Curves, function fields and Picard groups

Notes for a mini-course at the UNCG Summer School in Number Theory:
Algorithms for Extensions of Large Degree
University of North Carolina, Greensboro
28 May–1 June 2018

Peter Bruin (Universiteit Leiden)
P.J.Bruin@math.leidenuniv.nl

Introduction

The goal of these notes is to introduce algebraic curves, function fields, and their Picard groups. The emphasis will be on algorithmic aspects of curves of large genus, in particular Khuri-Makdisi's algorithmic framework for computing with curves and their Picard groups.

The main prerequisite is some basic algebraic geometry, such as Fulton's book [3] or the first chapter of Hartshorne's book [4]. This includes a few concepts from commutative algebra that are widely used in algebraic geometry, such as prime ideals, local rings, tensor products of vector spaces. We will mention sheaves or line bundles in some places where they are helpful, but we will not use any deep techniques. Some knowledge of schemes may be helpful, but is not strictly necessary.

1. Curves and function fields

Throughout these notes, k will be a field. In practice, k will often be a finite field; we will make this assumption when it is needed.

1.1. Curves

The following definition is only meant for readers who know about schemes and who want to know exactly how general our curves will be.

Definition. A *variety* over k is a quasi-projective k-scheme of finite type, or equivalently an open subscheme of a projective k-scheme.

Definition. An *curve* over k is a one-dimensional variety over k.

Like any k-scheme, a curve X is in particular a topological space equipped with a sheaf of k-algebras, the structure sheaf $\mathcal{O}_X$. For every open subset $U \subseteq X$, the k-algebra $\mathcal{O}_X(U)$ consists of the regular functions on U.

Definition. Let X be a curve, and let x be any point of X. The *local ring* of X at x, denoted by $\mathcal{O}_{X,x}$, is the direct limit

$$\mathcal{O}_{X,x} = \varinjlim_{x \in U \subseteq X} \mathcal{O}_X(U),$$

where U runs over all open subsets of X containing x. The *residue field of* x, denoted by $k(x)$, is the residue field of the local ring $\mathcal{O}_{X,x}$.

Definition. If x is a closed point of X, the *degree* of x, denoted by $\deg x$, is the degree $[k(x) : k]$.

Recall that a topological space X is *irreducible* if for any two closed subsets $Y, Z \subseteq X$ with $Y \cup Z = X$, at least one of Y and Z is equal to X. Recall that a ring A is *reduced* if the only nilpotent element of A is 0.

Definition. Let X be a curve over k. We say that X is *irreducible* if its underlying topological space is irreducible. We say that X is *reduced* if for every open subset $U \subseteq X$, the k-algebra $\mathcal{O}_X(U)$ is reduced. We say that X is *integral* if X is both irreducible and reduced.

Let X be an integral curve over k. Topologically, the curve X consists of infinitely many closed points and one generic point, the closure of which is the whole curve. The open subsets are the empty set and the complements of finitely many closed points.

Definition. Let X be an integral curve over K. The *function field* of X, denoted by $K(X)$, is the local ring of X at its generic point.

Note that for every point of X, we have an inclusion $\mathcal{O}_{X,x} \to K(X)$ because every open subset of X containing x also contains the generic point. Moreover, the fraction field of $\mathcal{O}_{X,x}$ can be identified with $K(x)$.

Definition. Let X be a projective integral curve over k. The *field of constants* of X is the k-algebra $\mathcal{O}_X(X)$ of global sections of $\mathcal{O}_X$.

The assumptions on X imply that $\mathcal{O}_X(X)$ is indeed a field and that it is a finite extension of k. Furthermore, $\mathcal{O}_X(X)$ is a subring of $k(x)$ for any closed point x of X. Finally, $\mathcal{O}_X(X)$ is equal to k if and only if X is geometrically integral. (This can be taken as the definition of "geometrically integral".)

1.2. Function fields

Definition. A *function field* over k is a finitely generated extension field K of k such that K has transcendence degree 1 over k.

The notion of function fields is designed in such a way that function fields are exactly the fields arising as fields of rational functions on (integral) algebraic curves.

Notation. If R is a domain, we write $\operatorname{Frac} R$ for the field of fractions of R.

Example. The field $k(t) = \operatorname{Frac} k[t]$ (where $k[t]$ is a polynomial ring in one variable over k) is a function field.

Example. Let $f = x^2 + y^2 - 1 \in \mathbf{R}[x, y]$. Then $\operatorname{Frac}(\mathbf{R}[x, y]/(f))$ is a function field.

Example. Let $g = y^2 + 1 \in \mathbf{R}[x, y]$. Then $\operatorname{Frac}(\mathbf{R}[x, y]/(g))$ is *not* a function field, because the image of y generates a subfield isomorphic to $\mathbf{C}$.

Definition. A *discrete valuation ring* is a principal ideal domain R with exactly two prime ideals, namely 0 and a unique maximal ideal $\mathfrak{m}_R$. A *uniformiser* of R is a generator of the ideal $\mathfrak{m}_R$.

It is known that principal ideal domains are unique factorisation domains. It follows that if R is a discrete valuation ring with field of fractions K and x is an element of $K^\times$, then there is a unique $n \in \mathbf{Z}$ with $xR = \mathfrak{m}_R^n$; this n is denoted by $\operatorname{ord}_R(x)$. This gives a surjective group homomorphism

$$\operatorname{ord}_R \colon K^\times \to \mathbf{Z}.$$

Definition. A *valuation ring* is a domain R such that for every x in $(\operatorname{Frac} R)^\times$, either x or x^{-1} is in R.

Example. Fields and discrete valuation rings are valuation rings.

Definition. Let K be a function field K over k. A *valuation ring* or *place* of K (over k) is a subring $R \subseteq K$ such that R is a valuation ring containing k.

There is a well-known correspondence between curves and function fields.

Definition. A curve X is *regular* if for every closed point x of X, the local ring $\mathcal{O}_{X,x}$ is a discrete valuation ring.

Theorem 1.1.

(a) *If X is an integral curve over k, then its function field $K(X)$ (i.e. the field of fractions of $\mathcal{O}_X(U)$ for any non-empty affine open subset $U \subset X$) is a finitely generated extension of transcendence degree* 1 *over k.*

(b) *If $\phi \colon X \to Y$ is a non-constant morphism of integral curves over k, then ϕ induces an inclusion $\phi^* \colon K(Y) \to K(X)$.*

(c) *If X is a regular projective integral curve over k, then there is a bijection from the set of points of X to the set of valuation rings of $K(X)$ mapping a point x to the local ring $\mathcal{O}_{X,x}$ viewed as a subring of $K(X)$.*

(d) *If X is a regular projective integral curve over k, then the canonical map $\mathcal{O}_X(X) \to K(X)$ identifies the field of constant functions on X with the algebraic closure of k in $K(X)$.*

(e) *Let $\mathcal{C}_k$ be the category of regular projective integral curves over k with dominant morphisms, and let $\mathcal{F}_k$ be the category of function fields over k with k-algebra homomorphisms. The association $X \mapsto K(X)$ and $(\phi\colon X \to Y) \longmapsto (\phi^*\colon K(Y) \to K(X))$ is a contravariant equivalence of categories from $\mathcal{C}_k$ to $\mathcal{F}_k$.*

Proof. This is essentially [3, § 7.5, Corollary to Theorem 3]. □

The above theorem implies that for every integral curve X over k, there exists a regular projective curve X' over k, unique up to isomorphism, such that $K(X')$ and $K(X)$ are isomorphic. This X' is called the regular projective model of X over k. It can be constructed as follows. First embed X into a projective curve $\bar{X}$ (if X is given as a subvariety of an affine space $\mathbf{A}^n_k$, embed $\mathbf{A}^n_k$ into $\mathbf{P}^n_k$ and take the closure of X in $\mathbf{P}^n_k$.) Next, take a covering of $\bar{X}$ by affine open subsets U. For each U, take the integral closure of the k-algebra $\mathcal{O}_{\bar{X}}(U)$. This is the coordinate ring of an regular affine integral curve $\tilde{U}$. Because taking integral closures is compatible with localisation, these affine curves $\tilde{U}$ can be glued together to obtain the desired regular projective integral curve X'.

1.3. Divisors

Let X be a regular projective integral curve over k.

Definition. The group of *divisors* on X is the free Abelian group $\operatorname{Div} X$ on the closed points of X. When viewed as a divisor, a closed point is called a *prime divisor*.

Notation. We often write divisors D as

$$D = \sum_{x\in X} n_x x,$$

where x ranges over the set of closed points of X and n_x are integers that are equal to 0 for all but finitely many x.

Definition. A divisor in the above form is *effective* if $n_x \ge 0$ for all closed points x of X.

Notation. If D and E are two divisors on X, we write $D \ge E$ if the divisor $D - E$ is effective.

Definition. The *degree map* is the group homomorphism

$$\begin{aligned} \deg\colon \operatorname{Div} X &\longrightarrow \mathbf{Z} \\ \sum_{x\in X} n_x x &\longmapsto \sum_{x\in X} n_x \deg x. \end{aligned}$$

Definition. For $f \in K(X)^\times$ and x a closed point of X, the *order* or *valuation* of f at x is

$$\operatorname{ord}_x(f) = \operatorname{ord}_{\mathcal{O}_{X,x}}(f).$$

Definition. For all $f \in K(X)^\times$, the *divisor* of f is

$$\operatorname{div} f = \sum_{x\in X} \operatorname{ord}_x(f) x.$$

Definition. The group of *principal divisors* on X is $\{\operatorname{div} f \mid f \in K(X)^\times\}$.

Proposition 1.2. *Every principal divisor on X has degree* 0.

Definition. Two divisors D, D' on X are *linearly equivalent* if $D - D'$ is a principal divisor.

The following construction of a line bundle $\mathcal{O}_X(D)$ for a divisor D (and in particular its space of global sections) will be of fundamental importance for us.

Definition. Let X be a smooth integral curve over k, and let $D = \sum_{x\in X} n_x x$ be a divisor on X. We define a presheaf $\mathcal{O}_X(D)$ on X by

$$\mathcal{O}_X(D)(U) = \begin{cases} \{f \in K(X) \mid \operatorname{ord}_x f + n_x \ge 0 \text{ for all closed points } x \in U\} & \text{if } U \ne \emptyset, \\ 0 & \text{if } U = \emptyset. \end{cases}$$

It is not hard to check that this is a sheaf on X, and in fact a line bundle (locally free sheaf of $\mathcal{O}_X$-modules of rank 1).

1.4. Differentials

Definition. Let R be a k-algebra. The *module of (Kähler) differentials* of R over k is the R-module $\Omega_{R/k}$ generated by the symbols df for $f \in R$ subject to the relations

$$d(f+g) = df + dg, \quad d(cf) = c\,df, \quad d(fg) = g\,df + f\,dg$$

for all $f, g \in R$ and all $c \in k$.

The map

$$d\colon R \to \Omega_{R/k}$$

sending an element $f \in R$ to $df \in \Omega_{R/k}$ is a derivation of R over k, i.e. a k-linear map satisfying the Leibniz rule $d(fg) = g\,df + f\,dg$.

Proposition 1.3. *Let K be a function field over K.*

(a) The K-vector space $\Omega_{K/k}$ has dimension 1 over K.

(b) If K has characteristic 0 and $f \in K \setminus k$, then $\Omega_{K/k}$ is generated by df as a K-vector space.

Proof. See Fulton [3, Proposition 8.4.6]. □

Definition. Let X be an integral curve over k. The space of *meromorphic differentials* on X is the one-dimensional $K(X)$-vector space $\Omega_{K(X)/k}$.

Let X be a curve over k, and let x be a closed point of X. We have the $\mathcal{O}_{X,x}$-module

$$\Omega_{X/k,x} = \Omega_{\mathcal{O}_{X,x}/k}.$$

Viewing $\mathcal{O}_{X,x}$ as a k-subalgebra of $K(X)$, we can similarly view $\Omega_{X/k,x}$ as an $\mathcal{O}_{X,x}$-submodule of $K(X)$.

Definition. We say that the curve X over k is *smooth at x* if $\Omega_{X/k,x}$ is free of rank 1 as an $\mathcal{O}_{X,x}$-module. We say that X is *smooth* if it is smooth at every point.

Proposition 1.4. *Let X be a curve over k.*

(a) If X is smooth over k, then X is regular.

(b) If X is regular and k is perfect, then X is smooth over k.

Proof. See for example the Stacks Project [7, tag 00TQ]. □

Let X be a smooth integral curve over k. If ω is a non-zero element of $\Omega_{K(X)/K}$, then $\mathcal{O}_{X,x}\omega$ is a free $\mathcal{O}_{X,x}$-submodule of rank 1 of $\Omega_{K(X)/K}$. This implies that $\mathcal{O}_{X,x}\omega$ equals $\mathfrak{m}_{X,x}^n \Omega_{X/k,x}$ for a unique $n \in \mathbf{Z}$.

Definition. Let X be a smooth integral curve over k, let ω be a non-zero meromorphic differential on X, and let x be a closed point of X. The *order* or *valuation* of ω at x, denoted by $\operatorname{ord}_x \omega$, is the unique $n \in \mathbf{Z}$ such that

$$\mathcal{O}_{X,x}\omega = \mathfrak{m}_{X,x}^n \Omega_{X/k,x}$$

as $\mathcal{O}_{X,x}$-submodules of $\Omega_{K(X)/k}$.

Example. Let $X = \mathbf{P}^1_k$ be the projective line over k. The function field of X is $k(t)$, and dt is a meromorphic differential on X. On the subset $\mathbf{A}^1_k \subset \mathbf{P}^1_k$, which has coordinate ring $k[t]$, the element dt generates the module of differentials at every point, i.e. for every point $x \in \mathbf{A}^1_k$, we have

$$\Omega_{X/k,x} = \mathcal{O}_{X,x} dt.$$

On the other hand, the module of differentials at the point $\infty \in \mathbf{P}^1_k$ is generated by du, where u is the uniformiser at ∞ defined by $u = 1/t$. This shows

$$\mathcal{O}_{X,\infty} dt = \mathcal{O}_{X,\infty} \cdot -u^{-2} du = \mathfrak{m}_{X,\infty}^{-2} \Omega_{X/k,\infty}.$$

We conclude that

$$\operatorname{ord}_x dt = \begin{cases} 0 & \text{if } x \in \mathbf{A}^1_k, \\ -2 & \text{if } x = \infty. \end{cases}$$

Definition. Let X be a smooth curve over k. The *canonical line bundle* on X is the presheaf $\Omega_{X/k}$ on X defined by

$$\Omega_{X/k}(U) = \begin{cases} \{\omega \in \Omega_{K(X)/k} \mid \operatorname{ord}_x(\omega) \ge 0 \text{ for all closed points } x \in U\} & \text{if } U \ne \emptyset, \\ 0 & \text{if } U = \emptyset \end{cases}$$

with the obvious restriction maps.

It is not hard to check that $\Omega_{X/k}$ is in fact a sheaf on X. Because of the assumption that X is a smooth curve, $\Omega_{X/k}$ is in fact a line bundle on X.

Definition. The space of *global differentials* on X is the k-vector space $\Omega_{X/k}(X)$.

Theorem 1.5. *If X is a smooth projective curve over k, then the k-vector space $\Omega_{X/k}(X)$ of global differentials is finite-dimensional.*

From now on, unless mentioned otherwise, a *curve* will be a smooth, projective, geometrically integral curve over k.

Definition. Let X be a smooth, projective, geometrically integral curve over k. The *genus* of X is the dimension of the k-vector space $\Omega_{X/k}(X)$.

Definition. Let ω be a non-zero meromorphic differential on X. The *divisor* of ω is

$$\operatorname{div}\omega = \sum_{x\in X} \operatorname{ord}_x(\omega)x.$$

Definition. A *canonical divisor* on X is any divisor $\mathcal{K}$ such that there exists a non-zero meromorphic differential ω on X with $\operatorname{div}_{\Omega_{X/k}}(\omega) = \mathcal{K}$.

Note that all canonical divisors on X are linearly equivalent.

Example. For $X = \mathbf{P}^1_k$ with coordinate t, we can take

$$\mathcal{K} = \operatorname{div}(dt) = -2\cdot\infty.$$

Remark. In the language of line bundles, a canonical divisor is nothing but the divisor of a non-zero rational section of the canonical line bundle. Equivalently, a canonical divisor is any divisor in the linear equivalence class corresponding to the canonical line bundle under the standard isomorphism between the divisor class group and the group of isomorphism classes of line bundles.

1.5. Exercises

1.1. Let X be a curve over k. Show that if x is a closed point of X, then the residue field $k(x)$ is a finite extension of k.

1.2. Let X be an integral curve over k. Show that $K(X)$ is a field.

1.3. Let S be the power series ring $k[[x,y]]$, let $\mathfrak{m} = (x,y)$ be its maximal ideal, and let $f \in \mathfrak{m}$ be a non-zero element. Let $R = S/(f)$.

(a) Suppose that at least one of the two partial derivatives $\partial f/\partial x$ and $\partial f/\partial y$ is a unit in R. Show that R is isomorphic to a power series ring $k[[t]]$ in one variable; in particular, f is irreducible and R is a discrete valuation ring.

(b) Take $f = y^2 - x^3$. Show that f is irreducible, but R is not a discrete valuation ring.

1.4. Let K be a function field over k. Show that the algebraic closure of k in K equals the intersection of all valuation rings of K.

1.5. Show that if R is given by a k-algebra presentation

$$R = k[x_1,\dots,x_n]/(f_1,\dots,f_m),$$

then $\Omega_{R/k}$ has an R-module presentation

$$\Omega_{R/k} \cong (R\,dx_1 + \cdots + R\,dx_n)/(R\,df_1 + \cdots + R\,df_m),$$

where $R\,dx_1 + \cdots + R\,dx_n$ is a free R-module with basis $(dx_1,\dots,dx_n)$ and df_1, …, df_m are the elements of this module defined by $df_i = \sum_{j=1}^n \frac{\partial f_i}{\partial x_j} dx_j$.

1.6. Let k be a field of characteristic different from 2, and consider a square-free polynomial

$$f = a_n x^n + a_{n-1} x^{n-1} \cdots + a_1 x + a_0 \in k[x].$$

of degree $n > 0$. Let X be the smooth projective curve given by the affine equation

$$y^2 = f(x).$$

(a) Show that there are either one or two points "at infinity" with respect to the above affine model, and find a uniformiser at each of these points.

(b) Compute the divisor of the meromorphic differential $\omega = \frac{dx}{2y}$.

2. More on curves and divisors

Throughout this section, X will be a smooth projective integral curve over k.

2.1. The vector spaces $L(X, D)$

If D is a divisor on X, we abbreviate

$$L(X, D) = \mathcal{O}_X(D)(X).$$

Thus $L(X, D)$ is the k-vector space of functions with prescribed minimal orders of vanishing and maximal pole orders at the points occurring in D. We note that the non-zero elements of $L(X, D)$ are exactly the rational functions $f \neq 0$ such that the divisor $\operatorname{div} f + D$ is effective. Furthermore, if $D = \sum_{x \in X} n_x x$, the definition of $L(X, D)$ is equivalent to

$$L(X, D) = \bigcap_{x \in X} \mathfrak{m}_{X,x}^{-n_x} \subset K(X), \tag{2.1}$$

where x ranges over the set of closed points of X and $\mathfrak{m}_{X,x}$ is the maximal ideal of $\mathcal{O}_{X,x}$ viewed as an invertible $\mathcal{O}_{X,x}$-ideal.

Theorem 2.1. *For every divisor D on X, the k-vector space $L(X, D)$ is finite-dimensional.*

Example. Take $X = \mathbf{P}^1_k$ and $D = n\infty$ with $n \in \mathbf{Z}$. The space $L(X, n\infty)$ consists of rational functions that have no poles on $\mathbf{A}^1_k$ (i.e. polynomials) and a pole of order at most n at ∞. Hence

$$L(X, n\infty) = \{f \in k[t] \mid \deg f \leq n\}$$

and

$$\dim_k L(X, n\infty) = \max\{0, n+1\}.$$

For any extension field k' of k, we write $X_{k'}$ for the base change of the curve X to k'. From now on, we will assume that X is *geometrically integral*, i.e. that the base change $X_{\bar{k}}$ to an algebraic closure $\bar{k}$ of k is an integral curve.

It is often useful to know that the spaces $L(X, D)$ are "stable under base change". Since X is geometrically integral, the curve $X_{k'}$ is integral and the function field $K(X_{k'})$ is canonically isomorphic to $K(X) \otimes_k k'$. If D is a divisor on X, we have an induced divisor $D_{k'}$ on $X_{k'}$. Writing $D = \sum_{x \in X} n_x x$, we have

$$D_{k'} = \sum_{x \in X} n_x \sum_{y \mapsto x} e(y/x) y, \tag{2.2}$$

where y ranges over the closed points of $X_{k'}$ mapping to the closed point x of X and $e(y/x)$ is the ramification index of y over x.

Remark. When k is perfect, all ramification indices $e(y/x)$ are equal to 1. When k is imperfect, the extensions of discrete valuation rings can be ramified; take $k = \mathbf{F}_p(v)$, let $X = \mathbf{P}^1_k$ with parameter t, let x be the closed point defined by $t^p = v$, and consider the inseparable extension $k' = k[w]/(w^p - v)$. Then $X_{k'}$ has a unique point y over x, defined by $t = w$, and the ramification index equals p.

Furthermore, we have a k'-linear isomorphism

$$L(X,D)\otimes k' \xrightarrow{\sim} L(X,D)k' \subset K(X_{k'}).$$

Proposition 2.2. *For every divisor D on X and every extension field k' of k, we have*

$$L(X,D)k' = L(X_{k'},D_{k'}) \subset K(X_{k'})$$

and hence a canonical k'-linear isomorphism

$$L(X,D)\otimes_k k' \longrightarrow L(X_{k'},D_{k'})$$

In particular, we have

$$\dim_k L(X,D) = \dim_{k'} L(X_{k'},D_{k'}).$$

Proof. It is clear that the map is injective because it can be viewed as a restriction of the isomorphism $K(X)\otimes_k k' \xrightarrow{\sim} K(X)k' = K(X_{k'})$ to $L(X,D)\otimes_k k'$. Using the description (2.1) of $L(X,D)$ and the description (2.2) of $D_{k'}$, we see that it suffices to show that for every $x \in X$ we have an equality

$$m_{X,x}k' = \prod_{y\mapsto x} m_{X_{k'},y}^{e(y/x)}.$$

This follows from the definition of the ramification indices $e(y/x)$. □

The following theorem is one of the most important facts about spaces of global sections.

Theorem 2.3 (Riemann–Roch). *Let X be a smooth, projective, geometrically integral curve of genus g over k, and let $\mathcal{K}$ be a canonical divisor on X. For every divisor D on X, we have*

$$\dim_k L(X,D) - \dim_k L(X,\mathcal{K}-D) = 1 - g + \deg D.$$

Remark. The term $\dim_k L(X,\mathcal{K}-D)$ may also be viewed as the dimension of the space of global sections of the line bundle $\Omega_{X/k}(-D)$.

Remark. The space $L(X,\mathcal{K}-D)$ can be identified, via *Serre duality*, with the k-linear dual of the first cohomology group $\mathrm{H}^1(X,\mathcal{O}_X(D))$.

Corollary 2.4. *If $\mathcal{K}$ is a canonical divisor on X, then we have*

$$\deg\mathcal{K} = 2g-2.$$

Proof. Take $D=\mathcal{K}$ in the Riemann–Roch theorem. □

Definition. A divisor D on X is *special* if the space $L(X,\mathcal{K}-D)$ is non-zero.

For non-special divisors D, the Riemann–Roch formula simplifies to

$$\dim_k L(X,D) = 1-g+\deg D. \tag{2.3}$$

Corollary 2.5. *For every divisor D on X, we have*

$$\begin{aligned}\deg D < 0 &\implies L(X,D)=0,\\ \deg D \ge 2g-1 &\implies D \textit{ is non-special.}\end{aligned}$$

Proof. If $\deg D < 0$, then for any non-zero element $f \in L(X,D)$ the divisor $\operatorname{div} f + D$ would be an effective divisor of negative degree, which is impossible; this implies the first claim. If $\deg D \ge 2g-1$, then we have $\deg(\mathcal{K}-D) < 0$, so $L(X,\mathcal{K}-D)=0$ by the first claim, so D is non-special. □

2.2. Basepoint-free divisors and very ample divisors

Let X be a smooth projective geometrically integral curve of genus g over k.

Definition. A divisor D on X is *basepoint-free* if for any divisor E such that $L(X, E) = L(X, D)$, we have $E \geq D$.

Remark. This is a slight abuse of terminology; usually the adjective "basepoint-free" is used for linear systems, and "generated by global sections" for the corresponding line bundles.

Note that D is basepoint-free if and only if for every prime divisor P on X, the space $L(X, D-P)$ is a strict subspace of $L(X, D)$.

Lemma 2.6. *Let k' be an extension field of k, and let D be a divisor on X. Then D is basepoint-free if and only if the divisor $D_{k'}$ on $X_{k'}$ is basepoint-free.*

Proof. We use the fact that there is a surjective map $r\colon X_{k'} \to X$ on topological spaces. Suppose $D_{k'}$ is not basepoint-free, and let Q be a prime divisor on $X_{k'}$ such that all elements of $L(X_{k'}, D_{k'}) \cong L(X, D) \otimes_k k'$ vanish in Q, where the isomorphism comes from Proposition 2.2. Then all elements of $L(X, D)$ vanish on the prime divisor $r(Q)$ of X, so D is not basepoint-free.

Conversely, suppose D is not basepoint-free, and let P be a prime divisor on X satisfying $L(X, D-P) = L(X, D)$. Then $P_{k'}$ is a non-zero effective divisor (not necessarily prime) satisfying $L(X_{k'}, D_{k'} - P_{k'}) = L(X_{k'}, D_{k'})$, so $D_{k'}$ is not basepoint-free. □

Lemma 2.7. *Let F be a divisor of degree at least $2g$ on X. Then F is basepoint-free.*

Proof. Thanks to the Lemma 2.6, we may assume that k is algebraically closed. For every closed point P of X, both F and $F - P$ are non-special by Corollary 2.5, the Riemann–Roch formula implies

$$\dim_k L(X, F - P) = \deg F - g = \dim_k L(X, F) - 1.$$

The claim now follows from Hartshorne [4, IV, Proposition 3.1(a)]. □

Definition. Let D be a divisor on X. An *ideal generating set* for D is a subset $S \subseteq L(X, D)$ such that for any divisor E such that $S \subseteq L(X, E)$, we have $E \geq D$.

Remark. The reason for this terminology (which I borrowed from Khuri-Makdisi [6]) is that it is analogous to the concept of a generating set for a (fractional) ideal of a Dedekind domain.

Let F be a basepoint-free divisor on X. We write $V = L(X, F)$. To any point P of X over some extension field k' of k, we associate the linear subspace

$$V_P = L(X_{k'}, F - P) \subseteq V \otimes_k k'.$$

Because F is basepoint-free, V_P is a hyperplane in $V \otimes_k k'$. Let $\mathbf{P}V$ be the projective space of hyperplanes in V; this can be defined as a projective k-scheme by

$$\mathbf{P}V = \operatorname{Proj}\Biggl(\bigoplus_{n\geq 0} \operatorname{Sym}_k^n V\Biggr).$$

For any point $P \in X(k')$ with k' an extension field of k, the hyperplane V_P defines a point in $(\mathbf{P}V)(k')$ that we also denote by V_P. More generally, any point of X over a k-algebra R defines an R-valued point of $\mathbf{P}V$. We get a map

$$\begin{aligned} i_F\colon X &\to \mathbf{P}V \\ P &\mapsto V_P. \end{aligned}$$

Definition. A divisor F on X is *very ample* if F is basepoint-free and the map i_F is a closed immersion.

Lemma 2.8. *Let F be a divisor of degree at least $2g + 1$ on X. Then F is very ample.*

Proof. Lemma 2.7 implies that F is basepoint-free, so it remains to show that i_F is a closed immersion. We may assume that k is algebraically closed, since extension of the base field does not affect the property of i_F being a closed immersion. For every two closed points P, Q of X, we have

$$\dim_k L(X, F - P - Q) = \deg F - g - 1 = \dim_k(X, F) - 2.$$

The claim now follows from Hartshorne [4, IV, Proposition 3.1(b)]. □

2.3. Picard groups and Jacobian varieties

In the correspondence between number fields and function fields, the analogue of the class group of a number field is the *Picard group* of a curve or function field.

Definition. The *Picard group* of X (or of $K(X)$), denoted by $\operatorname{Pic} X$, is the quotient of the group of divisors on X by the subgroup of principal divisors, i.e. it is defined by the exact sequence

$$K(X)^\times \xrightarrow{\text{div}} \operatorname{Div} X \longrightarrow \operatorname{Pic} X \longrightarrow 0.$$

The class of a divisor D in $\operatorname{Pic} X$ is denoted by $[D]$.

Remark. The Picard group can also be defined as the group of isomorphism classes of line bundles on X, with the tensor product as the group operation.

Because principal divisors have degree 0, the degree map

$$\deg\colon \operatorname{Div} X \to \mathbf{Z}$$

induces a homomorphism

$$\deg\colon \operatorname{Pic} X \to \mathbf{Z}.$$

Notation. We write $\operatorname{Pic}^0 X$ for the kernel of the degree map, i.e.

$$\operatorname{Pic}^0 X = \{[D] \in \operatorname{Pic} X \mid \deg D = 0\}.$$

Theorem 2.9. *Let X be a smooth projective geometrically integral curve over k. Assume that X has a k-rational point. Then there exists an Abelian variety (projective connected group variety) $\operatorname{Jac} X$ over k with the property that for every extension field L of k, there is an isomorphism*

$$(\operatorname{Jac} X)(L) \xrightarrow{\sim} \operatorname{Pic}^0(X_L)$$

that is functorial in L.

2.4. The zeta function of a curve over a finite field

In this subsection, k will denote a finite field of q elements, and X will denote a smooth projective geometrically integral curve over k.

We define the *zeta function* of X by

$$\mathrm{Z}_X = \prod_{P \in \operatorname{PDiv} X} \frac{1}{1 - t^{\deg P}} = \prod_{d \ge 1} (1 - t^d)^{-\# \operatorname{PDiv}^d X} \in \mathbf{Z}[[t]],$$

where $\operatorname{PDiv}^d X$ is the set of prime divisors of degree d.

Theorem 2.10. *Let X be a smooth projective geometrically integral curve over a finite field k of q elements.*

(a) The zeta function of X can be written as

$$\mathrm{Z}_X = \frac{L_X}{(1-t)(1-qt)},$$

where $L_X \in \mathbf{Z}[t]$ is a polynomial of the form

$$L_X = 1 + a_1 t + \cdots + a_{2g-1} t^{2g-1} + q^g t^{2g}$$

(b) The polynomial L_X factors over $\mathbf{C}$ as

$$L_X = (1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_{2g} t),$$

where the α_i are complex number of absolute value $\sqrt{q}$.

(c) The polynomial L_X satisfies

$$q^g t^{2g} L_X(1/qt) = L_X(t).$$

(d) We have

$$\# X(k) = q + a_1 + 1$$

and

$$\# \operatorname{Pic}^0 X = L_X(1).$$

2.5. Exercises

2.1. Let D and D' be two divisors on X that are linearly equivalent. Show that the k-vector spaces $L(X,D)$ and $L(X,D')$ are isomorphic.

2.2. (a) Show that the group $\operatorname{Pic}^0_{\mathbf{P}^1_k}$ is trivial.

(b) Verify the Riemann–Roch theorem for all divisors D on $\mathbf{P}^1_k$.

2.3. Let X be a smooth projective geometrically integral curve over k, and let D be a divisor on X. Show that D is basepoint-free if and only if there exists an ideal generating set for D.

3. Algorithms for curves and Picard groups

Throughout this section, X will denote a smooth projective geometrically integral curve of genus g over k.

3.1. Khuri-Makdisi's representation of a curve

We fix a divisor F satisfying

$$\deg F \ge 2g+1.$$

For all $i \ge 0$, we write

$$V^i = L(X, iF).$$

Then we have

$$\dim V^i = \begin{cases} 1 & \text{for } i=0,\\ 1-g+i\deg F & \text{for } i>0.\end{cases}$$

If D is a divisor on X, we write

$$V^i_D = L(X, iF-D).$$

We will usually restrict to divisors D satisfying

$$\deg D \le i \deg F - (2g+1)$$

We note that for any two divisors D and E, we have a canonical k-bilinear multiplication map

$$L(X,D)\times L(X,E) \longrightarrow L(X,D+E),$$

which induces a k-linear map

$$\mu_{D,E}\colon L(X,D)\otimes_k L(X,E) \longrightarrow L(X,D+E).$$

Lemma 3.1. *Let D and E be two line bundles of degree at least $2g+1$. Then the k-linear map $\mu_{D,E}$ is surjective.*

Proof. This is more subtle than the statement might suggest; the proof that I know uses a small amount of of cohomology of vector bundles and a method known as the “basepoint-free pencil trick”. See [5, Lemma 2.2] for a sketch. □

Lemma 3.2. *Let D, E and F be three divisors on X such that D is effective. Assume that F is basepoint-free, and let W be a ideal generating set for F. Then the inclusion*

$$L(X,E-D) \subseteq \{g \in L(X,E) \mid g\cdot W \subseteq L(X,E+F-D)\} \tag{3.1}$$

is an equality.

Proof. By Proposition 2.2, it suffices to prove the claim after base extension to an algebraic closure $\bar{k}$ of k. We write

$$E-D = \sum_{x\in X(\bar{k})} m_x x, \quad F = \sum_{x\in X(\bar{k})} n_x x.$$

Let g be an element of the right-hand side of (3.1); we need to prove that g is in $L(X,E-D)$. For any $x\in X(\bar{k})$, we can find $h\in W$ such that $\operatorname{ord}_x h = -n_x$ because W is an ideal generating set for F. Since gh is in $L(X,E+F-D)$, we have $\operatorname{ord}_x(gh)+m_x+n_x \ge 0$. It follows that $\operatorname{ord}_x(g)+m_x \ge 0$. Since this holds for all $x\in X(\bar{k})$, we conclude that g is in $L(X,E-D)$. □

Motivated by these results, we represent our curve by giving the spaces

$$V^0, V^1, \ldots, V^7$$

together with the multiplication maps

$$V^i \times V^j \to V^{i+j} \quad \text{for } i, j \geq 0 \text{ and } i + j \leq 7.$$

(The number 7 is explained by the fact that all algorithms can be performed using only subspaces of the V^i with $i \leq 7$.)

For simplicity, we assume that the curve X has a k-rational point O. We fix a uniformiser t of the local ring $\mathcal{O}_{X,O}$. Elements of the spaces V^i are represented by power series in t up to sufficient precision to identify them uniquely as elements of V^i. The spaces V^i themselves are represented by k-bases of such power series. This allows us to easily evaluate the multiplication maps $V^i \times V^j \to V^{i+j}$.

Remark. To construct our curve, we actually only need to give a basis for V^1 to sufficient precision. Namely, by Lemma 3.1, we can compute bases for the other V^i by taking products of the basis elements of V^1.

Example. Let k be a field of characteristic not dividing 6, and let X be an elliptic curve over k given by a Weierstraß equation

$$y^2 = x^3 + ax + b.$$

Let O be the unique point at infinity, and let

$$R = k[x, y]/(y^2 - x^3 - ax - b).$$

We take $F = 3O$. We obtain

$$V^i = \{f \in R \mid \mathrm{ord}_O(f) \leq 3i\}.$$

More concretely,

$$\begin{aligned}
V^0 &= k, \\
V^1 &= \mathrm{span}\{1, x, y\}, \\
V^2 &= \mathrm{span}\{1, x, y, x^2, xy, x^3\}, \\
V^3 &= \mathrm{span}\{1, x, y, x^2, xy, x^3, x^2y, x^4, x^3y\}.
\end{aligned}$$

The element

$$t = x/y$$

is a uniformiser of the local ring $\mathcal{O}_{X,O}$, and one can compute

$$\begin{aligned}
x &= t^{-2} - at^2 - bt^4 - a^2t^6 - 3abt^8 - (2a^3 + 2b^2)t^{10} - 10a^2bt^{12} + O(t^{14}), \\
y &= t^{-3} - at - bt^3 - a^2t^5 - 3abt^7 - (2a^3 + 2b^2)t^9 - 10a^2bt^{11} + O(t^{13}).
\end{aligned}$$

3.2. Computing in the Picard group

Let x be an element of $\mathrm{Pic}^0 X$. We can write the divisor class x as $[F - D]$, where F is our fixed divisor of degree $d \geq 2g + 1$ and D is some effective divisor of degree d. We represent D by the subspace

$$V_D^2 = L(X, 2F - D) \subset L(X, 2F) = V^2$$

of codimension d.

In [5], Khuri-Makdisi developed a very elegant framework for computing in the Picard group of X using this representation of X and of divisors D as above. In [6], he improved the complexity by making clever use of ideal generating sets (basepoint-free subspaces) of the spaces $L(X, D)$ instead of the full spaces where possible. The resulting algorithms have the best known asymptotic complexity (as the genus grows) for general curves, thanks to the fact that the fundamental operations are reduced to linear algebra. We now very briefly sketch how this works.

A representative for the zero element of $\operatorname{Pic}^0 X$ can be generated as follows. We choose any non-zero element $s \in V^1$ and compute

$$sV^1 = \{st \mid t \in V^1\} \subset V^2.$$

For example, if F is effective and we take $s = 1$, we obtain $sV^1 = L(X, F) = L(X, 2F - F)$, which encodes the divisor $F - F = 0$.

Testing whether a subspace V_D^2 represents the zero element can be done using Lemma 3.2. Namely, we can compute

$$L(X, F - D) = \{s \in L(X, F) \mid s \cdot W \subseteq L(X, 2F - D)\},$$

or more compactly

$$V_D^1 = \{s \in V^1 \mid s \cdot W \subseteq V_D^2\},$$

where W is any basepoint-free subspace of $L(X, F)$. We then note that since the divisor $F - D$ has degree 0, the space $L(X, F - D)$ is non-zero if and only if $F - D$ is principal.

As in the case of elliptic curves, the group operation is reduced to the "addflip" operation

$$(x, y) \mapsto -x - y,$$

which is more fundamental from a computational point of view. This operation can be implemented as follows. Suppose we are given two elements $x, y \in \operatorname{Pic}^0 X$, represented by subspaces $V_D^2 = L(X, 2F - D)$ and $V_E^2 = L(X, 2F - E)$ as above. Using Lemma 3.1, we then compute

$$V_{D+E}^4 = V_D^2 \cdot V_E^2.$$

(Here we write $V_D^2 \cdot V_E^2$ for the image of $V_D^2 \otimes V_E^2$ under the multiplication map $V^2 \otimes V^2 \to V^4$, i.e. the subspace of V^4 spanned by all products st with $s \in V_D^2$ and $t \in V_E^2$.) Next, using Lemma 3.2, we can compute

$$V_{D+E}^3 = \{s \in V^3 \mid s \cdot W \subseteq V_{D+E}^4\},$$

where W is any basepoint-free subspace of $V = L(X, F)$. In the resulting space, we choose any non-zero element

$$s \in V_{D+E}^3 = L(X, 3F - D - E).$$

We may write $\operatorname{div} s = D + E + S - 3F$, where S is an effective divisor. Since $x = [F - D]$ and $y = [F - E]$, we have

$$-x - y = [D + E - 2F] = [F - S],$$

so that the subspace V_S^2 of V^2 represents $-x - y$. We compute

$$V_{D+E+S}^5 = L(X, 5F - D - E - S) = s \cdot V^2.$$

Finally, we compute (again using Lemma 3.2)

$$V_S^2 = \{t \in V^2 \mid t \cdot W \subseteq V_{D+E+S}^5\},$$

where W is any basepoint-free subspace of V_{D+E}^3.

From the addflip operation we immediately obtain negation by

$$-x = -0 - x$$

and addition by

$$x + y = -(-x - y).$$

The problem of testing for equality is easily reduced to testing for zero by

$$x = y \iff x - y = 0.$$

For more on these algorithms and for the complexity analysis, we refer to Khuri-Makdisi's papers [5] and [6].

3.3. Algorithms over finite fields

The type of function fields that most resemble number fields are function fields over finite fields. In this case, the author developed algorithms for various tasks in the paper [1]. These algorithms are implemented in the author's `modgalrep` package [2]. We just list the algorithms and refer to [1] and [2] for all details.

- Picking uniformly random divisors and elements of the Picard group
- Decomposing divisors as linear combinations of prime divisors
- Applying the Frobenius map to Picard group elements defined over an extension of the base field
- Computing Frey–Rück (or Tate) pairings and Weil pairings
- Computing a basis for the l-torsion of the Picard group for prime numbers l

References

[1] P. J. Bruin, Computing in Picard groups of projective curves over finite fields. Mathematics of Computation **82** (2013), 1711–1756.

[2] P. J. Bruin, `modgalrep` software package, `https://gitlab.com/pbruin/modgalrep`.

[3] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*. Benjamin, New York, 1969. Available at `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`.

[4] R. Hartshorne, *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[5] K. Khuri-Makdisi, Linear algebra algorithms for divisors on an algebraic curve. *Mathematics of Computation* **73** (2004), no. 245, 333–357.

[6] K. Khuri-Makdisi, Asymptotically fast group operations on Jacobians of general curves. *Mathematics of Computation* **76** (2007), no. 260, 2213–2239.

[7] The Stacks project authors, *The Stacks project*, 2018, `http://stacks.math.columbia.edu`.