Graduate Texts in Mathematics

Joseph H. Silverman

Advanced Topics in the Arithmetic of Elliptic Curves

椭圆曲线算术中的高等论题

Springer

世界图书出版公司
www.wpcbj.com.cn

Joseph H. Silverman

Advanced Topics in the Arithmetic of Elliptic Curves

With 17 Illustrations

Springer

图书在版编目（CIP）数据

椭圆曲线算术中的高等论题：英文/（美）西尔弗曼（Silverman，J. H.）著. —影印本. —北京：世界图书出版公司北京公司，2010. 2

书名原文：Advanced Topics in the Arithmetic of Elliptic Curves

ISBN 978-7-5100-0483-4

Ⅰ. ①椭… Ⅱ. ①西… Ⅲ. ①椭圆曲线—研究—英文

Ⅳ. 0187. 1

中国版本图书馆 CIP 数据核字（2010）第 010572 号

书　　名：	Advanced Topics in the Arithmetic of Elliptic Curves
作　　者：	Joseph H. Silverman
中 译 名：	椭圆曲线算术中的高等论题
责任编辑：	高蓉　刘慧
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：	23
版　　次：	2010 年 01 月
版权登记：	图字：01-2009-1056
书　　号：	978-7-5100-0483-4/O · 698　　定　　价：60.00 元

Preface

In the introduction to the first volume of *The Arithmetic of Elliptic Curves* (Springer-Verlag, 1986), I observed that "the theory of elliptic curves is rich, varied, and amazingly vast," and as a consequence, "many important topics had to be omitted." I included a brief introduction to ten additional topics as an appendix to the first volume, with the tacit understanding that eventually there might be a second volume containing the details. You are now holding that second volume.

Unfortunately, it turned out that even those ten topics would not fit into a single book, so I was forced to make some choices. The following material is covered in this book:

I. Elliptic and modular functions for the full modular group.
II. Elliptic curves with complex multiplication.
III. Elliptic surfaces and specialization theorems.
IV. Néron models, Kodaira-Néron classification of special fibers, Tate's algorithm, and Ogg's conductor-discriminant formula.
V. Tate's theory of q-curves over p-adic fields.
VI. Néron's theory of canonical local height functions.

So what's still missing? First and foremost is the theory of modular curves of higher level and the associated modular parametrizations of elliptic curves. There is little question that this is currently the hottest topic in the theory of elliptic curves, but any adequate treatment would seem to require (at least) an entire book of its own. (For a nice introduction, see Knapp [1].) Other topics that I have left out in order to keep this book at a manageable size include the description of the image of the ℓ-adic representation attached to an elliptic curve and local and global duality theory. Thus, at best, this book covers approximately half of the material described in the appendix to the first volume. I apologize to those who may feel disappointed, either at the incompleteness or at the choice of particular topics.

In addition to the complete areas which have been omitted, there are several topics which might have been naturally included if space had been available. These include a description of Iwasawa theory in Chapter II,

the analytic theory of p-adic functions (rigid analysis) in Chapter V, and Arakelov intersection theory in Chapter VI.

It has now been almost a decade since the first volume was written. During that decade the already vast mathematical literature on elliptic curves has continued to explode, with exciting new results appearing with astonishing rapidity. Despite the many omissions detailed above, I am hopeful that this book will prove useful, both for those who want to learn about elliptic curves and for those who hope to advance the frontiers of our knowledge. I offer all of you the best of luck in your explorations!

Computer Packages

There are several computer packages now available for performing computations on elliptic curves. PARI and SIMATH have many built-in elliptic curve functions, there are packages available for commercial programs such as Mathematica and Maple, and the author has written a small stand-alone program which runs on Macintosh computers. Listed below are addresses, current as of March 1994, where these packages may be acquired via anonymous ftp.

PARI (includes many elliptic curve functions)
    math.ucla.edu 128.97.4.254
    megrez.ceremab.u-bordeaux.fr 147.210.16.17
      (directory pub/pari)
      (unix, mac, msdos, amiga versions available)
SIMATH (includes many elliptic curve functions)
    ftp.math.orst.edu
    ftp.math.uni-sb.de
apecs (arithmetic of plane elliptic curves, Maple package)
    math.mcgill.ca 132.206.1.20
      (directory pub/apecs)
Elliptic Curve Calculator (Mathematica package)
Elliptic Curve Calculator (stand-alone Macintosh program)
    gauss.math.brown.edu 128.148.194.40
      (directory dist/EllipticCurve)

A description of many of the algorithms used for doing computations on elliptic curves can be found in H. Cohen [1, Ch. 7] and Cremona [1].

Acknowledgments

I would like to thank Peter Landweber and David Rohrlich for their careful reading of much of the original draft of this book. My thanks also go to the many people who offered corrections, suggestions, and encouragement, including Michael Artin, Ian Connell, Rob Gross, Marc Hindry, Paul Lockhart, Jonathan Lubin, Masato Kuwata, Elisabetta Manduchi, Michael Rosen, Glenn Stevens, Felipé Voloch, and Siman Wong.

As in the first volume, I have consulted a great many sources while writing this book. Citations have been included for major theorems, but

many results which are now considered "standard" have been presented as such. In any case, I claim no originality for any of the unlabeled theorems in this book, and apologize in advance to anyone who may feel slighted. Sources which I found especially useful included the following:

Chapter I	Apostol [1], Lang [1,2,3], Serre [3], Shimura [1]
Chapter II	Lang [1], Serre [6], Shimura [1]
Chapter IV	Artin [1], Bosch-Lütkebohmert-Raynaud [1], Tate [2]
Chapter V	Robert [1], Tate [9]
Chapter VI	Lang [3,4], Tate [3]

I would like to thank John Tate for providing me with a copy of his unpublished manuscript (Tate [9]) containing the theory of q-curves over complete fields. This material, some of which is taken verbatim from Professor Tate's manuscript, forms the bulk of Chapter V, Section 3. In addition, the description of Tate's algorithm in Chapter IV, Section 9, follows very closely Tate's original exposition in [2], and I appreciate his allowing me to include this material.

Portions of this book were written while I was visiting the University of Paris VII (1992), IHES (1992), Boston University (1993), and Harvard (1994). I would like to thank everyone at these institutions for their hospitality during my stay.

Finally, and most importantly, I would like to thank my wife Susan for her constant love and understanding, and Debby, Danny, and Jonathan for providing all of those wonderful distractions so necessary for a truly happy life.

Joseph H. Silverman
March 27, 1994

Acknowledgments for the Second Printing

I would like to thank the following people who kindly provided corrections which have been incorporated in this second revised printing: Andrew Baker, Brian Conrad, Guy Diaz, Darrin Doud, Lisa Fastenberg, Benji Fisher, Boris Iskra, Steve Harding, Sharon Kineke, Joan-C. Lario, Yihsiang Liow, Ken Ono, Michael Reid, Ottavio Rizzo, David Rohrlich, Samir Siksek, Tonghai Yang, Horst Zimmer.

Providence, Rhode Island *February, 1999*

Contents

Preface vii
Computer Packages viii
Acknowledgments viii

Introduction 1

CHAPTER I
Elliptic and Modular Functions 5
§1. The Modular Group 6
§2. The Modular Curve $X(1)$ 14
§3. Modular Functions 23
§4. Uniformization and Fields of Moduli 34
§5. Elliptic Functions Revisited 38
§6. q-Expansions of Elliptic Functions 47
§7. q-Expansions of Modular Functions 55
§8. Jacobi's Product Formula for $\Delta(\tau)$ 62
§9. Hecke Operators 67
§10. Hecke Operators Acting on Modular Forms 74
§11. L-Series Attached to Modular Forms 80
Exercises 85

CHAPTER II
Complex Multiplication 95
§1. Complex Multiplication over $\mathbb{C}$ 96
§2. Rationality Questions 104
§3. Class Field Theory — A Brief Review 115
§4. The Hilbert Class Field 121
§5. The Maximal Abelian Extension 128
§6. Integrality of j 140
§7. Cyclotomic Class Field Theory 151
§8. The Main Theorem of Complex Multiplication 157
§9. The Associated Grössencharacter 165
§10. The L-Series Attached to a CM Elliptic Curve 171
Exercises 178

CHAPTER III

Elliptic Surfaces 187

§1. Elliptic Curves over Function Fields 188
§2. The Weak Mordell-Weil Theorem 191
§3. Elliptic Surfaces 200
§4. Heights on Elliptic Curves over Function Fields 212
§5. Split Elliptic Surfaces and Sets of Bounded Height 220
§6. The Mordell-Weil Theorem for Function Fields 230
§7. The Geometry of Algebraic Surfaces 231
§8. The Geometry of Fibered Surfaces 236
§9. The Geometry of Elliptic Surfaces 245
§10. Heights and Divisors on Varieties 255
§11. Specialization Theorems for Elliptic Surfaces 265
§12. Integral Points on Elliptic Curves over Function Fields 274
Exercises 278

CHAPTER IV

The Néron Model 289

§1. Group Varieties 290
§2. Schemes and S-Schemes 297
§3. Group Schemes 306
§4. Arithmetic Surfaces 311
§5. Néron Models 318
§6. Existence of Néron Models 325
§7. Intersection Theory, Minimal Models, and Blowing-Up 338
§8. The Special Fiber of a Néron Model 350
§9. Tate's Algorithm to Compute the Special Fiber 361
§10. The Conductor of an Elliptic Curve 379
§11. Ogg's Formula 389
Exercises 396

CHAPTER V

Elliptic Curves over Complete Fields 408

§1. Elliptic Curves over $\mathbb{C}$ 408
§2. Elliptic Curves over $\mathbb{R}$ 413
§3. The Tate Curve 422
§4. The Tate Map Is Surjective 429
§5. Elliptic Curves over p-adic Fields 438
§6. Some Applications of p-adic Uniformization 445
Exercises 448

CHAPTER VI

Local Height Functions 454

§1. Existence of Local Height Functions 455
§2. Local Decomposition of the Canonical Height 461
§3. Archimedean Absolute Values — Explicit Formulas 463
§4. Non-Archimedean Absolute Values — Explicit Formulas 469
Exercises 476

APPENDIX A

Some Useful Tables 481

§1. Bernoulli Numbers and $\zeta(2k)$ 481
§2. Fourier Coefficients of $\Delta(\tau)$ and $j(\tau)$ 482
§3. Elliptic Curves over $\mathbb{Q}$ with Complex Multiplication 483

Notes on Exercises 484

References 488

List of Notation 498

Index 504

Introduction

In the first volume of *The Arithmetic of Elliptic Curves*, we presented the basic theory culminating in two fundamental global results, the Mordell-Weil theorem on the finite generation of the group of rational points and Siegel's theorem on the finiteness of the set of integral points. This second volume continues our study of elliptic curves by presenting six important, but somewhat more specialized, topics.

We begin in Chapter I with the theory of elliptic functions and modular functions for the full modular group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$. We develop this material in some detail, including the theory of Hecke operators and the L-series associated to cusp forms for $\Gamma(1)$. Chapter II is devoted to the study of elliptic curves with complex multiplication. The main theorem here states that if $K/\mathbb{Q}$ is a quadratic imaginary field and if $E/\mathbb{C}$ is an elliptic curve whose endomorphism ring is isomorphic to the ring of integers of K, then $K\big(j(E)\big)$ is the Hilbert class field of K; and further, the maximal abelian extension of K is generated by $j(E)$ and the x-coordinates[†] of the torsion points in $E(\mathbb{C})$. This is analogous to the cyclotomic theory, where the maximal abelian extension of $\mathbb{Q}$ is generated by the points of finite order in the multiplicative group $\mathbb{C}^*$. At the end of Chapter II we show that the L-series of an elliptic curve with complex multiplication is the product of two Hecke L-series with Grössencharacter, thereby obtaining at one stroke the analytic continuation and functional equation.

The common theme of Chapters III and IV is one-parameter families of elliptic curves. Chapter III deals with the classical geometric case, where the family is parametrized by a projective curve over a field of characteristic zero. Such families are called elliptic surfaces. Thus an elliptic surface consists of a curve C, a surface $\mathcal{E}$, and a morphism $\pi : \mathcal{E} \to C$ such that almost every fiber $\pi^{-1}(t)$ is an elliptic curve. The set of sections

$$\big\{\text{maps } \sigma : C \to \mathcal{E} \text{ such that } \pi \circ \sigma(t) = t\big\}$$

[†] If $j(E) = 1728$ or $j(E) = 0$, one has to use x^2 or x^3 instead of x.

to an elliptic surface forms a group, and we prove an analogue of the Mordell-Weil theorem which asserts that this group is (usually) finitely generated. In the latter part of Chapter III we study canonical heights and intersection theory on $\mathcal{E}$ and prove specialization theorems for both the canonical height and the group of sections.

Chapter IV continues our study of one-parameter families of elliptic curves in a more general setting. We replace the base curve C by a scheme $S = \operatorname{Spec} R$, where R is a discrete valuation ring. The generic fiber of the arithmetic surface $\mathcal{E} \to S$ is an elliptic curve E defined over the fraction field K of R, and its special fiber is a curve $\tilde{\mathcal{E}}$ (possibly singular, reducible, or even non-reduced) defined over the residue field k of R. We prove that if $\mathcal{C} \to S$ is a minimal proper regular arithmetic surface whose generic fiber is E, and if we write $\mathcal{E}$ for the part of $\mathcal{C}$ that is smooth over S, then $\mathcal{E}$ is a group scheme over S and satisfies Néron's universal mapping property. In particular, $E(K) \cong \mathcal{E}(R)$; that is, every K-rational point on the generic fiber E extends to an R-valued point of $\mathcal{E}$. We also describe the Kodaira-Néron classification of the possible configurations for the special fiber $\tilde{\mathcal{C}}$ and give Tate's algorithm for computing the special fiber. At the end of Chapter IV we discuss the conductor of an elliptic curve and prove (some cases of) Ogg's formula relating the conductor, minimal discriminant, and number of components of $\tilde{\mathcal{C}}$.

In Chapter V we return to the analytic theory of elliptic curves. We begin with a brief review of the theory over $\mathbb{C}$, which we then use to analyze elliptic curves defined over $\mathbb{R}$. But the main emphasis of Chapter V is on elliptic curves defined over p-adic fields. Every elliptic curve E defined over $\mathbb{C}$ is analytically isomorphic to $\mathbb{C}^*/q^{\mathbb{Z}}$ for some $q \in \mathbb{C}^*$. Similarly, Tate has shown that if E is defined over a p-adic field K and if the j-invariant of E is non-integral, then E is analytically isomorphic to $K^*/q^{\mathbb{Z}}$ for some $q \in K^*$. (It may be necessary to replace K by a quadratic extension.) Further, the isomorphism $E(\bar{K}) \cong \bar{K}^*/q^{\mathbb{Z}}$ respects the action of the Galois group $G_{\bar{K}/K}$, a fact which is extremely important for the study of arithmetic questions. In Chapter V we describe Tate's theory of q-curves and give some applications.

The final chapter of this volume contains a brief exposition of the theory of canonical local height functions. These local heights can be used to decompose the global canonical height described in the first volume [AEC, VIII §9]. We prove the existence of canonical local heights and give explicit formulas for them. Local heights are useful in studying some of the more refined properties of the global height.

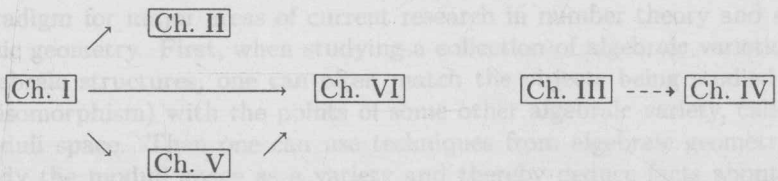
As with the first volume, this book is meant to be an introductory text, albeit at an upper graduate level. For this reason we have occasionally made simplifying assumptions. We mention in particular that in Chapter II we restrict attention to elliptic curves whose ring of complex multiplications is integrally closed; in Chapter III we only consider elliptic surfaces over fields of characteristic 0; and in Chapter IV we assume that all Dedekind

domains and discrete valuation rings have perfect residue fields. Possibly it would be preferable not to make these assumptions, but we feel that the loss of generality is more than made up for by the concomitant clarity of the exposition.

Prerequisites

The main prerequisite for reading this book is some familiarity with the basic theory of elliptic curves as described, for example, in the first volume. Beyond this, the prerequisites vary enormously from chapter to chapter. Chapter I requires little more than a first course in complex analysis. Chapter II uses class field theory in an essential way, so a brief summary of class field theory has been included in (II §3). Chapter III requires various classical results from algebraic geometry, such as the theory of surfaces and the theory of divisors on varieties. As always, summaries, references, and examples are supplied as needed.

Chapter IV is technically the most demanding chapter of the book. The reader will need some acquaintance with the theory of schemes, such as given in Hartshorne [1, Ch. II] or Eisenbud-Harris [1]. But beyond that, there are portions of Chapter IV, especially IV §6, which use advanced techniques and concepts from modern algebraic geometry. We have attempted to explain all of the main points, with varying degrees of precision and reliance on intuition, but the reader who wants to fill in every detail will face a non-trivial task. Finally, Chapters V and VI are basically self-contained, although they do refer to earlier chapters. More precisely, the interdependence of the chapters of this book is illustrated by the following guide:



The dashed line connecting Chapter III to Chapter IV is meant to indicate that although there are few explicit cross-references, mastery of the subject matter of Chapter III will certainly help to illuminate the more difficult material covered in Chapter IV.

References and Exercises

The first volume of *The Arithmetic of Elliptic Curves* (Springer-Verlag, 1986) is denoted by [AEC], so for example [AEC, VIII.6.7] is Theorem 6.7 in Chapter VIII of [AEC]. All other bibliographic references are given by the author's name followed by a reference number in square brackets, for example Tate [7, theorem 5.1]. Cross-references within the same chapter are given by number in parentheses, such as (3.7) or (4.5a). References from within one chapter to another chapter or appendix are preceded by the appropriate Roman numeral or letter, as in (IV.6.1) or (A §3). Exercises

appear at the end of each chapter and are numbered consecutively, so, for example, exercise 4.23 is the 23rd exercise at the end of Chapter IV.

Just as in the first volume, numerous exercises have been included at the end of each chapter. The reader desiring to gain a real understanding of the subject is urged to attempt as many as possible. Some of these exercises are (special cases of) results which have appeared in the literature. A list of comments and citations for the exercises will be found at the end of the book. Exercises marked with a single asterisk are somewhat more difficult, and two asterisks signal an unsolved problem.

Standard Notation

Throughout this book, we use the symbols

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{F}_q,\ \text{and}\ \mathbb{Z}_p$$

to represent the integers, rational numbers, real numbers, complex numbers, field with q elements, and p-adic integers respectively. Further, if R is any ring, then R^* denotes the group of invertible elements of R; and if A is an abelian group, then $A[m]$ denotes the subgroup of A consisting of all elements with order dividing m. A more complete list of notation will be found at the end of the book.

CHAPTER I

Elliptic and Modular Functions

In most of our previous work in [AEC], the major theorems have been of the form *"Let E/K be an elliptic curve. Then E/K has such-and-such a property."* In this chapter we will change our perspective and consider the set of elliptic curves as a whole. We will take the collection of all (isomorphism classes of) elliptic curves and make it into an algebraic curve, a so-called modular curve. Then by studying functions and differential forms on this modular curve, we will be able to make deductions about elliptic curves. Further, the Fourier coefficients of these modular functions and modular forms turn out to be extremely interesting in their own right, especially from a number-theoretic viewpoint. We will be able to prove some of their properties in the last part of the chapter.

This chapter thus has two main themes, each of which provides a paradigm for major areas of current research in number theory and algebraic geometry. First, when studying a collection of algebraic varieties or algebraic structures, one can often match the objects being studied (up to isomorphism) with the points of some other algebraic variety, called a moduli space. Then one can use techniques from algebraic geometry to study the moduli space as a variety and thereby deduce facts about the original collection of objects. A subtheme of this first main theme is that the moduli space itself need not be a projective variety, so a first task is to find a "natural" way to complete the moduli space.

Our second theme centers around the properties of functions and differential forms on a moduli space. Using techniques from algebraic geometry and complex analysis, one studies the dimensions of these spaces of modular functions and forms and also gives explicit Laurent, Fourier, and product expansions. Next one uses the geometry of the objects to define linear operators (called Hecke operators) on the space of modular forms, and one shows that the Hecke operators satisfy certain relations. One then takes a modular form which is a eigenfunction for the Hecke operators and deduces that the Fourier coefficients of the modular form satisfy the same relations. Finally, one reinterprets all of these results by associating an L-series to a modular form and showing that the L-series has an Euler

product expansion and analytic continuation and that it satisfies a functional equation.

§1. The Modular Group

Recall [AEC VI.3.6] that a lattice $\Lambda \subseteq \mathbb{C}$ defines an elliptic curve $E/\mathbb{C}$ via the complex analytic map

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E_\Lambda(\mathbb{C}) : y^2 = 4x^3 - g_2 x - g_3 \\ z &\longmapsto \big(\wp(z;\Lambda), \wp'(z;\Lambda)\big). \end{aligned}$$

Here

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is the Weierstrass $\wp$-function relative to the lattice Λ. (See [AEC VI,§3].) Further, if Λ_1 and Λ_2 are two lattices, then we have

$$E_{\Lambda_1} \cong_{/\mathbb{C}} E_{\Lambda_2} \qquad \text{if and only if} \qquad \Lambda_1 \text{ and } \Lambda_2 \text{ are homothetic.}$$

(See [AEC VI.4.1.1]. Recall Λ_1 and Λ_2 are *homothetic* if there is a number $c \in \mathbb{C}^*$ such that $\Lambda_1 = c\Lambda_2$.)

Thus the set of elliptic curves over $\mathbb{C}$ is intimately related to the set of lattices in $\mathbb{C}$, which we denote by $\mathcal{L}$:

$$\mathcal{L} = \{\text{lattices in } \mathbb{C}\}.$$

We let $\mathbb{C}^*$ act on $\mathcal{L}$ by multiplication,

$$c\Lambda = \{c\omega : \omega \in \Lambda\}.$$

Then the above discussion may be summarized by saying that there is an injection

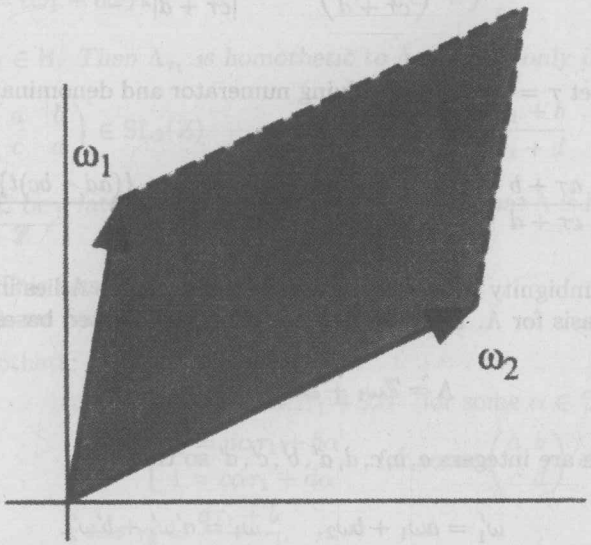
$$\mathcal{L}/\mathbb{C}^* \hookrightarrow \frac{\{\text{elliptic curves defined over } \mathbb{C}\}}{\mathbb{C}\text{-isomorphism}}.$$

According to the Uniformization Theorem for Elliptic Curves (stated but not proven in [AEC VI.5.1]), this map is a bijection. One of our goals in this chapter is to prove this fact (4.3). But first we will need to describe the set $\mathcal{L}/\mathbb{C}^*$ more precisely. We will put a complex structure on $\mathcal{L}/\mathbb{C}^*$, and ultimately we will show that $\mathcal{L}/\mathbb{C}^*$ is isomorphic to $\mathbb{C}$.

Let $\Lambda \in \mathcal{L}$. We can describe Λ by choosing a basis, say

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

Switching ω_1 and ω_2 if necessary, we always assume that the pair (ω_2, ω_1) gives a positive orientation. (That is, the angle from ω_2 to ω_1 is positive and between $0°$ and $180°$. See Figure 1.1.)



An Oriented Basis for the Lattice Λ

Figure 1.1

Since we only care about Λ up to homothety, we can normalize our basis by looking instead at

$$\frac{1}{\omega_2}\Lambda = \mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}.$$

Our choice of orientation implies that the imaginary part of ω_1/ω_2 satisfies

$$\mathrm{Im}(\omega_1/\omega_2) > 0,$$

which suggests looking at the upper half-plane

$$\mathsf{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

We have just shown that the natural map

$$\begin{aligned} \mathsf{H} &\longrightarrow \mathcal{L}/\mathbb{C}^*, \\ \tau &\longmapsto \Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z} \end{aligned}$$

is surjective. It is not, however, injective. When do two τ's give the same lattice? We start with an easy calculation.

Lemma 1.1. *Let $a, b, c, d \in \mathbb{R}$, $\tau \in \mathbb{C}$, $\tau \notin \mathbb{R}$. Then*

$$\operatorname{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{(ad - bc)\operatorname{Im}(\tau)}{|c\tau + d|^2}.$$

PROOF. Let $\tau = s + it$. Multiplying numerator and denominator by $c\bar{\tau} + d$, we find

$$\frac{a\tau + b}{c\tau + d} = \frac{\{ac|\tau|^2 + (ad + bc)s + bd\} + \{(ad - bc)t\}i}{|c\tau + d|^2}.$$

□

The ambiguity in associating a $\tau \in \mathbf{H}$ to a lattice Λ lies in choosing an oriented basis for Λ. Suppose that we take two oriented bases,

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'.$$

Then there are integers $a, b, c, d, a', b', c', d'$ so that

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2, & \omega_1 &= a'\omega_1' + b'\omega_2', \\ \omega_2' &= c\omega_1 + d\omega_2, & \omega_2 &= c'\omega_1' + d'\omega_2'. \end{aligned}$$

Substituting the left-hand expressions into the right-hand ones and using the fact that ω_1 and ω_2 are $\mathbb{R}$-linearly independent, we see that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Further, using Lemma 1.1 (with $\tau = \omega_1/\omega_2$) and the fact that our bases are oriented, we find that

$$0 < \operatorname{Im}\left(\frac{\omega_1'}{\omega_2'}\right) = \operatorname{Im}\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right) = \frac{(ad - bc)\operatorname{Im}(\omega_1/\omega_2)}{|c(\omega_1/\omega_2) + d|^2};$$

and so

$$ad - bc > 0.$$

In other words, the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is in the special linear group over $\mathbb{Z}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) = \left\{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \alpha\delta - \beta\gamma = 1\right\}.$$

This proves the first half of the following lemma.