Curves, function fields and Picard groups, Part 1

Preliminary version, 26 May 2018

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

Abstract: In the current version of these notes, we give a brief introduction to curves and function fields. The final version will treat algorithmic aspects of function fields of large genus, in particular Khuri-Makdisi’s algorithmic framework for computing with curves and their Picard groups.

Introduction
The goal of these notes (which are still under construction) is to introduce some algorithmic aspects of algebraic curves, function fields, and their Picard groups and Jacobian varieties.

The main prerequisite is some basic algebraic geometry, such as Fulton’s book [1] or the first chapter of Hartshorne’s book [2]. 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

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

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 Frac $R$ for the field of fractions of $R$.

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

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

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

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

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 $n \in \mathbb{Z}$ with $xR = m_R^n$; this $n$ is denoted by ord$_R(x)$. This gives a surjective group homomorphism

$$\text{ord}_R: K^\times \to \mathbb{Z}.$$ 

**Definition.** A valuation ring is a domain $R$ such that for every $x$ in $(\text{Frac} R)^\times$, 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 $U \subseteq X$) is a finitely generated extension of transcendence degree $1$ over $k$.

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

2
(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 $O_{X,x}$ viewed as a subring of $K(X)$.

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

(e) Let $C_k$ be the category of regular projective integral curves over $k$ with dominant morphisms, and let $F_k$ be the category of function fields over $k$ with inclusions. The association $X \mapsto K(X)$ and $(\phi: X \to Y) \mapsto (\phi^*: K(Y) \to K(X))$ is a contravariant equivalence of categories from $C_k$ to $F_k$.

Proof. This is essentially [1, §7.5, Corollary to Theorem 3].

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 $\text{Div } X$ 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 $n_x \geq 0$ for all closed points $x$ of $X$.

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

Definition. The degree map is the group homomorphism

$$\text{deg}: \text{Div } X \rightarrow \mathbb{Z}$$

$$\sum_{x \in X} n_x x \mapsto \sum_{x \in X} n_x \text{deg } x.$$

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

$$\text{ord}_x(f) = \text{ord}_{O_{X,x}}(f).$$

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

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

Definition. The group of principal divisors on $X$ is

$$\text{PDiv } X = \{ \text{div } f \mid f \in K(X)^\times \}.$$ 

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 $O_X(D)$ 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 $O_X(D)$ on $X$ by

$$O_X(D)(U) = \begin{cases} \{ f \in K(X) \mid \text{ord}_x f + n_x \geq 0 \text{ for all closed points } x \in U \} & \text{if } U \neq \emptyset, \\ 0 & \text{if } U = \emptyset. \end{cases}$$

It is not hard to check that this is a sheaf on $X$, and in fact a line bundle (locally free sheaf of $O_X$-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

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

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

The map

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

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 $d(fg) = gdf + f dg$.

**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 [1, 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 [5, tag 00TQ].

Let $X$ be a smooth integral curve over $k$. If $\omega$ 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 $m_{X,x}^n \mathcal{O}_{X/k,x}$ for a unique $n \in \mathbb{Z}$.

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

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

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

Alternatively, $\text{ord}_x \omega$ can be computed as follows. Let $t \in \mathcal{O}_{X,x}$ be a uniformiser, and let $f$ be the unique element of $K(X)^\times$ such that $\omega = f dt$. Then we have

$$\text{ord}_x \omega = \text{ord}_x(f).$$

One can show that this is independent of the choice of $t$ [1, § 8.5].
Example. Let $X = \mathbb{P}^1_k$ 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 $\mathbb{A}^1_k \subset \mathbb{P}^1_k$, which has coordinate ring $k[t]$, the element $dt$ generates the module of differentials at every point, i.e. for every point $x \in \mathbb{A}^1_k$, we have

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

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

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

We conclude that

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

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

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

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 $\omega$ be a non-zero meromorphic differential on $X$. The divisor of $\omega$ is

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

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

Note that all canonical divisors on $X$ are linearly equivalent.

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

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

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 $m = (x, y)$ be its maximal ideal, and let $f \in m$ 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 finite extension of $k$ of transcendence degree 1. 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

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

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 $(dx_1, \ldots, dx_n)$ and $df_1, \ldots, df_m$ are the elements of this module defined by $df_i = \sum_j \frac{\partial f_i}{\partial x_j} \, dx_j$.

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 $\text{div} \, f + D$ is effective. Furthermore, if $D = \sum x \in X n_x x$, the definition of $L(X, D)$ is equivalent to

$$L(X, D) = \bigcap_{x \in X} m_X^{n_x} \subset K(X),$$

where $x$ ranges over the set of closed points of $X$ and $m_X$ 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 $X = \mathbb{P}^1_k$ and $D = n\infty$ with $n \in \mathbb{Z}$. The space $L(X, n\infty)$ consists of rational functions that have no poles on $\mathbb{A}^1_k$ (i.e. polynomials) and a pole of order at most $n$ at $\infty$. Hence

$$L(X, n\infty) = \{f \in k[t] \mid \deg f \leq n\}$$
Proof. In particular, we have
\[ \dim_k L(X, n\infty) = \max\{0, n + 1\} . \]

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 \textit{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
\[ D_{k'} = \sum_{x \in X} n_x \sum_{y \to x} e(y/x)y, \quad (2.2) \]
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 \( x \).

\textbf{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 \( k = \mathbb{F}_p(v) \), let \( X = \mathbb{P}_k^1 \) 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
\[ L(X, D) \otimes k' \rightarrow L(X, D)k' \subset K(X_{k'}). \]

\textbf{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
\[ L(X, D) \otimes_k k' \rightarrow L(X_{k'}, D_{k'}) \]
In particular, we have
\[ \dim_k L(X, D) = \dim_{k'} L(X_{k'}, D_{k'}). \]

\textbf{Proof.} It is clear that the map is injective because it can be viewed as a restriction of the isomorphism \( K(X) \otimes_k k' \rightarrow K(X)k' = K(X_{k'}) \) 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
\[ m_{x, k'} = \prod_{y \to x} m_{x_{k'}, y}^{e(y/x)}. \]
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.

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

\textbf{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 \( \Omega_{X/k}(-D) \).

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

\textbf{Corollary 2.4.} If \( \mathcal{K} \) is a canonical divisor on \( X \), then we have
\[ \deg \mathcal{K} = 2g - 2. \]

\textbf{Proof.} Take \( D = \mathcal{K} \) in the Riemann–Roch theorem. \( \Box \)
**Definition.** A divisor $D$ on $X$ is *special* if the space $L(X, K - D)$ is non-zero.

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

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

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

$$\deg D < 0 \implies L(X, D) = 0,$$

$$\deg D \geq 2g - 1 \implies D\text{ is non-special}.$$

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

**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 $r: X_{k'} \to X$ 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 $L(X_{k'}, D_{k'}) = L(X, D) \otimes_k k'$ vanish in $Q$. 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. \hfill \Box

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

**Proof.** Thanks to the previous lemma, 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 [2, IV, Proposition 3.1(a)]. \hfill \Box

**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 [4]) 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 $PV$ be the projective space of hyperplanes in $V$; this can be defined as a projective $k$-scheme by

$$PV = \text{Proj} \left( \bigoplus_{n \geq 0} \text{Sym}_k^n V \right).$$
For any point $P \in X(k')$ with $k'$ an extension field of $k$, the hyperplane $V_P$ defines a point in $(PV)(k')$ that we also denote by $V_P$. More generally, any point of $X$ over a $k$-algebra $R$ defines an $R$-valued point of $PV$. We get a map

$$i_F: X \to PV$$

$$P \mapsto V_P.$$ 

**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 [2, 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 $K(X)$) is the quotient of the group of divisors on $X$ by the subgroup of principal divisors, i.e.

$$\text{Pic} X = (\text{Div} X) / (\text{PDiv} X).$$

The class of a divisor $D$ in $\text{Pic} X$ 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

$$\deg: \text{Div} X \to \mathbb{Z}$$

induces a homomorphism

$$\deg: \text{Pic} X \to \mathbb{Z}.$$ 

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

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

**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) $\text{Jac} X$ over $k$ with the property that for every extension field $L$ of $k$, there is an isomorphism

$$(\text{Jac} X)(L) \sim \rightarrow \text{Pic}^0(X_L)$$

that is functorial in $L$.

### References


