

Title

D. Zack Garza

Contents

1	Lecture 7: Riemann-Roch	3
1.1	Divisors	3
1.2	The Degree of the Divisor of a Rational Function is Zero	6

1 | Lecture 7: Riemann-Roch

1.1 Divisors

Definition 1.1.1 (Divisor group)

The **divisor group** $\text{Div } K$ is the free \mathbb{Z} -module with basis $\Sigma(K/k)$, so

$$\text{Div } K := \bigoplus_{p \in \Sigma(K/k)} \mathbb{Z}.$$

Thus every $D \in \text{Div } K$ is of the form $D = \sum_{p \in \Sigma(K/k)} n_p p$ where $n_p \in \mathbb{Z}$ and are almost all zero, recalling that a point $p \in \Sigma(K/k)$ is an equivalence class of valuations.

Definition 1.1.2 (Effective Divisor)

A divisor $D = \sum n_p p$ is **effective** iff $n_p \geq 0$ for all p and write $D \geq 0$.

Definition 1.1.3 (Support of a divisor)

The **support** of a divisor D is the set of places $p \in \Sigma(K/k)$ such that $n_p(D) \neq 0$. Note that this is always a finite set, and the zero divisor is the unique divisor supported on \emptyset .

Definition 1.1.4 (Partial order on divisor)

We write $D_1 \leq D_2$ iff $D_2 - D_1 \geq 0$ is effective. Note that this holds iff for all places $p \in \Sigma(K/k)$, if $D_1 = \sum_p m_p p$ and $D_2 = \sum_p n_p p$, then $m_p \leq n_p$ for all p .

This is a partially ordered commutative group, which came up when we were talking about groups of divisibility. It's a reasonable group when studying domains with nice factorization properties: if R is a UFD with a set of principal prime ideals¹ denoted $\Sigma(R)$, then the group of divisibility $G(R)$ is isomorphic to $\bigoplus_{(p) \in \Sigma(R)} \mathbb{Z}$ as a partially ordered commutative group.

There is an analogy: comparing UFDs to Dedekind domains, we trade unique factorization of elements for factorization of ideals, and the group of all fractional ideals in a Dedekind domain is a free commutative group on its set of prime ideals. So $\text{Div } K$ is analogous to the group of divisibility of a UFD and to the group of fractional ideals of a Dedekind domain, the latter of which is the closer analogy. So $\text{Div } K$ is a geometric or projective analog of the group of fractional ideals, and is more than an analogy as we'll see later.

¹Note that primes in a UFD are principal.

Definition 1.1.5 (Degree of a Divisor)

There is a group morphism

$$\deg : \operatorname{Div} K \rightarrow \mathbb{Z}$$

$$D = \sum_p n_p p \mapsto \sum_p n_p \deg p.$$

Its kernel is denoted $\operatorname{Div}^0 K$, the **degree zero divisors**. Note that if $k = \bar{k}$, then $\deg p = 1$ for all p .

Remark 1.1.6: Note that this is similar to the augmentation in a group ring. This construction can be done with any free \mathbb{Z} -module, and makes sense because only finitely many terms are nonzero. Recall that to define the degree of a place $v \in \Sigma(K/k)$, we consider $R_v := \{x \in K \mid v(x) \geq 0\}$ and $\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$, and $k(v) := R_v/\mathfrak{m}_v$ is the residue field. Note that $k(v)$ is a field extension of k by composing $k \hookrightarrow R_v \twoheadrightarrow k(v)$, and we proved used affine grounding and Zariski's lemma that this was a finite degree extension. We can then define $\deg v := [k(v) : k]$. Note that it's more natural to think of valuations v as points p .

Definition 1.1.7 (Index of a divisor)

The **index** of K is defined as

$$I(K) := |\operatorname{coker} \deg|.$$

^a

^aThis quantity made an appearance near the end of Pete's advanced course on elliptic curves.

Remark 1.1.8: Note that $I(K)$ is nonzero, since we can think of $p \in \operatorname{Div} K$ as the divisor with $n_q = 1$ [$q = p$], so the image contains a subset consisting of all degrees of all places, so the image is of the form $d\mathbb{Z}$ for some d . Some other characterizations:

- $\deg(\operatorname{Div} K) = I(K)\mathbb{Z}$, so $I(K)$ is the generator of the degree ideal.
- $I(K)$ is the least positive degree of a divisor on K .
- $I(K) = \gcd\left(\left\{\deg p \mid p \in \Sigma(K/k)\right\}\right)$, i.e. the gcd of the closed points.

The last characterization follows because we have generators of $\operatorname{Div} K$ given by “skyscraper” divisors p where $n_q = 1 \iff p = q$, so the image is the subgroup of \mathbb{Z} generated by the degrees of the points, i.e. the gcd of the degrees.

Exercise 1.1.9(?): Let K/k be a one variable function field.

- Show that if $\Sigma_1(K/k) \neq \emptyset$ then $I(K) = 1$.
- Later we will show that if $|k| < \infty$ then $I(K) = 1$ but $\Sigma_1(K/k)$ may be empty. Try to show this.

c. Show that if $k = \bar{k}$ then $I(K) = 1$.

Remark 1.1.10: (a) follows from the Riemann hypothesis for curves over a finite field, although this is not how you should prove it. It was proved by F.K. Schmidt much earlier in the 20th century, and this is the basic way of understanding the zeta function of a curve.
 (b) says that over a finite ground field, you may not have any degree 1 places. You can try constructing a hyperelliptic curve over a finite field \mathbb{F}_q with no rational points, which is always possible if the genus is large compared to the size of \mathbb{F}_q .

Lemma 1.1.11(?).

For a nonzero rational function $f \in K^\times$ we have $v_p(f) = 0$ for almost every place $p \in \Sigma(K/k)$.

Proof (?).

See previous lecture, in particular [lem:poles_and_zeros].



This says that the set of places for which the valuation is nonzero is finite, so except for finitely many places the valuation is zero. This allows us to define the divisor of a rational function:

$$(\cdot) : K^\times \rightarrow \text{Div } K$$

$$f \mapsto (f) := \sum_p v_p(f)p,$$

which is a group morphism.

Exercise 1.1.12(?): Show that $(f) = 0 \iff f \in \kappa(K)$, which we're assuming is equal to k . This happens when it has neither zeros nor poles, so it's an intersection of all of the R_v , which is the integral closure of k in K . In general, this would mean that f is algebraic over k . So $\ker(\cdot) = k^\times$.

Definition 1.1.13 (Poles and Zeros of Elements of K)

For any $D \in \text{Div } K$ one may uniquely write it as $D = D_+ - D_-$, which are both effective divisors and so $D_+, D_- \geq 0$, and the uniqueness follows from requiring $\text{supp}(D_+) \cap \text{supp}(D_-) = \emptyset$. Note that this is just collecting positive and negative n_p into each term, and leaving out all divisors for which $n_p = 0$.

For $f \in K^\times$, we define

$$(f)_+ := \text{the divisor of zeros of } f$$

$$(f)_- := \text{the divisor of poles of } f,$$

where we can note that $(f) = (f)_+ - (f)_-$.

The next proposition shows that these geometric divisors can be interpreted in terms of \mathbb{F}_q points.

Proposition 1.1.14(?).

Let $f \in K \setminus k$ be transcendental.

a. Let B_0 be the integral closure of $k[f]$ in K , which is an affine Dedekind domain of K ,

i.e. its fraction field is K .^a

Then

$$fB_0 = \prod_{j=1}^r p_j^{a_j} \implies (f)_+ = \sum_{j=1}^r a_j p_j.$$

b. Let B_∞ be the integral closure of $k[1/f]$ in K , which is an affine Dedekind domain of K . Then

$$\left(\frac{1}{f}\right)B_\infty = \prod_{j=1}^s q_j^{b_j} \implies (f)_- = \sum_{j=1}^s b_j q_j.$$

^aAs usual for an extension of Dedekind domains, we push forward an ideal (maybe principal) into its integral closure and see how it factors.

Exercise 1.1.15(?): Prove this proposition.

Remark 1.1.16: This says that pushing forward an ideal and looking at the factorization is precisely what's needed to determine the divisor of zeros. There aren't many new ideas for this proof, the point is that the set of places upstairs is being controlled by mSpec of Dedekind domains.

Slogan 1.1.17: In any affine coordinate chart, the divisor of a function is a principal fractional ideal.

1.2 The Degree of the Divisor of a Rational Function is Zero

Corollary 1.2.1 (*Excruciatingly Important: the degree of the divisor of any rational function is zero.*).

Let $f \in K \setminus k$ be transcendental, then

- a. $\deg(f)_+ = [K : k(f)] = \deg(f)_-$
- b. $\deg(f) = 0$.

Remark 1.2.2: Here think of f as a holomorphic map from a curve to $\mathbb{P}^1_{\mathbb{C}}$, and the degree of this extension is the degree of the corresponding branched cover. For \mathbb{C} , this is literally the cardinality of any finite fibers. Note that (a) follows by symmetry since $k(f) \cong k(1/f)$.

Proof (?).

This comes down to NTI. We know $\deg(f)_+ = \sum_{j=1}^r a_j \deg p_j$. In $K/k(f)$, the places p_1, \dots, p_r all lie over the degree 1 place v_f of $k(f)$. The places where upstairs you have a zero are the places where downstairs is equal to zero, which corresponds to the irreducible polynomial in f given by f itself. Since the residue field at v_f downstairs is

k itself, since it is $k[f]/\langle f \rangle$. So the downstairs places has degree 1, and so the degree of the upstairs places, whatever the residue field is, its degree over k is equal to its degree over the downstairs residue field. Thus the geometric $\deg p_j$ coincides with the residual degree f_i , and a_i is the ramification index in the extension of Dedekind domains $B_0/k[f]$.

So we have a degree equality,

$$\sum_{j=1}^r a_j \deg p_j = \sum e_j f_j = [K : k(f)],$$

where the second equality follows from having an extension of Dedekind domains with this nice finite generation hypothesis. We similarly get $[k : k(f)] = \deg(f)_-$.

Note that part (b) follows immediately, since $(f) = (f)_+ - (f)_-$ implies that

$$\deg(f) = \deg(f)_+ - \deg(f)_- = [k : k(f)] - [k : k(f)] = 0.$$

■

Remark 1.2.3: We have two different things that sound like the degree of a rational function. We define the degree of a rational function $f \in K \setminus k$ as $[K : k(f)]$, otherwise it is the degree (number of sheets) of the corresponding branched covering of \mathbb{P}^1 . But note that we also attached a divisor to f , which may be confusing, be hard to confuse in practice because we found that $\deg(f) = 0$ always.

Definition 1.2.4 (Principal Divisors)

The divisor of a rational function is called **principal**, we define $\text{Prin } K$ to be the group of principal divisors.

Exercise 1.2.5 ($\text{Prin } K$ is a group): For $f, g \in K^\times$, show that

- $(1/f) = -(f)$,
- $(fg) = (f) + (g)$,
- $\text{Prin } K \leq \text{Div}^0 K$ is a subgroup (since we know they're degree zero).

Definition 1.2.6 (Linear Equivalence)

For $D_i \in \text{Div } K$, we set $D_1 \sim D_2 \iff D_1 - D_2 \in \text{Prin } K$, in which case we say these divisors are **linearly equivalent**.

Remark 1.2.7: Near the end of the course we'll see why this is good terminology: it's related to morphisms of projective space attached to linear systems.

Definition 1.2.8 (Divisor Class Group)

We define the **divisor class group** as

$$\mathrm{cl} K := \mathrm{Div} K / \sim = \mathrm{Div} K / \mathrm{Prin} K.$$

But note that there's something between $\mathrm{Prin} K$ and $\mathrm{Div} K$, namely $\mathrm{Div}^0 K$:

Definition 1.2.9 (Degree 0 Divisor Class Group (Important! Fundamental!))

We define the **degree 0 divisor class group** as

$$\mathrm{Cl}^0 K := \mathrm{Div}^0 K / \sim = \mathrm{Div}^0 K / \mathrm{Prin} K.$$

Remark 1.2.10: This is extremely important! Attached to a curve is a Jacobian abelian variety, a nice group variety whose dimension is equal to the genus of the curve, and the k -rational point of the Jacobian will become a commutative group that is isomorphic to $\mathrm{Div}^0 K$.

Exercise 1.2.11(?): Show that we have the following exact sequences:

a.

$$1 \rightarrow k^\times \rightarrow K^\times \xrightarrow{(\cdot)} \mathrm{Prin} K \rightarrow 0.$$

b.

$$0 \rightarrow \mathrm{Cl}^0 K \rightarrow \mathrm{Cl} K \xrightarrow{\deg} I(K)\mathbb{Z} \rightarrow 0.$$

Deduce that $\mathrm{Cl} K \cong \mathrm{Cl}^0 K \oplus \mathbb{Z}$.

Remark 1.2.12: For (a), we saw that rational functions that have zero divisors are constants, assuming that $\kappa(K) = k$. For (b), because principal divisors have degree zero, the degree map factors through the quotient. The deduction comes from that fact that we have a free and hence project \mathbb{Z} -module, yielding a splitting.

Exercise 1.2.13 (Very important, Pete insists that someone solves it!):

a. Show that $\mathrm{Div}^0 k(t) = \mathrm{Prin} k(t)$.

b. Deduce that $\deg : \mathrm{Cl} k(t) \xrightarrow{\sim} \mathbb{Z}$ and $\mathrm{cl}^0 k(t) = 0$.

Remark 1.2.14: Note that $I(K) = 1$ in this case since both the t -adic or ∞ -adic valuation have degree one. Moral: the class groups are not interesting on rational function fields. You have to take a degree zero divisor on a rational function field and build a rational function whose divisor is any given degree. This is extremely useful!

Remark 1.2.15: More general if K/k has genus zero (e.g. a rational function field), then working over \mathbb{C} we would have $\mathrm{Cl}^0 K$ equal to the points of some compact complex Lie group of \mathbb{C} -dimension g , so a large complex torus, unless $g = 0$. So if $k = \bar{k}$, $\mathrm{Cl}^0 K$ will be uncountably infinite when $g > 0$. If not, it might be trivial, or it might be anything in between.

The following result appears in a 1973 paper of Rosen, where he attributes it to F. K. Schmidt. It gives a close relationship between $\text{Cl}^0 K$ and the class groups $\text{Cl } R^S$ of the affine Dedekind domains of K . This shows that instead of $\text{Cl}^0 K$ just being an analogue of the class group of a Dedekind domain, there's almost the same. If you fix K , $\text{Cl}^0 K$ is just one group attached to it, but there are infinitely many R^S since there are infinitely many places. So these groups can not be equal, since we could change the size of S to obtain overrings of Dedekind domains, where the resulting class groups are quotients. So you could kill finitely many elements in the class group of the Dedekind domain by just passing to an overring by adding finitely more places.

Theorem 1.2.16 (Rosen).

Let $S \subset \Sigma(K/k)$ be nonempty and finite, and recall that the holomorphy ring was defined as

$$R^S = \cap_{v \in \Sigma(K/k)} R_v.$$

Define the following:

- $D^0(S)$: the degree 0 divisors with support in S .
- $P(S) := \text{Prin } K \cap D^0(S)$, the principal divisors supported in S .
 - Divisors of rational functions all of whose zeros and poles lie in S .
- d_S : The least positive degree of a divisor supported on S .
 - Note that this is different to the index in that we restrict to S , and is thus a multiple of $I(K)$.

Then there is an exact sequence

$$0 \rightarrow D^0(S)/P(S) \xrightarrow{\iota} \text{Cl}^0 K \xrightarrow{\alpha} \text{Cl } R^S \xrightarrow{\beta} C(d/I(K)) \rightarrow 0.$$

Proof (?).

See NTII, Theorem 3.27. ■


Remark 1.2.17: Note that the kernel $D(S)/P(S)$ could be infinite but is always finitely generated. The map α is induced by

$$\alpha' : \text{Div } K \rightarrow \text{Frac } R^S$$

$$\sum n_p p \mapsto \prod_{p \in \text{mSpec } R^S} p^{n_p},$$

where we note that $\text{mSpec } R^S \subset \Sigma(K/k)$, and in fact $\Sigma(K/k) = \text{mSpec } R^S \amalg S$. We can do this because if p is already in $\text{maxSpec } R^S$, we raise it to an appropriate power, and otherwise, for the finitely many $p \in S$ we just get rid of them. But this kills off some elements, namely those things supported in S , hence the kernel in the exact sequence.

Note that the last group appearing is finite cyclic of order $d/I(K)$. If you just looked at $D^0(S)$

before modding out by principal divisors, if you didn't impose degree zero, the subgroup would be isomorphic to $\mathbb{Z}^{|S|}$. But there's a linear condition that the degree is equal to zero, which cuts down the dimension by 1, yielding $\mathbb{Z}^{|S|-1}$. It's hard to say how much $P(S)$ is cutting down the size. 

Remark 1.2.18: The moral is that there is a map, but the kernel and cokernel both depend on S . If you understand $\text{Cl}^0 K$, however, you have a good handle on all $\text{Cl} R^S$. 