A Number Theorist's Guide to the Riemann-Roch Theorem

Giancarlo Castellano

Abstract

The Riemann-Roch Theorem (RRT) is the name commonly given to either of two formally analogous results in the areas of complex analysis and algebraic geometry respectively, each of which yields a formula for the dimension of certain spaces of functions with "prescribed poles" on the geometric object at hand. Our main goal is to give an "adelic proof" of the algebraic RRT, following the treatments of Iwasawa [1] and Weil [2], and use it as motivation for the complex-analytic RRT, whose proof we shall only sketch. Finally, in the last section we shall present a well-known application of number-theoretic significance.

Introduction

Originally proved for compact Riemann surfaces and subsequently extended to projective curves over arbitrary fields, the Riemann-Roch Theorem (RRT) is a useful tool for describing spaces of functions with "prescribed poles" (see below) on a given curve. In these notes, we shall ultimately deal with both versions separately, but we wish to start with a simultaneous description of both the complex-analytic and the algebraic-geometric setting which highlights their similarity.

In either version of the RRT, the starting point is a curve X over a ground field F; more precisely, in what we will call the "complex-analytic" case $F = \mathbb{C}$ and X is taken to be a compact connected Riemann surface, while in the "algebraic-geometric" version X denotes a smooth projective curve over an arbitrary field F. Associated to X is field K of maps $f : X \to F \cup \{\infty\}$, which are assumed meromorphic in the complex-analytic case and rational in the algebraic case. Note that K strictly contains a copy of F, namely the subfield of constant functions. Finally, for each $P \in X$ we have a normalized discrete valuation[1] ord_P on K which is trivial on F; in either version of the theorem, it is given by

$$\mathrm{ord}_P f = \begin{cases} m & \text{if } f \text{ has a zero of order } m \text{ in } P, \\ -m & \text{if } f \text{ has a pole of order } m \text{ in } P, \\ 0 & \text{otherwise.} \end{cases}$$

[1] See Appendix A.

The aforementioned problem of finding functions with "prescribed poles", which was the original motivation for the complex-analytic Riemann-Roch theorem, can be stated as follows: given finitely many points $P_1, ..., P_k$ on the curve X, and non-negative integers $n_1, ..., n_k$, determine all $f \in K$ such that:

> *if f has a pole at $P \in X$, then $P = P_i$ for some $i \in \{1, ..., k\}$ and the pole has order not worse than n_i.*

This is customarily formalized and generalized by considering *divisors* on X, which we now define. Let us remark that the concept of divisors makes sense on more general algebraic varieties or complex manifolds, but we shall not need this in full generality and so we settle for an *ad hoc* definition for curves.

A *divisor* on X is defined as an element of the *free abelian group* $\mathcal{D}$ on X, i.e. of the direct sum $\oplus_{P \in X} \mathbb{Z}$. We shall denote a divisor D on X as a formal finite $\mathbb{Z}$-linear combination $\sum_{P \in X} n_P P$, where $n_P = 0$ for almost all[2] $P \in X$. Then the above problem reduces to a special case of the following

Problem. Let $D = \sum_{P \in X} n_P P = \sum_{i=1}^{k} n_i P_i$ be a divisor on X. By the properties of ord_P, the elements $f \in K$ such that $\mathrm{ord}_P(f) \geq -n_P$ for all $P \in X$, i.e. such that

$$\mathrm{ord}_P f \geq \begin{cases} -n_i & \text{if } P = P_i \\ 0 & \text{otherwise,} \end{cases}$$

form an F-linear space[3], which we denote $L(D)$. Is its dimension over F finite? If so, what is it?

As we shall see, either version of the Riemann-Roch Theorem yields a thorough and effective solution to the above problem. The algebraic case will be discussed in chapter 1: the key observation here is that, by the assumptions on X, the function field K behaves analogously to algebraic number fields from a valuation-theoretic viewpoint, and so we can associate to K an object called the *adèle ring* of K after the analogous construction from number theory. The statement and proof of the RRT will now follow naturally from the topological structure of the adèle ring.

In chapter 2, we shall move on to the statement of the complex RRT, and briefly discuss how it can be proved. Finally, in chapter 3 we shall discuss an application of the Riemann-Roch Theorem that shows how powerful the theorem is, namely the computation of the dimension of spaces of modular forms.

At the end of these notes three appendices can be found, on the topics of valuation theory, projective geometry and locally compact groups respectively; we have included them for the sake of completeness, and as a practical reservoir of information to look up definitions and results in. They are listed in decreasing order of how essential they are to an understanding of the main text: the contents of the first

[2]Throughout these notes, "almost all" means "all except at most finitely many".
[3]Here it is convenient to follow the convention $\mathrm{ord}_P(0) = \infty$ for all P.

appendix are heavily relied upon in many passages, while knowledge of projective geometry is only relevant to a few observations and remarks, and, with the exception of a handful of definitions, the contents of Appendix C serve merely as the "classical counterpart" of (and motivation for) some contents of Chapter 1.

Acknowledgements

These notes have evolved from handwritten notes that I prepared for a two-part talk on the adelic proof of the Riemann-Roch Theorem. I am grateful to professors Harald Grobner and Herwig Hauser for sharing my enthusiasm for the subject matter and encouraging me to give talks on the topic, as well as providing me with the occasion and the means to do so. Furthermore, I would like to thank my colleagues Sascha Biberhofer and Christopher Chiu for sharing their knowledge and their insights with me during the preparation of these notes.

1. The algebraic Riemann-Roch Theorem

In this section, we focus exclusively on the "algebraic case" of the problem discussed in the introduction, with the ultimate goal to derive the RRT from properties of the adèle ring of K. For the purposes of the proof we shall present, there is (surprisingly) no need to formally define smooth projective curves or their fields of rational functions; the only relevant fact for us, whose validity we justify in Appendix B, is the following:

Let X be a smooth projective curve over F and let $K = F(X)$ be the field of rational functions on X. Then:

(i) K is an algebraic function field in one variable *over F , i.e., there exists some $x \in K$ which is transcendental over F and such that $[K : F(x)] < \infty$, and*

(ii) the points of X are in bijection with the nontrivial places of K which are trivial on F, cf. Appendix A.

A few observations are in order:

(O1) We may assume, and shall do so for the rest of this chapter, that *F is algebraically closed in K*, see also Appendix A.

(O2) For any $x \in K^\times$, the formal sum $\operatorname{div}(x) := \sum_{P \in X} \operatorname{ord}_P(x)P$ is a divisor on X, the *principal divisor* associated to x.

(O3) The map $P \mapsto [F_P : F]$, where F_P is the residue class field of K at P, extends to a group homomorphism $\deg : \mathcal{D} \to \mathbb{Z}$. If $D = \operatorname{div}(x)$ is a principal divisor, then $\deg(D) = 0$ by the product formula for K, see also Appendix A.3.

(O4) If two divisors D, $D' \in D$ differ by a principal divisor, i.e. if $D' = D + \operatorname{div}(x)$ for some $x \in K^\times$, then $L(D)$ defined in the introduction is isomorphic to $L(D')$ via $f \mapsto f \cdot x$.

For the next definition, we draw from the strong formal analogy between algebraic number fields and algebraic function fields, which is explored in Appendix A. Historically, this analogy has been very fruitful in the development of number theory: for instance, Kurt Hensel introduced p-adic valuations on $\mathbb{Q}$ as an analogue of valuations of the form ord_P discussed in the introduction. Here, we shall do the opposite: in order to tackle a problem concerning function fields, we shall draw inspiration from number theory, more precisely from the notion of the *adèle ring* of an algebraic number field, see also Appendix C4.

Thus, let K be a function field[4] over a field F, and let $X = X_K$ denote the set of nontrivial places of K which are trivial on F. Then the *adèle ring* of K is defined as

$$\mathbb{A}_K := \{a = (a_P)_P \in \prod_{P \in X} K_P : \mathrm{ord}_P(a_P) \geq 0 \text{ for almost all } P \in X\},$$

where K_P denotes the completion of K at the place $P \in X$ and ord_P denotes the canonical discrete valuation on K_P, cf. Appendix A. We regard each K_P as equipped with the topology induced by ord_P; thus, we can consider subsets of $\mathbb{A}_K$ of the form

$$\prod_{Q \in S} U_Q \times \prod_{P \notin S} O_P,$$

where $S \subset X$ is finite, U_Q is an open subset of K_Q for each $Q \in S$ and $O_P := \{x \in K_P : \mathrm{ord}_P(x) \geq 0\} \subset K_P$. These sets form the basis for a topology on $\mathbb{A}_K$, which makes $\mathbb{A}_K$ into a topological ring (cf. Appendix C), and each K_P is isomorphic (as a topological field) to the quotient $\mathbb{A}_K/\mathfrak{m}_P$, where $\mathfrak{m}_P$ denotes the maximal ideal $\{a = (a_P) \in \mathbb{A}_K : a_P = 0\} \subset \mathbb{A}_K$. Finally, we note that, since

(i) $K \subset K_P$ for each P, and

(ii) for each $x \in K^\times$, $\mathrm{ord}_P(x) = 0$ for almost all $P \in X$,

the ring $\mathbb{A}_K$ contains the subfield $\{(x)_P = (x, x, x, ...) \in \prod K_P : x \in K\}$ which is clearly isomorphic to K. Thus, everything so far is completely analogous to the number-theoretic case and the same arguments go through.

The first notable discrepancy becomes apparent upon taking a closer look at the topology on $\mathbb{A}_K$. If K is an algebraic number field, then each K_P is a locally compact field, and thus $\mathbb{A}_K$ is a locally compact ring, see also Appendix C. This is also true if K is a function field over a *finite field* F, but does not hold in general. Nevertheless, if the notion of (local) compactness is suitably weakened then many results can be derived which are strikingly similar to well-known properties of compact topological spaces or locally compact groups as the case may be. Accordingly, the next section is devoted to developing the notion of *(local) linear compactness*, and our process of deriving the Riemann-Roch Theorem will resume in §2.

[4]We shall henceforth write "function field (over F)" instead of "algebraic function field in one variable (over F)" whenever no confusion can arise.

1.1. Linear compactness

Recall that a topological space X is *compact* if and only if

(C) for each family $\{F_\alpha\}_{\alpha\in A}$ of closed subsets of X with the finite intersection property[5], $\bigcap_{\alpha\in A} F_\alpha \neq \emptyset$.

The concept of linear compactness, which Solomon Lefschetz introduced in his 1942 book *Algebraic Topology* with "applications to homology" in mind, can be seen as a natural adaptation of (C) to vector spaces, and in fact, the contents of this section will show that "linearly compact spaces are to vector spaces as compact (Hausdorff) spaces are to topological spaces". Interestingly, this somewhat vague statement can be made precise (and proved!) in the context of category theory, cf. [5].

Keeping this analogy in mind, we now delve into a rigorous treatment of the theory of linearly compact spaces. For the entirety of this section, we fix a ground field F, endowed with the discrete topology. A Hausdorff topology on a vector space V over F will be called a *linear topology* if:

(i) the additive group of V is a topological group (cf. Appendix C),

(ii) the scalar multiplication $F \times V \to V$ is continuous, and

(iii) $0 \in V$ has a neighbourhood basis consisting of linear subspaces of V.

An F-vector space equipped with a linear topology is said to be *linearly topologized*.

EXAMPLE. (0) If V is any vector space over F, then the discrete topology on V is a linear topology on V.

(1) Let K be a function field over F, and $X = X_K$ be the set of nontrivial places of K which are trivial on F. Then it is a routine check of the definition that any place $P \in X$ is a linear topology on K (hint: a neighbourhood basis around 0 is given by the powers of $m(P)$ as defined in Appendix A). Similarly, each completion K_P, $P \in X$ is linearly topologized and so is the adèle ring of K defined above. $\diamond$

REMARK. (0) Let V be a linearly topologized F-vector space. Since translations by elements of V are homoeomorphisms, any neighbourhood (basis) around a point of V is given by translation of some neighbourhood (basis) around 0. It follows easily that a linear subspace of V which is also a neighbourhood of 0 is automatically open. Moreover, an open linear subspace U is automatically closed, since V is partitioned by translates of U.

All these facts are special cases of results on general (abelian) topological groups. The general theory also tells us that any discrete linear subspace of V (i.e., a linear subspace on which the subspace topology is discrete) is automatically closed in V. $\diamond$

Let W be a linearly topologized F-linear space. By an *affine subspace* of W we mean a subset V of the form $v + U$ where $U \subseteq W$ is a linear subspace and $v \in W$. An affine subspace $V \subseteq W$ is *linearly compact* if

[5] We say that $\{F_\alpha\}_{\alpha\in A}$ has the finite intersection property if $\bigcap_{\alpha\in S} F_\alpha \neq \emptyset$ for any finite subset $S \subset A$.

(LC) for each family $\{U_\alpha\}_{\alpha\in A}$ of closed[6] affine subspaces of V with the finite intersection property, $\bigcap_{\alpha\in A} U_\alpha \neq \emptyset$.

Obviously, by a *linearly compact (vector) space* over F we mean a linearly topologized vector space V over F which is linearly compact as an affine subspace of itself.

EXAMPLE. (0') Consider $V = F$ as a discrete F-linear space. Then the only affine subspaces of V are singletons and V itself, so V is obviously linearly compact. $\diamond$

In accordance with our earlier claim, most desirable consequences of compactness are preserved when passing to linear compactness, as shown by (a)-(f) below.

(a) An arbitrary product of linearly compact spaces is itself linearly compact in the product topology.

This is an analogue of a well-known theorem of Tychonoff on compact spaces, which can be proved in a way that only makes use of condition (C) above, see [4, p. 19]. The proof for the linearly compact case only requires minor modifications.

Let V be a linearly compact vector space over F. Then:

(b) Every closed affine subspace of V is linearly compact.

(c) If W is a linearly topologized F-vector space and $\varphi : V \to W$ is a continuous F-linear map, then the image of V under φ is again linearly compact.

(d) If U is a closed affine subspace of V, then U is discrete (i.e., the subspace topology on U is the discrete topology) if and only if U is finite-dimensional over F.

The proofs of (b) and (c) are straightforward and virtually identical to the standard proofs for the compact case. Moreover, sufficiency in (d) follows from choosing an F-linear isomorphism $U \cong F \times ... \times F$ (which is also a homoeomorphism since both spaces are discrete) and applying Ex.(0') and claim (a).

As for necessity, the claim is trivial if $U = \{0\}$, so we may assume $U \neq \{0\}$. Now fix a basis B for U, and for $u \in U$ write $u = \sum_{b\in B} u_b b$ where of course almost all u_b vanish. Then the sets $U_b = \{u \in U : u_b = 1\}$ form a family $\{U_b\}_{b\in B}$ of closed affine subspaces of U with the finite intersection property; by linear compactness, $\bigcap_{b\in B} U_b$ is non-empty, which is only possible if B is a finite set.

REMARK. (1) It is easy to check that, if V is linearly topologized and U is a closed linear subspace of V, then both the subspace topology on U and the quotient topology on V/U are linear topologies (the Hausdorff property follows from the fact that U is closed). By (b) and (c), if V is linearly compact then so are U and V/U. $\diamond$

Let V be a linearly topologized vector space over F. Then:

(e) If U is a linearly compact subspace of V, then U is closed.

[6] Each U_α is required to be closed in the subspace topology on V.

(f) Let $\{U_\alpha\}_{\alpha\in A}$ be a non-empty family of linearly compact subspaces of V. Then $\bigcap_{\alpha\in A} U_\alpha$ is linearly compact.

We observe that (f) follows immediately from (e) and (b), so we focus on (e). To prove the claim, pick $v \in V$ in the closure of U, and let $\mathcal{F}$ denote the family of neighbourhoods of v which are also affine subspaces of V. Then each $E \in \mathcal{F}$ is of the form $v + E'$, where E' is some linear subspace which is also a neighbourhood of 0. By Rmk.(0), E' is closed, so $E \in \mathcal{F}$ is as well closed.

We see that $E \cap U$ is non-empty for every $E \in \mathcal{F}$ by the assumption on v, and $\bigcap_{E\in\mathcal{F}}(E \cap U) \subseteq \bigcap_{E\in\mathcal{F}} E = \{v\}$. But $\{E \cap U\}_{E\in\mathcal{F}}$ is a family of non-empty closed affine subspaces of U with the finite intersection property, so linear compactness implies $\bigcap_{E\in\mathcal{F}}(E \cap U) = \{v\}$ and therefore $v \in U$.

Let V be a linearly topologized vector space over F, and let U_1, U_2 be open, linearly compact subspaces of V. Then:

(g) If $W \subseteq U_1 \cap U_2$ is an open, linearly compact subspace, then $\dim_F(U_i/W)$ is finite for $i = 1, 2$.

(g') The difference $\dim_F(U_1/W) - \dim_F(U_2/W)$ is independent of W; we denote it by $\lambda_V(U_1, U_2)$.

(h) If U is a closed linear subspace of V, then

$$\lambda_V(U_1, U_2) = \lambda_U(U_1 \cap U, U_2 \cap U) + \lambda_{V/U}\left(U_1/(U_1 \cap U), U_2/(U_2 \cap U)\right),$$

where each term makes sense by Rmk.(1).

In order to prove (g), note first that W is closed in U_i by (e), so U_i/W is linearly compact by Rmk.(1). But W is also open in U_i, so the quotient topology on U_i/W is discrete, and the claim follows from (d).

As for (g'), let $W_0 := U_1 \cap U_2$. This is obviously an open linear subspace of V and it is linearly compact by (f). Moreover, $\dim_F(U_i/W_0) = \dim_F(U_i/W) - \dim_F(W_0/W)$ for $i = 1, 2$, whence the claim follows immediately.

Finally, (h) follows from a simple computation that is left to the reader.

REMARK. (2) If K_1, K_2 are compact subsets of a locally compact group G, then the "relative measure" $\mu(K_1)/\mu(K_2)$, where μ is any Haar measure on G, is well-defined even though the Haar measure μ is itself not unique, cf. Appendix C1. The function λ_V defined above can be thought of as an analogue of this "relative measure". The formula in (h) mirrors the corresponding equality for Haar measures on subgroups and quotients, cf. Appendix C1. ◇

1.2. The adèle ring and divisors

We now have all the information necessary to describe the topology of the adèle ring of a function field. For this section, we fix a field F and a function field K over F,

and keep the notations $X = X_K$, K_P, ord_P, O_P, $\mathbb{A}_K$ from the beginning of Chapter 1. We further identify K with the corresponding subfield of $\mathbb{A}_K$.

Theorem 1. *With the above notations, the following hold.*

(i) For $P \in X$, O_P is linearly compact. More generally, every fractional ideal of O_P is linearly compact.

(ii) The F-linear subspace

$$O := \{a = (a_P)_P \in \mathbb{A}_K : \mathrm{ord}_P(a_P) \geq 0 \ \forall P \in X\} \subset \mathbb{A}_K$$

is an open, linearly compact neighbourhood of $0 \in \mathbb{A}_K$.

(iii) $K \subset \mathbb{A}_K$ is discrete, hence closed.

(iv) The quotient $\mathbb{A}_K/K$ is linearly compact.

Proof. (i) Let $m_P = \{x \in K_P : \mathrm{ord}_P(x) > 0\}$, and consider the F-linear isomorphism (and homoeomorphism) $O_P \cong O_P/m_P \times m_P/m_P^2 \times m_P^2/m_P^3 \times ....$ Each factor on the right-hand side is a copy of F_P, and is discrete since all powers of m_P are open in K_P. Since F_P is a finite-degree extension of F, the linear compactness of O_P follows from claims (d) and (a) of the previous section.

As for the last claim, it suffices to observe that a fractional ideal of O_P is either $\{0\}$, which is trivially linearly compact, or of the form $t^k O_P$ for some $k \in \mathbb{Z}$, where t is any element of K_P with $\mathrm{ord}_P(t) = 1$. But multiplication with t^k is continuous, so $t^k O_P$ is linearly compact by (c) of §1.

(ii) Clearly O is a linear subspace of $\mathbb{A}_K$. Further, O is open by the definition of the topology on $\mathbb{A}_K$. Finally, since $O = \prod_{P \in X} O_P$, the linear compactness of O follows from (i) together with claim (a) of the previous section.

(iii) It suffices to show that there exists a neighbourhood U of 0 in $\mathbb{A}_K$ such that $U \cap K = \{0\}$. Accordingly, fix a nonzero $x \in K$, and let S be the finite set of places $P \in X$ for which $\mathrm{ord}_P(x) < 0$. Then

$$U := \{a = (a_P)_P \in \mathbb{A}_K : \mathrm{ord}_P(a_P) \geq 0 \ \forall P \in X, \ \mathrm{ord}_P(a_P) > 0 \text{ for } P \in S\}$$

has the desired property. The last claim follows using Rmk.(0).

(iv) The claim follows from the fact that $\mathbb{A}_K = K + \widetilde{U}$, where $\widetilde{U}$ is a linearly compact neighbourhood of 0 defined similarly as U in the proof of (iii). For a proof of this, we refer the reader to [1], or [2] for the special case that F is finite. □

The main achievement of this section is the following reinterpretation of the spaces $L(D)$, $D \in \mathcal{D}$ defined in the introduction. For a divisor $D = \sum n_P P = \sum n_i P_i$ on X, let $M(D)$ be the set of adèles $a = (a_P)_P \in \mathbb{A}_K$ such that $\mathrm{ord}_P(a_P) \geq n_P$ for all P, i.e. such that

$$\mathrm{ord}_P(a_P) \geq \begin{cases} n_i & \text{if } P = P_i, \\ 0 & \text{otherwise.} \end{cases}$$

Then clearly $L(D) = K \cap M(-D)$ for any D.

Proposition 1. *Let K, X, $\mathbb{A}_K$ be as above, and $O = \prod O_P \subset \mathbb{A}_K$ as in Thm. 1.*

(i) $M(D)$ is an open, linearly compact O-module for any $D = \sum n_P P \in \mathcal{D}$.

(ii) If $M \subset \mathbb{A}_K$ is an open, linearly compact O-module, then $M = M(D)$ for some divisor D.

Proof. (i) Let $\mathfrak{i} = (\mathfrak{i}_P)_P$ be any element of $\mathbb{A}_K$ such that $\mathfrak{i}_P \neq 0$ for every $P \in X$ and $\mathrm{ord}_P(\mathfrak{i}_P) = n_P$ for all P. Then $\mathfrak{i}$ is invertible in $\mathbb{A}_K$, so multiplication by $\mathfrak{i}$ is a homoeomorphism. It follows that $M = \mathfrak{i}O$ is again open and linearly compact, since O is; moreover, M is obviously a principal O-module.

(ii) For $P \in X$, the projection $\pi_P : \mathbb{A}_K \to K_P$ is an open, continuous, F-linear surjective ring homomorphism. In particular, the image M_P of M under π_P is an open fractional ideal of O_P, and thus is of the form $M_P = t^{n_P} O_P$, where t is an element of K_P with $\mathrm{ord}_P(t) = 1$ and $n_P \in \mathbb{Z}$, cf. the proof of Thm. 1.(i).

Clearly $M = \prod_P M_P$; since M is open, it must possible to write M as a union of basic open sets in $\mathbb{A}_K$, so necessarily $M_P = O_P$, i.e. $n_P = 0$, for almost all P. Thus, $\sum n_P P$ is a divisor on X, and $M = M(D)$. □

Since obviously $M(D) \neq M(D')$ for distinct divisors D, D', the content of Proposition 1 is that the open linearly compact O-submodules of $\mathbb{A}_K$ are in bijection with the divisors on X.

Remark. (3) Let $M, M' \subset \mathbb{A}_K$ be open, linearly compact O-modules. We wish to compute $\lambda(M, M')$, where $\lambda = \lambda_{\mathbb{A}_K}$ is as in claim (g') of §1. By (g') and Prop. 1.(ii), it suffices to compute $\lambda\big(O, M(D)\big)$ for a divisor $D \in \mathcal{D}$.

We first consider the special case $D = 1 \cdot P$, where $P \in X$. In this case, $M(D) = m_P \times \prod_{Q \neq P} O_Q$, where $m_P = \{x \in K_P : \mathrm{ord}_P(x) > 0\} \subset O_P$. In particular, $M(D)$ is contained in O and indeed both are equal at each component except at P. Thus, $\lambda\big(O, M(D)\big) = \dim_F O_P/m_P = \dim_F F_P = [F_P : F]$, where F_P is the residue field at P. Accordingly, for arbitrary D we have $\lambda\big(O, M(D)\big) = \deg D$ as defined at the beginning of this chapter. ◇

We can now reap the first fruit of our adelic approach by answering the first part of the problem posed in the introduction, namely whether the F-dimension of the linear spaces $L(D)$ is finite. Since $M(D)$ is linearly compact for any divisor $D \in \mathcal{D}$, and $K \subset \mathbb{A}_K$ is discrete by Thm. 1.(iii), the intersection $L(D) = M(-D) \cap K$ is indeed a finite-dimensional F-vector space by claim (d) of §1.

1.3. Pairings and duality

Central to either version of the Riemann-Roch Theorem (see also Chapter 2) is an involution, i.e. a self-inverse bijection, of the group $\mathcal{D}$ of divisors on X. A divisor and its image under this involution may thus also be seen as "dual" to each other. In this section, we show that, in the algebraic version of the RRT, where divisors are identified with certain subspaces of the adèle ring as in §2, this duality of sorts arises naturally from the familiar concept of "dual spaces" from linear algebra.

When discussing dual spaces, we shall need some facts about so-called "pairings", which we now mention. For the rest of this section, the ground field F is fixed and is equipped with the discrete topology, as in §1.

In our terminology, a *pairing* of F-vector spaces V and W (to F) is simply an F-bilinear map $V \times W \to F$, $(v, w) \mapsto vw$, the prototypical example being of course (symmetric) bilinear forms $V \times V \to F$. For a subset $S \subseteq V$, the *annihilator* S' of S is defined as $S' := \{w \in S : sw = 0 \ \forall s \in S\} \subseteq W$, cf. the notion of the orthogonal complement. The annihilator of $T \subseteq W$ is defined similarly.

Lemma 1. *Let V and W be F-vector spaces with a pairing $V \times W \to F$, $(v, w) \mapsto vw$. If $V' = \{0\} \subset W$ and $W' = \{0\} \subset V$, then $\dim_F V$ is finite if and only if $\dim_F W$ is, in which case they are equal.*

Proof. Let $v_1, ..., v_n$ be linearly independent elements of V, and suppose for the sake of contradiction that $\dim_F W = m < n$. If $w_1, ..., w_m$ is a basis for W, then the $(n \times m)$-matrix $M = \left(v_i w_j\right)$ has nontrivial kernel. But if $(x_1, ..., x_n) \cdot M = 0$, then $x_1 v_1 + ... + x_n v_n \in W' = \{0\}$, a contradiction, so indeed $\dim_F W \geq n$. The claim now follows upon interchanging V and W. □

Recall that, for any F-vector space V, the F-linear maps $\chi : V \to F$ form an F-vector space, called the *dual space* of V and denoted V^*. The elements of V^* are called *(F-)linear functionals* on V, but we shall also call them *(field) characters* of V after the analogous concept for abelian groups, cf. Appendix C2.

Clearly $V \times V^* \to F$, $(v, \chi) \mapsto \chi(v)$ is a pairing of V and V^*, called the *dual pairing* of V and V^*. If $S \subseteq V$ is a linear subspace, then we quickly check that the annihilator $S' \subseteq V^*$ is isomorphic to $(V/S)^*$, and analogously if the roles of V and V^* are interchanged. In particular, this dual pairing satisfies the assumptions of the above proposition, so $\dim_F V^* = \dim_F V$ if the latter is finite.

Let V be a linearly topologized F-vector space, V^* its dual space.

(0) The annihilators $E' \subseteq V^*$, where E runs over the linearly compact subspaces of V, form the neighbourhood basis around $0 \in V^*$ for a linear topology on V^*.

From now on, V^* shall always be equipped with the topology from (0).

(1) The dual pairing of V and V^* is continuous. In particular, for a subset $T \subseteq V^*$, the annihilator $T' \subseteq V$ is always closed linear subspace of V, and for a subset $S \subseteq V$ we have $(S')' = \overline{\mathrm{span}(S)}$.

(2) The aforementioned linear isomorphism $S' \cong (V/S)^*$ is a homoeomorphism for any closed subspace $S \subseteq V$.

(3) If V is linearly compact, then V^* is discrete.

(3') Conversely, if V is discrete, then V^* is linearly compact.

The proof of (0) is a routine check of the definition given in §1 and is left to the reader. Claim (1) is also straight-forward, since F is equipped with the discrete topology, and (2) follows by comparing the subspace topology on $S' \subseteq V^*$ with the

topology on $(V/S)^*$ and keeping in mind that $E' \cap S' = (E+S)'$ for any linear subspace $E \subseteq V$.

The proof of (3) is again nearly trivial: by the definition of the topology on V^*, the subspace $V' = \{0\} \subset V^*$ is a neighbourhood of 0, so V^* is discrete.

As for (3'), we fix a basis B for V and identify V with the direct sum $\oplus_{b\in B} F$ both algebraically and topologically. The F-vector space $W := \prod_{b\in B} F$ is linearly compact by the results of §1, and is isomorphic (as an F-vector space) to V^* via $\tau : (w_b)_{b\in B} \mapsto (\chi : b \mapsto w_b)$, with inverse map $\chi \mapsto \big(\chi(b)\big)_{b\in B}$.

Furthermore, τ is continuous: for let E' be a fundamental neighbourhood of 0, i.e. the annihilator of some linearly compact $E \subseteq V$. Since V is discrete, E is finite-dimensional by claim (d) of §1, so E is contained in the span of some finite subset $B' \subset B$. Then $\tau^{-1}(E')$ is contained in $U = \{w = (w_b) \in W : w_b = 0\ \forall b \in B'\}$, which by Rmk.(0) is an open neighbourhood of $0 \in W$, proving continuity. By combining claims (b), (c) and (e) of §1, we finally obtain that τ is also a closed map, so τ is a homoeomorphism by elementary topology and V^* is linearly compact as claimed.

Remark. (3) The above claims (3) and (3') are similar to certain statements for group characters which are developed in the theory of Pontrjagin duality, cf. Appendix C2. One can also show that, if V is *locally linearly compact*, then so is V^*, and in fact we have the following stronger statement: if V, W are locally linearly compact F-vector spaces with a pairing $V \times W \to F$, $(v, w) \mapsto vw$, such that $v \mapsto (w \mapsto vw)$ is an isomorphism $V \xrightarrow{\sim} W^*$, then $w \mapsto (v \mapsto vw)$ is an isomorphism $W \xrightarrow{\sim} V^*$, and the given pairing is precisely the dual pairing of V and V^*. ◇

Let us now return to the adèle ring $\mathbb{A}_K$ of the function field K, viewed as an F-vector space. We shall fix a nonzero element $\chi : \mathbb{A}_K \to F$ of $\mathbb{A}_K^*$ which is *trivial on* K, i.e. $\chi(K) = 0$. Then we have a map $\psi : \mathbb{A}_K \to \mathbb{A}_K^*$ given by $a \mapsto \big(\chi_a : b \mapsto \chi(ab)\big)$. With some patience and ingenuity, it is possible to show that ψ is a linear isomorphism and a homoeomorphism; in other words, we may say that $\mathbb{A}_K$ is *self-dual*, again cf. Appendix C2. In particular, for each subspace $H \subset \mathbb{A}_K$, the annihilator H' can be seen as a subspace of $\mathbb{A}_K$ upon identifying a with $\psi(a) = \chi_a$, and if H is closed then $(H')' = H$ by claim (1) above.

Remark. (4) Consider $K \subset \mathbb{A}_K$ as an F-linear subspace, and consider $K' \subset \mathbb{A}_K$. Since $\chi(K) = 0$, we have $K \subset K'$ and $KK' \subset K'$, i.e., K' is a K-vector space. But K' is also discrete as the dual of the linearly compact group $\mathbb{A}_K/K$, see Thm. 1.(iv) and claims (2) and (3) above. Moreover, K'/K is linearly compact as a closed subspace of $\mathbb{A}_K/K$, and so K'/K is a finite-dimensional F-vector space by claim (d) of §1. But since $\dim_F K = \infty$, this is only possible if $K' = K$.

(4') Thus, if $\widehat{\chi}$ is another nonzero element of $\mathbb{A}_K^*$ which is trivial on K, then $\widehat{\chi} = \chi_a$ for some $a \in K' = K$. ◇

We conclude this section by addressing the issue of "duality" between divisors that we mentioned at the beginning of this section. Let $D \in \mathcal{D}$ be a divisor, and let

$M = M(D) \subset \mathbb{A}_K$. Then M is an an open, linearly compact O-module by Prop. 1, where O is as in Thm 1.(ii).

Now by the above claims (2) and (3'), the annihilator $M' \subset \mathbb{A}_K$ is linearly compact since it is isomorphic to the dual of the quotient $\mathbb{A}_K/M$, which is discrete since M is open. By a "dual" argument, M' is open since M is linearly compact. Finally, M' is again an O-module: if $o \in O$ and $n \in M'$, i.e. $\chi(Mn) = 0$, then $\chi\big(M(on)\big) = \chi\big((oM)n\big) = 0$ since M is an O-module, so $on \in M'$. Thus, by Prop. 1.(ii), $M' = M(\widetilde{D})$ for some divisor $\widetilde{D} \in \mathcal{D}$.

In particular (put $M = O$), there is a unique divisor $W \in \mathcal{D}$ with $M(-W) = O'$ (mind the sign change). W shall be called the *canonical divisor* associated to the field character χ. Note that $M(D)' = M(-W - D)$ for all divisors $D \in \mathcal{D}$.

1.4. Statement and proof

We finally use the knowledge we have gained in the last three sections to state and prove the algebraic RRT. We henceforth use the notation $l(D) := \dim_F L(D)$ for a divisor D on X; it was proved in §2 that $l(D)$ is finite for any D. Furthermore, we shall make free use of the observations (O1)-(O4) at the beginning of this chapter and the notations introduced there.

Theorem 2 (Riemann-Roch Theorem for smooth projective curves)**.** *Let X be a smooth projective curve over F, and let $K = F(X)$ be the field of rational functions on F. Then there exist a non-negative integer g and a divisor W on X such that, for any divisor $D \in \mathcal{D}$,*

$$l(D) = \deg D + 1 - g + l(W - D).$$

Proof. Fix a nonzero character $\chi : \mathbb{A}_K \to F$ which is trivial on K and let W be the canonical divisor associated to χ, see §3. The non-negative integer $g := l(W)$ is independent of χ: if $\widehat{\chi}$ is as in Rmk.(4') and $\widehat{W}$ is the corresponding canonical divisor, then W and $\widehat{W}$ differ by the principal divisor $\mathrm{div}(a)$, where a is also as in Rmk.(4'), thus $l(W) = l(\widehat{W})$ by (O4).

Now let D be an arbitrary divisor on X. Then $L(W - D) = M(D - W) \cap K$, so, by claim (2) of §3, Rmk.(4) and the discussion thereafter,

$$\begin{aligned} L(W - D) &\cong \Big(\mathbb{A}_K / \big(M(D - W) \cap K\big)'\Big)^* \\ &= \Big(\mathbb{A}_K / \big(M(D - W)' + K'\big)\Big)^* \\ &= \Big(\mathbb{A}_K / \big(M(-D) + K\big)\Big)^*. \end{aligned}$$

Analogously, $L(W)$ is isomorphic to the dual of $\mathbb{A}_K/(O + K)$. We set $M := M(-D)$.

Then, using Lemma 1 and claims (g), (g') and (h) from §1, we obtain

$$\begin{aligned} l(W-D)-g &= \dim_F L(W-D) - \dim_F L(W) \\ &= \dim_F \big(\mathbb{A}_K/(M+K)\big) - \dim_F \big(\mathbb{A}_K/(O+K)\big) \\ &= \lambda_{\mathbb{A}_K/K}\big(\mathbb{A}_K/K, (M+K)/K\big) - \lambda_{\mathbb{A}_K/K}\big(\mathbb{A}_K/K, (O+K)/K\big) \\ &= \lambda_{\mathbb{A}_K/K}\big((O+K)/K, (M+K)/K\big) \\ &= \lambda_{\mathbb{A}_K/K}\big(O/(O\cap K), M/(M\cap K)\big) \\ &= \lambda_{\mathbb{A}_K}(O,M) - \lambda_K(O\cap K, M\cap K). \end{aligned}$$

By Rmk.(3), the minuend is $\deg(-D) = -\deg D$. As for the subtrahend, this is $\dim_F(O\cap K) - \dim_F(M\cap K) = 1 - \dim_F(M\cap K)$ since (O1) implies $O\cap K = F$, cf. also Appendix A. Thus, the proof is complete. □

REMARK. (5) If the constant field F of K is finite, then $\mathbb{A}_K$ is a locally compact ring and so we can prove the Riemann-Roch theorem using a Haar measure μ on $\mathbb{A}_K$ instead of the function $\lambda_{\mathbb{A}_K}$. This is the approach followed in Weil's book [2]. As a matter of fact, Weil's formulation of the Riemann-Roch Theorem is stronger, being a statement on "coherent systems of lattices" belonging to finite-dimensional vector spaces E over K, and the usual Riemann-Roch Theorem is a reinterpretation of the special case $E = K$.

(5') Since $\mathbb{A}_K$ is also locally compact if K is an algebraic number field, one may wonder to what extent the Riemann-Roch Theorem can be rephrased or altered so as to hold over algebraic number fields as well. Those who wish to put an end to their wondering are referred to [6, p. 264], but we take the liberty of spoiling the surprise: there does exist a version of the Riemann-Roch Theorem which also holds over number fields, it is *stronger* than the original result and it relies on the definition of the Fourier transform on $\mathbb{A}_K$; indeed may be regarded as a multiplicative analogue of the (adelic) Poisson summation formula. ◇

The nonnegative integer g in the statement of the theorem is called the *(arithmetic) genus* of X and only depends on X (and F). It is *invariant* in the sense that, if C is a curve which is *birationally equivalent* to X, then their genera coincide.

For an arbitrary smooth projective curve X over an algebraically closed field F, it is known, see [3], that there exists a plane curve C which is birationally equivalent to X and all whose singular points are *ordinary* multiple points. If C is the vanishing set of $h(x,y) \in F[x,y]$, then the common genus of X and C equals

$$\frac{(n-1)(n-2)}{2} - \sum_{P\in X \text{ multiple point}} \frac{r_P(r_P-1)}{2},$$

where n is the degree of a h and r_P is the multiplicity of P, cf. also Appendix B. In particular, any conic (= smooth quadratic plane curve) over F has genus 0, and any smooth cubic curve over F has genus 1.

To conclude the chapter, we now present a surprisingly straight-forward application of the Riemann-Roch Theorem. First, we shall need a corollary.

Corollary 1. *If D is a divisor with $\deg D > 2g-2$, then $l(D) = \deg D + 1 - g$.*

Proof. Plugging in $D = W$ in the statement of the Riemann-Roch Theorem, we obtain $\deg W = 2g-2$, so we have to prove that, if $\deg(W-D) < 0$, then $l(W-D) = 0$. But this is clear: if some $f \in K^\times$ were in $L(W-D)$, then we would find that $\operatorname{div}(f) > D-W$ component-wise and hence $0 = \deg(\operatorname{div}(f)) > \deg(D-W) > 0$. □

Now consider a smooth projective curve X over F, and suppose that the genus of X is 1. Such a curve is called an *elliptic curve* over F.

By the corollary, for any divisor D with $\deg D > 0$ we have $l(D) = \deg D$. In particular, for any point $P \in X$, we have $l(n \cdot P) = n$ if $n \geq 1$. (As for $n = 0$, we have $l(D) = l(0) = 1$ since F is algebraically closed in $K = F(X)$ by assumption.)

Accordingly, $L(1 \cdot P) = F$. Next, we obtain $l(2 \cdot P) = \deg(2 \cdot P) = 2$, so $L(2 \cdot P)$ can be identified with $F \oplus Fx$ for some x; necessarily $\operatorname{ord}_P(x) = -2$, for otherwise $x \in L(1 \cdot P) = F$.

Analogously, $L(3 \cdot P) = F \oplus Fx \oplus Fy$ where $\operatorname{ord}_P(y) = -3$. Then by comparing orders we find: $L(4 \cdot P) = \operatorname{span}(1, x, y, x^2)$ and $L(5 \cdot P) = \operatorname{span}(1, x, y, x^2, xy)$.

For $n = 6$ things get interesting, since all *seven* functions $1, x, y, x^2, xy, x^3, y^2 \in K$ have a pole of order ≤ 6 at P, but $l(D) = 6$. Thus, we obtain a linear dependence relation between these seven monomials, i.e. a cubic equation in two variables. An equation of this form is called a *Weierstraß equation* and it describes the curve X in the sense that X is precisely the set of points (x, y) whose coordinates satisfy the equation. If the characteristic of F is neither 2 nor 3, then we can make a change of coordinates and rewrite this equation in the form

$$y^2 = 4x^3 - Ax - B,$$

where the cubic polynomial on the right-hand side has no multiple roots, or equivalently its *discriminant* $A^3 - 27B^2$ is nonzero.

2. The complex Riemann-Roch Theorem

In this chapter, we briefly discuss the complex version of the Riemann-Roch Theorem. Accordingly, we consider a compact connected Riemann surface X and the field $K = \mathcal{M}(X)$ of meromorphic functions on X. We quickly review these concepts before formulating the statement of the complex RRT.

Recall that an *n-dimensional complex manifold* is a (topological) manifold with an atlas of charts to the open unit disk in $\mathbb{C}^n$. A 1-dimensional complex manifold is obviously a 2-dimensional real manifold and is hence called a *Riemann surface*.

Example. (1) Any smooth irreducible projective curve over $\mathbb{C}$ can be given the

structure of a compact Riemann surface. The prototypical example of this is 1-dimensional complex projective space $\mathbb{P}^1(\mathbb{C})$, i.e. the Riemann sphere. $\diamond$

Just as there is a natural notion of smooth maps between smooth real manifolds, there is also an obvious definition of holomorphic and even meromorphic maps on complex manifolds. The meromorphic maps $X \to \mathbb{C}$ on a connected Riemann surface X form a field, which we denote by $K = \mathcal{M}(X)$.

REMARK. (1) With the above definitions, meromorphic maps $X \to \mathbb{C}$ are the same as holomorphic maps from X to the Riemann sphere $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.

(2) If X is a compact connected Riemann surface, then $\mathcal{M}(X)$ is actually an algebraic function field in one variable over $\mathbb{C}$, see e.g. [8, p. 36]. $\diamond$

Let $\mathcal{D}$ be the free abelian group on X. As we did in the algebraic version, we can associate to each $f \in K^\times$ a divisor $\operatorname{div}(f) = \sum \operatorname{ord}_P(f)P$. Recall that $\operatorname{ord}_P(f) \geq 0$ if and only if f is holomorphic at P, so, by a form of Liouville's Theorem, a function f with $\operatorname{ord}_P(f) = 0$ for all P is necessarily a constant $f \in \mathbb{C}$, $f \neq 0$.

Futhermore, for a divisor $D = \sum n_P P \in \mathcal{D}$, we set[7] $\deg D = \sum n_P$. Then, by compactness of X, it must hold that $\deg\big(\operatorname{div}(f)\big) = 0$ for any $f \in K^\times$.

Finally, let us remark that $L(D)$, see the introduction, is the set $\{f \in K : f = 0$ or $\operatorname{div}(f) \geq -D\}$, where by $\geq$ we mean that the inequality holds at every P. We again denote $l(D) := \dim_{\mathbb{C}} L(D)$.

The statement of the complex Riemann-Roch Theorem is as follows:

Theorem 3. *Let X, K and $\mathcal{D}$ as above. Then there exist a non-negative integer g and a divisor $W \in \mathcal{D}$ on X such that, for all divisors $D \in \mathcal{D}$,*

$$l(D) = \deg D + 1 - g + l(W - D).$$

As was the case for the algebraic RRT, the *genus* g is an intrinsic invariant of the Riemann surface X. It has the following topological interpretation: as a real manifold, the compact connected Riemann surface X is homoeomorphic to a sphere with a finite number of "handles", and this number is precisely g. In particular, a compact connected Riemann surface of genus 0 is homoeomorphic to a (real) sphere, the obvious example being $\mathbb{P}^1(\mathbb{C})$, cf. Rmk.(1). Another interesting case is $g = 1$, where X is homoeomorphic to a torus.

It is sensible to spend a few words on the canonical divisor W. In the complex-analytic case, canonical divisors are obtained from *meromorphic 1-forms* on X, which locally around each point $P \in X$ are given by $f\,dz$ for some meromorphic function $f = f_P$ defined locally around P and some local coordinate $z = z_P$. For a nonzero meromorphic 1-form ω on X, the formal sum $\operatorname{div}(\omega) := \operatorname{ord}_P(f_P)P$ is a divisor on X, the *canonical divisor* associated to ω. But the space Ω of meromorphic

[7] Thus, $\deg P = 1$ for any point P. This is, in a way, consistent with definition of deg from Chapter 1 since $F = \mathbb{C}$ is algebraically closed.

1-forms on X is a one-dimensional K-vector space, because one can show that if $\omega, \omega' \in \Omega$ are nonzero, then there exists a nonzero meromorphic function f on X such that $f\omega = \omega'$. Since $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$, canonical divisors are well-defined up to a principal divisor, again cf. Chapter 1.

REMARK. (3) Let ω be a nonzero meromorphic 1-form on X, and let $W = \mathrm{div}(\omega)$ the corresponding canonical divisor. Then $f \mapsto f\omega$ is a complex-linear isomorphism of $L(W - D)$ onto the space $I(D) := \{\omega \in \Omega : \omega = 0 \text{ or } \mathrm{div}(\omega) \geq D\}$, where again $\geq$ means that the inequality holds at each place P. In particular, the space of *holomorphic* 1-forms on X has dimension $\dim_{\mathbb{C}} I(0) = l(W) = g$. $\diamond$

Review of proofs. There exist several different proofs of the complex Riemann-Roch Theorem. A direct proof is possible, see e.g. [9]. On the other hand, one of the most conceptual proofs relies on reinterpreting the various quantities that appear in the formula as dimensions of cohomology groups and then applying Serre's duality theorem, see e.g. [8].

It is also possible to reduce the complex-analytic RRT to the algebraic version. First, one has to embed X into some projective space $\mathbb{P}^N(\mathbb{C})$ via a so-called "very ample line bundle". The usual criterion for a line bundle to be very ample follows from (some version of) the Riemann-Roch Theorem itself, but it is also possible to bypass this by applying the theory of elliptic PDEs, see [10]. Next, *Chow's Theorem* shows that the image of X in $\mathbb{P}^N(\mathbb{C})$ is algebraic, i.e. a vanishing set of polynomials; this result can in turn be proved in a simple way by applying the *Remmert-Stein Theorem*. Then K and g reprise their exact roles from Chapter 1. $\square$

We conclude this chapter by giving a glimpse into the theory of elliptic functions. Recall that a *lattice* Λ in the complex plane $\mathbb{C}$ is a discrete subgroup of rank 2; in other words, $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent. The quotient $X = \mathbb{C}/\Lambda$ can be equipped with the structure of a (1-dimensional) complex manifold. If we imagine this quotient as a fundamental parallelogram $\{a\omega_1 + b\omega_2 : a, b \in \mathbb{R}, 0 \leq a, b < 1\}$ where parallel sides have been identified with each other, then it is clear that, topologically, $\mathbb{C}/\Lambda$ is a torus and so its genus if 1. Following the above sketch of proof, together with the discussion at the end of Chapter 1, we find functions $x, y \in K = \mathcal{M}(X)$ such that X is given by the equation $y^2 = 4x^3 - Ax - B$. Indeed, we can take

$$
\begin{aligned}
A &= 60G_4(\Lambda) := 60 \sum_{0 \neq l \in \Lambda} \frac{1}{l^4}, \\
B &= 140G_6(\Lambda) := 140 \sum_{0 \neq l \in \Lambda} \frac{1}{l^6}, \\
x &= \wp : z \mapsto \frac{1}{z^2} + \sum_{0 \neq l \in \Lambda} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right), \\
y &= \wp' : z \mapsto -2 \sum_{l \in \Lambda} \frac{1}{(z-l)^3}.
\end{aligned}
$$

It is well-known that any meromorphic function on X, i.e. any meromorphic function on $\mathbb{C}$ which is periodic with respect to Λ, is a rational function in $\wp$ and $\wp'$. But the equation $(\wp')^2 = 4\wp^3 - A\wp - B$ shows that $\wp$ and $\wp'$ are algebraically dependent over $\mathbb{C}$, and so $K = \mathcal{M}(X)$ is indeed an algebraic function field in one variable over $\mathbb{C}$, in accordance with Rmk.(2).

3. Modular forms

In this final chapter, we briefly review some aspects of the theory of modular forms and sketch how the Riemann-Roch Theorem can be used to compute the dimensions of spaces of modular forms.

3.1. Modular groups

Recall that a *modular group* is a subgroup of $SL_2(\mathbb{Z})$ of finite index. In particular, $SL_2(\mathbb{Z})$ itself is called the *full modular group*. The key observation for us is that any modular group Γ acts on $\mathbb{C} \cup \{\infty\}$ as follows: if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $z \in \mathbb{C}$, then

$$\gamma \cdot z := \frac{az + b}{cz + d} \in \mathbb{C} \cup \{\infty\}.$$

Clearly $\gamma \cdot z \in \mathbb{R} \cup \{\infty\}$ if and only if $z \in \mathbb{R} \cup \{\infty\}$. If this is not the case then an easy computation shows that $\Im(\gamma \cdot z)\Im(z) > 0$, where $\Im(w) := \frac{w - \bar{w}}{2i}$ denotes the imaginary part of $w \in \mathbb{C}$. Therefore, we may restrict the above action to the *upper half-plane* $\mathbb{H} := \{z \in \mathbb{C} : \Im(z) > 0\}$.

Remark. (1) A point $x \in \mathbb{R} \cup \{\infty\}$ is called a *parabolic point*, or a *cusp*, of Γ if there exists some $\gamma \in \Gamma$ such that $\gamma \cdot x = x$ and $\mathrm{tr}(\gamma)^2 = 4\det(\gamma)$, where $\mathrm{tr}(\gamma)$ and $\det(\gamma)$ denote the trace and the determinant of γ respectively.

If, for instance, $\Gamma = \Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : N|c\}$ for some $N \in \mathbb{Z}$, then $x = \infty$ is always a cusp of Γ since $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ satisfies (i) and (ii).

(2) A point $z \in \mathbb{H}$ is called an *elliptic point* of Γ if there exists some $\gamma \in \Gamma$ such that $\gamma \cdot z = z$ and $\mathrm{tr}(\gamma)^2 < 4\det(\gamma)$.

Consider for instance the full modular group $\Gamma = SL_2(\mathbb{Z})$. Then $z = i$ and $z = \rho = e^{2\pi i/3}$ are elliptic points of Γ: take $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ respectively.

(3) For any modular group Γ and any $z \in \mathbb{H}$, we define the *order* of z as the index of $Z(\Gamma)$ in Γ_z, where $Z(\Gamma) = \Gamma \cap \{\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ is the center of Γ and Γ_z is the stabilizer of z. It can be shown that this index is finite, and that it is > 1 if and only if z is an elliptic point of Γ.

(3') Let $\Gamma = SL_2(\mathbb{Z})$. Then it is easy to verify that i and ρ have order 2 and 3 respectively, cf. Rmk.(2). ◇

It is a standard fact that the orbit space $Y_\Gamma = \Gamma \setminus \mathbb{H}$ can be given the structure of a Hausdorff topological space. This space is not compact in general, but it can be *compactified* by adding finitely many points. More precisely, for a fixed Γ we denote

by $\mathbb{H}^*$ the union of $\mathbb{H}$ with the *cusps* of Γ, see Rmk.(1) for the definition, and then check that $X_\Gamma := \Gamma \setminus \mathbb{H}^*$ is the disjoint union of Y_Γ with a finite (!) set of orbits coming from the cusps of Γ, which are themselves called the *(inequivalent) cusps* of X_Γ. Again, X_Γ has the structure of a Hausdorff space, and indeed *it can be equipped with the structure of a compact (*1*-dimensional) complex manifold.*

Let $K = \mathcal{M}(X_\Gamma)$ be the field of meromorphic functions on X_Γ, as in Chapter 2, and let π_Γ denote the canonical projection of $\mathbb{H}$ onto $\Gamma \setminus \mathbb{H} \subseteq X_\Gamma$. For $\varphi \in K$, the composition $f = \varphi \circ \pi_\Gamma$ is a meromorphic function on $\mathbb{H}$, and the fact that φ is meromorphic at the cusps translates into a condition on the behaviour of $f(z)$ as $z \in \mathbb{H}$ approaches a cusp $x \in \mathbb{R} \cup \{\infty\}$ of Γ, which is also phrased as f being "meromorphic at the cusp x". We illustrate this in a special but representative case.

For this paragraph, consider the full modular group $\Gamma = SL_2(\mathbb{Z})$ and the cusp $x = \infty$ of Γ, cf. Rmk.(1). Since $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and $f(\gamma \cdot z) = f(z+1)$, we infer that $f(z+1) = f(z)$ for all $z \in \mathbb{H}$. As a real periodic function, f has a Fourier series expansion $f(z) = \sum_{n \in \mathbb{Z}} (e^{2\pi i z})^n$, and the map $\widetilde{f} : q = e^{2\pi i z} \mapsto f(z)$ is a well-defined meromorphic function on the punctured open unit disk $\{q : 0 < |q| < 1\}$. Then f being meromorphic at x amounts to $\widetilde{f}$ having a meromorphic continuation to $q = 0$. (Analogously, f is called holomorphic at the cusp x if $\widetilde{f}$ extends holomorphically to $q = 0$, and is said to vanish at x if $\widetilde{f}(0) = 0$.)

In summary, a meromorphic function on X_Γ induces a meromorphic function f on $\mathbb{H}$ which satisfies $f(\gamma \cdot z) = z$ for all γ and all z and which is "meromorphic at all cusps of Γ". Such a function will be called a *modular function of weight* 0 for Γ. Conversely, it is not hard to show that, if f is a modular function of weight 0 for Γ, then there exists some $\varphi \in \mathcal{M}(X_\Gamma)$ such that $f = \varphi \circ \pi_\Gamma$.

3.2. Modular forms and Riemann-Roch

Let Γ be a modular group as in §1, k be an integer and f be a meromorphic function on $\mathbb{H}$ which is also meromorphic at each cusp of Γ, again see §1. Then f is called a *modular function of weight* k for Γ if

$$f(\gamma \cdot z) = (cz + d)^k f(z) \qquad \text{for all } z \in \mathbb{H}, \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma.$$

Example. (1) Let $z \in \mathbb{H}$, and let $\Lambda = \mathbb{Z} + z\mathbb{Z}$ denote the lattice spanned by 1 and z in $\mathbb{C}$. For $k \in 2\mathbb{Z}$, $k \geq 4$ we define

$$G_k(z) := G_k(\Lambda) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m+nz)^k},$$

cf. Chapter 2. If $\omega_1, \omega_2 \in \mathbb{C}$ are another $\mathbb{Z}$-basis for Λ, i.e. $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, then there exists some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \subset SL_2(\mathbb{C})$ such that $\left(\begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix}\right) = \gamma \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$. But then $G_k(\Lambda) = \omega_2^{-k} G_k(\mathbb{Z} + \tau\mathbb{Z})$, where $\tau = \frac{\omega_1}{\omega_2} = \frac{az+b}{cz+d} = \gamma \cdot z$. In other words,

$$G_k(\gamma \cdot z) = (cz + d)^k G_k(z) \qquad \text{for all } z \in \mathbb{H}, \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma,$$

i.e., G_k is a modular function of weight k for $\Gamma = SL_2(\mathbb{Z})$. $\diamond$

REMARK. (4) If f and g are modular functions of weight k and l respectively, then fg is a modular function of weight $k+l$. $\diamond$

The modular functions of weight k form a complex vector space, which we denote $\mathscr{A}_k(\Gamma)$. We further write

$$M_k(\Gamma) := \{f \in \mathscr{A}_k(\Gamma) : f \text{ is holomorphic on } \mathbb{H} \text{ and at each cusp of } \Gamma\},$$
$$S_k(\Gamma) := \{f \in M_k(\Gamma) : f \text{ vanishes at each cusp of } \Gamma\}$$

and call the elements of M_k and S_k *modular forms* and *cusp forms* respectively.

EXAMPLE. (2) The *Eisenstein series* G_k for $k \in 2\mathbb{Z}$, $k \geq 4$ from Ex.(1) are actually modular forms of weight k for $\Gamma = SL_2(\mathbb{Z})$, and hence for every modular group $\Gamma \subset SL_2(\mathbb{Z})$. In particular, $M_k(\Gamma)$ is nonzero for $k \in 2\mathbb{Z}$, $k \geq 4$.

(3) The *modular discriminant* $\Delta : z \mapsto \big(60G_4(z)\big)^3 - \big(140G_6(z)\big)^2$ is a modular form of weight 12 for the full modular group. This form is holomorphic on $\mathbb{H}$ and a direct computation using $G_k(\infty) = 2\zeta(k)$ shows that Δ vanishes at the cusp ∞.

(3') The *j-invariant* $z \mapsto 12^3 \frac{\big(60G_4(z)\big)^3}{\Delta(z)}$ is a modular function of weight 0 for the full modular group. It is holomorphic on all $\mathbb{H}$ but it has a pole at ∞, so it is not a modular form. $\diamond$

Fix a modular group Γ and an even integer $k \geq 4$. In the next few paragraphs, we sketch how one can compute the dimensions of $M_k(\Gamma)$ and $S_k(\Gamma)$ over $\mathbb{C}$ using the Riemann-Roch Theorem.

One way to do this is to first associate to each nonzero $f \in M_k(\Gamma)$ a *divisor with rational coefficients* $\mathrm{div}(f_0)$, i.e. an element $\sum_{P\in\Gamma} \nu_P(f)P$ of the free $\mathbb{Q}$-vector space $\oplus_{P\in X_\Gamma}\mathbb{Q}$. The precise definition of the rational number $\nu_P(f)$ depends on whether P is a cusp, an elliptic point or neither, cf. §1, and becomes natural once one identifies the elements of $\mathscr{A}_k(\Gamma)$ with *differentials of degree* $m = \frac{k}{2}$ *on* X_Γ, see [12]. The information we shall need on ν_P is that $f \in M_k(\Gamma)$ if and only if $\nu_P(f) \geq 0$ for all P, and that f vanishes at a cusp P if and only if $\nu_P(f) \geq 1$.

Let D denote the divisor $\lfloor \mathrm{div}(f_0) \rfloor := \lfloor \nu_P(f_0) \rfloor P$, where $\lfloor \cdot \rfloor$ is the floor function. Then D is a divisor on X_Γ in the usual sense. We claim that $M_k(\Gamma) \cong L(D)$.

First, we observe that, by Ex.(2), $M_k(\Gamma)$ contains a nonzero element f_0, and by Rmk.(4), $f \mapsto f/f_0$ is an isomorphism of $\mathscr{A}_k(\Gamma)$ with $\mathscr{A}_0(\Gamma)$, which in turn is isomorphic to $K = \mathcal{M}(X_\Gamma)$ by §1. Next we check that the elements of $M_k(\Gamma)$ correspond precisely to the maps $f \in K$ such that either $f = 0$ or $\mathrm{div}(f) \geq -\mathrm{div}(f_0)$ component-wise, and then essentially deduce the claim from the definition of the floor function. Similarly, one proves that $S_k(\Gamma)$ is isomorphic to $L(D - P_1 - ... - P_t)$ where $P_1, ..., P_t$ are the inequivalent cusps of Γ, see §1.

In order to apply the Riemann-Roch theorem, we need to determine the genus of X_Γ. This is done by applying the *Riemann-Hurwitz formula* to the *branched covering*

$X_\Gamma \mapsto X_{\Gamma(1)}$, where $\Gamma(1) = SL_2(\mathbb{Z})$. Without digressing too far, let us simply remark that the Riemann-Hurwitz formula relates the genus of X_Γ to the genus of $X_{\Gamma(1)}$, which is known to be 0, and involves computing how many points of X_Γ are mapped to cusps or elliptic points of $X_{\Gamma(1)}$. The formula yields

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2},$$

where: μ is the index of $\Gamma/Z(\Gamma)$ in $PSL_2(\mathbb{Z})$, cf. Rmk.(2); ν_2 and ν_3 are the numbers of (inequivalent) elliptic points of Γ of order 2 and 3, respectively[8]; and ν_∞ is the number of (inequivalent) cusps of Γ, cf. Rmk.(1), (2) and (3).

REMARK. (5) Not unlike the Riemann-Roch theorem, the Riemann-Hurwitz formula can be proved both for a smooth projective curve X over an algebraically closed field F (the branched covering being $X \to \mathbb{P}^1(F)$) and for branched coverings of compact Riemann surfaces. The algebraic version can be derived from the Riemann-Roch theorem itself, see [3, Problem 8.36], while the complex version can be proved directly by triangulating both surfaces and keeping in mind that the *Euler characteristic* χ of a compact Riemann surface is related to its genus g via $\chi = 2 - 2g$. $\diamond$

The Riemann-Roch theorem now yields:

$$\dim S_k(\Gamma) = (k-1)(g-1) + \left(\frac{k}{2} - 1\right) t + \frac{k}{2} \sum_{i=1}^{r} \left(1 - \frac{1}{e_i}\right),$$

$$\dim M_k(\Gamma) = \dim S_k(\Gamma) + t,$$

where: $t = \nu_\infty$ is the number of (inequivalent) cusps of X_Γ; $r = \nu_2 + \nu_3$ is the number of (inequivalent) elliptic points of Γ; e_i denotes the order of the i-th elliptic point, cf. Rmk.(2)-(3) from §1. A more explicit formula can be obtained if $\Gamma = \Gamma_0(N) := \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : N|c\}$ for some $N \in \mathbb{Z}$, in which case the quantities μ, ν_2, ν_3 and ν_∞ depend solely on N and can be explicitly computed, see [13], yielding

$$\dim S_k(X_\Gamma) = \frac{k-1}{12} N \prod_{p|N} \left(1 + \frac{1}{p}\right) - \frac{1}{2}\nu_\infty(N) + \left(1 + \frac{k}{4} + \left\lfloor \frac{k}{4} \right\rfloor\right) \nu_2(N) + \left(1 + \frac{k}{3} + \left\lfloor \frac{k}{3} \right\rfloor\right) \nu_3(N).$$

REMARK. (6) The case $k = 2$ is best treated separately but is also extraordinarily interesting in itself. It follows from a fact that was mentioned earlier that the elements f of $\mathscr{A}_2(\Gamma)$ can be identified with differentials on X_Γ of degree 1, i.e. with meromorphic 1-forms ω_f on X_Γ, and that in particular $S_2(\Gamma)$ is isomorphic to the space of holomorphic 1-forms on X_Γ. Thus, $\dim S_2(\Gamma)$ equals the genus g of X_Γ by Rmk.(3) of Chapter 2.

[8] It is well-known, and we shall tacitly use it in the next computations, that X_Γ only has finitely many elliptic points, and that their orders are either 2 or 3.

Using the formula for the genus of Γ given above, together with the formulas for $\nu_2(N)$, $\nu_3(N)$, $\nu_\infty(N)$ found in the references, one can directly compute that $\dim S_2\big(\Gamma_0(N)\big) = 0$ for $N < 11$, and in particular for $N = 2$. This fact was used to show that Fermat's Last Theorem follows from the *modularity theorem for semistable elliptic curves*, which was established by Andrew Wiles and Roger Taylor in 1995. For suppose that there exists a nontrivial solution $(a, b, c) \in \mathbb{Z}^3$ to the equation $a^p + b^p = c^p$ for some prime $p \geq 5$. Then $y^2 = x(x - a^p)(x + b^p)$ is a smooth cubic plane curve over $\mathbb{Q}$, hence an elliptic curve, see Chapter 1, and it can be checked to be semistable, so by the modularity theorem it must correspond to a nonzero element f of $S_2\big(\Gamma_0(N)\big)$ for some even N. By a theorem of Ribet, formerly known as the "ε conjecture", f must already lie in $S_2\big(\Gamma_0(2)\big)$, the sought-after contradiction. $\diamond$

Appendix A. Valuation theory

Here are gathered some of the most basic definitions and results of valuation theory which are used in the main text.

A.1. Two examples

We begin with two examples, discussed parallelly. Let A denote either the ring $\mathbb{Z}$ of (so-called *rational*) integers or a polynomial ring $F[t]$ in one variable t over a field F, and let K denote the field of fractions of A, i.e. either $K = \mathbb{Q}$ or $K = F(t)$ for some field F.

In both cases, A is known to be Euclidean: for $A = \mathbb{Z}$, a Euclidean function on A is given by the modulus $|n| := \max\{n, -n\}$, while for $A = F[t]$ we can take $\big|p(t)\big| := q^{\deg p}$ where q is any[9] integer greater than 1. This map $|\cdot|$ can be extended to a map $K \to \mathbb{R}_{\geq 0}$, again denoted $|\cdot|$, given by

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ |a| \,/ |b| & \text{if } x = a/b \text{ for } a, b \in A, b \neq 0; \end{cases}$$

it is *positive-definite*, *multiplicative* and satisfies the *triangle inequality*, i.e.:
(A1) $|x| = 0$ if and only if $x = 0$;
(A2) $|xy| = |x||y|$ for all $x, y \in K$;
(A3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$;
in other words, it is an *absolute value* on K. In the case $K = F(t)$ we even have the *strong triangle inequality*
(A3') $|x + y| \leq \max\{|x|\,, |y|\}$ for all $x, y \in K$.

Now let $\mathbf{P}$ be defined as follows: if $A = \mathbb{Z}$, then $\mathbf{P} = \{2, 3, 5, ...\}$ is the set of prime numbers; if $A = F[t]$, then $\mathbf{P}$ is the set of monic irreducible polynomials $\pi(t) \in F[t]$. Since A is Euclidean, it is a UFD, and so each $0 \neq a \in A$ can be written as a product $\varepsilon \prod_{\pi \in \mathbf{P}} \pi^{v_\pi(a)}$, where $\varepsilon \in A^*$, $v_\pi(a) \in \mathbb{Z}_{\geq 0}$ and $v_\pi(a) = 0$ for almost all π, i.e., the product is finite. For $\pi \in \mathbf{P}$ and $x \in K$, set

$$v_\pi(x) = \begin{cases} \infty & \text{if } x = 0, \\ v_\pi(a) - v_\pi(b) & \text{if } x = a/b \text{ for } a, b \in A, b \neq 0. \end{cases}$$

The map v_π is a *normalized discrete valuation on* K, i.e. a surjective map from $K^\times$ to $\mathbb{Z}$, extended via $v_\pi(0) = \infty$, satisfying
(V1) $v_\pi(xy) = v_\pi(x) + v_\pi(y)$ for all $x, y \in K$;
(V2) $v_\pi(x + y) \geq \min\{v_\pi(x),\ v_\pi(y)\}$ for all $x, y \in K$.
Accordingly, for each $\pi \in \mathbf{P}$ the map $x \mapsto |x|_\pi := |\pi|^{-v_\pi(x)}$ satisfies (A1), (A2) and

[9] If F is a finite field, then the canonical choice for q is the cardinality of F.

(A3'). It follows at once from the definitions that the *product formula*

$$|x|_\infty \cdot \prod_{\pi \in \mathbf{P}} |x|_\pi = 1 \qquad \forall x \in K^\times$$

holds, where $|\cdot|_\infty$ denotes the Euclidean function $|\cdot|$. Moreover, in the case $K = F(t)$, we can define $\deg(\infty) := 1$ as well as $v_\infty(a/b) := \deg(b) - \deg(a)$ for $a, b \in A, b \neq 0$; then, after taking logarithms to the base q, the product formula reads:

$$\sum_{P \in \mathbf{P} \cup \{\infty\}} v_P(x) \deg(P) = 0 \qquad \forall x \in K^\times. \tag{1}$$

A.2. The general theory

At this point, it is convenient to introduce the concept of places of a field. A *place* of a field K is commonly defined as an equivalence class of absolute values on K, where two absolute values $|\cdot|, |\cdot|'$ on K are *equivalent* if there exists a $\rho \in \mathbb{R}_{>0}$ such that $|x|' = |x|^\rho$ for all $x \in K$. Since two absolute values on K are equivalent if and only if they induce[10] the same topology on K, by a *place* of K we shall often mean a topology on K which is induced by some absolute value. In either case, a *valued field* is a pair (K, P) where K is a field and P is a place of K.

Example. (0) The *trivial place* on any field K is the discrete topology, i.e. the topology in which singletons are open. It is induced by the *trivial absolute value* $|\cdot|$ given by $|x| = 1$ for $x \neq 0$.

(1) The standard, "Euclidean" topology on $\mathbb{R}$ is a place of $\mathbb{R}$, induced by the standard absolute value. Similarly for the standard topology on $\mathbb{C}$.

(2) Let $A, K, \mathbf{P}$ be as in §1. If $\pi, \pi' \in \mathbf{P} \cup \{\infty\}$ are distinct, then $|\pi|_\pi < 1$ but $|\pi|_{\pi'} = 1$, thus π and π' induce different places of K. ◇

Remark. (1) Keep the notations from Ex.(2). It is a theorem of Ostrowski that, if P is a nontrivial place of $K = \mathbb{Q}$, then P comes from some $\pi \in \mathbf{P} \cup \{\infty\}$.

Analogously, if P is a nontrivial place of $K = F(t)$ which is trivial on F, i.e. whose restriction to F is the trivial place (see also (ii) below), then it can be shown that P comes from some $\pi \in \mathbf{P} \cup \{\infty\}$. ◇

Let (K, P) be a valued field, and let $|\cdot|$ be an absolute value on K belonging to P. By the definition of a place, the following are well-defined, i.e. independent of $|\cdot|$:

(i) the subsets $O(P) := \{x \in K : |x| \leq 1\}$ and $m(P) := \{x \in K : |x| < 1\}$ of K;
(ii) the "restriction" of P to any subfield $K' \subseteq K$, i.e. the subspace topology;
(iii) the set $\mathcal{CS}(K, P)$ of sequences in K which are Cauchy with respect to the metric $(x, y) \mapsto |x - y|$, equipped with component-wise addition and multiplication;
(iv) the field K_P defined as the quotient of $\mathcal{CS}(K, P)$ by its maximal ideal $\mathfrak{n} := \{(x_n) \in \mathcal{CS}(K, P) : |x_n| \xrightarrow{n \to \infty} 0\}$;

[10] The topology *induced* by $|\cdot|$ is the one generated by the "open balls" $B_r(x) := \{y \in K : |x - y| < r\}$, where $x \in K$, $r \in \mathbb{R}_{>0}$.

(v) the place P on K_P induced by $|\cdot| : K_P \to \mathbb{R}_{\geq 0}$, $x \mapsto \lim|x_n|$ where (x_n) is an arbitrary element of $\mathcal{CS}(K,P)$ with $\lim x_n = x$.

The valued field (K_P, P) is called the *completion* of (K,P), cf. the well-known construction for general metric spaces.

EXAMPLE. (2) Again, let $A, K, \mathbf{P}$ be as in §1, and consider a place $\pi \in \mathbf{P}$. Then the completion K_π is given[11] by the "formal Laurent series field"

$$K_\pi := \left\{ \sum_{i=n}^{\infty} a_i \pi^i : n \in \mathbb{Z},\ |a_i|_\infty < |\pi|_\infty \ \ \forall i \right\},$$

and the place on K_π is the one induced by the normalized discrete valuation

$$\mathrm{ord}_\pi \left(\sum_{i=n}^{\infty} a_i \pi^i \right) := \inf\{i \in \mathbb{Z} : a_i \neq 0\}.$$

When $K = \mathbb{Q}$ and π is a positive prime integer p, it is customary to denote K_π by $\mathbb{Q}_p$. The elements of $\mathbb{Q}_p$ are called *p-adic numbers*.

(2') If $K = F(t)$ and $\pi = \infty$, then one quickly checks that the completion K_∞ is precisely the Laurent series field $F((1/t))$. On the other hand, if $K = \mathbb{Q}$ and $\pi = \infty$ then the completion $\mathbb{Q}_\infty$ is clearly $\mathbb{R}$, cf. Ex.(1). ◇

REMARK. (2) Ex.(2) is a special case of the following situation: let (K,P) be a valued field, $|\cdot|$ be an absolute value on K which induces P, and suppose that $|\cdot| = C^{-v(\cdot)}$ for some real constant $C > 1$ and a normalized discrete valuation v on K. Let $|\cdot|$ also denote the extension of $|\cdot|$ to K_P as in (v) above. Then $x \mapsto -\frac{\log|x|}{\log C}$ is a normalized discrete valuation ord_P on K_P whose restriction to K is precisely v.

(3) Let $|\cdot|$ be a nontrivial absolute value on an field K and P the corresponding place of K. If $|\cdot|$ satisfies the strong triangle inequality (A3') from §1, then $O(P) \subset K$ as defined above is a ring. Moreover, $m(P)$ is a maximal ideal of $O(P)$, so the quotient $O(P)/m(P) =: F_P$ is a field, the *residue field* of K at P.

Conversely, suppose that $O(P)$ is a ring. Then, since $1 \in O(P)$, the ring $O(P)$ contains the image of the canonical ring map $\mathbb{Z} \to K$, $1 \mapsto 1$, and it can be shown that this implies the strong triangle inequality for $|\cdot|$. In this case, both the place P and the absolute value $|\cdot|$ are called *non-archimedean*.

Finally, if $O(P)$ is Noetherian, then it is already a PID, and there is a unique normalized discrete valuation ord_P on K such that $|\cdot| = C^{-\mathrm{ord}_P(\cdot)}$ for some real constant $C > 1$. Then P is called a *discrete place*, and $|\cdot|$ is called a *discrete absolute value*. ◇

[11] If $K = F(t)$ and $\pi \in \mathbf{P}$, then any $p(t) \in F[t]$ can be written as a polynomial $a_0 + a_1\pi + ... + a_k\pi^k$ with $|a_i|_\infty < |\pi|_\infty$ for all i: this is just Euclidean division. If, instead, $A = \mathbb{Z}$, then this is also possible if $a \geq 0$, while for $a < 0$ we only have a "formal power series expansion", e.g. $-1 = (\pi-1)+(\pi-1)\pi+(\pi-1)\pi^2+...$ (cf. geometric series). In either case, K embeds densely into K_π.

A.3. Number fields and function fields

Again let $A, K, \mathbf{P}$ as in §1, and let L be a field containing a copy of K so that L/K is a finite-degree field extension. In the case $K = \mathbb{Q}$, L is called an *algebraic number field*; otherwise, if $K = F(t)$, then L is called an *algebraic function field in one variable over F*, or a *function field over F* for short.

REMARK. (4) If L is a function field over F and $x \in L$ is transcendental over F, then it is not hard to show that $[L : F(x)]$ is finite. $\diamond$

Let L be a number field and let $\mathcal{O}_L$ denote the integral closure of $\mathbb{Z}$ in L. Then $\mathcal{O}_L$ is a *Dedekind domain*, i.e., every nonzero ideal I of $\mathcal{O}_L$ can be written uniquely as a finite product $\prod \mathfrak{p}^{v_\mathfrak{p}(I)}$ of prime ideals. As in §1, we obtain a normalized discrete valuation $v_\mathfrak{p}$ on L for each nonzero prime ideal $\mathfrak{p} \subset A$, and a corresponding absolute value $|\cdot|_\mathfrak{p} := (N\mathfrak{p})^{-v_\mathfrak{p}(\cdot)}$, where $N\mathfrak{p}$ denotes the cardinality of $\mathcal{O}_L/\mathfrak{p}$.

On the other hand, L has $n = [L : Q]$ distinct embeddings σ_1, ..., σ_n into $\mathbb{C}$. The product formula

$$\prod_{i=1}^{n} |\sigma_i(x)|_\mathbb{C} \cdot \prod_\mathfrak{p} |x|_\mathfrak{p} = 1 \qquad \forall x \in L^\times$$

holds, where $|\cdot|_\mathbb{C}$ is just the standard absolute value on $\mathbb{C}$, and every nontrivial place of L is induced either by some $\mathfrak{p}$ or by some σ_i, cf. Rmk.(1).

If L is a function field over F and we fix some t such that $[L : F(t)] < \infty$, then the above proof carries over to L with almost no modifications. In particular, let $X = X_L$ denote the set of nontrivial places Q of L which are trivial on F. Then:

- for every $Q \in X$ there is a canonical absolute value $|\cdot|_Q$ belonging to Q;
- for every $x \in L^\times$, it holds that $|x|_Q = 1$ for almost all $Q \in X$;
- the product formula holds:

$$\prod_{Q \in X} |x|_Q = 1 \qquad \forall x \in L^\times.$$

In the sequel, we make some observations and partially provide new proofs for the above. To that end, we record the following general facts from valuation theory (that were also implicitly used in the proof for number fields):

(F1) For a finite extension L/K and a place P of K, the number r of places Q of L whose restriction to K is precisely P satisfies $1 \leq r \leq n$.

(F2) Let Q be a non-archimedean place, cf. Rmk.(3), and let $A \subseteq L$ be a subring whose field of fractions is L. If $A \subseteq O(Q)$ and $\alpha \in L$ is integral over A, then $\alpha \in O(Q)$.

We remark that (F1) is well-known for separable extensions, but is valid in the general case, see e.g. [16], and (F2) is not especially tricky.

Now let L be a function field over F, and let $X = X_L$ denote the set of nontrivial places Q of L which are trivial on F. Then *each place $Q \in X$ is discrete, in particular non-archimedean*, where the definitions are as in Rmk.(3). (This is not hard to see

once one has some familiarity with valuation theory.) We henceforth denote the normalized discrete valuation corresponding to $Q \in X$ by ord_Q.

(F3) If $x \in L$ is transcendental over F, then there is at least one $Q \in X$ with $x \in m(Q)$ and at least one $Q' \in X$ with $x \notin O(Q')$. Moreover, there are only finitely many of either type.

(F4) If F' denotes the algebraic closure of F in K, then $F' = \bigcap_{Q \in X} O(Q)$.

(F5) For each $Q \in X$, the field extension F_Q/F has finite degree.

(F6) The degree of the extension F'/F is finite, where F' is as in (F4).

The proofs are as follows. To show (F3), let $K = F(x) \subset L$, and observe that there is exactly one place $\pi \in \mathbf{P} \cup \{\infty\}$ on $F(x)$ with $x \in m(\pi)$, namely the place corresponding to the irreducible polynomial $x \in F[x]$, and exactly one place π with $x \notin O(\pi)$, namely $\pi = \infty$. The claim now follows from (F1) and Rmk.(4).

We now turn to (F4). If $x^\times \in L$ is algebraic over F, then applying (F2) to both x and x^{-1} yields that $\mathrm{ord}_Q(x) = 0$ for all $Q \in X$, and in particular $F \subseteq \bigcap_{Q \in X} O(Q)$, while the reverse inclusion follows from (F3).

To prove (F5), let $0 \neq x \in m(Q)$. Then, by the proof of (F4), x must be transcendental over F, so $[L : F(x)]$ is finite by Rmk.(4). Now let $z_1, ..., z_n \in O(Q)$, then it is not hard to show that $z_1, ..., z_n$ are $F(x)$-linearly independent if their images under the canonical projection $O(Q) \to O(Q)/m(Q) = F_Q$ are F-linearly independent, hence $[F_Q : F] \leq [L : F(x)] < \infty$.

Finally, we set out to prove (F6). But for any $Q \in X$ we observe that $F' \subseteq O(Q)$ and $\{0\} = F' \cap m(Q)$, so F' embeds in F_Q and the claim follows from (F5).

Remark. (5) Let F' be as in (F4). Then, by (F6), L is again an algebraic function field in one variable over F', so upon replacing F by F' if necessary we *may always assume that the ground field F of a function field L is algebraically closed in L.* $\diamond$

Now if for $Q \in X$ we define $\deg Q := [F_Q : F]$, then $|\cdot|_Q := (q^{\deg Q})^{-\mathrm{ord}_Q(\cdot)}$ is the canonical absolute value mentioned earlier in this section, and so the product formula holds for L. Taking logarithms to the base q, we obtain $\sum_{Q \in X} \mathrm{ord}_Q(x) \deg Q = 0$ for all $x \in L^\times$. The reader is referred to [16] for a complete and direct proof of this equation which does not rely on the analogy with algebraic number fields.

Appendix B. Projective geometry

Here we would like to spend a few words on projective geometry, including a sketch of the proof of the observation at the beginning of Chapter 1.

First of all, recall that the *n-dimensional projective space* $\mathbb{P}^n(F)$ over a field F is, in a way, regular n-dimensional space enlarged with some "points at infinity". More rigorously, $\mathbb{P}^n(F)$ is a set of points $[v_0 : ... : v_n]$ with $(v_0, ..., v_n) \neq (0, ..., 0)$, subject to the condition that $[v_0 : ... : v_n] = [\lambda v_0 : ... : \lambda v_n]$ for all $\lambda \in F^\times$; the points with $v_0 \neq 0$ can be written as $[1 : \frac{v_1}{v_0} : ... : \frac{v_n}{v_0}]$ and thus form a copy of F^n inside $\mathbb{P}^n(F)$, while the points with $v_0 = 0$ are the "points at infinity".

A subset X of $\mathbb{P}^n(F)$ is called a *(projective) variety* if there exist homogeneous polynomials $F_j(x_0, ..., x_n)$, $j = 1, ..., r$ with coefficients in F such that $X = \{[v_0 : ... : v_n] : F_j(v_0, ..., v_n) = 0 \text{ for all } j\}$; this is indeed well-defined by homogeneity of the F_j's. The points of X with $v_0 \neq 0$ can be regarded as a subset of F^n which is again defined by polynomial equations, i.e. as an *affine subvariety* of F^n, and conversely every affine variety can be embedded into a projective one by homogenizing the polynomials which define it.

We now want to define rational functions on X. Let f, g be polynomials in $n+1$ variables over F, homogeneous of the same degree. Then the map $X \to F \cup \{\infty\}$, $P = [v_0 : v_1 : ...v_n] \mapsto f(v_0, ..., v_n)/g(v_0, ..., v_n)$ is well-defined, provided that g does not vanish identically on X. A map of this form is called a *rational function* on X, and the field of rational functions on X is denoted $F(X)$. The *dimension* of X is defined as the transcendence degree of $F(X)$; in particular, X is a *projective curve*, i.e. 1-dimensional, if and only if $F(X)$ is a function field in one variable as defined in Chapter 1 or Appendix A.

A projective variety X is *smooth* if for each point $P \in X$ there exists a normalized discrete valuation ord_P on $F(X)$, trivial on F, such that for each $x \in F(X)$, $\mathrm{ord}_P(x) \geq 0$ if and only if $x = \frac{f}{g}$ where $g(P) \neq 0$.

Remark. The motivation for the definition of smoothness is the following: consider an *affine plane curve* C over an algebraically closed field F, i.e. the vanishing set in F^2 of a polynomial $f(x, y)$ in two variables over F. We again have a concept of a *field of rational functions* $F(C)$, whose elements are maps $C \to F \cup \{\infty\}$ of the form g/h where $g, h \in K[x, y]$ and h is not identically zero on C. More precisely, if g and h can be chosen so that h does not vanish at $P \in C$, then the rational function is said to be *defined at* P.

For a point $P = (a, b) \in F^2$ we can write any polynomial $g(x, y)$ as a polynomial in the variables $x - a$ and $y - b$,

$$g(x,y) = c_{00} + c_{10}(x-a) + c_{01}(y-b) + c_{20}(x-a)^2 + c_{11}(x-a)(y-b) + c_{02}(y-b)^2 + ...;$$

we define the *multiplicity* of g at P as the smallest integer n for which there exists some k with $c_{k,n-k} \neq 0$. Moreover, for another polynomial $h(x, y)$, the *intersection number* of g and h at P is defined as the multiplicity of $g - h$ at P.

Now, $P \in C$ if and only if the multiplicity m of f at P is positive. If P is a *simple point* of C, i.e. $m = 1$, then the assignment $g \mapsto$ "intersection number of f and g at P", which makes sense whenever g is defined at P, can be extended to a normalized discrete valuation on $F(C)$.

Conversely, suppose that P is a *multiple point* of C, i.e. $m > 1$. Then, since F is algebraically closed, the homogeneous polynomial

$$c_{m0}(x-a)^m + c_{m-1,1}(x-a)^{m-1}(y-b) + ... + c_{0m}(y-b)^m$$

splits as a product of m linear factors $L_1(x,y)$, ..., $L_m(x,y)$. Note that the intersection number of f and L_i is clearly one for each i, while the intersection number of f and $\prod L_i$ is necessarily $> m$, so ord_P defined as above is not a normalized discrete valuation on $F(X)$. $\diamond$

Now let X be a smooth projective curve over F and $F(X)$ denote its field of fractions, and suppose that F *is an algebraically closed field*. Then (see [3]):

- Every nontrivial place Q of $F(X)$ which is trivial on F is induced by a valuation ord_P for some $P \in X$;
- If K is an algebraic function field in one variable over F, then there exists a smooth projective curve X over F with $K = F(X)$.

We sketch the proof of the first claim. As was hinted at in Appendix A, Q must be discrete, so there exists a (unique) normalized discrete valuation ord associated to Q. Moreover, we have argued earlier that $\mathbb{P}^n(F)$ contains a copy $\mathbb{A}^n$ of F^n, and we shall henceforth denote by C the *affine curve* obtained as $\mathbb{A}^n \cap X$. By a couple of technical results, one can choose $\mathbb{A}^n$ so that the *coordinate ring* $F[C]$ of C embeds into $F(X)$ and $\mathrm{ord}(x) \geq 0$ for all $x \in F[C]$. But then $\mathfrak{p} = \{x \in F[C] : \mathrm{ord}(x) > 0\}$ is a nonzero prime ideal of $F[C]$, hence it corresponds to a proper irreducible subvariety of C, i.e. to a point $P \in C$. Thus $\mathrm{ord} = \mathrm{ord}_P$ and the claim is proved.

Appendix C. Locally compact groups

Recall that a *topological group* is a group G (whose operation we denote as multiplication) equipped with a topology τ such that the maps

(i) $G \times G \to G, \quad (g,h) \mapsto gh,$

(ii) $G \to G, \quad g \mapsto g^{-1}$

are continuous in the topology τ (of course $G \times G$ is to be equipped with the product topology). A topological group G will be called *locally compact* if the topology is Hausdorff and if each point has a compact neighbourhood.

EXAMPLE. (1) Consider $\mathbb{R}$ with the Euclidean topology. Then the additive group $(\mathbb{R}, +)$ is a locally compact topological group. The same holds for the additive group of $\mathbb{R}^n$ or $\mathbb{C}^n$ for all $n \geq 1$. $\diamond$

C1. The Haar measure

Recall that a *measure* on a set X is a function $\mu : \mathcal{M}(\mu) \to [0, \infty]$ where:

- $\mathcal{M}(\mu)$ is a *σ-algebra* on X, i.e. a subset of the power set of X which contains $\emptyset$ and is closed under taking complements and countable unions;
- μ maps $\emptyset$ to 0 and is *countably additive* in the sense that $\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n)$ whenever the subsets $A_n \in \mathcal{M}(\mu)$ are pairwise disjoint.

The elements of $\mathcal{M}(\mu)$ are called the *measurable subsets* of X.

If X is a (Hausdorff) topological space and μ is a measure on X, then it is often desirable that every open subset of X be measurable, in which case μ is called a *Borel measure*. A Borel measure μ on X is called *inner regular* if it is compatible in a certain precise sense with approximation "from below" by compact measurable subsets, and *outer regular* if it is similarly compatible with approximation "from above" by open subsets.

It is a well-known theorem of Haar that if G is a locally compact group, then there exists a nonzero regular Borel measure μ on G such that:

(i) every compact subset K of G is measurable and $\mu(K) < \infty$;

(ii) μ is *left-invariant*, i.e. $\mu(gA) = \mu(g)$ for any $A \subseteq G$ and $g \in G$.

Any such measure is called a *Haar measure* on G. Furthermore, if μ and μ' are Haar measures on G, then $\mu' = \kappa\mu$ for some $\kappa \in \mathbb{R}_{>0}$, so one sometimes speaks of "the" Haar measure on G.

EXAMPLE. (2) Let μ be the function which assigns to each compact interval $[a_1, b_1] \times ... \times [a_n, b_n] \subset \mathbb{R}^n$ its n-dimensional volume $(b_1 - a_1) \cdots (b_n - a_n)$. Then μ can be extended to a regular Borel measure λ on $\mathbb{R}^n$ which is additionally "complete" in a certain precise sense; λ is called the *n-dimensional Lebesgue measure*. It is immediate that λ is a Haar measure for the locally compact additive group $(\mathbb{R}^n, +)$, normalized in such a way that the n-dimensional cube of side length 1 has volume 1. $\diamond$

REMARK. (1) If H is a closed normal subgroup of a locally compact group G, then both H and G/H are locally compact groups. It is then known that one can choose

Haar measures on G, H and G/H so that $\mu_G = \mu_H \cdot \mu_{G/H}$, i.e. so that

$$\mu_G(A) = \mu_H(A \cap H)\ \mu_{G/H}\left(A/(A \cap H)\right)$$

for all $A \subseteq G$. ◇

C2. Pontrjagin duality

For this subsection, we fix an *abelian* topological group G, denoted additively.

Let $\mathbb{T} = U(1)$ denote the *circle group*, i.e. the group of complex numbers with modulus equal to 1. The continuous group homomorphisms $\chi : G \to \mathbb{T}$ together with the pointwise operations $(\chi+\psi)(g) = \chi(g)\psi(g)$ form an abelian group, denoted G^*. We equip G^* with the *compact-open topology*, i.e. the topology generated by the subsets $\{\chi \in G^* : \chi(K) \subset U\}$, where K runs over the compact subsets of G and U runs over the open subsets of $\mathbb{T}$. Then G^* turns into a topological group.

One can prove that, if G is discrete, compact or locally compact, then G^* is compact, discrete or locally compact, respectively. Moreover, let G and H are locally compact abelian groups with a continuous distributive "multiplication" $G \times H \to \mathbb{T}$, $(g, h) \mapsto gh$, and suppose that $g \mapsto (h \mapsto gh)$ is an isomorphism $G \to H^*$. Then H is isomorphic to G^* via $h \mapsto (g \mapsto gh)$, and the "multiplication" is simply the map $(g, \chi) \mapsto \chi(g)$. In particular, a locally compact abelian group G is (canonically) isomorphic to its bidual $(G^*)^*$.

Example. (3) Let G be the additive group of the reals, and consider the character $\chi \in G^*$ given by $x \mapsto e^{2\pi i x}$. Then every element of G^* is of the form $\chi_y : x \mapsto \chi(xy)$ for some $y \in \mathbb{R}$, and indeed the map $y \mapsto \chi_y$ is an isomorphism of topological groups. In other words, $\mathbb{R}$ is *self-dual*, and so $\mathbb{R}^*$ can be identified with $\mathbb{R}$.

(4) Let $G = \mathbb{Z}$. Then G^* is isomorphic to $\mathbb{T}$ via $\chi \mapsto \chi(1)$.

(4') Conversely, let $G = \mathbb{T}$. To an element χ of G^* we associate the degree of the covering $\chi : \mathbb{T} \to \mathbb{T}$, and so we obtain an isomorphism $G^* \xrightarrow{\sim} \mathbb{Z}$. ◇

Let us finally remark that Pontrjagin duality allows one to introduce Fourier analysis in a very general setting. Indeed, the Fourier transform of a real-valued function, the discrete-time Fourier transform and the Fourier series expansion of a periodic function (i.e. a function on $U(1)$) can all be seen as special instances of this general theory, cf. examples (3), (4) and (4'), respectively.

C3. Locally compact rings and fields

A *topological ring* is a ring R equipped with a topology τ such that

(i) the additive group of R is a topological group;

(ii) $R \times R \to R$, $\quad (r, s) \mapsto rs$ is continuous in the topology τ.

A topological ring R is *locally compact* if its additive group $(R, +)$ is a locally compact topological group with the given topology.

Moreover, if a topological ring R is a field K and

(i) $K^\times \to K^\times, \quad x \mapsto x^{-1}$ is continuous in the topology τ,

then K is called a *topological field*. A *locally compact field* is just a topological field that is locally compact as a topological ring.

EXAMPLE. (5) Both $\mathbb{R}$ and $\mathbb{C}$ are locally compact in the Euclidean topology. Moreover, the field $\mathbb{Q}_p$ of p-adic numbers as defined in Ex.(2) of Appendix A is locally compact since, for each $\varepsilon > 0$, the ring $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : \mathrm{ord}_p(x) \geq 0\}$ of *p-adic integers* can be covered by finitely many balls of radius less than ε. The same argument shows that, if F is a finite field, $K = F(t)$ and $\pi \in \mathbf{P}$, then K_π as defined in Ex.(2) of Appendix A is locally compact. $\diamond$

C4. Adèle rings of number fields

Let K be a number field, and let V denote the set of nontrivial places of K. Then X is partitioned into an infinite set V_{fin} of non-archimedean places, corresponding to nonzero prime ideals of the ring of integers $\mathcal{O}_K$, and a finite set S_∞ of archimedean places, induced by embeddings $K \hookrightarrow \mathbb{C}$, cf. §3 of Appendix A. For each P let K_P denote the completion of K at P, and for $P \in V_{\mathrm{fin}}$ let ord_P denote the canonical discrete valuation on K_P. Arguing as in Ex.(5), one shows that each K_P is locally compact and picks a canonical absolute value $|\cdot|_P$.

The *adèle ring* of K is defined as

$$\mathbb{A}_K := \left\{ a = (a_P)_P \in \prod_{P \in V} K_P : \mathrm{ord}_P(a_P) \geq 0 \text{ for almost all } P \in V_{\mathrm{fin}} \right\}.$$

This is a topological ring, cf. §3, with the topology generated by subsets of the form

$$\prod_{Q \in S} U_Q \times \prod_{P \notin S} O_P,$$

where $S \subset V$ is finite and contains S_∞, U_Q is an open subset of K_Q for each $Q \in S$ and $O_P := \{x \in K_P : \mathrm{ord}_P(x) \geq 0\} \subset K_P$. Moreover, each K_P is isomorphic (as a topological field) to the quotient $\mathbb{A}_K/\mathfrak{m}_P$, where $\mathfrak{m}_P := \{a = (a_P) \in \mathbb{A}_K : a_P = 0\} \subset \mathbb{A}_K$ is a maximal ideal. Finally, since

(i) $K \subset K_P$ for each P, and

(ii) for each $x \in K^\times$, $|x|_P = 1$ for almost all P,

the set $\{(x)_P = (x, x, x, ...) \in \prod K_P : x \in K\}$ is a subfield of $\mathbb{A}_K$ isomorphic to K. This subfield is discrete and the quotient $\mathbb{A}_K/K$ is compact, and these properties, together with the local compactness of $\mathbb{A}_K$, are essentially enough to characterize adèle rings of so-called *global fields*, i.e. algebraic number fields and algebraic function fields in one variable over a finite field F. The interested reader may wish to consult [1] and the references listed there, especially the paper of Emil Artin and George Whaples on the axiomatization of global fields via the product formula.

References

[1] Kenkichi Iwasawa, *On the rings of valuation vectors*, Annals of Mathematics, Vol. 57, No. 2, March, 1953.

[2] André Weil, *Basic Number Theory*, Springer-Verlag New York Heidelberg Berlin, Third Edition, 1974.

[3] William Fulton, *Algebraic Curves, An Introduction to Algebraic Geometry*, now available online, http://www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf, 2008.

[4] Solomon Lefschetz, *Algebraic Topology*, American Mathematical Society, Providence, Rhode Island, 1942.

[5] Tom Leinster, *Codensity and the ultrafilter monad*, https://arxiv.org/abs/1209.3606, 2013.

[6] Dinakar Ramakrishnan, Robert J. Valenza, *Fourier Analysis on Number Fields*, Springer New York, 1999.

[7] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, Second Edition, 1993.

[8] Raghavan Narasimhan, *Compact Riemann Surfaces*, Springer Basel AG, 1992.

[9] M. Kapovich, *The Riemann-Roch Theorem*, electronic, https://www.math.ucdavis.edu/∼kapovich/RS/RiemannRoch.pdf.

[10] Kenny Wong, *Prove that every compact Riemann surface is an algebraic curve.*, Answer at Math StackExchange, https://math.stackexchange.com/questions/2332562/, 2017.

[11] James Stankiewicz, *The Riemann-Roch Theorem*, electronic, stankewicz.net/Riemann-Roch.pdf, formerly at http://www.math.uga.edu/∼jstankew/Riemann-Roch.pdf.

[12] Toshitsune Miyake, *Modular Forms*, Springer Berlin Heidelberg New York, 1989.

[13] Greg Martin, *Dimension of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, Journal of Number Theory 112 (2005), pp. 298-331.

[14] Henri Darmon, *A Proof of the Full Shimura-Taniyama-Weil Conjecture Is Announced*, Notices of the AMS, 1999.

[15] Paulo Ribenboim, *The Theory of Classical Valuations*, Springer-Verlag New York Berlin Heidelberg, 1999.

[16] Kenkichi Iwasawa, *Algebraic Functions*, Translations of Mathematical Monographs, vol. 118, American Mathematical Society, 1991.