14. Lecture 14 (Mar 17): Divisors

Recommended reading: Hartshorne II.6, Kempf 5.5.

14.1. Overview

Let X be an algebraic set (over our algebraically closed field k). We shall work under the following simplifying assumptions:

X is a smooth variety (separated and irreducible).

(See Remark 14.3.7 below for a brief discussion what needs to be changed if we relax these conditions.) The assumption implies that the local rings $\mathcal{O}_{X,x}$ (or more generally the stalks $\mathcal{O}_{X,Z}$ for irreducible $Z \subseteq X$) are regular. Since regular rings are UFDs (as already mentioned in Lecture 6, §6.2), they are integrally closed, and hence for every non-empty affine $U \subseteq X$, the algebra $\mathcal{O}(U)$ is an integrally closed domain. For a big portion of the remainder of the course we shall be interested in the special case X being a smooth and projective curve, in which case the local rings are $\mathcal{O}_{X,x}$ are discrete valuation rings, and the algebras $\mathcal{O}(U)$ for $U \subseteq X$ non-empty affine are Dedekind domains.

A **prime divisor** on X is a codimension one irreducible closed subscheme $D \subseteq X$ (if X is a curve, this means D is simply a point of X). The local ring (see Lecture 5, Definition 5.5.1) $\mathcal{O}_{X,D}$ is then a discrete valuation ring with fraction field $k(X)$. We denote by

$$\nu_D : k(X) \longrightarrow \mathbb{Z} \cup \{+\infty\}$$

the associated valuation (i.e. $\nu_D(f)$ is the "order of vanishing" — or pole, if negative — of f along D). A **divisor** on X is a formal combination

$$D = \sum_{i=1}^{r} a_i D_i, \qquad a_i \in \mathbb{Z}$$

of prime divisors D_i. To a rational function $f \in k(X)$ one can associate a divisor

$$\operatorname{div}(f) = \sum_{D} \nu_D(f) \cdot D \tag{14.1.1}$$

the sum taken over all prime divisors $D \subseteq X$ (Proposition 14.2.2(a) below ensures that this sum is finite). Such divisors are called **principal**. The main goal of the lecture is to describe the Picard group of isomorphism classes of invertible sheaves $\operatorname{Pic}(X)$ in terms of divisors.

Theorem 14.1.1. *There is a natural exact sequence*

$$1 \longrightarrow \mathcal{O}(X)^\times \longrightarrow k(X)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}(X) \xrightarrow{\pi} \operatorname{Pic}(X) \longrightarrow 1. \tag{14.1.2}$$

Proof outline. The proof will occupy the next two subsections. Injectivity on the left is obvious, the map div is well-defined thanks to Proposition 14.2.2(a), and exactness at $k(X)^\times$ is proved in Proposition 14.2.2(c). The map π is defined in §14.3, and exactness at $\operatorname{Div}(X)$ is proved in Proposition 14.3.5. Finally, surjectivity of π is shown in Proposition 14.3.6. □

In simple terms, Theorem 14.1.1 states that

$$\text{line bundles} = \frac{\text{divisors}}{\text{principal divisors}}$$

Two divisors D, D' are **linearly equivalent** (denoted $D \sim D'$) if $D - D'$ is principal. Thus line bundles are linear equivalence classes of divisors.

14.2. Divisors associated to rational functions

We introduce some basic terminology:

Definition 14.2.1. Let $D = \sum a_i D_i \in \mathrm{Div}(X)$ be a divisor on X.

(a) We say that D is **effective** if $a_i \geq 0$ for all i.

(b) If $E \in \mathrm{Div}(X)$ is another divisor, we write $D \geq E$ if $D - E$ is effective.

(c) For an open $U \subseteq X$, we write $D|_U$ for the sum $\sum a_i(D_i \cap U)$ where we omit the indices i for which $D_i \cap U = \varnothing$.

Proposition 14.2.2. *Let $f \in k(X)^\times$ be a nonzero rational function.*

(a) There are only finitely many prime divisors $D \subseteq X$ such that $\nu_D(f) \neq 0$.

(b) The function f is regular (meaning that $f \in \mathcal{O}(X)$) if and only if $\nu_D(f) \geq 0$ for all prime divisors D.

(c) The function f is invertible on X if and only if $\nu_D(f) = 0$ for all prime divisors D.

The first assertion means that the divisor $\mathrm{div}(f)$ in (14.1.1) is well defined, and since $\nu_D(fg) = \nu_D(f) + \nu_D(g)$ we have a homomorphism

$$\mathrm{div}\colon k(X)^\times \longrightarrow \mathrm{Div}(X), \qquad \mathrm{div}(f) = \sum_{D \subseteq X \text{ prime}} \nu_D(f) \cdot D.$$

Part (b) means that regular functions are those which map to effective divisors, and part (c) that invertible functions comprise the kernel. In particular, we have an exact sequence (the left part of (14.1.2))

$$1 \longrightarrow \mathcal{O}(X)^\times \longrightarrow k(X)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(X).$$

Proof of Proposition 14.2.2. To prove (a) we may assume that X is affine and that $f \in A = \mathcal{O}(X)$ is a regular function (why?). In this case prime divisors $D \subseteq X$ correspond to height one prime ideals $\mathfrak{p} \subseteq A$. We have $\nu_D(f) \geq 0$ for all $f \in A$, and $\nu_D(f) > 0$ if and only if the image of f in $\mathcal{O}_{X,D} = A_\mathfrak{p}$ belongs to the maximal ideal $\mathfrak{m}_D = \mathfrak{p} \cdot A_\mathfrak{p}$, which happens precisely when $f \in \mathfrak{p}$. Since $\dim(A/f) = \dim(A) - 1$, the height one primes $\mathfrak{p} \subseteq A$ correspond to minimal primes of A/f, of which there are finitely many since A/f is noetherian.

To prove (b) we again reduce to the case X affine and let $A = \mathcal{O}(X)$. Using the above reasoning, the first claim is equivalent to the commutative algebra statement: *A is equal to the intersection, inside its field of fractions, of its localizations $A_\mathfrak{p}$ at all height one prime ideals.* The proof of this result, given in the appendix to this lecture (see Proposition 14.4.3), relies on A being integrally closed.

Part (c) follows from (b) since f belongs to $\mathcal{O}^\times(X)$ if and only if both f and f^{-1} are regular. □

14.3. Invertible sheaves associated to divisors

Our next goal is to construct the map $\pi\colon \mathrm{Div}(X) \to \mathrm{Pic}(X)$ in (14.1.2), i.e. to associate to every divisor D on X an invertible sheaf, which we denote by $\mathcal{O}_X(D)$ (and which Hartshorne denoted by $\mathcal{L}(D)$). Intuitively, sections of $\mathcal{O}_X(D)$ corresponding to D are rational functions whose poles are 'no worse than D.' The following definition makes this precise.

Definition 14.3.1. Let D be a divisor on X. We define $\mathcal{O}_X(D)$ to be the following presheaf on X:

$$\mathcal{O}_X(D)(U) = \{0\} \cup \{f \in k(X)^\times : (\mathrm{div}(f) + D)|_U \geq 0\} \subseteq k(X)$$

(if $U \neq \varnothing$). By definition, $\mathcal{O}_X(D)$ is a sub-presheaf of the constant sheaf $\mathcal{K}_X$ with value $k(X)$.

Examples 14.3.2. (a) Let $D \subseteq X$ be a prime divisor and let $\mathcal{I}_D \subseteq \mathcal{O}_X$ be the corresponding coherent ideal. Then $\mathcal{O}_X(-D) = \mathcal{I}_D$. Consequently, we have a short exact sequence

$$0 \longrightarrow \mathcal{O}_X(-D) \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_D \longrightarrow 0.$$

The same holds for every effective divisor $D = \sum a_i D_i$, which we may identify with the closed subscheme $V(\mathcal{I}_D)$ for $\mathcal{I}_D = \prod \mathcal{I}_{D_i}^{a_i}$ (note that if $a_i > 1$ for some i then this is non-reduced, so if we do not work with schemes we cannot really consider D as a geometric subobject of X). Note that we have $D \geq 0$ if and only if $\mathcal{O}_X \subseteq \mathcal{O}_X(D)$, in which case we have a canonical section $1 \in \Gamma(X, \mathcal{O}_X(D))$.

A bit more generally, if D and E are divisors with $D \geq 0$, we have a short exact sequence

$$0 \longrightarrow \mathcal{O}_X(E-D) \longrightarrow \mathcal{O}_X(E) \longrightarrow \mathcal{O}_X(E)|_D \longrightarrow 0.$$

Note that we cannot in general write $\mathcal{O}_X(E)|_D$ as $\mathcal{O}_D(E \cap D)$ since D and E may have a common component.

(b) Let $X = \mathbb{P}^n$ for $n > 0$ and let $D \subseteq X$ be a prime divisor. Then $D = V(f)$ for an irreducible homogeneous $f \in k[x_0, \ldots, x_n]$ of degree d. In this case we have $\mathcal{O}_X(D) \simeq \mathcal{O}(d)$. Combined with Theorem 14.1.1 (still to be proved), this completes our proof from Lecture 12 that $\operatorname{Pic}(\mathbb{P}^n) = \mathbb{Z}$, generated by $\mathcal{O}(1)$.

Definition 14.3.1 introduced (implicitly) the sheaf of rational functions $\mathcal{K}_X$. Let us note that it is quasi-coherent: indeed, if X is affine, we have $\mathcal{K}_X = \widetilde{k(X)}$ (check this!). Since we are discussing invertible subsheaves of $\mathcal{K}_X$, let us carefully distinguish between *equality* (=) and *isomorphism* ($\simeq$).

Lemma 14.3.3. *Every divisor D on X is locally principal. That is, locally on X there exists a rational function $f \in k(X)^\times$ such that* $\operatorname{div}(f) = D$.

Proof. Since divisors are combinations of prime divisors, and combinations of locally principal divisors are locally principal, it suffices to show that every prime divisor is locally principal. Let thus D be a prime divisor on X and let $x \in X$; we seek to show that D is principal in a neighborhood of x. If $x \notin D$ there is nothing to show, so let us assume $x \in D$. Let $A = \mathcal{O}_{X,x}$ which is regular (as X is smooth) and hence a UFD. As we have remarked already in Lecture 13, this implies that every height one prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{X,x}$ is principal. Thus $\mathcal{I}_D \cdot \mathcal{O}_{X,x}$ is principal, generated by the image of a regular function $f \in \mathcal{O}(U)$ defined on an open affine neighborhood U of x. Shrinking U, we may ensure that $\mathcal{I}_D \cdot \mathcal{O}(U) = (f)$, so that $D|_U = \operatorname{div}(f)|_U$ is principal. □

Remark 14.3.4 (Cohomological interpretation)**.** By the above lemma, a divisor can be described in terms of an open cover $X = \bigcup U_\alpha$ and nonzero rational functions f_α such that $g_{\alpha\beta} = f_\alpha / f_\beta \in \mathcal{O}^\times(U_\alpha \cap U_\beta)$. If you think carefully what happens when we refine the cover, you will deduce from this an isomorphism

$$\operatorname{Div}(X) \simeq \Gamma(X, \mathcal{K}_X^\times / \mathcal{O}_X^\times).$$

The functions $g_{\alpha\beta}$ form an $\mathcal{O}^\times$-valued cocycle which defines the line bundle $\mathcal{O}_X(D)$. Once we learn about cohomology, we will be able to recognize the sequence (14.1.2) as part of the cohomology exact sequence associated to

$$1 \longrightarrow \mathcal{O}_X^\times \longrightarrow \mathcal{K}_X^\times \longrightarrow \mathcal{K}_X^\times / \mathcal{O}_X^\times \longrightarrow 1$$

which reads

$$\begin{array}{ccccccccccc} 1 \longrightarrow \mathcal{O}_X^\times(X) \longrightarrow k(X)^\times \longrightarrow & \Gamma(X, \mathcal{K}_X^\times / \mathcal{O}_X^\times) & \xrightarrow{\delta} & H^1(X, \mathcal{O}_X^\times) & \longrightarrow & H^1(X, \mathcal{K}_X^\times) & \longrightarrow \ldots \\ & \| & & \| & & \| & \\ & \operatorname{Div}(X) & & \operatorname{Pic}(X) & & 1. & \end{array}$$

Here the last group $H^1(X, \mathcal{K}_X^\times)$ is trivial since the sheaf $\mathcal{K}_X^\times$ is flabby (being a constant sheaf on an irreducible space).

Proposition 14.3.5. *Let D be a divisor on X.*

(a) The presheaf $\mathcal{O}_X(D)$ is an invertible subsheaf of the quasi-coherent sheaf $\mathcal{K}_X$.

(b) If $E \in \mathrm{Div}(X)$ is another divisor, we have

$$\mathcal{O}_X(D) \otimes \mathcal{O}_X(E) = \mathcal{O}_X(D) \cdot \mathcal{O}_X(E) = \mathcal{O}_X(D+E) \subseteq \mathcal{K}_X.$$

(c) If $D = \mathrm{div}(f)$ for a rational function $f \in k(X)^\times$, then $\mathcal{O}_X(D) = f^{-1} \cdot \mathcal{O}_X$. In particular, $\mathcal{O}_X(D) \simeq \mathcal{O}_X$ in this case.

(d) Conversely, if $\mathcal{O}_X(D) \simeq \mathcal{O}_X$, then D is principal.

(e) Every invertible subsheaf of $\mathcal{K}_X$ is of the form $\mathcal{O}_X(D)$ for a unique divisor D.

Proof. Let us first show (c). By Proposition 14.2.2(b) we have

$$\mathcal{O}_X(\mathrm{div}(f))(U) = \{g : \mathrm{div}(fg) \geq 0\} = \{g : fg \in \mathcal{O}(U)\} = f^{-1}\mathcal{O}(U).$$

We show (a). This is a local property, so we may assume thanks to Lemma 14.3.3 that $D = \mathrm{div}(f)$ is principal. In this case the assertion follows from (c). Part (b) is easy and left as an exercise.

To show (d), suppose we have an isomorphism $\mathcal{O}_X \xrightarrow{\sim} \mathcal{O}_X(D)$ and let $f \in \mathcal{O}_X(D)(X)$ be the image of 1 under this isomorphism, which is a nowhere-vanishing global section of $\mathcal{O}_X(D)$. We claim that $D = -\mathrm{div}(f)$. This can easily be checked directly by looking at the local rings $\mathcal{O}_{X,P}$ for all prime divisors $P \subseteq X$.

The proof of (e) follows the same strategy: since both invertible subsheaves of $\mathcal{K}_X$ and divisors can be defined locally (i.e. both form sheaves of sets on X), we can work locally, thus reducing the problem to the case of trivial (isomorphic to $\mathcal{O}_X$) invertible subsheaves of $\mathcal{K}_X$. But these are of the form $f \cdot \mathcal{O}_X$ for some rational function $f \in k(X)^\times$, and hence equal to $\mathcal{O}_X(D)$ where $D = \mathrm{div}(f)$. Moreover, $f \cdot \mathcal{O}_X = \mathcal{O}_X$ precisely when f is invertible, i.e. when $D = 0$, which shows uniqueness. □

Looking back at our target Theorem 14.1.1, defining $\pi : \mathrm{Div}(X) \to \mathrm{Pic}(X)$ as $D \mapsto \mathcal{O}_X(D)$, Proposition 14.3.5 gives the exactness of the following portion of the sequence

$$k(X)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(X) \xrightarrow{\pi} \mathrm{Pic}(X).$$

Therefore what is left to show is that the map π is surjective.

Proposition 14.3.6. *Let $\mathcal{L}$ be an invertible sheaf on X. Then $\mathcal{L}$ embeds into $\mathcal{K}_X$. Consequently, there exists a divisor D on X such that $\mathcal{L} \simeq \mathcal{O}_X(D)$.*

Proof. For every invertible sheaf $\mathcal{L}$ on X we have

$$\mathrm{Hom}(\mathcal{L}, \mathcal{K}_X) = \mathrm{Hom}(\mathcal{O}_X, \mathcal{L}^{-1} \otimes \mathcal{K}_X) = \Gamma(X, \mathcal{L}^{-1} \otimes \mathcal{K}_X) = \varinjlim_{U \neq \varnothing} \mathcal{L}^{-1}(U).$$

An element of $\Gamma(X, \mathcal{L} \otimes \mathcal{K}_X)$ is called a **rational section** of $\mathcal{L}$. Note that this is a one-dimensional vector space over $k(X)$. Via the above identification, nonzero rational sections of $\mathcal{L}^{-1}$ correspond to injective maps $\mathcal{L} \hookrightarrow \mathcal{K}_X$. □

Remark 14.3.7 (Weil divisors vs Cartier divisors)**.** Parts of what we have proved works under less restrictive assumptions. Here is a brief overview (for a more complete picture, see Hartshorne II.6).

- All results from this lecture work for any integral normal noetherian scheme which is locally factorial, meaning that the local rings $\mathcal{O}_{X,x}$ are UFDs (for example, X regular).
- On a general noetherian integral scheme X one has to distinguish between **Weil divisors** $\mathrm{WDiv}(X)$, which are defined as here as integer combinations of codimension one closed irreducible subsets, and **Cartier divisors** $\mathrm{CDiv}(X)$, which are the locally principal ones.
- The map $\mathrm{div}\colon k(X)^\times \to \mathrm{CDiv}(X)$ is well defined as long as the local rings $\mathcal{O}_{X,\xi}$ at codimension one points $\xi \in X$ are discrete valuation rings. This will hold for example if X is normal. In this case we define the **divisor class group** $\mathrm{Cl}(X)$ as the quotient

$$\mathrm{Cl}(X) = \mathrm{WDiv}(X)/\mathrm{im}(\mathrm{div}\colon k(X)^\times \to \mathrm{CDiv}(X))$$

  of Weil divisors by principal ones. Under the same assumptions,

$$\mathrm{Pic}(X) = \mathrm{CDiv}(X)/\mathrm{im}(\mathrm{div}\colon k(X)^\times \to \mathrm{CDiv}(X))$$

  which is therefore a subgroup of $\mathrm{Cl}(X)$.

Exercise 14.3.8. Suppose that X is projective and let $\mathcal{L}$ be an invertible sheaf on X. Prove that if both $\mathcal{L}$ and $\mathcal{L}^{-1}$ have nonzero global sections, then $\mathcal{L}$ is trivial.

14.4. Appendix: commutative algebra background

Proposition 14.4.1 (Stacks Project 0AFT)**.** *A noetherian domain is a UFD if and only every height prime is principal.*

Proof. We only prove the "only if" part, which is what we need for our treatment of divisors. Let A be a noetherian UFD and let $\mathfrak{p} \subseteq A$ be a height one prime ideal. Let $x \in \mathfrak{p}$ be a nonzero element. We can write

$$x = x_1 \cdot \ldots \cdot x_r, \qquad x_1, \ldots, x_r \text{ irreducible.}$$

Since $\mathfrak{p}$ is prime, we have $x_i \in \mathfrak{p}$ for some i. We have thus constructed a nonzero irreducible element $y = x_i \in \mathfrak{p}$. We claim that it generates $\mathfrak{p}$.

Since A is a UFD, the ideal $\mathfrak{q} = (y)$ is prime: if $uv \in \mathfrak{q}$, i.e. $uv = wy$, unique factorization implies that y divides either u or v, so $u \in \mathfrak{q}$ or $v \in \mathfrak{q}$. Since $0 \neq \mathfrak{q} \subseteq \mathfrak{p}$ and $\mathfrak{p}$ has height one, we must have $\mathfrak{q} = \mathfrak{p}$, and we are done. □

Example 14.4.2 (Quadratic cone)**.** The ring $A = k[x,y,z]/(xy - z^2)$ is an integrally closed domain of dimension 2 and the ideal $\mathfrak{p} = (x,z) \subseteq A$ (corresponding to a line passing through the vertex) is a prime of height one which is not principal. At the same time, the equality $xy = z^2$ exhibits the lack of unique factorization in A.

Proposition 14.4.3 (Stacks Project 031T)**.** *Let A be an integrally closed noetherian domain and let K be its field of fractions. Then*

$$A = \bigcap_{\mathrm{ht}(\mathfrak{p})=1} A_{\mathfrak{p}}$$

(intersection of the localizations of A at all height one primes, taken inside K).

Proof. If $\dim(A) = 0$ then A is a field, and if $\dim(A) = 1$ then A is a discrete valuation ring and there is a unique height one prime $\mathfrak{m}$ for which $A = A_{\mathfrak{m}}$. We might therefore assume that $\dim(A) \geq 2$.

The ($\subseteq$) inclusion is clear, so let us show ($\supseteq$). Let $g/f \in K$ be a nonzero rational function $(f, g \in A \smallsetminus \{0\})$ which belongs to $A_{\mathfrak{p}}$ for every height one prime $\mathfrak{p} \subseteq A$. We want to show that $g/f \in A$, or equivalently that $g \in (f)$, or that the image of g in $B = A/(f)$ is zero. Let us denote the maximal ideal of A by $\mathfrak{m}$ and of B by $\mathfrak{n}$.

By Krull's theorem all irreducible components of $\operatorname{Spec}(B) = V(f) \subseteq \operatorname{Spec}(A)$ have dimension $n-1$, or equivalently for every minimal prime $\mathfrak{q} \subseteq B$ its preimage $\mathfrak{p} \subseteq A$ has height one. The assumption that $f/g \in A_{\mathfrak{p}}$ implies that g maps to zero in $B_{\mathfrak{q}}$. In other words, the open subset $D(f) \cap V(f) \subseteq V(f) = \operatorname{Spec}(B)$ contains all of the generic points of $\operatorname{Spec}(B)$ and hence is dense in $\operatorname{Spec}(B)$. We are therefore left with showing the following property of the ring B:

If $g \in B$ vanishes on a dense open subset of $\operatorname{Spec}(B)$ *then it is zero.*

Suppose that $g \neq 0$ in B. Let $\mathfrak{q} \subseteq B$ be a minimal prime among the support $V(\operatorname{Ann}_B(g)) \neq \varnothing$ of g, and let $\mathfrak{p} \subseteq A$ be its preimage. By our assumption, $\mathfrak{q}$ is not a minimal prime of B, and hence $\dim(B_{\mathfrak{q}}) \geq 1$ and $\dim(A_{\mathfrak{p}}) \geq 2$. In order to obtain the desired contradiction with $g \neq 0$ in B, we may replace B with $B_{\mathfrak{q}}$ and A with $A_{\mathfrak{p}}$. In other words, we may assume that $\mathfrak{q} = \mathfrak{n}$ and $\mathfrak{p} = \mathfrak{m}$. Thus g is identically zero on $\operatorname{Spec}(B)$ away from its closed point, and $\sqrt{\operatorname{Ann}_B(g)} = \mathfrak{q}$.

Let $n \geq 1$ be the smallest such that $\mathfrak{n}^n \subseteq \operatorname{Ann}_B(g)$ (i.e. $g \cdot \mathfrak{n}^n = 0$). Suppose first that $n = 1$, so $g \cdot \mathfrak{n} = 0$ in B, or $g \cdot \mathfrak{m} \subseteq (f)$ in A. There are two cases:

- If $g\mathfrak{m} = (f)$ in A, we have $\mathfrak{m} = (f/g)$ (as submodules of K), so $\mathfrak{m}$ is principal, contradicting our assumption that $\dim(A) \geq 2$.
- Otherwise, we have $g\mathfrak{m} \subseteq f\mathfrak{m}$. In this case we have a well-defined endomorphism $g/f : \mathfrak{m} \longrightarrow \mathfrak{m}$. By the Cayley–Hamilton trick (see Atiyah–Macdonald, Propositions 5.1 and 2.4) this implies that h/f is integral over A, and (since A is integrally closed) that $h/f \in A$, so $h \in (f)$, contradiction.

If $n > 1$, pick $h \in \mathfrak{n}^{n-1} \smallsetminus \operatorname{Ann}_B(g)$ and replace g with $g' = gh \neq 0$, so that $g' \cdot \mathfrak{n} = 0$, and run the previous argument. □

14.5. Problem session (Mar 17)

Before stating the problems we discussed (prompted by Yurii) the origin of the name "divisor." This was a good opportunity to talk about some algebraic number theory.

Remark 14.5.1 (Why are divisors called *divisors*?)**.** The terminology comes from algebraic number theory, in which problems with lack of unique factorization in rings of integers in number fields play a big role. Suppose for example that you want to prove that $x^p + y^p = z^p$ has no nontrivial solutions for a prime $p > 2$. Rewrite this as

$$x^p = z^p - y^p = \prod_{i=0}^{p-1} (z - \zeta_p^i y), \qquad \zeta_p = \exp(2\pi i/p),$$

an equality in the ring $\mathbb{Z}[\zeta_p]$. Were this ring a UFD, the above equality would look at least unlikely.

Let K be a number field (a finite extension of $\mathbb{Q}$) and let $A = \mathcal{O}_K$ be its ring of integers (integral closure of $\mathbb{Z}$). Then A is a Dedekind domain (its local rings are DVRs), but not a PID/UFD in general (in dimension 1, UFD and PID mean the same thing, thanks to Proposition 14.4.1). A nonzero ideal $I \subseteq A$ can be written uniquely as a product of powers of prime ideals. Thus, if we work with ideals, we always have unique factorization (N.B. that's why we call them *ideals* — for "ideal divisors"). Since they do not form a group, we work with *fractional* ideals, which are finitely generated $\mathcal{O}_K$-submodules of K. The **class group** $\mathrm{Cl}(\mathcal{O}_K)$ is the quotient of the group of nonzero fractional ideals by the subgroup of principal fractional ideals. Thus $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K))$, and $\mathcal{O}_K$ is a UFD if and only if $\mathrm{Cl}(\mathcal{O}_K) = 0$. One of the first results in algebraic number theory (whose proof requires a bit of convex geometry) is that $\mathrm{Cl}(\mathcal{O}_K)$ is always finite. Its order, called the **class number** of K, is a mysterious invariant which can be computed explicitly in special cases. For example, for the case of the cyclotomic extension $K = \mathbb{Q}(\zeta_p)$ we have $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ and the class number is related to Bernoulli numbers. A prime p is **regular** if p does not divide the class number of $\mathbb{Q}(\zeta_p)$. Following ideas of Kummer, it is not difficult to prove Fermat's Last Theorem for regular exponents p (and thus for all $p \le 100$ except for $\{37,59,67\}$).

Problem 14.5.2. Let $\mathcal{L}$ be an invertible sheaf on a projective variety X such that $\Gamma(X,\mathcal{L})$ and $\Gamma(X,\mathcal{L}^{-1})$ are both nonzero. Show that $\mathcal{L} \simeq \mathcal{O}_X$.

Solution. We first check that every nonzero morphism $\mathcal{L}_1 \to \mathcal{L}_2$ between invertible sheaves on a variety (or integral scheme) is injective. Since this is a local question, we may assume X is affine and $\mathcal{L}_i$ both trivial. In this case the map can be viewed as a map $\mathcal{O}_X \to \mathcal{O}_X$, given by multiplication by a nonzero element $f \in \mathcal{O}(X)$. Since $\mathcal{O}(X)$ is a domain, this map is injective.

Now, we have

$$\Gamma(X,\mathcal{L}) = \mathrm{Hom}(\mathcal{O}_X,\mathcal{L}), \qquad \Gamma(X,\mathcal{L}^{-1}) = \mathrm{Hom}(\mathcal{O}_X,\mathcal{L}^{-1}) = \mathrm{Hom}(\mathcal{L},\mathcal{O}_X)$$

(the last equality obtained by tensoring with $\mathcal{L}$). Thus by assumption we have nonzero maps $\mathcal{O}_X \to \mathcal{L}$ and $\mathcal{L} \to \mathcal{O}_X$. By the previous paragraph, these maps are injective. Further, the composition $\mathcal{O}_X \to \mathcal{L} \to \mathcal{O}_X$ corresponds to an element $f \in \mathcal{O}(X)$, which is nonzero since the composition is injective. But X is projective, so $\mathcal{O}(X) = k$. Thus $f \in k^\times$, and $\mathcal{O}_X \to \mathcal{L} \to \mathcal{O}_X$ is an isomorphism. Therefore the second map $\mathcal{L} \to \mathcal{O}_X$ is surjective, and since as already observed it is also injective, it is an isomorphism. □

In the next problems we discuss smooth projective curves. For a divisor $D = \sum a_P P$ on a smooth projecitve curve X we define its **degree** as

$$\deg(D) = \sum a_P \in \mathbb{Z}.$$

Problem 14.5.3. Suppose $X = \mathbb{P}^1$. Show that for every principal divisor D we have $\deg(D) = 0$.

Solution. Let $f \in k(X)^\times$ be a nonzero rational function, which we may write as p/q for a pair of polynomials $p,q \in k[T]$. It suffices to treat p and q separately, so we may assume that $f \in k[T]$ is a polynomial. In this case we have

$$\mathrm{div}(f) = \sum_{x:f(x)=0} m_x \cdot x - m \cdot \infty$$

where the sum is over all zeros of f and m_x are their multiplicities. Thus $\sum m_x = \deg(f)$. The multiplicity m at infinity is calculated as the order of the pole at zero of $f(1/T)$, which equals $\deg(f)$. Thus $\deg \mathrm{div}(f) = 0$. □

Remark 14.5.4. The result can also be deduced from our computation of $\mathrm{Pic}(\mathbb{P}^1)$ in Lecture 14. Indeed, the maps $\deg\colon \mathrm{Div}(\mathbb{P}^1) \to \mathbb{Z}$ and $\pi\colon \mathrm{Div}(\mathbb{P}^1) \to \mathrm{Pic}(\mathbb{P}^1) = \mathbb{Z}$ are "the same" map.

Problem 14.5.5. Same as the previous problem but without assuming $X = \mathbb{P}^1$.

This result allows us to define the degree of an invertible sheaf on a smooth projective curve:

$$\begin{array}{ccccccc} k(X)^\times & \longrightarrow & \mathrm{Div}(X) & \longrightarrow & \mathrm{Pic}(X) & \longrightarrow & 1 \\ & \searrow^{0} & \downarrow{\scriptstyle \deg} & \swarrow_{\exists!\deg} & & & \\ & & \mathbb{Z} & & & & \end{array}$$

In order to attack Problem 14.5.5, we need two very useful facts.

Lemma 14.5.6. *Let X be a normal (i.e. $\mathcal{O}(U)$ is integrally closed for every open affine $U \subseteq X$) variety with function field K and let L/K be a finite extension. Then there exists a unique normal variety Y with function field L and a finite dominant map $Y \to X$ inducing the field extension L/K.*

Proof. Suppose first that X is affine and let $A = \mathcal{O}(X)$. In this case, let B be the integral closure of A in L. Then $Y = \mathrm{MSpec}(B)$ is a normal variety with function field $\mathrm{Frac}(B) = L$ and the induced $Y \to X$ is finite (by finiteness of integral closure) and dominant (as $A \to B$ is injective). The uniqueness is also clear: any other candidate has to be of the form $\mathrm{MSpec}(B')$ where B' is integrally closed, $\mathrm{Frac}(B') = L$, and $A \to B'$ finite (and hence integral). Thus $B = B'$.

In order to globalize this, we check easily that this construction is compatible with localization: for every nonzero $f \in A$, the localization $B[f^{-1}]$ coincides with the integral closure of $A[f^{-1}]$ in L. This is clear since again $B[f^{-1}]$ is normal, has function field L, and $A[f^{-1}] \to B[f^{-1}]$ is finite.

For the general case, let $X = \bigcup_{\alpha \in I} U_\alpha$ be an affine open cover. For each $\alpha, \beta \in I$ let

$$U_\alpha \cap U_\beta = \bigcup_{\gamma \in J_{\alpha\beta}} U_{\alpha\beta\gamma}$$

be an open cover such that $U_{\alpha\beta\gamma}$ is a distinguished affine open in both U_α and U_β (see Problem 1 on Problem Set 4). Define $V_\alpha = \mathrm{MSpec}(B_\alpha)$ where B_α is the integral closure of $A_\alpha = \mathcal{O}(U_\alpha)$ in L. The previous paragraph allows us to identify the preimage of each $U_{\alpha\beta\gamma}$ in V_α and V_β. This way we glue the V_α to obtain a normal variety Y with function field L together with a finite dominant map $Y \to X$, as desired. □

Lemma 14.5.7. *Let X be a smooth curve, let $U \subseteq X$ be a dense open subset, and let $\phi: U \to \mathbb{P}^n$ be a map. Then ϕ extends uniquely to a map $\psi: X \to \mathbb{P}^n$.*

Proof. We have $U = X \smallsetminus S$ for a finite set S. By induction it suffices to treat the case $\#S = 1$, i.e. $U = X \smallsetminus \{x\}$. The ring $R = \mathcal{O}_{X,x}$ is a discrete valuation ring with fraction field $K = k(X)$. From this point on we can either work over $\mathrm{Spec}(\mathcal{O}_{X,x})$ to extend the map locally at x, or (more clumsily) give a complete proof in the language of varieties. We go the second route.

Let $U_i \subseteq U$ be the preimages of the standard opens $D(x_i) \subseteq \mathbb{P}^n$. Since they cover the irreducible U, one of them has to be dense, say U_0. Then $X_0 = U_0 \cup \{x\}$ is an open neighborhood of x (we are on a curve!). Since the problem is local we can replace X with X_0. This means that ϕ can be represented by a map $(1 : f_1 : \cdots : f_n)$ for some $f_1, \ldots, f_n \in \mathcal{O}(U)$. Similarly, shrinking X around x we may assume that $x = V(\pi)$ for some $\pi \in \mathcal{O}(X)$, so that $\mathcal{O}(U) = \mathcal{O}(X)[1/\pi]$. If $f_1, \ldots, f_n$ belong to $\mathcal{O}(X) \subseteq \mathcal{O}(U)$, we extend the map with the same formula. In general (ignoring the indices for which $f_i = 0$), we can write $f_i = g_i/\pi^{m_i}$ where $g_i \in \mathcal{O}(X)$, $g_i \notin (\pi)$. Let $m = \min(m_1, \ldots, m_n)$ and set $f_0' = \pi^m$, $f_i' = \pi^m g_i$. Then one of the f_i' is a unit in a neighborhood of x, and after shrinking X again the map $(f_0' : \cdots : f_n')$ gives the desired extension $\psi: X \to \mathbb{P}^n$. □

Remark 14.5.8. The same ideas combined with Proposition 14.4.3 imply that a rational map from a normal variety to a projective variety is defined on an open subset whose complement has codimension at least two.

Corollary 14.5.9. *A birational map between smooth projective curves is an isomorphism.*

Corollary 14.5.10. *Let X be a smooth projective curve and let $f \in k(X)$ be a non-constant rational function. Then there exists a unique finite map $\phi: X \to \mathbb{P}^1$ (in practice denoted also by f) such that $\phi^*(t) = f$ (here T is the coordinate on $\mathbb{A}^1 \subseteq \mathbb{P}^1$, so that $k(\mathbb{P}^1) = k(t)$).*

Proof. Since f is non-constant, it is not algebraic over k, so there exists a unique k-algebra map of fields $k(t) \hookrightarrow k(X)$ sending t to f. So we have a finite extension of fields $k(X)/k(t)$, and by Lemma 14.5.6 there exists a unique finite dominant map $X' \to \mathbb{P}^1$ where X' is a normal variety and $k(X') = k(X)$. Since $\dim(X') = 1$, normal means smooth, so X' is a smooth projective curve. Since $k(X') = k(X)$, Lemma 14.5.7 implies that $X = X'$. □

Lemma 14.5.11. *Let $\phi: Y \to X$ be a finite map between smooth curves. Let $d = \deg(k(Y)/k(X))$ be the degree of the field extension of function fields. Then for every $x \in X$ the number of points in $\phi^{-1}(x)$, counted with multiplicity, equals d.*

Proof. We may assume that X is affine. Let $A = \mathcal{O}_{X,x}$ and $B = \mathcal{O}(Y) \otimes_{\mathcal{O}(X)} A = \mathcal{O}(Y)_x$. Then $A \to B$ is finite and A is a dvr. Moreover, being a localization of $\mathcal{O}(Y)$, B is a domain (with fraction field $k(Y)$) and hence torsion-free as an A-module. By the classification of modules over PIDs we see that B is a free A-module of finite rank. By tensoring with $k(X)$, we see that this rank is equal to d. By tensoring with k, we obtain the sum of the multiplicities of all $y \mapsto x$. Indeed, if π is a uniformizer of A, then for every such y, the multiplicity is $v_y(\pi)$, which is the length of $\mathcal{O}_{Y,y}/(\pi)$, and we have

$$B \otimes_A k = \prod_{y \mapsto x} \mathcal{O}_{Y,y}/(\pi).$$

□