The arithmetic Riemann–Roch theorem

Håkon Kolderup

November 6, 2018

1 Classical Riemann–Roch

The Riemann–Roch theorem is a classical and very important result in complex analysis and algebraic geometry. The basic question the theorem answers goes as follows. Given a compact and connected Riemann surface X, how many linearly independent functions with prescribed zeros and poles are there on X? The Riemann–Roch theorem provides a formula which allows to easily compute the number of such functions. The answer depends heavily on the topology of X, or more precisely, the *genus* of X (i.e., the "number of holes in X").

To formulate the Riemann–Roch formula more precisely, recall that a *divisor* on the Riemann surface X is a finite formal sum $D = \sum_{P \in X} a_P P$, where the a_P's are integers and the P's are points on X. Thus, to "specify zeros and poles" means to give a divisor on X: if you for instance are looking for functions with a zero of order 2 at $P \in X$ and a pole of order 3 at $Q \in X$, you can concatenate this information into a divisor $D = 2P - 3Q$. On the contrary, any rational function f on X gives rise to a divisor $\mathrm{div}(f)$ by letting

$$\mathrm{div}(f) := \sum_{P \in X} \mathrm{ord}_P(f) P,$$

where $\mathrm{ord}_P(f)$ means the order of f at the point $P \in X$. For any divisor $D = \sum_{P \in X} a_P P$, we can also define the *degree* of D as $\deg D := \sum_P a_P$.

Definition 1.1. For any divisor $D = \sum_{P \in X} a_P P$ on X, set

$$H^0(D) := H^0(X, \mathcal{O}(D)) := \{\text{rational functions } f \text{ on } X : \mathrm{ord}_P(f) \geq -a_P\}.$$

Then $H^0(D)$ is a $\mathbf{C}$-vector space, and we let $h^0(D)$ denote its dimension.

The number $h^0(D)$ is precisely what we are interested in computing. The Riemann–Roch theorem does this for us:

Theorem 1.2. *Let X be a compact and connected Riemann surface of genus g. For any divisor D on X, we have*

$$h^0(D) - h^1(D) = \deg(D) + 1 - g.$$

The number $\chi(D) := h^0(D) - h^1(D)$ is referred to as the Euler characteristic of D. Here $h^1(D) = \dim_{\mathbf{C}} H^1(X, \mathcal{O}(D))$ is a "correction term" that we will not go further into here. However, let us mention that there is a deep theorem known as Serre duality that identifies $h^1(D) = h^0(K_X - D)$, where K_X is the canonical divisor on X. The number $h^0(K_X - D)$ is in general much easier to compute than $h^1(D)$, yielding the following strong version of the Riemann–Roch theorem:

Theorem 1.3. *Let X be a compact and connected Riemann surface of genus g. For any divisor D on X, we have*

$$h^0(D) - h^0(K_X - D) = \deg(D) + 1 - g.$$

1.1 The arithmetic version

In these notes we will show the analog of the Riemann–Roch formula $\chi(D) = \deg(D) + 1 - g$ for number fields (see Theorem 6.9). To do this, we need to make sense of, among other things, "divisors on rings of integers" and the "genus of a number field".

So let K be a number field. The first question we ask is, what kind of space should play the role of a compact Riemann surface? The answer is, approximately, the ring of integers $\mathcal{O}_K$. If you know some algebraic geometry, you know that the spectrum $\mathrm{Spec}(\mathcal{O}_K) = \{\text{prime ideals } \mathfrak{p} \text{ of } \mathcal{O}_K\}$ of $\mathcal{O}_K$ is a reasonable thing to work with: it is a smooth affine curve, and the field of rational functions of $\mathrm{Spec}(\mathcal{O}_K)$ is precisely the number field K we started with. So the prime ideals of $\mathcal{O}_K$ should be the analog of the points of a compact Riemann surface X, and the elements of the number field K should be the analog of rational functions on X.

However, there is one big difference between $\mathrm{Spec}(\mathcal{O}_K)$ and the compact Riemann surface X: $\mathrm{Spec}(\mathcal{O}_K)$ is not projective! So it is not a good analog of a *compact* Riemann surface. The maneuver we will perform in order to remedy this is the starting point of the so-called "Arakelov geometry", and can intuitively be thought of as adding additional points to $\mathrm{Spec}(\mathcal{O}_K)$ coming from the real and complex embeddings of K, as we considered in Minkowski theory. We are thus performing a sort of a "one point compactification" of $\mathrm{Spec}(\mathcal{O}_K)$, resulting in a new space $\widehat{\mathrm{Spec}}(\mathcal{O}_K)$ which behaves very much like a compact Riemann surface. Indeed, in this setting we can define divisors (which will be referred to as *Arakelov divisors*), genus and Euler characteristic, leading to an arithmetic version of the classical Riemann–Roch theorem.

2 Divisors and Chow groups

We start out with a short review of divisors and Chow groups of arbitrary integral domains, before specializing to rings of integers in number fields. Thus, let A be a noetherian integral domain with field of fractions K.

Definition 2.1. A *divisor* on A is a finite, formal sum

$$D = \sum_{\mathfrak{p} \in \mathrm{Max}(A)} a_{\mathfrak{p}} \mathfrak{p} \in \bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} \mathbf{Z},$$

where the sum is taken over all maximal ideals of A.

We let

$$Z^1(A) := \bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} \mathbf{Z}$$

denote the group of divisors on A (also known as 1-cycles, hence the notation Z^1).

Recall that the *length* $\ell_A(M)$ of an A-module M is the maximal length of a chain of submodules

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_\ell = 0.$$

Definition 2.2. Let $f \in K^\times$, so that we may write $f = a/b$ for $a, b \in A$. Let also $\mathfrak{p} \in \mathrm{Max}(A)$ be a maximal ideal of A. The *order of f at $\mathfrak{p}$* is

$$\mathrm{ord}_{\mathfrak{p}}(f) := \ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}/aA_{\mathfrak{p}}) - \ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}/bA_{\mathfrak{p}}).$$

The *divisor associated to f* is

$$\mathrm{div}(f) := \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f)\mathfrak{p}.$$

A divisor $D \in Z^1(A)$ is called a *principal divisor* if $D = \operatorname{div}(f)$ for some $f \in K^\times$.

We let

$$\operatorname{Rat}^1(A) := \{\operatorname{div}(f) : f \in K^\times\}$$

denote the subgroup of $Z^1(A)$ consisting of principal divisors.

The quotient

$$\operatorname{CH}^1(A) := Z^1(A)/\operatorname{Rat}^1(A)$$

is called the *Chow group* of A.

Proposition 2.3. *If A is a Dedekind ring, then there is a canonical isomorphism*

$$\operatorname{CH}^1(A) \xrightarrow{\cong} \operatorname{Cl}_K$$

induced by $D = \sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p} \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$.

Example 2.4. Let $K = \mathbf{Q}$ and consider the rational function $f = 18/125 \in \mathbf{Q}^\times$. Then

$$\operatorname{ord}_{(3)}(18) = \ell(\mathbf{Z}_{(3)}/18\mathbf{Z}_{(3)}) = \ell(\mathbf{Z}/9) = 2,$$

as $(\overline{0}) \subsetneq (\overline{3}) \subsetneq \mathbf{Z}/9$ is a maximal chain of submodules in $\mathbf{Z}/9$. Here we have used that $18\mathbf{Z}_{(3)} = 9\mathbf{Z}_{(3)}$ since 2 is a unit in $\mathbf{Z}_{(3)}$, hence $\mathbf{Z}_{(3)}/18\mathbf{Z}_{(3)} \cong \mathbf{Z}_{(3)}/9\mathbf{Z}_{(3)} \cong \mathbf{Z}/9$.

Similarly we find $\operatorname{ord}_{(2)}(18) = 1$ and $\operatorname{ord}_{(5)}(125) = 3$, so

$$\operatorname{div}(f) = (2) + 2(3) - 3(5) \in \bigoplus_p \mathbf{Z}.$$

Under the isomorphism of Proposition 2.3, the divisor $\operatorname{div}(f)$ corresponds to the principal fractional ideal $(18/125)$ of $\mathbf{Q}$.

3 Arakelov divisors and arithmetic Chow groups

We will now specialize to the case when $A = \mathcal{O}_K$ is the ring of integers in a number field K. Then the ring A carries extra information coming from the real and complex embeddings of K, which we will bake into the definition of divisors in this setting. Thus, let K be a number field, with ring of integers $\mathcal{O}_K$. We first recall some notation from Minkowski theory:

Definition 3.1. Let Σ_K denote the set of $\mathbf{Q}$-embeddings of K in $\mathbf{C}$—that is, embeddings $\sigma\colon K \hookrightarrow \mathbf{C}$ such that $\sigma|_{\mathbf{Q}} = \mathrm{id}$. Set:

- $K_{\mathbf{C}} := K \otimes_{\mathbf{Q}} \mathbf{C} \cong \prod_{\sigma\in\Sigma_K} \mathbf{C}$;
- $K_{\mathbf{R}} := K \otimes_{\mathbf{Q}} \mathbf{R} \cong \left[\prod_{\sigma\in\Sigma_K} \mathbf{C}\right]^+ = \{(z_\sigma)_\sigma \in K_{\mathbf{C}} : z_{\overline{\sigma}} = \overline{z}_\sigma\}$;
- $\widehat{H}(K) := [\prod_{\sigma\in\Sigma_K} \mathbf{R}]^+ = \{(x_\sigma)_\sigma \in \prod_\sigma \mathbf{R} : x_{\overline{\sigma}} = x_\sigma\} \cong \mathbf{R}^{r+s}$.

An element $\mathfrak{g} \in \widehat{H}(K)$ is called a *Green object*, or a *Green current*.

Furthermore, we define the following maps:

- $j\colon K^\times \to K_{\mathbf{R}}^\times$, $j(\alpha) = (\sigma(\alpha))_\sigma$;
- $\log\colon K_{\mathbf{R}}^\times \to \widehat{H}(K)$, $\log((z_\sigma)_\sigma) = (\log|z_\sigma|)_\sigma$;

- $N\colon K_{\mathbf{R}}^{\times} \to \mathbf{R}^{\times}$, $N((z_\sigma)_\sigma) = \prod_\sigma z_\sigma$;
- $\mathrm{Tr}\colon \widehat{H}(K) \to \mathbf{R}$, $\mathrm{Tr}((x_\sigma)_\sigma) = \sum_\sigma x_\sigma$;
- $\rho := \log \circ j\colon K^{\times} \to \widehat{H}(K)$.

Finally, let

$$\widehat{H}(K)^0 := \{\mathfrak{g} \in \widehat{H}(K) : \mathrm{Tr}(\mathfrak{g}) = 0\} \cong \mathbf{R}^{r+s-1}$$

be the trace zero-hyperplane in $\widehat{H}(K)$, and put $\Gamma_K := \rho(\mathcal{O}_K^{\times}) \subseteq \widehat{H}(K)^0$. The proof of Dirichlet's unit theorem shows that Γ_K is a full lattice in $\widehat{H}(K)^0$, i.e., $\Gamma_K \cong \mathbf{Z}^{r+s-1}$.

We summarize the situation with the following commutative diagram:

$$\begin{array}{ccccc} & & \overset{\rho}{\frown} & & \\ K^{\times} & \xrightarrow{j} & K_{\mathbf{R}}^{\times} & \xrightarrow{\log} & \widehat{H}(K) \\ \big\downarrow{\scriptstyle N_{K/\mathbf{Q}}} & & \big\downarrow{\scriptstyle N} & & \big\downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbf{Q}^{\times} & \hookrightarrow & \mathbf{R}^{\times} & \xrightarrow{\log} & \mathbf{R}. \end{array}$$

Definition 3.2. The group of *Arakelov divisors* on $\mathcal{O}_K$ is

$$\widehat{Z}^1(\mathcal{O}_K) := Z^1(\mathcal{O}_K) \times \widehat{H}(K).$$

Thus an Arakelov divisor on $\mathcal{O}_K$ is a pair $(D, \mathfrak{g})$ of a divisor $D \in Z^1(\mathcal{O}_K)$ and a Green current $\mathfrak{g} \in \widehat{H}(K)$.

For any $f \in K^{\times}$, we define the *principal Arakelov divisor* of f as

$$\widehat{\mathrm{div}}(f) := (\mathrm{div}(f), (-\log|\sigma(f)|)_{\sigma \in \Sigma_K}).$$

Let $\widehat{\mathrm{Rat}}^1(\mathcal{O}_K)$ denote the group of principal Arakelov divisors.

The quotient group

$$\widehat{\mathrm{CH}}^1(\mathcal{O}_K) := \widehat{Z}^1(\mathcal{O}_K)/\widehat{\mathrm{Rat}}^1(\mathcal{O}_K)$$

is the *arithmetic Chow group* of $\mathcal{O}_K$.

Example 3.3. Let us return to Example 2.4, where $K = \mathbf{Q}$ and $f = 18/125 \in \mathbf{Q}^{\times}$. Then $\widehat{H}(K) = \mathbf{R}$, and we have

$$\widehat{\mathrm{div}}(f) = ((2) + 2(3) - 3(5), \log(125/18)) \in \bigoplus_p \mathbf{Z} \oplus \mathbf{R}.$$

Proposition 3.4. *The following sequence is exact:*

$$0 \to \mu(K) \hookrightarrow \mathcal{O}_K^{\times} \xrightarrow{\rho} \widehat{H}(K) \xrightarrow{a} \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \xrightarrow{\zeta} \mathrm{Cl}_K \to 0, \tag{1}$$

where $a(\mathfrak{g}) = [0, -\mathfrak{g}]$ *and* $\zeta\Big([\sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p}, \mathfrak{g}]\Big) = [\prod_{\mathfrak{p}} \mathfrak{p}^{-a_{\mathfrak{p}}}]$.

Proof. From Minkowski theory we know that the sequence is exact at the first two stages. Moreover, it is clear that ζ is surjective, and that $\ker(\zeta) = \{[0, \mathfrak{g}]\} = \mathrm{im}(a)$. It remains to show that $\mathrm{im}(\rho) = \ker(a)$.

Assume first that $\mathfrak{g} \in \operatorname{im}(\rho)$. Then $\mathfrak{g} = \rho(\epsilon) = (\log|\sigma(\epsilon)|)_\sigma$ for some unit $\epsilon \in \mathcal{O}_K^\times$. But then we have

$$a(\mathfrak{g}) = [0, -\mathfrak{g}] = [0, (-\log|\sigma(\epsilon)|)_\sigma] = [\widehat{\operatorname{div}}(\epsilon)] = 0 \in \widehat{\operatorname{CH}}^1(\mathcal{O}_K),$$

since $\operatorname{div}(\epsilon) = 0$. Hence $\mathfrak{g} \in \ker(a)$.

Now let $\mathfrak{g} \in \ker(a)$, so that $a(\mathfrak{g}) = [0, -\mathfrak{g}] = 0$ in $\widehat{\operatorname{CH}}^1(\mathcal{O}_K)$. This means that $(0, -\mathfrak{g}) \in \widehat{\operatorname{Rat}}^1(\mathcal{O}_K)$, i.e., there is a function $f \in K^\times$ such that $\widehat{\operatorname{div}}(f) = (0, -\mathfrak{g})$. Then $-\mathfrak{g} = (-\log|\sigma(f)|)_\sigma$, hence $\mathfrak{g} = \rho(f)$. Moreover, that $\operatorname{div}(f) = 0$ means that f is a global unit, i.e., $f \in \mathcal{O}_K^\times$. Hence $\mathfrak{g} \in \operatorname{im}\rho$. ☐

Corollary 3.5. *We have an exact sequence*

$$0 \to \widehat{H}(K)/\Gamma_K \xrightarrow{a} \widehat{\operatorname{CH}}^1(\mathcal{O}_K) \xrightarrow{\zeta} \operatorname{Cl}_K \to 0. \tag{2}$$

Proof. This is just a short exact sequence split off of the exact sequence (1) above. ☐

Example 3.6. For $K = \mathbf{Q}$ we have $\widehat{H}(K) = \mathbf{R}$, $\Gamma_K = 0$, and $\operatorname{Cl}_K = 0$. Hence the short exact sequence (2) yields $\widehat{\operatorname{CH}}^1(\mathbf{Z}) = \mathbf{R}$.

In topology we are often more interested in the *reduced* homology of a topological space, which is obtained from the kernel of an augmentation map. We can define a similar notion for arithmetic Chow groups via the following map:

Definition 3.7. The *arithmetic degree map*

$$\widehat{\deg}\colon \widehat{Z}^1(\mathcal{O}_K) \to \mathbf{R}$$

is defined by

$$\widehat{\deg}\left(\sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p}, (g_\sigma)_\sigma\right) = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \log(\mathcal{N}(\mathfrak{p})) + \sum_\sigma g_\sigma.$$

Proposition 3.8. *The arithmetic degree map induces a homomorphism* $\widehat{\deg}\colon \widehat{\operatorname{CH}}^1(\mathcal{O}_K) \to \mathbf{R}$.

Proof. We need to show that $\widehat{\deg}|_{\widehat{\operatorname{Rat}}^1(\mathcal{O}_K)} = 0$. Let $f \in K^\times$. Then

$$\begin{aligned}\widehat{\deg}(\widehat{\operatorname{div}}(f)) &= \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(f)\log(\mathcal{N}(\mathfrak{p})) + \sum_\sigma(-\log|\sigma(f)|)\\ &= \log\left(\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}}(f)} \prod_\sigma |\sigma(f)|^{-1}\right)\\ &= \log(1) = 0.\end{aligned}$$

Here we have used the *product formula*, which precisely states that $\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}}(f)} \prod_\sigma |\sigma(f)|^{-1} = 1$. This is easily seen for $K = \mathbf{Q}$: the left hand product $\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}}(f)}$ is then nothing but the prime factorization of $|f| \in \mathbf{Q}^\times$, i.e., $\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}}(f)} = \prod_p p^{\operatorname{ord}_p(f)} = |f|$. This of course equals the inverse of $\prod_\sigma |\sigma(f)|^{-1} = |f|^{-1}$, so their product is 1. We will come back to the general product formula when we discuss local fields later on. ☐

Definition 3.9. Let $\widehat{\operatorname{CH}}^1(\mathcal{O}_K)^0$ denote the kernel of the degree map $\widehat{\deg}\colon \widehat{\operatorname{CH}}^1(\mathcal{O}_K) \to \mathbf{R}$.

Exercise 1. In this exercise we will show that the two fundamental theorems of algebraic number theory, namely Dirichlet's unit theorem and the finiteness of the class group, are closely related (in fact equivalent) to the assertion that the group $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)^0$ is compact.

(a) Let $T^0 := \widehat{H}(K)^0/\Gamma_K$. Prove that T^0 is a compact real torus of dimension $r+s-1$.

(b) Show that there is an exact sequence

$$0 \to T^0 \to \widehat{\mathrm{CH}}^1(\mathcal{O}_K)^0 \to \mathrm{Cl}_K \to 0.$$

Use this to show that $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)^0$ is a compact topological group consisting of h_K copies of a torus.

(c) Compute and draw pictures of $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)^0$ for $K = \mathbf{Q}, \mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\theta)$, where $\theta^3 = 11$.

3.1 Functoriality

Let $i\colon K \hookrightarrow L$ be an extension of number fields.

Definition 3.10. The *pullback homomorphism*

$$i^*\colon \widehat{Z}^1(\mathcal{O}_K) \to \widehat{Z}^1(\mathcal{O}_L)$$

is defined as follows:

- For $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$, set $i^*(\mathfrak{p}) = \sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p})\mathfrak{q} \in Z^1(\mathcal{O}_L)$, where $e(\mathfrak{q}/\mathfrak{p})$ is the ramification index. This definition extends by linearity to a homomorphism $i^*\colon Z^1(\mathcal{O}_K) \to Z^1(\mathcal{O}_L)$.
- For $\mathfrak{g} = (g_\sigma)_{\sigma\in\Sigma_K} \in \widehat{H}(K)$ we put $i^*(\mathfrak{g}) = (g_{\tau|_K})_{\tau\in\Sigma_L} \in \widehat{H}(L)$.

This defines the pullback map $i^*\colon \widehat{Z}^1(\mathcal{O}_K) \to Z^1(\mathcal{O}_L)$. In formulas,

$$i^*\left(\sum_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)} a_\mathfrak{p}\mathfrak{p}, (g_\sigma)_{\sigma\in\Sigma_K}\right) = \left(\sum_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)} a_\mathfrak{p}\left(\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p})\mathfrak{q}\right), (g_{\tau|_K})_{\tau\in\Sigma_L}\right).$$

Proposition 3.11. *The map i^* induces a pullback homomorphism*

$$i^*\colon \widehat{\mathrm{CH}}^1(\mathcal{O}_K) \to \widehat{\mathrm{CH}}^1(\mathcal{O}_L)$$

on arithmetic Chow groups.

Proof. We must show that $i^*(\widehat{\mathrm{Rat}}^1(\mathcal{O}_K)) \subseteq \widehat{\mathrm{Rat}}^1(\mathcal{O}_L)$. Let $f \in K^\times$. Then we have

$$\begin{aligned}
i^*(\widehat{\mathrm{div}}_{\mathcal{O}_K}(f)) &= \left(\sum_{\mathfrak{p}} \mathrm{ord}_\mathfrak{p}(f) i^*(\mathfrak{p}), i^*(-\log|\sigma(f)|)_{\sigma\in\Sigma_K}\right) \\
&= \left(\sum_{\mathfrak{p}} \mathrm{ord}_\mathfrak{p}(f)\left(\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p})\mathfrak{q}\right), \left((-\log|\sigma(f)|)_{\tau|_K=\sigma}\right)_{\tau\in\Sigma_L}\right) \\
&= \left(\sum_{\mathfrak{q}} \mathrm{ord}_\mathfrak{q}(f)\mathfrak{q}, (-\log|\tau(f)|)_{\tau\in\Sigma_L}\right) \\
&= \widehat{\mathrm{div}}_{\mathcal{O}_L}(f),
\end{aligned}$$

which shows the claim. □

Definition 3.12. The *pushforward homomorphism*

$$i_*\colon \widehat{Z}^1(\mathcal{O}_L) \to \widehat{Z}^1(\mathcal{O}_K)$$

is defined as follows:

- For $\mathfrak{q} \in \operatorname{Max}(\mathcal{O}_L)$, set $i_*(\mathfrak{q}) = N_{L/K}(\mathfrak{q})$.
- For $\mathfrak{g} = (g_\tau)_{\tau\in\Sigma_L} \in \widehat{H}(L)$, let $i_*(\mathfrak{g}) = (\sum_{\tau|_K=\sigma} g_\tau)_{\sigma\in\Sigma_K}$.

Extending by linearity, this defines the pushforward map $i_*\colon \widehat{Z}^1(\mathcal{O}_L) \to \widehat{Z}^1(\mathcal{O}_K)$. In symbols,

$$i_*\left(\sum_{\mathfrak{q}} a_{\mathfrak{q}}\mathfrak{q}, (g_\tau)_\tau\right) = \left(\sum_{\mathfrak{q}} a_{\mathfrak{q}} N_{L/K}(\mathfrak{q}), \left(\sum_{\tau|_K=\sigma} g_\tau\right)_{\sigma\in\Sigma_K}\right).$$

Proposition 3.13. *The map i_* induces a pushforward homomorphism*

$$i_*\colon \widehat{\mathrm{CH}}^1(\mathcal{O}_L) \to \widehat{\mathrm{CH}}^1(\mathcal{O}_K)$$

on arithmetic Chow groups.

Proof. Exercise. □

Remark 3.14. If you are confused that the pullback is covariant and the pushforward is contravariant, you should keep in mind that secretly we are really considering Chow groups of Spec of the rings of integers, which reverses all the arrows.

Definition 3.15. We set $\widehat{\mathrm{CH}}^0(\mathcal{O}_K) := \mathbf{Z}$.

Moreover, the *arithmetic Chow ring* of $\mathcal{O}_K$ is defined as

$$\widehat{\mathrm{CH}}^*(\mathcal{O}_K) := \widehat{\mathrm{CH}}^0(\mathcal{O}_K) \oplus \widehat{\mathrm{CH}}^1(\mathcal{O}_K) = \mathbf{Z} \oplus \widehat{\mathrm{CH}}^1(\mathcal{O}_K),$$

with multiplication defined by

$$(n_1, d_1)\cdot(n_2, d_2) := (n_1n_2, n_1d_2 + n_2d_1)$$

for any $(n_1, d_1), (n_2, d_2) \in \widehat{\mathrm{CH}}^*(\mathcal{O}_K)$.

Definition 3.16. Let L/K be an extension of number fields, with inclusion $i\colon K \hookrightarrow L$. We extend the pullback and pushforward homomorphisms to the Chow ring by letting $i^*(n, d) = (n, i^*(d))$ for any $(n, d) \in \widehat{\mathrm{CH}}^*(\mathcal{O}_K)$, and $i_*(n', d') = ([L : K]n', i_*(d'))$ for any $(n', d') \in \widehat{\mathrm{CH}}^*(\mathcal{O}_L)$

Proposition 3.17. *Let L/K be an extension of number fields, with inclusion $i\colon K \hookrightarrow L$. Then the following hold:*

(1) The pullback map $i^*\colon \widehat{\mathrm{CH}}^*(\mathcal{O}_K) \to \widehat{\mathrm{CH}}^*(\mathcal{O}_L)$ is a ring homomorphism. Moreover, the composition $i_* \circ i^*$ is multiplication by $[L : K]$.

(2) For any $\alpha \in \widehat{\mathrm{CH}}^*(\mathcal{O}_K)$, $\beta \in \widehat{\mathrm{CH}}^*(\mathcal{O}_L)$, the following projection formula holds:

$$i_*(i^*(\alpha)\cdot\beta) = \alpha \cdot i_*(\beta).$$

Proof. (1) We have

$$\begin{aligned} i^*(n_1,(D_1,\mathfrak{g}_1))\cdot i^*(n_2,(D_2,\mathfrak{g}_2)) &= (n_1n_2, n_1(i^*D_2, i^*\mathfrak{g}_2)+n_2(i^*D_1,i^*\mathfrak{g}_1)) \\ &= i^*(n_1n_2, n_1(D_2,\mathfrak{g}_2)+n_2(D_1,\mathfrak{g}_1)) \\ &= i^*((n_1,(D_1,\mathfrak{g}_1))\cdot(n_2,(D_2,\mathfrak{g}_2))). \end{aligned}$$

For the other statement, use that $N_{L/K}(\mathfrak{a}\mathcal{O}_L)=\mathfrak{a}^{[L:K]}$ for any ideal of $\mathcal{O}_K$.

(2) Write $\alpha=(n_1,(D_1,\mathfrak{g}_1))$ and $\beta=(n_2,(D_2,\mathfrak{g}_2))$. We compute

$$\begin{aligned} i_*(i^*\alpha\cdot\beta) &= i_*(n_1n_2, n_1(D_2,\mathfrak{g}_2)+n_2(D_1,\mathfrak{g}_1)) \\ &= ([L:K]n_1n_2, n_1(i_*D_2, i_*\mathfrak{g}_2)+n_2(i_*i^*D_1, i_*i^*\mathfrak{g}_1)) \\ &= ([L:K]n_1n_2, n_1(i_*D_2, i_*\mathfrak{g}_2)+[L:K]n_2(D_1,\mathfrak{g}_1)) \\ &= (n_1(D_1,\mathfrak{g}_1))\cdot i_*(n_2,(D_2,\mathfrak{g}_2)). \end{aligned}$$

□

4 Replete ideals and the replete ideal class group

Let K be a number field. Recall that we have an isomorphism

$$\mathrm{CH}^1(\mathcal{O}_K)\xrightarrow{\cong}\mathrm{Cl}_K$$

from the Chow group of $\mathcal{O}_K$ to the class group of K. This gives an ideal-theoretic interpretation of the Chow group.

In this section we aim to show a similar comparison result between the arithmetic Chow group $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)$ of $\mathcal{O}_K$, and the so-called *replete ideal class group of* K, $\widehat{\mathrm{Cl}}_K$.

The first step in this direction will be to give meaning to $\widehat{\mathrm{Cl}}_K$—i.e., to define fractional ideals in the setting of Arakelov theory. As is by now a familiar maneuver, this should involve attaching to a fractional ideal data coming from the real and complex embeddings of K.

Definition 4.1. A *replete ideal* of K is a pair $\overline{\mathfrak{a}}=(\mathfrak{a},(r_\sigma)_{\sigma\in\Sigma_K})$ of a fractional ideal $\mathfrak{a}$ of K and a vector $(r_\sigma)_\sigma\in K_{\mathbf{R}}$ such that $r_\sigma\in\mathbf{R}_{>0}$ for all $\sigma\in\Sigma_K$.

We define multiplication of replete ideals componentwise: for $\overline{\mathfrak{a}}=(\mathfrak{a},(r_\sigma)_\sigma)$ and $\overline{\mathfrak{b}}=(\mathfrak{b},(s_\sigma)_\sigma)$, set

$$\overline{\mathfrak{a}}\cdot\overline{\mathfrak{b}}:=(\mathfrak{a}\cdot\mathfrak{b},(r_\sigma\cdot s_\sigma)_\sigma).$$

This defines an abelian group $\widehat{J}_K$ of replete ideals of K.

We can decompose any replete ideal $\overline{\mathfrak{a}}=(\mathfrak{a},(r_\sigma)_\sigma)\in\widehat{J}_K$ as

$$\overline{\mathfrak{a}}=\mathfrak{a}_{\mathrm{f}}\cdot\mathfrak{a}_\infty,$$

where $\mathfrak{a}_{\mathrm{f}}:=(\mathfrak{a},(1)_\sigma)$ is the "finite part" of $\overline{\mathfrak{a}}$, and $\mathfrak{a}_\infty:=((1),(r_\sigma)_\sigma)$ is the "infinite part", or "Archimedean part" of $\overline{\mathfrak{a}}$.

Finally, any element $x\in K^\times$ defines a *replete principal fractional ideal* by $\overline{(x)}:=((x),(|\sigma(x)|^{-1})_\sigma)$. The subgroup of $\widehat{J}_K$ consisting of replete principal fractional ideals is denoted by $\widehat{P}_K$. The quotient group

$$\widehat{\mathrm{Cl}}_K:=\widehat{J}_K/\widehat{P}_K$$

is the *replete ideal class group of* K.

Definition 4.2. Define the map $\widehat{c}_1 \colon \widehat{J}_K \to \widehat{Z}^1(\mathcal{O}_K)$ as

$$\widehat{c}_1(\overline{\mathfrak{a}}) := \left(\sum_{\mathfrak{p}} - \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})\mathfrak{p}, (-\log(r_\sigma))_{\sigma \in \Sigma_K} \right),$$

where $\overline{\mathfrak{a}} = (\mathfrak{a}, (r_\sigma)_{\sigma\in\Sigma_K})$. The element $\widehat{c}_1(\overline{\mathfrak{a}})$ is called the *arithmetic Chern class* of $\overline{\mathfrak{a}}$.

Proposition 4.3. *The homomorphism* $\widehat{c}_1$ *induces an isomorphism* $\widehat{\mathrm{Cl}}_K \xrightarrow{\cong} \widehat{\mathrm{CH}}^1(\mathcal{O}_K)$.

Proof. The map $\widehat{Z}^1(\mathcal{O}_K) \to \widehat{J}_K$ given by

$$\left(\sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p}, (r_\sigma)_{\sigma\in\Sigma_K} \right) \mapsto \left(\prod_{\mathfrak{p}} \mathfrak{p}^{-a_{\mathfrak{p}}}, (e^{-r_\sigma})_{\sigma\in\Sigma_K} \right)$$

is inverse to $\widehat{c}_1$, which induces an isomorphism $\widehat{\mathrm{Rat}}^1(\mathcal{O}_K) \cong \widehat{P}_K$. The result follows. $\square$

The inverse map to $\widehat{c}_1$ appearing in the proof above will be of interest later on, so let us afford treating it with a proper name. It is the Arakelov analog of passing from a divisor to a line bundle on a variety:

Definition 4.4. For any Arakelov divisor $D = (\sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p}, (r_\sigma)_\sigma) \in \widehat{Z}^1(\mathcal{O}_K)$, set

$$\overline{\mathcal{O}(D)} := \left(\prod_{\mathfrak{p}} \mathfrak{p}^{-a_{\mathfrak{p}}}, (e^{-r_\sigma})_{\sigma\in\Sigma_K} \right) \in \widehat{J}_K.$$

In particular, if $D = 0$, the corresponding ideal is $\overline{(1)} = ((1), (1)_{\sigma\in\Sigma_K})$, which we denote by $\overline{\mathcal{O}_K}$.

5 The arithmetic Euler–Minkowski characteristic

In this section we will show the first version of the arithmetic Riemann–Roch theorem, which computes the arithmetic Euler–Minkowski characteristic of replete ideals in terms of the degree of the arithmetic Chern class.

Let $\overline{\mathfrak{a}} = (\mathfrak{a}, (r_\sigma)_\sigma) \in \widehat{J}_K$ be a replete fractional ideal of K. Recall that we can write $\overline{\mathfrak{a}} = \mathfrak{a}_{\mathrm{f}}\mathfrak{a}_\infty$. The finite part $\mathfrak{a}_{\mathrm{f}}$ of $\overline{\mathfrak{a}}$ defines a lattice $j(\mathfrak{a}_{\mathrm{f}})$ in $K_{\mathbf{R}}$ via the embedding $j\colon K \to K_{\mathbf{R}}$. On the other hand, the infinite part $\mathfrak{a}_\infty$ defines a linear endomorphism

$$\mathfrak{a}_\infty \colon K_{\mathbf{R}} \to K_{\mathbf{R}}$$

of $\mathbf{R}$-vector spaces, by $(s_\sigma)_\sigma \mapsto (r_\sigma s_\sigma)_\sigma$.

Definition 5.1. Define a map

$$\widehat{\chi}\colon \widehat{J}_K \to \mathbf{R}$$

by $\widehat{\chi}(\overline{\mathfrak{a}}) := -\log(\mathrm{vol}(\mathfrak{a}_\infty \cdot j(\mathfrak{a}_{\mathrm{f}})))$.

Proposition 5.2. *The map* $\widehat{\chi}(\overline{\mathfrak{a}})$ *depends only on the class of* $\overline{\mathfrak{a}}$ *in* $\widehat{\mathrm{Cl}}_K$.

Proof. Consider another representative $\overline{(a)}\overline{\mathfrak{a}}$ of $[\overline{\mathfrak{a}}]$ in $\widehat{\mathrm{Cl}}_K$. Then $\overline{(a)}\overline{\mathfrak{a}} = a\mathfrak{a}_{\mathrm{f}} \cdot a_\infty \mathfrak{a}_\infty$, where $a_\infty = (|\sigma(a)|^{-1})_\sigma$. Let m_a denote the map $m_a\colon K_{\mathbf{R}} \to K_{\mathbf{R}}$ defined by $(s_\sigma) \mapsto (\sigma(a)s_\sigma)$. We then have $j(a\mathfrak{a}_{\mathrm{f}}) = m_a(j(\mathfrak{a}_{\mathrm{f}}))$ and $\det(m_a) = N_{K/\mathbf{Q}}(a)$. Thus the multiplication by a_∞-map $a_\infty\colon K_{\mathbf{R}} \to K_{\mathbf{R}}$ has determinant $\det(a_\infty) = N_{K/\mathbf{Q}}(a)^{-1}$. Using this, we compute

$$\begin{aligned}
\widehat{\chi}\Big(\overline{(a)}\overline{\mathfrak{a}}\Big) &= -\log(\mathrm{vol}(a_\infty(\mathfrak{a}_\infty(m_a(j(\mathfrak{a}_{\mathrm{f}}))))))\\
&= -\log(\det(a_\infty)\cdot\det(m_a)\,\mathrm{vol}(\mathfrak{a}_\infty\cdot j(\mathfrak{a}_{\mathrm{f}})))\\
&= -\log(N_{K/\mathbf{Q}}(a)\cdot N_{K/\mathbf{Q}}(a)^{-1}\,\mathrm{vol}(\mathfrak{a}_\infty\cdot j(\mathfrak{a}_{\mathrm{f}})))\\
&= \widehat{\chi}(\overline{\mathfrak{a}}).
\end{aligned}$$

□

Definition 5.3. The induced map

$$\widehat{\chi}\colon \widehat{\mathrm{Cl}}_K \to \mathbf{R}$$

is called the *aritmetic Euler–Minkowski characteristic.*

6 Arithmetic Riemann–Roch

We are now in a position to formulate and prove the arithmetic version of the Riemann–Roch theorem. Recall that we have two maps from $\widehat{\mathrm{Cl}}_K$ to $\mathbf{R}$, namely $\widehat{\chi}$ and the composite $\widehat{\deg}\circ\widehat{c}_1$:

$$\begin{array}{ccc}
\widehat{\mathrm{Cl}}_K & \xrightarrow{\widehat{c}_1} & \widehat{\mathrm{CH}}^1(\mathcal{O}_K)\\
{\scriptstyle\widehat{\chi}}\big\downarrow & & \big\downarrow{\scriptstyle\widehat{\deg}}\\
\mathbf{R} & & \mathbf{R},
\end{array}$$

and we may ask to what extent these two maps coincide. This is precisely the Riemann–Roch problem: it turns out that the two maps are equal up to a constant, namely the Euler–Minkowski characteristic of $\overline{\mathcal{O}_K}$. This is the first formulation of the arithmetic Riemann–Roch theorem.

Lemma 6.1. *We have* $\widehat{\chi}(\overline{\mathcal{O}_K}) = -\log(\sqrt{|d_K|})$, *where* d_K *is the discriminant of* K.

Proof. Let $\alpha_1,\dots,\alpha_n$ be an integral basis, and write $\Sigma_K = \{\sigma_1,\dots,\sigma_n\}$. Then the lattice $j(\mathcal{O}_K)$ is spanned by the vectors $(\sigma_1(\alpha_i),\dots,\sigma_n(\alpha_i))$ for $i = 1,\dots,n$, and $\mathrm{vol}(j(\mathcal{O}_K)) = |\det(\sigma_i(\alpha_k)_{i,k})|$. But then the lemma follows, since $d_K = \det(\sigma_i(\alpha_k)_{i,k})^2$. □

Theorem 6.2 (Arithmetic Riemann–Roch for replete ideals)**.** *For any* $\overline{\mathfrak{a}}\in\widehat{\mathrm{Cl}}_K$, *we have*

$$\widehat{\chi}(\overline{\mathfrak{a}}) = \widehat{\deg}(\widehat{c}_1(\overline{\mathfrak{a}})) + \widehat{\chi}(\overline{\mathcal{O}_K}).$$

Proof. We may write $\overline{\mathfrak{a}} = \mathfrak{a}_{\mathrm{f}}\cdot\mathfrak{a}_\infty$ with $\mathfrak{a}_{\mathrm{f}} = \prod_{\mathfrak{p}}\mathfrak{p}^{-a_{\mathfrak{p}}}$ and $\mathfrak{a}_\infty = ((e^{-g_\sigma})_{\sigma\in\Sigma_K})$. Then we have

$$\widehat{\deg}(\widehat{c}_1(\overline{\mathfrak{a}})) = \sum_{\mathfrak{p}} a_{\mathfrak{p}}\log\mathcal{N}(\mathfrak{p}) + \sum_{\sigma} g_\sigma.$$

Consider the sublattice $j(\mathfrak{a}_{\mathrm{f}})$ of $j(\mathcal{O}_K)$. It defines a linear endomorphism $m_{\mathfrak{a}_{\mathrm{f}}}\colon K_{\mathbf{R}}\to K_{\mathbf{R}}$ such that $m_{\mathfrak{a}_{\mathrm{f}}}(j(\mathcal{O}_K)) = j(\mathfrak{a}_{\mathrm{f}})$. Then

$$|\det(m_{\mathfrak{a}_{\mathrm{f}}})| = [j(\mathcal{O}_K) : j(\mathfrak{a}_{\mathrm{f}})] = [\mathcal{O}_K : \mathfrak{a}_{\mathrm{f}}] = \mathcal{N}(\mathfrak{a}_{\mathrm{f}}) = \prod_{\mathfrak{p}}\mathcal{N}(\mathfrak{p})^{-a_{\mathfrak{p}}}.$$

Using this, we compute

$$\begin{aligned}\widehat{\chi}(\overline{\mathfrak{a}}) &= -\log(\mathrm{vol}(\mathfrak{a}_\infty \cdot j(\mathfrak{a}_f))) \\ &= -\log(\mathrm{vol}(\mathfrak{a}_\infty \cdot m_{\mathfrak{a}_f}(j(\mathcal{O}_K)))) \\ &= -\log(\det(\mathfrak{a}_\infty) \cdot \det(m_{\mathfrak{a}_f}) \cdot \mathrm{vol}(j(\mathcal{O}_K))) \\ &= -\log(\det(\mathfrak{a}_\infty)) - \log(\det(m_{\mathfrak{a}_f})) - \log(\mathrm{vol}(j(\mathcal{O}_K))) \\ &= \sum_{\sigma \in \Sigma_K} g_\sigma + \sum_{\mathfrak{p}} a_{\mathfrak{p}} \log(\mathcal{N}(\mathfrak{p})) + \widehat{\chi}(\overline{\mathcal{O}_K}),\end{aligned}$$

which coincides with the right hand side. □

We can also reformulate the above arithmetic Riemann–Roch theorem into a formula more reminiscent of the one we have for Riemann surfaces, i.e.,

$$h^0(D) - h^1(D) = \deg(D) + 1 - g.$$

To this end, we need an analog of the vector space $H^0(D)$. This is done in an entirely analogous manner as in the classical case, but note however that the result will not be a finite dimensional $\mathbf{C}$-vector space, but rather a finite set:

Definition 6.3. Let $D \in \widehat{Z}^1(\mathcal{O}_K)$ be an Arakelov divisor, and write $\overline{\mathcal{O}(D)} = \mathcal{O}(D) \cdot \mathcal{O}(D)_\infty$ for the corresponding replete ideal. We then set

$$H^0(D) := \{f \in K^\times : \widehat{\mathrm{div}}(f) \geq -D\}.$$

Thus, if $D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \mathfrak{p} + (g_\sigma)_\sigma$, then a nonzero rational funciton $f \in K^\times$ lies in $H^0(D)$ if and only if $\mathrm{ord}_{\mathfrak{p}}(f) \geq -a_{\mathfrak{p}}$ for all $\mathfrak{p}$, and $-\log|\sigma(f)| \geq -g_\sigma$ for all $\sigma \in \Sigma_K$.

Proposition 6.4. *The set $H^0(D)$ is finite and depends only on the class of D in $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)$.*

Proof. We have that

$$H^0(D) = \{f \in \mathcal{O}(D) : |\sigma(f)| \leq e^{g_\sigma}\}.$$

Now $j(\mathcal{O}(D))$ is a lattice in $K_{\mathbf{R}}$. Since the subset $\{z = (z_\sigma) \in K_{\mathbf{R}} : |z_\sigma| \leq e^{g_\sigma}\} \subseteq K_{\mathbf{R}}$ is compact, it follows that $j(\mathcal{O}(D))$ is compact and discrete, hence finite. Thus $H^0(D)$ is finite.

Now let $D' = D + \widehat{\mathrm{div}}(g)$ be another representative of $[D]$ in $\widehat{\mathrm{CH}}^1(\mathcal{O}_K)$. Then

$$\begin{aligned}H^0(D') &= \{f \in K^\times : \widehat{\mathrm{div}}(f) \geq -D - \widehat{\mathrm{div}}(g)\} \\ &= \{f \in K^\times : \widehat{\mathrm{div}}(fg) \geq -D\} \\ &= \{g^{-1}h \in K^\times : \widehat{\mathrm{div}}(h) \geq -D\} \\ &= g^{-1}H^0(D) \\ &\cong H^0(D),\end{aligned}$$

where we have used that the map $K^\times \to K^\times$ given by multiplication by g^{-1} induces an bijection $H^0(D) \cong g^{-1}H^0(D)$. □

Exercise 2. Show that $H^0(\overline{\mathcal{O}_K}) = \mu(K)$.

Definition 6.5. Let D be an Arakelov divisor. We define the "dimension" $h^0(D)$ of $H^0(D)$ as follows. If $H^0(D) = \varnothing$, set $h^0(D) := 0$. Otherwise, we define

$$h^0(D) := \log \frac{|H^0(D)|}{2^r(2\pi)^s},$$

where r is the number of real embeddings of K, and s is the number of complex conjugate pairs of complex embeddings of K.

Remark 6.6. The denominator in the definition of $h^0(D)$ is precisely the volume of the set

$$W = \{z = (z_\sigma) \in K_{\mathbf{R}} : |z_\sigma| \leq 1\},$$

and can be thought of as a normalizing factor.

The following definition goes back to Weil:

Definition 6.7. The *genus* of the number field K is

$$g_K := \log \frac{|\mu(K)|\sqrt{|d_K|}}{2^r(2\pi)^s}.$$

Example 6.8. For $K = \mathbf{Q}$ we have $g_{\mathbf{Q}} = 0$.

With this definition, we can reformulate the arithmetic Riemann–Roch theorem as follows:

Theorem 6.9. *For any* $\overline{\mathfrak{a}} \in \widehat{\mathrm{Cl}}_K$*, we have*

$$\widehat{\chi}(\overline{\mathfrak{a}}) = \widehat{\deg}(\widehat{c}_1(\overline{\mathfrak{a}})) + h^0(\overline{\mathcal{O}_K}) - g_K.$$