. Select elements

$$y_{11}, \ldots, y_{1e_1}, \ldots, y_{r1}, \ldots, y_{re_r}$$

of $E$ such that $y_{i\nu}$ ($\nu = 1, \ldots, e_i$) represent distinct cosets of $\Gamma$ in $\Gamma_i$, and have zeroes of high order at the other valuations $v_j$ ($j \neq i$). We contend that the above elements are linearly independent over $K$. Suppose we have a relation of linear dependence

$$\sum_{i,\nu} c_{i\nu} y_{i\nu} = 0.$$

Say $c_{11}$ has maximal value in $\Gamma$, that is, $v(c_{11}) \geqq v(c_{i\nu})$ all $i$, $v$. Divide the equation by $c_{11}$. Then we may assume that $c_{11} = 1$, and that $v(c_{i\nu}) \leqq 1$. Consider the value of our sum taken at $v_1$. All terms $y_{11}, c_{12}y_{12}, \ldots, c_{1e_1}y_{1e_1}$ have distinct values because the $y$'s represent distinct cosets. Hence

$$v_1(y_{11} + \cdots + c_{1e_1}y_{1e_1}) \geqq v_1(y_{11}).$$

On the other hand, the other terms in our sum have a very small value at $v_1$ by hypothesis. Hence again by that property, we have a contradiction, which proves the corollary.

## §2. The Riemann-Roch Theorem

Let $k$ be an algebraically closed field, and let $K$ be a function field in one variable over $k$ (briefly a **function field**). By this we mean that $K$ is a finite extension of a purely transcendental extension $k(x)$ of $k$, of transcendence degree 1. We call $k$ the **constant field**. Elements of $K$ are sometimes called **functions**.

By a **prime**, or **point**, of $K$ over $k$, we shall mean a discrete valuation ring of $K$ containing $k$ (or over $k$). As we saw in the example of §1, the residue class field of this ring is then $k$ itself. The set of all such discrete valuation rings (i.e., the set of all points of $K$) will be called a **curve**, whose function field is $K$. We use the letters $P$, $Q$ for points of the curve, to suggest geometric terminology.

By a **divisor** (on the curve, or of $K$ over $k$) we mean an element of the free abelian group generated by the points. Thus a divisor is a formal sum.

$$\mathfrak{a} = \sum n_i P_i = \sum n_P P$$

where $P_i$ are points, and $n_i$ are integers, all but a finite number of which are 0. We call

$$\sum n_i = \sum_P n_P$$

the **degree** of $\mathfrak{a}$, and we call $n_i$ the **order** of $\mathfrak{a}$ at $P_i$.

If $x \in K$ and $x \neq 0$, then there is only a finite number of points $P$ such that $\mathrm{ord}_P\, x \neq 0$. Indeed, if $x$ is constant, then $\mathrm{ord}_P(x) = 0$ for all $P$. If $x$ is not constant, then there is one point of $k(x)$ at which $x$ has a zero, and one point at which $x$ has a pole. Each of these points extends to only a finite number of points of $K$, which is a finite extension of $k(x)$. Hence we can associate a divisor with $x$, namely

$$(x) = \sum n_P P$$

where $n_P = \mathrm{ord}_P(x)$. Divisors $\mathfrak{a}$ and $\mathfrak{b}$ are said to be **linearly equivalent** if $\mathfrak{a} - \mathfrak{b}$ is the divisor of a function. If $\mathfrak{a} = \sum n_P P$ and $\mathfrak{b} = \sum m_P P$ are divisors, we write

$$\mathfrak{a} \geqq \mathfrak{b} \quad \text{if and only if} \quad n_P \geqq m_P \quad \text{for all} \quad P.$$

This clearly defines a (partial) ordering among divisors. We call $\mathfrak{a}$ **positive** if $\mathfrak{a} \geqq 0$.

If $\mathfrak{a}$ is a divisor, we denote by $L(\mathfrak{a})$ the set of all elements $x \in K$ such that $(x) \geqq -\mathfrak{a}$. If $\mathfrak{a}$ is a positive divisor, then $L(\mathfrak{a})$ consists of all the functions in $K$ which have poles only in $\mathfrak{a}$, with multiplicities at most those of $\mathfrak{a}$. It is clear that $L(\mathfrak{a})$ is a vector space over the constant field $k$ for any divisor $\mathfrak{a}$. We let $l(\mathfrak{a})$ be its dimension.

Our main purpose is to investigate more deeply the dimension $l(\mathfrak{a})$ of the vector space $L(\mathfrak{a})$ associated with a divisor $\mathfrak{a}$ of the curve (we could say of the function field).

Let $P$ be a point of $V$, and $\mathfrak{o}$ its local ring in $K$. Let $\mathfrak{p}$ be its maximal ideal. Since $k$ is algebraically closed, $\mathfrak{o}/\mathfrak{p}$ is canonically isomorphic to $k$. We know that $\mathfrak{o}$ is a valuation ring, belonging to a discrete valuation. Let $t$ be a generator of the maximal ideal. Let $x$ be an element of $\mathfrak{o}$. Then for some constant $a_0$ in $k$, we can write $x \equiv a_0 \bmod \mathfrak{p}$. The function $x - a_0$ is in $\mathfrak{p}$, and has a zero at $\mathfrak{o}$. We can therefore write $x - a_0 = ty_0$, where $y_0$ is in $\mathfrak{o}$. Again by a similar argument we get $y_0 = a_1 + ty_1$ with $y_1 \in \mathfrak{o}$, and

$$x = a_0 + a_1 t + y_1 t^2.$$

Continuing this procedure, we obtain an expansion of $x$ into a power series,

$$x = a_0 + a_1 t + a_2 t^2 + \cdots.$$

It is trivial that if each coefficient $a_i$ is equal to 0, then $x = 0$.

The quotient field $K$ of $\mathfrak{o}$ can be embedded in the power series field $k((t))$