

In this lecture (and henceforth)  $k$  denotes a perfect but not necessarily algebraically closed field, and  $\bar{k}$  denote a fixed algebraic closure of  $k$ .

### 19.1 Curves and function fields

Henceforth we adopt the following definitions.

**Definition 19.1.** A *curve*  $C/k$  is a smooth projective variety of dimension one defined over  $k$ . A *function field*  $F/k$  is a finitely generated extension of  $k$  with transcendence degree one, such that  $k$  algebraically closed in  $F$ .

Other authors distinguish the curves we have defined as *nice curves*: one-dimensional varieties that are smooth, projective, and geometrically irreducible (irreducible over  $\bar{k}$ ); for us varieties are geometrically irreducible by definition, so this last requirement is automatic. But perhaps a more fundamental characterization is that nice curves are isomorphic to the abstract curve defined by their function field.

In our definition of a function field, the requirement that  $k$  be algebraically closed in  $F$  is not a serious restriction, it is automatically satisfied when  $F$  is the function field of a curve  $C/k$ , so it is necessary for us to obtain the following equivalence of categories.<sup>1</sup>

**Theorem 19.2.** *The category of curves  $C/k$  with nonconstant morphisms and the category of function fields  $F/k$  with field homomorphisms that fix  $k$  are contravariantly equivalent under the functor that sends a curve  $C$  to the function field  $k(C)$  and a nonconstant morphism of curves  $\phi: C_1 \rightarrow C_2$  defined over  $k$  to the field homomorphism  $\phi^*: k(C_2) \rightarrow k(C_1)$  defined by  $\phi^*f = f \circ \phi$ .*

*Proof.* For  $k = \bar{k}$  this follows from: (1) a nonconstant morphism of smooth projective curves is surjective (Corollary 18.7), (2) a smooth projective curve is isomorphic to the abstract curve defined by its function field (Theorem 18.10). The inverse functor sends  $F/k$  to the smooth projective curve isomorphic to the abstract curve defined by  $F/k$  (Theorem 18.13), which is unique up to isomorphism (Corollary 18.8).

For  $k \neq \bar{k}$ , recall from Lecture 15 that if  $C_1$  is defined over  $k$  and the morphism  $\phi: C_1 \rightarrow C_2$  is defined over  $k$  then the induced morphism of function fields  $\bar{k}(C_2) \rightarrow \bar{k}(C_1)$  restricts to a morphism  $k(C_2) \rightarrow k(C_1)$ . Conversely, given a function field  $F/k$  with  $k$  a perfect field, by Theorem 17.8 and Remark 17.9, we can write  $F = k(x, \alpha)$ , with  $\alpha$  algebraic over the rational function field  $k(x)$ . If we then consider the minimal polynomial of  $\alpha$  as an element of  $k(x)[y]$  and clear denominators in the coefficients, we obtain an irreducible polynomial  $f \in k[x, y]$ . Because  $k$  is algebraically closed in  $F$ , this polynomial remains irreducible as an element of  $\bar{k}[x, y]$  (by [1, III.3.6.8]), and therefore defines an affine variety of dimension one in  $\mathbb{A}^2$  whose ideal is generated by  $f \in k[x, y]$ . We may then take  $C/k$  to be the (projective) desingularization of this affine variety, which is still defined over  $k$ .<sup>2</sup>  $\square$

<sup>1</sup>This follows from [1, III.3.6.8] which implies that  $F/k$  is the function field of some curve  $C/k$  if and only if  $k$  is algebraically closed in  $F$  (we can always use  $F$  to construct an algebraic set, but if  $k$  is not algebraically closed in  $F$  this set will not be irreducible (over  $\bar{k}$ ), hence not a variety).

<sup>2</sup>The fact that the desingularization is defined over  $k$  is not obvious from our proof of its existence, but it can be proved by other means (the assumption that  $k$  is perfect is necessary).

From Theorem 19.2 we see that the study of curves and the study of function fields are one and the same, a fact that we shall frequently exploit by freely moving between the two categories. It is worth noting that this categorical equivalence does not hold for varieties of dimension greater than one.

**Definition 19.3.** The *degree* of a morphism of curves  $\phi: C_1 \rightarrow C_2$  is the degree of the corresponding extension of function fields  $\deg \phi = [k(C_1) : \phi^*(k(C_2))]$ .

**Remark 19.4.** A note of caution. Since the field homomorphism  $\phi^*: k(C_2) \rightarrow k(C_1)$  is necessarily injective, it is standard practice to identify  $k(C_2)$  with its image in  $k(C_1)$ . Under this convention, one may then write  $\deg \phi = [k(C_1) : k(C_2)]$ . But the notation  $[L : K]$  for the degree of a field extension  $L/K$  is ambiguous if  $K$  is simply a field embedded in  $L$ , rather than an actual subfield. Without knowing the embedding, there is in general no way to know what  $[L : K]$  actually is!

This does not cause a problem for number fields, but function fields are another story; there are many different ways to embed one function field into another, and different embeddings may have different degrees. As a simple example, consider the map  $\varphi: k(x) \rightarrow k(x)$  that sends  $x$  to  $x^2$  and fixes  $k$ . The image of  $\varphi$  is a proper subfield of  $k(x)$  (namely,  $k(x^2)$ ) which is isomorphic to  $k(x)$  but not equal to  $k(x)$  as a subfield. Indeed, as a  $k(x^2)$ -vector space,  $k(x)$  has dimension 2, and we have  $[k(x) : \varphi(k(x))] = \deg \varphi = 2$  as expected. But if we identify  $k(x)$  with its image  $\varphi(k(x))$  then we would write  $[k(x) : k(x)] = 2$ , which is confusing to say the least.

**Corollary 19.5.** *A morphism of curves is an isomorphism if and only if its degree is one.*

## 19.2 Divisors

**Definition 19.6.** Let  $C/k$  be a curve with  $k = \bar{k}$ . A *divisor* of  $C$  is a formal sum

$$D := \sum_{P \in C} n_P P$$

with  $n_P \in \mathbb{Z}$  and all but finitely many  $n_P = 0$ . The set of points  $P$  for which  $n_P \neq 0$  is called the *support* of  $D$ . The divisors of  $C$  form a free abelian group under addition, the *divisor group* of  $C$ , denoted  $\text{Div } C$ .

**Definition 19.7.** Let  $F/k$  be a function field with  $k = \bar{k}$ . A *divisor* of  $F$  is a formal sum

$$D := \sum_{P \in X_F} n_P P$$

with  $n_P \in \mathbb{Z}$  and all but finitely many  $n_P = 0$ . Here  $X_F$  denotes the abstract curve defined by  $F/k$ , whose points  $P$  are the maximal ideals of the discrete valuation rings of  $F/k$ . The divisors of  $F$  form a free abelian group  $\text{Div } F$  under addition; if  $C$  is the smooth projective curve with function field  $F$ , this group is isomorphic to  $\text{Div } C$  and we may use them interchangeably.

We now want to generalize to the case where  $k$  is not necessarily algebraically closed. Let  $G_k = \text{Gal}(\bar{k}/k)$  be the absolute Galois group of  $k$  (as usual  $\bar{k}$  is a fixed algebraic closure).

**Definition 19.8.** A divisor  $D = \sum n_P P \in \text{Div } C$  is *defined over  $k$*  if for all  $\sigma \in G_k$  we have  $D^\sigma = D$ , where

$$D^\sigma = \left( \sum n_P P \right) = \sum n_P P^\sigma.$$

The subset of  $\text{Div } C$  defined over  $k$  forms the subgroup of  *$k$ -rational divisors*.

Note that  $D = D^\sigma$  does not necessarily imply  $P = P^\sigma$  for all  $P$  in the support of  $D$ . But if  $D = D^\sigma$  for all  $\sigma \in G_k$ , then it must be the case that  $n_{P^\sigma} = n_P$  for all  $\sigma \in G_k$ . Thus we can group the terms of a  $k$ -rational divisor into  $G_k$ -orbits with a single coefficient  $n_P$  applied to all the points in the orbit. Equivalently, we can view a  $k$ -rational divisor as a sum over  $G_k$ -orbits of points  $P \in C(\bar{k})$ . This turns out to be a better way of defining the group of  $k$ -rational divisors on a curve that is defined over  $k$ .

**Definition 19.9.** Let  $C/k$  be a curve defined over  $k$ . The  $G_k$ -orbits of  $C(\bar{k})$  are called *closed points*, which we also denote by  $P$ . A *rational divisor* of  $C/k$  is a formal sum

$$D := \sum n_P P$$

where  $P$  ranges over the closed points of  $C/k$ , with  $n_P \in \mathbb{Z}$  and all but finitely many  $n_P = 0$ . The group of rational divisors on  $C$  is denoted  $\text{Div}_k C$ .

For function fields  $F/k$  the divisor class group is defined exactly as when  $k = \bar{k}$ . As before,  $X_F$  is the set of maximal ideals of discrete valuation rings of  $F/k$ , which we shall henceforth call *places* of  $F/k$  in order to avoid confusion. The places of  $F/k$  are in one-to-one correspondence with the closed points of the corresponding curve  $C/k$ . In the case that  $k = \bar{k}$  this follows from the *Nullstellensatz*, each point  $P$  on  $C$  is the zero locus of a place of  $F/k$  (the maximal ideal  $m_P$ ), and vice versa. When  $k$  is not algebraically closed the same statement still holds, provided we replace “point” with “closed point”. To see this, just apply the action of  $G_k$  to a point  $P \in C(\bar{k})$  and its corresponding maximal ideal  $M_P \in \bar{k}[x_1, \dots, x_n]$ ; the  $G_k$ -orbit of  $P$  is a closed point of  $C/k$  and the intersection of  $k[x_1, \dots, x_n]$  with the union of the ideals in the  $G_k$ -orbit of  $M_P$  is a maximal ideal of  $k[x_1, \dots, x_n]$  whose reduction modulo  $I(C)$  is a place of  $F/k$ .

**Remark 19.10.** Be sure not to confuse the closed points of  $C/k$  with the set of rational points  $C(k)$ . The points in  $C(k)$  correspond to a proper subset of the set of closed points, the trivial  $G_k$ -orbits that consist of a single element. But every point in  $C(\bar{k})$  is contained in a closed point of  $C/k$ . Indeed, this is the key advantage to working with closed points; they contain all the essential information about  $C/k$  (even in cases where  $C(k)$  is empty), while allowing us to work over  $k$  rather than  $\bar{k}$ , which has both theoretical and practical advantages. But it is important to remember that the set of closed points depends on the ground field  $k$ , not just  $C$ . We will consistently write  $C/k$  to remind ourselves of this fact. In more advanced treatments one writes  $C_k$  and regards  $C_k$  and  $C_{k'}$  as distinct objects for any extension  $k'/k$ , even when the equations defining  $C$  are exactly the same; switching from  $C_k$  to  $C_{k'}$  is known as *base extension*.

**Definition 19.11.** Let  $f$  be a nonzero element of a function field  $F/k$ . The *divisor of  $f$*  is

$$\text{div } f := \sum_{P \in X_F} \text{ord}_P(f) P.$$

Such divisors are said to be *principal*.<sup>3</sup>

<sup>3</sup>The principal divisor  $\text{div } f$  is also often denoted by  $(f)$ , but we will not use this notation.

In order for the definition above to make sense, we need to know that  $\text{ord}_P(f)$  is zero for all but finitely many  $P$ . Under our categorical equivalence, we can assume that  $F = k(C)$  for some curve  $C/k$ , which makes this easy to prove. Note that for any closed point, a function  $f \in k(C)$  vanishes at a point  $P \in C(\bar{k})$  if and only if it vanishes on the entire  $G_k$ -orbit of  $P$ . Thus it makes sense to say whether a closed point  $P$  of  $C/k$  lies in the zero locus of  $f$  or not.

**Theorem 19.12.** *Let  $F/k$  be a function field. For any  $f \in F^\times$  we have  $\text{ord}_P(f) = 0$  for all but finitely many places  $P$  of  $F$ .*

*Proof.* Let  $C$  be the smooth projective curve with function field  $k(C) \simeq F$ , and let us identify  $F$  with  $k(C)$ . Let  $f$  be a nonzero element of the coordinate ring  $k[C]$ . We then have  $\text{ord}_P(f) = 0$  unless the closed point  $P$  lies in the zero locus of  $f$ . But the zero locus of  $f$  is a closed set properly contained in the one-dimensional variety  $C$  (since  $f \neq 0$ ), hence finite. The general case  $f = g/h \in k(C)$  is similar, now  $\text{ord}_P(f) = 0$  unless  $P$  is in the zero locus of either  $g$  or  $h$ , both of which are finite.  $\square$

A sum of principal divisors is a principal divisor, since

$$\text{div } f + \text{div } g = \text{div } fg$$

(this follows from the fact that each  $\text{ord}_P: k(C)^\times \rightarrow \mathbb{Z}$  is a homomorphism). We also have  $\text{div } 1 = 0$ , thus the map  $k(C)^\times \rightarrow \text{Div}_k C$  defined by  $f \mapsto \text{div } f$  is a group homomorphism. Its image is  $\text{Princ}_k C$ , the group of  $k$ -rational principal divisors of  $C$ .

**Definition 19.13.** Let  $C/k$  be a curve. The quotient group

$$\text{Pic}_k C := \text{Div}_k C / \text{Princ}_k C$$

is the *Picard group* of  $C$  (also known as the *divisor class group* of  $C$ ). Elements  $D_1$  and  $D_2$  of  $\text{Div}_k C$  that have the same image in  $\text{Pic}_k C$  are said to be *linearly equivalent*. We write  $D_1 \sim D_2$  to indicate this equivalence.

**Theorem 19.14.** *We have an exact sequence*

$$1 \rightarrow k^\times \rightarrow k(C)^\times \xrightarrow{\text{div}} \text{Div}_k C \rightarrow \text{Pic}_k C \rightarrow 0.$$

*Proof.* The only place where exactness is not immediate from the definitions is at  $k(C)^\times$ ; we need to show that  $\ker \text{div} = k^\times$ . It is clear that  $k^\times$  lies in  $\ker \text{div}$ ; any  $f \in k^\times$  lies in the unit group of every discrete valuation ring of  $k(C)/k$ , in which case  $\text{ord}_P(f) = 0$  for all  $P$ . Equality follows from the fact that  $k$  is algebraically closed in  $k(C)$ . This means that  $k$  is equal to the full field of constants of the function field  $k(C)/k$ , which is precisely the intersection of the unit groups of all the valuation rings of  $k(C)/k$ , equivalently, the set of functions  $f \in k(C)$  for which  $\text{ord}_P(f) = 0$  for all  $P$  (another way to see this is to note that if  $f$  is nonzero on every closed point of  $C/k$ , then the zero locus of  $f$  is the empty set and therefore  $f$  is a unit in the coordinate ring).  $\square$

**Definition 19.15.** For a principal divisor  $\text{div } f = \sum n_P P$ , the divisors

$$\text{div}_0 f = \sum_{n_P > 0} n_P P \quad \text{and} \quad \text{div}_\infty f = \sum_{n_P < 0} -n_P P$$

are called the *divisor of zeros* and the *divisor of poles* of  $f$ , respectively. We have

$$\text{div } f = \text{div}_0 f - \text{div}_\infty f.$$

The quantities  $\deg \operatorname{div}_0 f$  and  $\deg \operatorname{div}_\infty f$  count the zeros and poles of  $f$ , with appropriate multiplicities. While it is intuitively clear that these two quantities should be equal (recall that we can represent  $f$  as the ratio of two homogeneous polynomials of the same degree), to prove this rigorously we will establish a more general result that tells us that the fibers (inverse images) of a morphism of curves  $\phi$  all have cardinality equal to  $\deg \phi$ , provided that we count the points in each fiber with the correct multiplicities.

**Remark 19.16.** In what follows we work exclusively with morphisms  $\phi: C_1 \rightarrow C_2$  defined over  $k$ , by which we mean that both the curves *and the morphism* are over  $k$ . There are situations where one does want to consider morphisms that are not defined over  $k$  (even though the curves are defined over  $k$ ), but in order to keep things simple we will not consider this at this stage (we can always base extend to a field where everything is defined).

**Lemma 19.17.** *Let  $\phi: C_1 \rightarrow C_2$  be a morphism of curves defined over  $k$  and let  $P$  be a closed point of  $C_1/k$ . Then  $\phi(P)$  is a closed point of  $C_2/k$ .*

*Proof.* Let  $P$  be the  $G_k$ -orbit  $\{P_1, \dots, P_d\}$ , where  $d = \deg P$ . We have  $\phi(P_i)^\sigma = \phi(P_i^\sigma)$  for all  $\sigma \in G_k$ , since  $\phi$  is defined over  $k$ , and it follows that the set  $\phi(P) = \{\phi(P_1), \dots, \phi(P_d)\}$  is fixed by  $G_k$ , hence a union of  $G_k$ -orbits. For each  $P_i$  we have  $P_i = P_1^\sigma$  for some  $\sigma \in G_k$ , and it follows that  $\phi(P_i) = \phi(P_1^\sigma) = \phi(P_1)^\sigma$ , so every  $\phi(P_i)$  is in the  $G_k$ -orbit of  $\phi(P_1)$ , so  $\phi(P)$  consists of a single  $G_k$ -orbit and is a closed point.  $\square$

With Lemma 19.17 in hand, we can now sensibly speak of a morphism  $\phi: C_1 \rightarrow C_2$  defined over  $k$  as a map of closed points.

**Definition 19.18.** Let  $\phi: C_1 \rightarrow C_2$  be a morphism defined over  $k$ , and  $\phi^*: k(C_2) \rightarrow k(C_1)$  the corresponding morphism of function fields. The *ramification index* (also called the *ramification degree*) of  $\phi$  at a closed point  $P$  of  $C_1$  (equivalently, a place  $P$  of  $k(C_1)$ ) is

$$e_\phi(P) := \operatorname{ord}_P(\phi^* t_Q),$$

where  $t_Q \in k(C_2)$  is a uniformizer at  $Q = \phi(P)$ , that is, a generator for the place  $Q$  of  $k(C_2)$ . If  $e_\phi(P) = 1$ , then  $\phi$  is *unramified at  $P$* , and if  $e_\phi(P) = 1$  for all closed points  $P$  of  $C_1/k$  we say that  $\phi$  is *unramified*.

**Definition 19.19.** Let  $\phi: C_1 \rightarrow C_2$  be a morphism defined over  $k$ . The *pullback map*  $\phi^*$  on divisors is the homomorphism  $\phi^*: \operatorname{Div}_k C_2 \rightarrow \operatorname{Div}_k C_1$  defined by

$$\phi^*(Q) := \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P,$$

where  $(Q)$  denotes the divisor in  $\operatorname{Div}_k C_2$  with support  $\{Q\}$  and  $n_Q = 1$ . We also define the *pushforward map*  $\phi_*$  on divisors as the homomorphism  $\phi_*: \operatorname{Div} C_1 \rightarrow \operatorname{Div} C_2$  defined by

$$\phi_*(P) = [k(P) : \phi^*(k(P))] \phi(P) = \frac{\deg P}{\deg \phi(P)} \phi(P).$$

When  $k = \bar{k}$  is algebraically closed, the pushforward map just sends the divisor  $(P)$  to the divisor  $(\phi(P))$ , but in general we want to scale things so that  $\deg \phi_*(P) = \deg P$ .

It is clear that both  $\phi^*$  and  $\phi_*$  are group homomorphisms, and if  $\phi$  is unramified then for all divisors  $D$  we have

$$\phi_*(\phi^*(D)) = \deg(\phi)D.$$

You will prove on the problem set that in fact this is true regardless; the composition  $\phi_* \circ \phi^*$  corresponds to multiplication by  $\deg(\phi)$  on  $\text{Div}_k C_2$ .

**Remark 19.20.** Using  $\phi^*$  to denote both the pullback map  $\text{Div}_k C_2 \rightarrow \text{Div}_k C_1$  and the dual morphism  $k(C_2) \rightarrow k(C_1)$  of function fields induced by  $\phi: C_1 \rightarrow C_2$  might seem like an unfortunate collision of notation, but it is standard and intentional. Recall that the kernel of the divisor map  $\text{div}: C \rightarrow \text{Div}_k C$  is just  $k^\times$ , so up to scalars we can identify a function  $f \in k(C)$  with the corresponding divisor  $\text{div} f \in \text{Div}_k C$ . The pullback map  $\phi^*$  maps principal divisors to principal divisors, thus for any  $f, g \in k(C_2)^\times$  we have

$$\phi^* \text{div} f = \phi^* \text{div} g \iff \phi^* f = \lambda \phi^* g \text{ for some } \lambda \in k^\times.$$

**Definition 19.21.** Let  $C/k$  be a curve and let  $F/k$  be the corresponding function field. If  $P$  is a closed point of  $C/k$ , or a place of  $F/k$ , we define the *degree* of  $P$  to be the dimension of the *residue field*  $k(P) = \mathcal{O}_P/m_P$  over  $k$  (where  $m_P = P$  if  $P$  is a place of  $F/k$ ), that is,

$$\deg P := [k(P) : k].$$

Equivalently,  $\deg P$  is the cardinality of the closed point  $P$  as a  $G_k$ -orbit of points in  $C(\bar{k})$  (see [1, Cor. 3.6.5] for a proof of this equivalence, which depends on the fact that  $k$  is a perfect field). The degree of a divisor  $D = \sum n_P P$  in the group of  $k$ -rational divisors is

$$\deg D := \sum n_P \deg P.$$

Note that when  $k = \bar{k}$ , we have  $\deg P = 1$  for all  $P$ , so in this case  $\deg D = \sum n_P$ .

**Theorem 19.22.** *Let  $\phi: C_1 \rightarrow C_2$  be a morphism of curves defined over  $k$ . Then for each closed point  $Q$  of  $C_2/k$ ,*

$$\deg \phi^*(Q) = \deg \phi \deg Q$$

Here  $\phi^*$  is the pullback map on divisors. This theorem effectively says that the fibers (inverse images of points) of the morphism  $\phi$  all have cardinality equal  $\deg \phi$ , provided that we count them correctly. Our definition of the degree of a divisor accounts for the size of the Galois orbit corresponding to a closed point (so we are effectively counting  $\bar{k}$ -points on both sides), and the ramification index  $e_\phi$  incorporated in the definition of the pullback map  $\phi^*$  correctly accounts for ramification.

We will prove Theorem 19.22 in the next lecture. Let us end this lecture by proving that any nonzero function on a curve has the same number of zeros and poles. The proof is essentially immediate from the definitions; in an advanced text it might be written in one line or simply left to the reader. But we will take the time to unravel all the definitions in gory detail, as this provides an excellent opportunity to check our understanding.

**Corollary 19.23.** *Let  $f \in k(C)^\times$  for some curve  $C/k$ . Then  $f$  has the same number of zeros and poles (counted with multiplicity), that is,*

$$\deg \text{div}_0 f = \deg \text{div}_\infty f.$$

*If  $f \in k^\times$  then this number is 0, and otherwise it is equal to  $[k(C) : k(f)]$ . In any case, we always have  $\deg \text{div} f = 0$ .*

*Proof.* For  $f \in k^\times$  we have  $\text{div } f = 0$  and the corollary holds. Otherwise  $f$  is transcendental over  $k$  (because  $k$  is algebraically closed in  $k(C)$ ), and it defines a morphism  $f: C \rightarrow \mathbb{P}^1$  as follows: if  $f = g/h$  with  $g, h \in k[C]$  represented by homogeneous functions of the same degree, with  $h$  nonzero, then the morphism  $f$  is given by  $(g : h)$ .<sup>4</sup> Recall that this represents an equivalence class of tuples that we can scale by any  $\lambda \in k(C)^\times$ .

Let  $(x : y)$  be homogeneous coordinates for  $\mathbb{P}^1$ , and define  $0 = (0 : 1)$  and  $\infty = (1 : 0)$ . Note that  $0$  and  $\infty$  are both rational points on  $\mathbb{P}^1$ , hence we may identify them with the corresponding closed points (they are each the unique element of their  $G_k$ -orbit).

The place of  $k(\mathbb{P}^1)$  corresponding to the closed point  $0$  is (the maximal ideal of) the discrete valuation that measures the order of vanishing of a homogeneous rational function  $r(x, y)$  at  $(0 : 1)$ , equivalently, it measures the order of vanishing of  $r(x/y, 1)$  at  $0/1$ . Similarly, the place corresponding to  $\infty$  measures the order of vanishing of  $r(x/y, 1)$  at  $1/0$ , equivalently, the order of vanishing of  $r(1, y/x)$  at  $0/1$ .

The obvious choice of uniformizers for the places  $0$  and  $\infty$  are the functions  $t_0 = x/y$  and  $t_\infty = y/x$ . The images of these uniformizers under the field embedding  $f^*: k(\mathbb{P}^1) \rightarrow k(C)$  induced by  $f$  are, by definition,

$$\begin{aligned} f^*t_0 &= t_0 \circ f = g/h = f, \\ f^*t_\infty &= t_\infty \circ f = h/g = 1/f. \end{aligned}$$

Now let us consider a closed point  $P$  of  $C$  for which  $f(P) = 0$  (so  $f(P') = 0$  for any/all points  $P'$  in the  $G_k$ -orbit  $P$ ). The ramification index of  $f$  at  $P$  is, by definition,

$$e_f(P) = \text{ord}_P(f^*t_0) = \text{ord}_P(f).$$

If we instead consider a closed point  $P$  of  $C$  for which  $f(P) = \infty$ , we then have

$$e_f(P) = \text{ord}_P(f^*t_\infty) = \text{ord}_P(1/f) = -\text{ord}_P(f).$$

Applying the pullback map  $f^*: \text{Div}_k \mathbb{P}^1 \rightarrow \text{Div}_k C$  to the divisor  $(0)$  yields<sup>5</sup>

$$f^*(0) = \sum_{f(P)=0} e_f(P)P = \sum_{f(P)=0} \text{ord}_P(f)P.$$

But notice that the places  $P$  of  $k(C)$  where  $f$  has positive valuation correspond exactly to the closed points  $P$  of  $C/k$  where  $f(P) = 0$  (hence we use the same symbol  $P$  in both cases). Thus, by definition,

$$f^*(0) = \sum_{f(P)=0} \text{ord}_P(f)P = \text{div}_0 f$$

Similarly, the places where  $f$  has negative valuation are those where  $f(P) = \infty = (1 : 0)$ , equivalently,  $(1/f)(P) = 0 = (0 : 1)$ . Thus

$$f^*(\infty) = \sum_{f(P)=\infty} e_f(P)P = \sum_{f(P)=\infty} -\text{ord}_P(f)P = \text{div}_\infty f.$$

<sup>4</sup>How do we know  $f$  is a morphism? Because every rational map from a (smooth projective) curve to a projective variety is a morphism; see Corollary 18.7.

<sup>5</sup>Note that this is not the zero element of  $\text{Div}_k C$ , which is the divisor whose support is the empty set. The divisor  $(0)$  has support  $\{0\}$ .

Applying Theorem 19.22 to  $f: C \rightarrow \mathbb{P}^1$  with  $Q = 0$  and  $Q = \infty$  (both of which have degree one, since they are rational points), we have

$$\deg \operatorname{div}_0 f = \deg f^*(0) = \deg f \deg 0 = \deg f = \deg f \deg \infty = \deg f^*(\infty) = \deg \operatorname{div}_\infty f,$$

where  $\deg f = [k(C) : f^*(k(\mathbb{P}^1))]$  is the degree of  $f$  as a morphism.<sup>6</sup> We know that  $k(\mathbb{P}^1)$  is isomorphic to the field of rational functions  $k(t)$ , thus the image of  $f^*: k(\mathbb{P}^1) \rightarrow k(C)$  is completely determined by the image of  $t$  (since  $f$  must fix  $k$ ), and we have  $f^*(t) = t \circ f = f$ , so  $\deg f = [k(C) : k(f)]$ . Finally, we note that

$$\deg \operatorname{div} f = \deg(\operatorname{div}_0 f - \operatorname{div}_\infty f) = \deg \operatorname{div}_0 f - \deg \operatorname{div}_\infty f = 0$$

as claimed. □

## References

- [1] H. Stichtenoth, *Algebraic function fields and codes*, Springer, 2009.

---

<sup>6</sup>This is almost certainly *not* the degree of the homogeneous polynomials  $g$  and  $h$  we chose to represent  $f$ . These were chosen arbitrarily and could have any degree; they are only defined modulo the equivalence relation on rational maps and modulo the ideal  $I(C)$  in any case.

MIT OpenCourseWare  
<http://ocw.mit.edu>

FÌ ÈÌ GQd[ à ~ &ç } Áí ÁEã@ ^ çãÖ^ [ { ^d^  
0æ| 201H

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.