Part IIB Algebraic Curves Course 1998 pmhw@dpmms.cam.ac.uk

Abbreviated Lecture Notes

Introduction. Let k be a field. Algebraic Geometry concerns itself with the zero loci in k^n of systems of polynomials in n variables. For instance, when $n = 2$, we might study the solutions of a single polynomial equation $f(x, y) = 0$. In this formulation however, questions of arithmetic arise; in order to concentrate on the geometry, we'll restrict ourselves to the case of k algebraically closed (i.e. $k = \bar{k}$).

There are two pieces of algebra from the Part 1B Optional course on Algebra (Groups, Rings and Fields) which we shall need.

(a) The ring of polynomials $k[X_1, \ldots, X_n]$ in n variables has unique factorization.

(b) Hilbert's Basis Theorem : Any ideal in $k[X_1, \ldots, X_n]$ is finitely generated.

It is Hilbert's Basis Theorem which always allows us to reduce down to a finite set of polynomial equations. For if $V \subset k^n$ is the zero locus of some (perhaps infinite) collection of polynomials, we set I to be the ideal in $k[X_1, \ldots, X_n]$ generated by these polynomials. It is clear that

$$V = \{\mathbf{x} \in k^n \ ; \ f(\mathbf{x}) = 0 \text{ for all } f \in I\}.$$

Hilbert's Basis Theorem tells us that I is generated by a finite set of polynomials $f_1, \ldots, f_m$ say, from which it follows that V is the zero locus of this finite collection. Since each f_i can be written as a finite combination of the original polynomials (with coefficients from the polynomial ring), we can take as the defining set for V a finite subset of the original collection of defining polynomials.

We can however say far more about the geometry if we consider not the *affine varieties* which have been described above, but instead *projective* varieties as defined below. In the case of algebraic curves, a projective curve may in fact be obtained from an affine one by adding finitely many points (see (1.3)); for instance $\mathbf{P}^1(\mathbf{C})$ defined below may be obtained by adding a single point ∞ to the affine curve $\mathbf{C}$, a fact you learnt in your first term of 1A, since $\mathbf{P}^1(\mathbf{C})$ may be identified as the Riemann sphere.

§1. If W is a vector space over a field k, define the associated *projective space*

$$\mathbf{P}(W) = \{\text{1-dimensional subspaces of } W\}.$$

A linear subspace is a subset of the form $\mathbf{P}(U)$ for U a subspace of W. If $\dim(W) = n+1$, we say that $\mathbf{P}(W)$ is an n-dimensional projective space and denote it by $\mathbf{P}^n$. A linear subspace $\mathbf{P}(U) \subset \mathbf{P}(W)$ is called a *hyperplane* if $\dim(W) = \dim(U)+1$. Note that $\mathbf{P}(U_1) \cap \mathbf{P}(U_2) = \mathbf{P}(U_1 \cap U_2)$, and so the intersection of two linear subspaces is a linear subspace. Moreover, if $\dim\mathbf{P}(U_1) + \dim\mathbf{P}(U_2) \geq \dim\mathbf{P}(W)$, then $\dim(U_1) + \dim(U_2) > \dim(W)$, from which it follows that $\dim(U_1 \cap U_2) > 0$, and so in particular $\mathbf{P}(U_1) \cap \mathbf{P}(U_2) \neq \emptyset$. For instance, two lines in $\mathbf{P}^2$ **always** meet.

An affine n-space $\mathbf{A}^n$ over k is just an n-dimensional affine subspace of a vector space defined over k, i.e. a coset of an n-dimensional linear subspace. If we choose a point on the affine n-space, the affine space then has the structure of a vector space, since its points have displacement vectors from the given point which are elements of the n-dimensional subspace.

Suppose now $\mathbf{P}(U) \subset \mathbf{P}(W)$ a hyperplane and let L be any coset of U not containing the origin, an affine n-space. There exists a natural embedding $L \hookrightarrow \mathbf{P}(W)$ with complement $\mathbf{P}(U)$ – easy check for reader (draw a picture). Thus the complement of a hyperplane in $\mathbf{P}^n$ has the natural structure of an affine n-space $\mathbf{A}^n$ over k.

By choosing a basis $e_0, \ldots, e_n$ for W, a point of $\mathbf{P}(W)$ corresponds to a equivalence class of vectors $\sum_{i=0}^n x_i e_i$ under the relation given by non-zero scalar multiplication. Thus a point of $\mathbf{P}(W)$ is given by *homogeneous coordinates* $(x_0 : x_1 : \ldots : x_n)$, where $\mathbf{x}$ and $\mathbf{y}$ represent the same point $\iff \mathbf{y} = \lambda\mathbf{x}$ for some $\lambda \in k^*$ (non-zero elements of field k).

In terms of homogeneous coordinates, a linear subspace of $\mathbf{P}(W)$ is defined by *homogeneous linear* equations in the coordinates. Given a hyperplane $\mathbf{P}(U)$ of $\mathbf{P}(W)$, we can assume wlog that $e_1, \ldots, e_n$ form a basis of U, and then the hyperplane is given by $x_0 = 0$. The complement of the hyperplane then consists of classes $[\mathbf{v}]$, where $\mathbf{v} = (x_0 : x_1 : \ldots : x_n)$ with $x_0 \neq 0$. Taking L to be given by $x_0 = 1$ (i.e. $L = e_0 + U$), we have the identification of $\mathbf{P}(W) \setminus \mathbf{P}(U)$ with L given in terms of coordinates via

$$(x_0 : x_1 : \ldots : x_n) \mapsto (1, x_1/x_0, \ldots, x_n/x_0)$$

i.e. we have affine coordinates $(x_1/x_0, \ldots, x_n/x_0)$ on L, thereby identifying it with k^n. Conversely, given $(y_1, \ldots, y_n) \in k^n$, we have a corresponding point $(1 : y_1 : \ldots : y_n) \in \mathbf{P}(W) \setminus \mathbf{P}(U)$.

A *projective variety* $V \subset \mathbf{P}^n$ is defined to be the zero locus of a (finite) set of *homogeneous* polynomials in $X_0, \ldots, X_n$. Let $I^h(V)$ denote the ideal in $k[X_0, \ldots, X_n]$ generated by homogeneous polynomials vanishing on V – observe that $F \in I^h(V)$ iff all its homogeneous parts are in $I^h(V)$. We say that V is *irreducible* if it cannot be written as the union $V = V_1 \cup V_2$ of two proper subvarieties.

Lemma 1.1. *Any projective (or affine) variety V may be written as a finite union of irreducible varieties.*

Proof. If not, then by induction (and countable Axiom of Choice) we obtain a strictly decreasing infinite sequence of subvarieties

$$V = V_0 \supset V_1 \supset V_2 \supset \ \ldots.$$

Suppose each V_i is defined by an ideal I_i and let $W = \cap_i V_i$, a subvariety of V defined by the ideal $I = \sum_i I_i$. Hilbert's Basis Theorem implies that I is generated by finitely many (homogeneous) polynomials $f_1, \ldots, f_m$. Each generator f_j may be written as a sum of elements from only finitely many I_i, and hence $I = \sum_{i \leq N} I_i$ for some N, and so $W = \cap_{i \leq N} V_i$, contradicting our assumption.

Remark. The decomposition of V into a finite union of irreducible subvarieties is unique modulo ordering, etc. This is a nice exercise for the reader (essentially an exercise in topological spaces), but may also be found for instance in Reid's book.

Lemma 1.2. *A projective variety V is irreducible iff $I^h(V)$ is a prime ideal.*

Proof. Suppose first that V is reducible, say $V = V_1 \cup V_2$; then we can find homogenous polynomials F, G, neither of which vanish on all of V, but with F vanishing on V_1 and G vanishing on V_2. The product FG therefore is in $I^h(V)$, implying that $I^h(V)$ is not prime.

The converse in similar; if $I^h(V)$ is not prime, we can find (not necessarily homogeneous) polynomials F, G which are not in $I^h(V)$ but whose product is. By replacing F, G by their homogeneous parts of lowest degree not in $I^h(V)$, we see easily that F, G may be assumed homogeneous and not in $I^h(V)$, but with a product which is. Now letting V_1 be the subvariety of V defined by the extra equation $F = 0$, and V_2 be the subvariety given by $G = 0$, the V_i are proper subvarieties of V whose union is all of V, and hence V is reducible.

Remark. The same (or even simpler) proof gives a similar result in the affine case. One should add here that whilst (1.2) is of theoretical importance (as we shall now see), it will usually be of little practical use to us for seeing if a given projective variety is irreducible. We'll comment on this again later in the case of algebraic curves, where a more useful test will be given.

If $V \subset \mathbf{P}^n$ irreducible, a *rational function* on V is given by a quotient F/G of homogeneous polynomials of the same degree, $G \notin I^h(V)$, subject to the equivalence relation $R/S \sim F/G \iff RG - SF \in I^h(V)$. Note that F/G represents the zero function iff $F \in I^h(V)$. A rational function f on V is said to be *regular* at $P \in V$ if there is a representation F/G for f with $G(P) \neq 0$. If f is regular at P, we can define $f(P)$ in a unique way, and in this way f induces an actual function on the subset of regular points. The set of rational functions on V forms (in an obvious way) a field $k(V)$, the *function field* of V. Note that $k(V)$ is a finitely generated extension of k (if V is not contained in the hyperplane $\{X_0 = 0\}$, then $k(V)$ is generated by the rational functions $X_1/X_0, \ldots, X_n/X_0$).

In this course we shall take k to be algebraically closed (for instance the complex numbers $\mathbf{C}$); we have not used this assumption yet, but from now on it will be needed. The dimension $\dim(V)$ of an irreducible projective variety V is the smallest integer n for which there exist functions $t_1, \ldots, t_n \in k(V)$ with $k(V)$ finite over $k(t_1, \ldots, t_n)$. Note that $\dim(V) = 0$ iff V is a point – this follows from the assumption that $k = \bar{k}$, and the fact that $k(V) = k$ iff all rational functions (including the coordinate functions X_i/X_0) are constant on V, which in turn is true iff V is a point. We say that V is a *projective curve over* k if $\dim(V) = 1$, i.e. $k(V)$ is a finite extension of the field $k(t)$ of rational functions in one variable. We observe that if this is the case, and s is any non-constant rational function on V (i.e. $s \in k(V) \setminus k$), then $k(V)$ is also a finite extension of $k(s)$. To see this, we note that s satisfies an equation over $k[t]$

$$a_n(t)s^n + a_{n-1}(t)s^{n-1} + \ldots + a_1(t)s + a_0(t) = 0$$

with $a_i(t) \in k[t]$, not all the a_i being in k (the latter since $s \notin k$ and k algebraically closed). This may also be regarded as an equation for t over $k[s]$, and so $k(t, s)$ is finite over $k(s)$. Since by assumption $k(V)$ is finite over $k(t)$, the assertion follows.

Suppose we have chosen homogeneous coordinates $X_0, \ldots, X_n$ on $\mathbf{P}^n$; the complement of the hyperplane $\{X_0 = 0\}$ is an affine n-space $\mathbf{A}_0^n$, which has affine coordinates $y_1, \ldots, y_n$ given by $y_i = X_i/X_0$. Similarly the complements of the other coordinate hyperplanes are affine n-spaces and have corresponding affine coordinates. These $n+1$ affine n-spaces form

an *affine cover* of $\mathbf{P}^n$. If now $V \subset \mathbf{P}^n$ is a projective variety, then $V_0 = V \cap \mathbf{A}_0^n$ is the subset of $\mathbf{A}_0^n$ defined by the polynomials $f(y_1, \ldots, y_n) = F(1, y_1, \ldots, y_n) \in k[y_1, \ldots, y_n]$ obtained from the homogeneous polynomials defining V. Such a subset of $\mathbf{A}^n$ is called an affine variety, and so in this way we obtain an *affine covering* of V by affine varieties.

If $U \subset \mathbf{A}^n$ is an affine variety, we define its *coordinate ring* $k[U]$ to be the ring of polynomial functions on U, which in turn may be identified as $k[U] = k[x_1, \ldots, x_n]/I(U)$, where $I(U) = \{f \in k[x_1, \ldots, x_n] \; ; f(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in U\}$. In fact, $k[U]$ is a k-algebra, which means that it contains k as a subring. If U is a non-empty affine piece of a projective variety $V \subset \mathbf{P}^n$, it is an easy check that $I(U)$ is prime if $I^h(V)$ is prime – if $fg \in I(U)$, then $X_0 FG \in I^h(V)$ and hence either F or G is in $I^h(V)$, and so either f or g is in $I(U)$. Hence by (1.2), U is irreducible if V is irreducible. Under these circumstances $k[U]$ is an integral domain, and its field of fractions (known as the function field of U) consists of rational functions f/g on U, with $f, g \in k[x_1, \ldots, x_n]$, $g \notin I(U)$, subject to the obvious equivalence relation analogous to that used in the projective case. Thus if U is the affine piece of V given by $X_0 \neq 0$, we have an isomorphism of function fields $k(V) \to k(U)$ obtained by 'putting $X_0 = 1$' in the representatives F/G of elements of $k(V)$ (more formally, writing F/G as $F(1, x_1, \ldots, x_n)/G(1, x_1, \ldots, x_n)$, with $x_i = X_i/X_0$ for $i > 0$); note here that if G vanishes on $V_0 = U$, then $X_0 G \in I^h(V)$, and thus $G \in I^h(V)$. Therefore we see (for V irreducible) that its function field $k(V)$ is determined by any (non-empty) affine piece.

Lemma 1.3. *If V is an irreducible algebraic (affine or projective) curve, then its only proper subvarieties are finite.*

Proof. By (1.1), proper subvarieties are finite unions of irreducible proper subvarieties. So we need to prove that every irreducible proper subvariety W consists of a single point.

By considering a finite affine cover, we can reduce to the affine case $W \subset V \subset \mathbf{A}^n$, and so we have a surjective homomorphism of coordinate rings

$$k[V] = k[x_1, \ldots, x_n]/I(V) \to k[W] = k[x_1, \ldots, x_n]/I(W).$$

Let $0 \neq f \in k[V]$ map to zero in $k[W]$; if W is not a point, we can choose a non-constant element $\bar{g} \in k[W] \subset k(W)$, and then for any lift $g \in k[V]$ of $\bar{g}$, we check easily that f, g are algebraically independent as elements of $k(V)$ over k, that is there is no polynomial relation over k between f and g (wlog such a relation is not a multiple of f since $k[V]$ integral, and then take its image in $k[W]$). This then contradicts our assumption that $\dim(V) = 1$ (by previous argument, neither f nor g being constant).

When studying specific examples, the converse to (1.3) is a useful criterion for showing that an algebraic curve is irreducible. If V is a projective or affine variety with infinitely many points, but such that the only proper subvarieties are finite, then by (1.1) it must be irreducible (it will in fact be a curve, but this will be clear in the examples we study).

As an example of the above ideas, let us consider the important case of $V \subset \mathbf{P}^2$ defined by a homogeneous polynomial $F(X_0, X_1, X_2)$ of positive degree; we have an affine piece U of V given by a polynomial $f(x, y)$ where $x = X_1/X_0$ and $y = X_2/X_0$. Assuming F is not divisible by X_0, we have that F is irreducible iff f is irreducible.

Lemma 1.4. *Given $f, g \in k[x, y]$ coprime polynomials, there exist polynomials $\alpha, \beta \in k[x, y]$ such that $\alpha f + \beta g = h$, where $0 \neq h \in k[x]$ is a polynomial in x only.*

This lemma follows easily (essentially just eliminate inductively the variable y, or alternatively use Gauss's Lemma). From Lemma 1.4, it follows that if F is irreducible, then the only proper subvarieties of V are finite sets of points. To prove this we observe that, since V has a finite affine cover, we can reduce to the affine case $U \subset \mathbf{A}^2$, given an irreducible (non-constant) polynomial $f(x, y)$. Suppose now we have any $g \in k[x, y]$, $g \notin I(U)$, then f and g are coprime and we can apply (1.4). In particular, if $P = (u, v)$ satisfies $f(P) = 0 = g(P)$, then $h(u) = 0$, so there are only finitely many x-coordinates for such points P; similarly, there are only finitely many y-coordinates, and hence only finitely many such points. However V has infinitely many points (for all but finitely many x-coordinates, can solve for a y-coordinate), and so it follows that V must be irreducible. Moreover, the above agument also shows that if $g \in I(U)$, then f divides g; i.e. that $I(U) = (f)$. The function field $k(V)$ is then naturally isomorphic to the field of fractions of the integral domain $k[x, y]/(f)$, and it is also then clear that $\dim(V) = 1$; such a variety V is called a *plane projective curve.*

Given a point P of an irreducible projective variety V, the *local ring of the variety at* P is defined as $\mathcal{O}_{V,P} = \{h \in k(V) \ : \ h \text{ regular at } P\}$. This is clearly a subring of $k(V)$ and has a maximal ideal $m_{V,P} = \{h \in \mathcal{O}_{V,P} \ : \ h(P) = 0\}$. Clearly the units (invertible elements) $U(\mathcal{O}_{V,P})$ of the ring are precisely the elements not in the maximal ideal, i.e. $m_{V,P} =$ non-units of $\mathcal{O}_{V,P}$. Since any proper ideal consists of non-units, this shows that $m_{V,P}$ is the *unique* maximal ideal of $\mathcal{O}_{V,P}$; in general, a ring with this property is called a *local ring.* The local properties of V at P are encoded in this ring. Note that $\mathcal{O}_{V,P}$ is an integral domain with $k(V)$ as its field of fractions, and that if V_0 is an affine piece of V

containing P, then $\mathcal{O}_{V,P}$ is determined by V_0, i.e. $\mathcal{O}_{V,P} = \{f/g \ ; \ f, g \in k[V_0], g(P) \neq 0\}$.

A local integral domain A with maximal ideal m is called a *discrete valuation ring* (DVR) if there exists $t \in m$ such that every non-zero element $a \in A$ can be written in the form $a = ut^n$ for some $n \geq 0$ and unit $u \in U(A)$. If V is an algebraic curve and $P \in V$, we say that P is a *smooth* or *non-singular* point of V if $\mathcal{O}_{V,P}$ is a DVR; an element $t \in m_{V,P}$ as above is called a *local parameter* or *local coordinate at* P. To motivate this definition, I observe (without proof) that for the case $k = \mathbf{C}$ a local parameter t will determine a local chart from a neighbourhood of P in V to a neighbourhood of $0 \in \mathbf{C}$, so that a *smooth* complex curve may also be considered as a Riemann Surface (as an exercise for the reader, I observe that a smooth complex *projective* curve will then be a *compact* Riemann surface). If P is not a smooth point, we say that P is a *singularity* of V. For plane curves, these definitions are seen (1.5) to be equivalent to the usual definitions in terms of vanishing of partial derivatives of an irreducible defining polynomial.

Lemma 1.5. *An affine plane curve $U \subset \mathbf{A}^2$ given by an irreducible polynomial $f \in k[x, y]$ is singular at $P \in U$ iff $\partial f/\partial x\,(P) = 0 = \partial f/\partial y\,(P)$.*

Proof. Easily checked that the vanishing of partial derivatives (which can be defined purely formally) is independent of the affine coordinate system chosen, and so in particular we may assume that P is the origin $(0, 0)$. Further, if we write $f = f_1 + f_2 + \ldots + f_d$, where $\deg(f_i) = i$, then the partial derivatives vanish at the origin iff the linear part f_1 is zero. Thus the Lemma is asserting that $f_1 = 0$ iff P is a singularity.

To see this, suppose first that P is non-singular; then there exists a local parameter $t \in k[U]$ such that $x = u_1 t^r$ and $y = u_2 t^s$, where u_1, u_2 are units, and **at least one of** r and s, wlog $s = 1$ (because $m_{U,P} = (x, y) \subset \mathcal{O}_{U,P}$). Therefore $x = uy^r$ for some unit u in $\mathcal{O}_{U,P}$, say $u = v_1/v_2$ with $v_i \in k[x, y]$ with $v_i(P) \neq 0$. Therefore $v_2 x = v_1 y^r$ as elements of $k[U]$, or as polynomials that $v_2 x - v_1 y^r \in I(U) = (f)$. Thus f divides the polynomial $v_2 x - v_1 y^r$, and hence $f_1 \neq 0$.

Conversely, suppose that $f_1 \neq 0$ and that affine coordinates have been chosen with $P = (0, 0)$ and $f = x - y +$ higher order terms. Thus $f = x\,p(x) - y\,q(x, y)$, with $p(0) \neq 0$ and $q(0, 0) \neq 0$. In particular we note that $x = vy$ in $\mathcal{O}_{U,P}$, with v a unit.

Claim. $\mathcal{O}_{U,P}$ is a DVR with local parameter y.

Given non-zero $a \in \mathcal{O}_{U,P}$, write $a = wg$ with w a unit and $g = g(x, y)$ a polynomial. If

$g(P) \neq 0$, we are done since it is a unit in $\mathcal{O}_{U,P}$; if not then we can use the relation $x = vy$ to substitute for x in g, and obtain the fact that g is a multiple of y in $\mathcal{O}_{U,P}$. Provided we can show that $g \notin (y^{(M+1)})$ for some $M \geq 0$, we shall then be home by induction, since the process then has to terminate. The required fact however follows from (1.4), since f, g are coprime polynomials, and hence there exist $\alpha, \beta \in k[x, y]$ with $\alpha f + \beta g = y^M h(y)$ for some $M \geq 0$ and some polynomial h with $h(0) \neq 0$. Thus h represents a unit in $\mathcal{O}_{U,P}$, and so $y^M \in (g)$ in $\mathcal{O}_{U,P}$; i.e. y^M is divisible by g, which rules out the possibility that g is divisible by $y^{(M+1)}$. QED

Given the DVR $\mathcal{O}_{V,P}$, we have a well-defined function $v_P : k(V)^* \to \mathbf{Z}$, where $v_P(ut^n) = n$ (notation as above), called the *valuation* at P; this gives the order of a *zero* or *pole* at P of a non-zero rational function. Note that $v_P(fg) = v_P(f) + v_P(g)$ (so that v_P is a homomorphism of abelian groups) and $v_P(f + g) \geq \min\{v_P(f), v_P(g)\}$.

For V an irreducible projective variety, a rational map $\phi : V - \to \mathbf{P}^m$ is given by an $(m+1)$-tuple $(f_0 : \ldots : f_m)$ of elements of $k(V)$ (not all zero) modulo that $(f_0 : \ldots : f_m)$ and $(h_0 : \ldots : h_m)$ define the same rational map iff for some $h \in k(V)^*$, we have $h_i = hf_i$ for all i. Interpreting rational functions in terms of homogeneous polynomials, we see that the rational map ϕ is given by an equivalence class of $(m+1)$-tuples of homogeneous polynomials of the same degree $(F_0 : \ldots : F_m)$, not all in $I^h(V)$, modulo the relation $\sim$, where $(F_0 : \ldots : F_m) \sim (G_0 : \ldots : G_m) \iff F_iG_j - F_jG_i \in I^h(V)$ for all i, j. We say that ϕ is *regular* at $P \in V$ if it can be written in the form $\phi = (f_0 : \ldots : f_m)$ with $f_i \in \mathcal{O}_{V,P}$ for all i and at least one non-vanishing at P – equivalently, ϕ is represented by an $(m+1)$-tuple $(F_0 : \ldots : F_m)$ such that $F_i(P) \neq 0$ for some i. We then have a well-defined image point $\phi(P)$. If $W \subset \mathbf{P}^m$ a projective variety, a rational map $\phi : V - \to W$ is just a rational map $\phi : V - \to \mathbf{P}^m$ such that $\phi(P) \in W$ for all points P at which ϕ is regular. A *morphism* $\phi : V \to W$ is a rational map which is everywhere regular. An *isomorphism* $\phi : V \to W$ is a morphism with an inverse morphism $\psi : W \to V$. Example of twisted cubic in $\mathbf{P}^3$ being isomorphic to $\mathbf{P}^1$.

Given a morphism (or even rational map) $\phi : V \to W$ of irreducible projective varieties, we can define $\phi^*(f) = f \circ \phi$ in an obvious way, **provided** the image $\phi(V)$ is not contained in a proper subvariety of W, i.e. if a homogeneous polynomial G vanishes on $\phi(V)$, then $G \in I^h(W)$. Namely, if $\phi = (h_0 : \ldots : h_m)$, and $f = F(Y_0, \ldots, Y_m)/G(Y_0, \ldots, Y_m)$, with $G \notin I^h(W)$, then $\phi^*(f) = F(h_0, \ldots, h_m)/G(h_0, \ldots, h_m) \in k(V)$; easily checked this is well-defined. If ϕ^* is an isomorphism of function fields, we say that ϕ is *birational*. An

isomorphism induces isomorphisms of the local rings (given by composition with ϕ), and intrinsic properties of the variety are not affected.

It follows immediately from the defining property of a DVR that for V a smooth projective curve, every rational map $\phi : V - \to \mathbf{P}^m$ is a morphism. To see this, write $\phi = (f_0 : f_1 : \ldots, f_m)$; for $P \in V$, let t be a local parameter at P, and write $f_i = u_i t^{n_i}$, with u_i a unit in $\mathcal{O}_{V,P}$ and $n_i \in \mathbf{Z}$, and then clear denominators and cancel out any common factors of t.

Let us now consider morphisms between curves.

Lemma 1.6. *If $\phi : V \to W$ is a non-constant morphism between irreducible (projective) curves, then ϕ has finite fibres, i.e. $\phi^{-1}(Q)$ is finite for all $Q \in W$.*

Proof. For $Q \in W$, I claim that $\phi^{-1}(Q)$ is a subvariety of V. For suppose that $Q = (a_0 : \ldots : a_m) \in W \subset \mathbf{P}^m$, then $\phi^{-1}(Q)$ is defined by all the polynomials of the form $a_i F_j - a_j F_i$, for $(F_0 : \ldots : F_m)$ ranging over $(m+1)$-tuples of homogeneous polynomials of the same degree representing ϕ (convince yourself of this statement). This is therefore a subvariety – remember that it doesn't matter that we may have written down infinitely many equations, since by Hilbert's Basis Theorem a finite subset of equations will suffice. If ϕ is non-constant, the fibre is a proper subvariety of V, and hence finite by (1.3).

In the circumstances of (1.6), the image of ϕ is not finite, since if it were then V would be finite. So any homogeneous polynomial F which vanishes on the image must be in $I^h(W)$. From this follows that there is an induced injective homomorphism of function fields $\phi^* : k(W) \hookrightarrow k(V)$ given by 'composition with ϕ'. It follows from the above facts that there exist non-constant rational functions $s \in \phi^* k(W)$, namely of the form $s = \phi^*(x)$ for x a rational function on W which is non-constant on the image of ϕ. Since $\dim(V) = 1$, we deduce that $k(V)$ is finite over the subfield $\phi^* k(W)$. The *degree* $\deg(\phi)$ of the morphism ϕ is by definition the degree of the field extension $[k(V) : \phi^* k(W)]$.

If now $\phi : V \to W$ is a non-constant morphism between irreducible *smooth* projective curves, it also satisfies an important additional property called *finiteness* :

Finiteness Theorem. *If $\phi : V \to W$ is a non-constant morphism of smooth (irreducible) projective curves, then ϕ is surjective, and for any point $Q \in W$ and local parameter t at Q, we have $\sum_{P \in \phi^{-1}(Q)} v_P(\phi^*(t)) = \deg(\phi)$.*

The proof is omitted here (it may be found for instance in Shafarevich, pages 141-143) and is **non-examinable**. I shall issue an Appendix containing the proof for those who are interested, but my initial recommendation is to take the result on trust. Over the complex numbers, the theorem may be alternatively proved using the (analytic) theory of Riemann Surfaces. In summary, the theorem says that, counting multiplicities, the number of points in each fibre is a constant finite number, equal to the degree of the morphism. From Question 9 on the first Example Sheet, it will be seen that both the conditions smooth and projective on the curves are needed for such a statement to be true.

§2. We now introduce some tools for the study of smooth projective curves. The first of these is the concept of divisors, the terminology taken from Algebraic Number Theory. Let V be a smooth projective curve; a *divisor* D on V is a formal finite sum $D = \sum n_i P_i$ with $P_i \in V$ and $n_i \in \mathbf{Z}$. The *degree* of D is just $\deg(D) = \sum n_i$. It is convenient to extend the notation of valuations to divisors by defining $v_P(D) = n_i$ if $P = P_i$, and $v_P(D) = 0$ otherwise.

For V a smooth irreducible curve and $f \in k(V)^*$, we can write $f = F/G$ with F, G homogeneous polynomials of the same degree, neither of which is in $I^h(V)$. It therefore follows from (1.3) that f has only finitely many zeros and poles, i.e. that $v_P(f) = 0$ for all but finitely many points $P \in V$. We define the divisor of f to be $(f) = \sum_{P \in V} v_P(f)P$. Such a divisor is called a *principal divisor*. Observe that $(fg) = (f) + (g)$ and that $(f) = 0$ if $f \in k^*$. We remark that our notations are consistent in that $v_P((f)) = v_P(f)$ for all $P \in V$. Two divisors D_1, D_2 are called *linearly equivalent* if the difference $D_1 - D_2$ is a principal divisor. The linear equivalence classes of divisors form a group under addition, called the *divisor class group* $\mathrm{Cl}(V)$. For example, when $V = \mathbf{P}^1$, a divisor D has degree 0 iff it is principal, and so $\mathrm{Cl}(\mathbf{P}^1) = \mathbf{Z}$.

More generally, for any smooth irreducible projective curve V and non-constant rational function f, we have a rational map (and hence a morphism) $\phi = (1 : f) : V \to \mathbf{P}^1$. Let $\mathbf{A}^1$ be the affine piece of $\mathbf{P}^1$ given by $X_0 \neq 0$, affine coordinate $x = X_1/X_0$. Then x is a local parameter at $0 = (1 : 0)$ and $1/x$ a local parameter at $\infty = (0 : 1)$. Observe that $\phi^*(x) = f$. But then, using the Finiteness Theorem,

$$\deg\,(f) = \sum_{P \in \phi^{-1}(0)} v_P(\phi^*(x)) - \sum_{P \in \phi^{-1}(\infty)} v_P(\phi^*(1/x)) \quad = \quad \deg(\phi) - \deg(\phi) = 0$$

i.e. any principal divisor has degree 0. Hence there is an induced homomorphism of abelian groups $\deg : \mathrm{Cl}(V) \to \mathbf{Z}$.

For a smooth projective curve $V \subset \mathbf{P}^n$, any hyperplane not containing V cuts out a divisor D on V in an obvious way; namely, if the hyperplane is given by a homogeneous linear form $L(X_0, \ldots, X_n)$, then for P in the affine piece V_i given by $X_i \neq 0$, we have $v_P(D) = v_P(L/X_i)$ – clearly well-defined. We also write $D = (L)$. Any two such divisors are linearly equivalent and so have the same degree; we call this the *degree* of V in $\mathbf{P}^n$. Similarly, for G homogeneous of degree m, we obtain a divisor (G) on V of degree $m.\deg(V)$. The twisted cubic $V \subset \mathbf{P}^3$, defined to be the image of the morphism $\phi : \mathbf{P}^1 \to \mathbf{P}^3$ given by $(s^3 : s^2t : st^2 : t^3)$, has degree 3. If $V \subset \mathbf{P}^2$ is defined by an irreducible homogeneous polynomial F of degree d, then easily seen that for a line H given a homogeneous linear polynomial L, the degree of (L) on V equals the degree of (F) on H, and hence that $\deg(V) = d$.

We say that a divisor $D = \sum n_i P_i$ is *effective* , written $D \geq 0$, if $n_i \geq 0$ for all i. Given any divisor D on V, define the vector space

$$\mathcal{L}(D) = \{f \in k(V)^* \ : \ (f) + D \geq 0\} \cup \{0\}$$

i.e. if $D = \sum n_i P_i$, then $0 \neq f \in \mathcal{L}(D) \iff v_{P_i}(f) \geq -n_i$ for all i and $v_P(f) \geq 0$ for all $P \neq P_i$. For example, if $V = \mathbf{P}^1$ with affine coordinate $x = X_1/X_0$ and point $P_\infty = (0 : 1)$ at infinity, and if $D = nP_\infty$, then $\mathcal{L}(D)$ consists precisely of polynomials in x of degree at most n.

We note that if $D_1 \sim D_2$, then $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$ (if $D_1 - D_2 = (g)$, then isomorphism given by multiplication by g). We let $l(D)$ denote the dimension of $\mathcal{L}(D)$; note that $l(D) > 0 \iff \exists\ D' \geq 0$ s.t. $D' \sim D$. Also note that for V projective, $l(D) = 0$ whenever $\deg(D) < 0$, since effective divisors have non-negative degree and linearly equivalent divisors have the same degree. Moreover $\mathcal{L}(0) = k$, i.e. $l(0) = 1$, since 0 is the only effective divisor of degree 0.

Lemma 2.1. *For D a divisor on a smooth projective curve V, $l(D - P) \geq l(D) - 1$.*

Proof. Let $n = v_P(D)$ and t a local parameter at P. Define a linear map of vector spaces over k,

$$\theta : \mathcal{L}(D) \to \mathcal{O}_{V,P}/(t) \cong k$$

by $\theta(f) = (t^n f)(P)$. The kernel of θ is then $\mathcal{L}(D - P)$, and so the quotient space $\mathcal{L}(D)/\mathcal{L}(D - P)$ has dimension at most one.

If D is an effective divisor on V, it follows from (2.1) by induction on the degree that $l(D) \leq \deg(D) + 1$. Since $l(D)$ depends only on the linear eqivalence *class* of D, it is true that $l(D) \leq \deg(D) + 1$ whenever $l(D) > 0$.

Given a divisor D with $l(D) > 0$, we can choose a basis $f_0, \ldots, f_m$ for $\mathcal{L}(D)$ and define a rational map (and hence a morphism) $\phi_D : V \to \mathbf{P}^m$ by $\phi_D = (f_0 : \ldots : f_m)$; we can in fact define ϕ_D without choosing a basis as a map $\phi_D : V \to \mathbf{P}(\mathcal{L}(D)^*)$ to the projective space associated to the dual of $\mathcal{L}(D)$, but don't worry about this unless you wish to. We note however that ϕ_D depends only on the divisor *class* of D, since if $D' = D - (g)$, then $gf_0, \ldots, gf_m$ is a basis of $\mathcal{L}(D')$. In particular, suppose that $V \subset \mathbf{P}^n$ is not contained in any hyperplane and D is a fixed hyperplane section of V, *wlog* given by $X_0 = 0$. We therefore have linearly independent elements $1, X_1/X_0, \ldots, X_n/X_0$ of $\mathcal{L}(D)$. If these also span, then

$$\phi_D = (1 : X_1/X_0 : \ldots : X_n/X_0) = (X_0 : X_1 : \ldots : X_n)$$

is the original embedding, and $\deg(V) = \deg(D)$ by definition. In this situation, a general non-zero element of $\mathcal{L}(D)$ has the form $L(X_0, \ldots, X_n)/X_0$ where L is a linear homogeneous form. Thus we obtain a bijection between the projective space $\mathbf{P}(\mathcal{L}(D))$ and the hyperplane sections of V, with the multiples of $h \neq 0$ corresponding to the hyperplane section $D + (h)$. Under this correspondence, the subspace $\mathcal{L}(D - P)$ corresponds to hyperplane sections containing P and $\mathcal{L}(D - P - Q)$ to those containing both P and Q (or if $P = Q$, the hyperplanes which are tangent at P – i.e. when $P \in V \cap \{X_i \neq 0\}$, hyperplanes $L = 0$ with $v_P(L/X_i) > 1$). This latter interpretation is left as an exercise for the reader. It is clear here that for any $P, Q \in V$ (not necessarily distinct), $l(D - P - Q) \leq l(D) - 2$, and hence from (2.1) we have equality. The extremely useful Embedding Criterion gives a converse to this, where D is a divisor on a smooth projective curve V.

Embedding Criterion. *If $l(D - P - Q) = l(D) - 2$ for all $P, Q \in V$ (not necessarily distinct), then $\phi_D : V \to \mathbf{P}^{l(D)-1}$ is an embedding, that is an isomorphism of V onto a subvariety W of $\mathbf{P}^{l(D)-1}$, where the image W has degree* $\deg(D)$.

This result is also one we don't fully prove, but let us prove that the conditions do imply that ϕ_D is injective, and then indicate how the rest of the proof proceeds.

Lemma 2.2. *If D is a divisor on a smooth projective curve V such that $l(D - P - Q) = l(D) - 2$ for all points $P \neq Q$ on V, then ϕ_D is an injective morphism.*

Proof. Required to prove that if $P \neq Q$, then $\phi_D(P) \neq \phi_D(Q)$. We show first that we can find $D' \sim D$ with $v_P(D') = 0 = v_Q(D')$. Wlog, we can assume that both P and Q are in the affine piece $V_0 = V \cap \{X_0 \neq 0\}$. Letting $x_i = X_i/X_0$ $(i = 1, \ldots, n)$ be the affine coordinates on V_0, we have $m_{V,P} = (x_1 - x_1(P), \ldots, x_n - x_n(P))$ in $\mathcal{O}_{V,P}$. If L is a homogeneous linear form in $X_0, \ldots, X_n$ with $L(P) = 0$, we have that $v_P(L/X_0) = 1$ for all such L outside a codimension one subspace (viz. the kernel of the map to $m_P/m_P^2 \cong k$). By choosing such an L with $L(Q) \neq 0$, we obtain a local coordinate t_1 at P which is a unit in $\mathcal{O}_{V,Q}$. Similarly, we obtain a local coordinate t_2 at Q which is a unit in $\mathcal{O}_{V,P}$. If now $v_P(D) = a$ and $v_Q(D) = b$, the required divisor D' is $D - (t_1^a t_2^b)$. Since however $\phi_D = \phi_{D'}$, we may assume wlog that $D' = D$, i.e. that $v_P(D) = 0 = v_Q(D)$.

The assumption from the Lemma together with (2.1) implies that $l(D-P) = l(D)-1$, and $l(D - P - Q) = l(D) - 2$. If we write down a basis $f_0, \ldots, f_{m-2}$ for $\mathcal{L}(D - P - Q)$, extend to a basis $f_0, \ldots, f_{m-1}$ for $\mathcal{L}(D - P)$, and then to a basis $f_0, \ldots, f_m$ of $\mathcal{L}(D)$, it follows that the f_i are regular at both P and Q for all i, that $f_m(P) \neq 0$, $f_{m-1}(P) = 0$ and $f_{m-1}(Q) \neq 0$. Hence $\phi_D(P) \neq \phi_D(Q)$, and ϕ_D is injective as claimed.

The proof of the Embedding Criterion then proceeds roughly as follows.
(a) Show that $\phi_D(V) = W \subset \mathbf{P}^m$ is a subvariety – this follows using ideas from the Appendix on the Finiteness Theorem, and in particular needs Hilbert's Nullstellensatz.
(b) Show that W is a smooth curve – one shows that $\phi_D^* : \mathcal{O}_{V,\phi(P)} \to \mathcal{O}_{V,P}$ is an isomorphism, using fact that $l(D - 2P) = l(D) - 2$ and an argument similar to the proof of Claim 2 from the Appendix.
(c) Since $\phi_D : V \to W$ is now an injective morphism between smooth projective curves, it follows easily from the Finiteness Theorem that it is an isomorphism.
(d) Verify that a hyperplane section on W corresponds on V to an effective divisor linearly equivalent to D; hence $\deg(W) = \deg(D)$ as claimed.

As a corollary of the Embedding Criterion, we note that if $P \neq Q \in V$ with $P \sim Q$, then $l(P) > 1$. It follows that $l(P) = 2$ and $\phi_P : V \to \mathbf{P}^1$ is an isomorphism. This however can be proved without recourse to the Theorem - see Example Sheet II, Question 5.

§3. The second tool we introduce is that of Kähler differentials. For V an irreducible smooth projective curve, we define the vector space $\Omega^1_{k(V)/k}$ over $k(V)$ of *rational differentials* on V to consist of finite sums $\sum f_i dg_i$ (with $f_i, g_i \in k(V)$) subject to the relations that

(i) $da = 0$ for all $a \in k$.

(ii) $d(f+g) = df + dg$ for all $f, g \in k(V)$.

(iii) $d(fg) = fdg + gdf$ for all $f, g \in k(V)$.

As an easy exercise, it follows that $d(f/g) = (gdf - fdg)/g^2$ for $f \in k(V)$, $g \in k(V)^*$.

For V a curve and $t \in k(V)$ non-constant, we know that $k(V)$ is a finite extension of $k(t)$. If char $k = p > 0$, we would need a further fact, that t can be chosen such that $k(V)$ is a *separable* extension of $k(t)$; i.e. any $y \in k(V)$ satisfies an irreducible polynomial $H \in k(t)[Y]$ which is not a polynomial in Y^p, or in other words with $\partial H/\partial Y \not\equiv 0$. Assuming standard results on separability from the Galois Theory course, this is not hard to prove (we suppose $k(V) = k(x_1, \ldots, x_n)$ and prove that one of the x_i must have the required property). In a first course on Algebraic Curves however, I believe that it is better not to get tied up with the details for characteristic $p > 0$, and so from now on we shall assume that char $k = 0$. The main results of the course remain valid for characteristic $p > 0$ (for hyperelliptic curves one should assume $p \neq 2$, for elliptic curves that $p \neq 2$ or 3, and for the Riemann-Hurwitz Formula that p does not divide the degree n of the map), and the really assiduous reader would be able to rewrite the notes below so that the proofs included the case of positive characteristic.

For any non-constant element $t \in k(V)$, we have (in characteristic zero) that $k(V)$ is a finite separable extension of $k(t)$. From this it follows that $\Omega^1_{k(V)/k}$ is 1-dimensional over $k(V)$ with generator dt (any $g \in k(V)$ satisfies a separable polynomial equation over k(t); taking d of this equation gives dg in terms of dt).

Given a non-zero rational differential ω on V and $P \in V$, choose a local parameter $t \in m_{V,P}$. Writing $\omega = fdt$, we define $v_P(\omega) = v_P(f)$.

Lemma 3.1. *(i) The numbers $v_P(dh)$ for $h \in \mathcal{O}_{V,P}$ are bounded below.*
(ii) $v_P(dh) \geq 0$ for all $h \in \mathcal{O}_{V,P}$.
(iii) $v_P(dt') = 0$ for any local parameter t' at P.

Proof. (i) Wlog we can assume $V \subset \mathbf{A}^n$ affine. An element of $\mathcal{O}_{V,P}$ has the form $h = f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$, where $g(P) \neq 0$ and $x_i \in \mathcal{O}_{V,P}$ is the ith coordinate function on V. Therefore

$$dh = (gdf - fdg)/g^2 = \sum \alpha_i \, dx_i \quad \text{for suitable } \alpha_i \in \mathcal{O}_{V,P} \; .$$

Thus $v_P(dh)$ is bounded below by $\min\{v_P(dx_i) : i = 1, \ldots, n\}$.

(ii) Let $m \geq 0$ be the minimum integer such that $v_P(dh) \geq -m$ for all $h \in \mathcal{O}_{V,P}$; such an m exists because of (i). We show that $m = 0$.

Suppose we have $h \in \mathcal{O}_{V,P}$ with $v_P(dh) = -m < 0$. Observe that $dh = d(h - h(P)) = d(th_1)$ for some $h_1 \in \mathcal{O}_{V,P}$. Thus $dh = h_1 dt + t dh_1$, and since $v_P(dh_1) \geq -m$, we deduce that $v_P(dh) > -m$, contrary to assumption. The claim therefore follows.

(iii) Write $t' = ut$ with u a unit in $\mathcal{O}_{V,P}$. Therefore

$$dt' = udt + tdu = (u + th)dt$$

for some $h \in \mathcal{O}_{V,P}$ with $du = hdt$. By (ii), we know that $v_P(h) = v_P(du) \geq 0$, and hence that $v_P(dt') = v_P(u + th) = 0$. QED

In particular, we deduce from (iii) that $v_P(\omega)$ does not depend on the choice of local parameter t, since for any other local parameter t', the rational differential dt' is a multiple of dt by a unit in $\mathcal{O}_{V,P}$. We say that ω is *regular* at P if $v_P(\omega) \geq 0$.

Lemma 3.2. *If V a smooth irreducible projective curve and ω a non-zero rational differential, then $v_P(\omega) = 0$ for all but finitely many points P on V.*

Proof. Reduce to the affine case and consider the differential dx_1 for $x_1 = X_1/X_0$ an affine coordinate function on the curve. Sufficient then to prove the result for dx_1. Clearly dx_1 has only finitely many poles (using (3.1)), and we show that it has only finitely many zeros by considering the finite extension of fields $k(V)/k(x_1)$. Each coordinate function x_i satisfies an irreducible polynomial equation $f_i(x_1, x_i) = 0$ in $k(V)$, for which $\partial f_i/\partial x_i$ defines a non-zero function on V. More precisely, by (1.3) there are only finitely many points P with $\partial f_i/\partial x_i(P) = 0$. This is true for all i, and so can reduce down to considering points P with $\partial f_i/\partial x_i(P) \neq 0$ for all $i > 1$. For such points P, we must have $v_P(dx_1) = 0$ – to see this, observe that $\partial f_i/\partial x_1 \; dx_1 + \partial f_i/\partial x_i \; dx_i = 0$ in $\Omega^1_{k(V)/k}$ for $i > 1$. Thus if $v_P(dx_1) > 0$, we would have $v_P(dx_i) > 0$ for all i, contradicting the fact that P is a smooth point, since one of the functions $x_i - x_i(P)$ must then be a local parameter at P, and hence in particular $v_P(dx_i) = 0$ for some i.

We can now define the divisor (ω) of ω in the obvious way: $(\omega) = \sum_{P \in V} v_P(\omega)P$; such a divisor is called a *canonical divisor*, usually denoted K_V. Any other non-zero rational differential ω' is of the form $\omega' = h\omega$ for some $h \in k(V)^*$, and so $(\omega') = (h) + (\omega)$, i.e. we have a uniquely defined divisor class on V, also denoted K_V, the *canonical class* on V.

For V a smooth projective curve, we can consider the vector space over k of rational differentials which are regular everywhere, i.e. $(\omega) \geq 0$. If ω_0 is a fixed non-zero rational differential with $(\omega_0) = K_V$, then an arbitrary rational differential $\omega = h\omega_0$ is regular everywhere iff $(h\omega_0) = (h) + K_V \geq 0$, i.e. $h \in \mathcal{L}(K_V)$. The space of global regular differentials on V is therefore isomorphic to $\mathcal{L}(K_V)$ and has dimension $l(K_V)$; by definition this is the *genus* $g(V)$ of V, the basic invariant of the curve. The genus is invariant under isomorphisms. Recall that an isomorphism of smooth projective curves $\phi : V \to W$ induces an isomorphism of function fields $\phi^* : k(W) \to k(V)$, and isomorphisms of the local rings $\phi^* : \mathcal{O}_{W,\phi(P)} \to \mathcal{O}_{V,P}$ for all $P \in V$. The obvious induced isomorphism $\phi^* : \Omega^1_{k(W)/k} \to \Omega^1_{k(V)/k}$ given by $\phi^*(\sum f_i dg_i) = \sum(\phi^* f_i)d(\phi^* g_i)$, has the property that $v_P(\phi^*\omega) = v_{\phi(P)}(\omega)$ for all $P \in V$, and hence $g(V) = g(W)$ as claimed. A closely related basic invariant is the degree of the canonical class (well defined since principal divisors have degree zero, and also clearly invariant under isomorphisms); we shall see from the Riemann–Roch Theorem below that this number is just $2g(V) - 2$.

We now consider various examples. An easy argument shows that $g(\mathbf{P}^1) = 0$. An irreducible curve V is said to be *rational* if its function field $k(V) \cong k(t)$. In the case of smooth projective curves, this translates into the condition that V is isomorphic to $\mathbf{P}^1$ (since rational maps between smooth projective curves are morphisms). Thus any smooth projective rational curve V has $g(V) = 0$. In §4 we shall see that the converse holds. A smooth plane conic is clearly rational. We now look at an example of a non-rational curve.

Example. Let V be the smooth plane cubic with equation $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda X_0)$, $\lambda \neq 0, 1$. Let V_0 denote the affine piece with affine equation $y^2 = x(x-1)(x-\lambda) = f(x)$.

Observe that $2ydy = f'(x)dx$ in $\Omega^1_{k(V)/k}$.

If $y \neq 0$, then $v_P(dx) = 0$ (since if $v_P(dx) > 0$, then also $v_P(dy) > 0$, a contradiction).

When $y = 0$, we have a point $P = (a, 0)$, where $f(a) = 0$ and hence $f'(a) \neq 0$. The above equation implies that $v_P(dx) > 0$, and so we must have $v_P(dy) = 0$.

Claim. $v_P(dx/y) = 0$ for all $P \in V_0$.

Proof. For $y \neq 0$, $v_P(dx/y) = v_P(dx) = 0$. For P with y-coordinate zero, $v_P(dx/y) = v_P(2dy/f'(x)) = v_P(dy) = 0$. Thus the Claim is true.

The point at infinity on V is the point $P_\infty = (0 : 0 : 1)$. We need to calculate

$v_\infty(dx/y)$. Consider the affine piece given by $X_2 \neq 0$, with affine coordinates $z = 1/y$ and $w = x/y$. The affine curve V_2 then has equation $z = w(w-z)(w-\lambda z)$. Since both $v_\infty(z)$ and $v_\infty(w) > 0$, we see from the equation that $v_\infty(z) \geq 3$, and hence that w is a local parameter at P_∞ (since one of z, w must be), i.e. $v_\infty(w) = 1$. We therefore have $v_\infty(z) = 3$, and so $v_\infty(y) = -3$ and $v_\infty(x) = -2$. From this it follows that $v_\infty(dx) = -3$, and $v_\infty(dx/y) = v_\infty(dx) - v_\infty(y) = -3 + 3 = 0$.

The canonical divisor $K_V = (dx/y)$ is therefore the zero divisor. The genus of V is just $g(V) = l(0) = 1$ by (2.1).

Definition. A curve of genus one is called *elliptic.* We'll see in §4 that any elliptic curve can be embedded in $\mathbf{P}^2$ with equation of the above type.

Note that the curve V with equation $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda X_0)$, $\lambda \neq 0, 1$, admits a degree 2 morphism $\pi : V \to \mathbf{P}^1$ (viz. $\pi = (X_0 : X_1)$), 'branched' over the four points $0, 1, \lambda, \infty$.

More generally, a smooth projective curve V is called *hyperelliptic* is there is a degree 2 morphism $\pi : V \to \mathbf{P}^1$, or equivalently that $k(V)$ is a degree 2 extension of $k(\mathbf{P}^1) = k(t)$. It will follow from the Riemann-Hurwitz formula in §4 that π is 'branched' over $2n$ points and that $g(V) = n - 1$.

Finally, we consider the case of an arbitrary smooth projective plane curve $V \subset \mathbf{P}^2$ defined by an irreducible homogeneous polynomial of degree d.

Proposition 3.3. *If V is a smooth plane projective curve defined by an irreducible homogeneous polynomial $F(X_0, X_1, X_2)$ of degree $d > 0$, then $K_V \sim (d-3)H_V$, where $H_V = (X_0)$ is the divisor cut out on V by the hyperplane $X_0 = 0$. In particular,* $\deg(K_V) = d(d-3)$.

Proof. Choose homogeneous coordinates so that $(0 : 0 : 1) \notin V$. Let U be the affine piece of V given by $X_0 \neq 0$. On U, we have affine coordinate functions $y_i = X_i/X_0$, $i = 1, 2$, and $U \subset \mathbf{A}^2$ is defined by $f \in k[y_1, y_2]$ of degree d, where $f(y_1, y_2) = X_0^{-d}\, F(X_0, X_1, X_2)$. In $\Omega^1_{k(V)/k}$ we have

$$0 = df = \partial f/\partial y_1 \; dy_1 + \partial f/\partial y_2 \; dy_2. \qquad (*)$$

Let $U_i = \{P \in U : \; \partial f/\partial y_i(P) \neq 0\}$, $i = 1, 2$. Since U smooth, $U = U_1 \cup U_2$. For all $P \in U_1$, we deduce using $(*)$ that $v_P(dy_1) = v_P(-\partial f/\partial y_2 \; dy_2) \geq v_P(dy_2)$. Since at least one of $y_i - y_i(P)$, $i = 1, 2$, is a local parameter at P, we must have $v_P(dy_2) = 0$ for all

$P \in U_1$. Similarly, $v_P(dy_1) = 0$ for all $P \in U_2$. Now consider

$$\omega = -(\partial f/\partial y_1)^{-1} dy_2 = (\partial f/\partial y_2)^{-1} dy_1 \in \Omega^1_{k(V)/k}.$$

This has $v_P(\omega) = 0$ for all $P \in U = U_1 \cup U_2$. We now need to consider ω at points at infinity.

Denote by W the affine piece of V given by $X_1 \neq 0$. By assumption, $V = U \cup W$. On W, we have affine coordinate functions $z_1 = 1/y_1$ and $z_2 = y_2/y_1$, and $W \subset \mathbf{A}^2$ is defined by $g \in k[z_1, z_2]$ of degree d, where $g(z_1, z_2) = z_1^d f(1/z_1, z_2/z_1)$. Observe that $dy_1 = -z_1^{-2} dz_1$ and $\partial g/\partial z_2 = z_1^{d-1} \partial f/\partial y_2$. We deduce that $\omega = z_1^{d-3} \omega_0$, where

$$\omega_0 = -(\partial g/\partial z_2)^{-1} dz_1 = (\partial g/\partial z_1)^{-1} dz_2 \in \Omega^1_{k(V)/k},$$

the second equality following from the analogous identity to $(*)$ for g. An analogous argument to that employed on U shows that $v_P(\omega_0) = 0$ for all $P \in W$, and thus that $(\omega) = (z_1^{d-3})$ on W. Since $(0 : 0 : 1) \notin V$, and $z_1 = X_0/X_1$, we deduce that $(\omega) = (d-3)H_V$, as required.

In particular, we note that any smooth plane cubic is elliptic, and that a smooth projective plane curve is rational iff its degree is 1 or 2. Of course singular plane curves of degree > 2 may be rational (for instance the nodal cubic $X_0 X_2^2 = X_1^2(X_1 + X_0)$ and the cuspidal cubic $X_0 X_2^2 = X_1^3$). The above formula translates into the statement that the genus $g(V) = \frac{1}{2}(d-1)(d-2)$, once one has the identity $\deg(K_V) = 2g - 2$ from §4. Thus the genus of a smooth projective plane curve is always a 'triangular number'. Thus for many values of the genus g, there is no hope of embedding a smooth projective curve of genus g as a plane projective curve. It is in fact true however that any smooth projective curve may be embedded as a curve in $\mathbf{P}^3$.

§4. The central result in the theory of algebraic curves is the Riemann–Roch Theorem. Unlike other results which have been stated only (whose proofs have been omitted through lack of time), the proof of this theorem is definitely too hard for a Part II course, but this should not prevent us understanding its statement and being able to use it.

Riemann–Roch Theorem. *Given a smooth projective curve V of genus g and a divisor D on V, $l(D) = 1 - g + \deg(D) + l(K_V - D)$.*

If we set $D = K_V$ in Riemann-Roch, we obtain $\deg(K_V) = 2g - 2$, a highly useful alternative characterization of the genus.

As another immediate consequence of Riemann–Roch, we note that if $g = 0$ and $P \in V$, then $l(P) = 2$ and V is rational (see comment at the end of §2).

Given a non-constant morphism $\phi : V \to W$ of smooth projective curves, the inclusion of function fields $\phi^* : k(W) \hookrightarrow k(V)$ yields obvious homomorphisms on the spaces of rational differentials and of global regular differentials (i.e. if $\omega = \sum f_i dg_i$, then $\phi^*\omega = \sum \phi^*(f_i)d(\phi^* g_i)$), which are clearly injective; this latter statement stops being true in characteristic p. The existence of a non-constant morphism therefore implies that $g(W) \leq g(V)$ – for a stronger statement, see Riemann–Hurwitz below. We can now deduce the geometric form of Lüroth's Theorem, that if $\phi : V \to W$ is a non-constant morphism of smooth projective curves with V rational, then W is also rational (since V rational implies that $g(V) = 0$ and hence $g(W) = 0$ and therefore W rational). Once one knows the existence of smooth projective models for any curve, this implies the algebraic version of Lüroth over k: if $K \subset k(t)$ is a finite extension, then K is a pure transcendental extension of k. Both forms of Lüroth are however proved more easily by a direct argument.

We now look at the case of elliptic curves. Let V be a smooth projective curve of genus 1 and $P_0 \in V$ some fixed point. Let $\mathrm{Cl}^0(V)$ denote the *divisor class group*, the abelian group whose elements are the linear equivalence classes of degree 0. For D a divisor of degree 0 on V, we note that the divisor $K_V - D - P_0$ has degree -1, and hence $l(K_V - D - P_0) = 0$. Therefore Riemann–Roch implies that $l(D + P_0) = 1 - 1 + 1 + 0 = 1$, and hence there exists a unique point $P \in V$ such that $D + P_0 \sim P$, or equivalently such that $D \sim P - P_0$. Hence the following result has been proved.

Proposition 4.1. *The map $V \to \mathrm{Cl}^0(V)$ given by $P \mapsto$ class$(P - P_0)$ is a bijection between the points of V and the divisor classes of degree 0.*

The abelian group structure on $\mathrm{Cl}^0(V)$ therefore induces an abelian group structure on the points of V, with identity element the point P_0. By Riemann–Roch and the embedding criterion stated in §2, we observe that $\phi_{3P_0} : V \hookrightarrow \mathbf{P}^2$ embeds V as a smooth plane cubic, with P_0 an inflexion point (i.e. $3P_0$ is cut out by a line). We note that three points P, Q, R add to zero in the group law on V iff $(P - P_0) + (Q - P_0) + (R - P_0) = 0$ in $\mathrm{Cl}^0(V)$, i.e. iff $P + Q + R \sim 3P_0$ as divisors on V. Since $l(3P_0) = 3$, the hyperplane sections of $V \subset \mathbf{P}^2$ are precisely the effective divisors linearly equivalent to $3P_0$, and thus we see that three points P, Q, R add to zero in the group law on V iff the divisor $P + Q + R$ is cut out by a line, i.e. the three points are 'collinear'.

We note moreover by Riemann–Roch that $l(2P_0) = 2$ and $l(3P_0) = 3$; thus we can choose a basis $\{1, x\}$ for $\mathcal{L}(2P_0)$ and extend to a basis $\{1, x, y\}$ for $\mathcal{L}(3P_0)$, and take the embedding $\phi_{3P_0} = (1 : x : y) : V \hookrightarrow \mathbf{P}^2$. Since $\mathcal{L}(6P_0)$ is six dimensional and contains the seven rational functions $\{1, x, y, x^2, xy, x^3, y^2\}$, they are linearly dependent over k, and this relation must involve both x^3 and y^2, these being the only ones with a 6-fold pole at P_0. This relation then says that the image of V under $\phi_{3P_0} = (1 : x : y)$ satisfies a cubic equation which involves both X_1^3 and $X_0X_2^2$. By making an obvious linear change of variables (corresponding to different choices of x and y), we may take this cubic equation to be in *Legendre normal form* $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda X_0) \quad (\lambda \neq 0, 1)$ (cf. §3). In particular, this exhibits V as a double cover of $\mathbf{P}^1$ branched over the four points $0, 1, \lambda, \infty$, where the double cover map is just $\pi = \phi_{2P_0} = (1 : x)$.

As promised, we return to the case of a non-constant morphism $\phi : V \to W$ of smooth projective curves, and the precise relation between $g(V)$ and $g(W)$. For $P \in V$, we define the *ramification index* e_P as follows: Let $Q = \phi(P)$ and t be a local parameter on W at Q, and define e_P to be $v_P(\phi^*(t))$, clearly independent of the choice of t. If $e_P > 1$, we say that ϕ is *ramified* at P and that Q is a *branch* point. If $e_P = 1$, we say that ϕ is *unramified* at P. In §3 we saw that ϕ induces an injection ϕ^* on rational differentials, and that ω regular at $Q = \phi(P)$ implies that $\phi^*\omega$ is regular at P. If s is now a local parameter at P and t a local parameter at Q, then $\phi^*(t) = us^{e_P}$ with u a unit in $\mathcal{O}_{V,P}$. Thus

$$\phi^*dt = d(\phi^*t) = e_P u s^{e_P - 1} ds + s^{e_P} du$$

and hence that $v_P(\phi^*dt) = e_P - 1$, a fact not true in characteristic p. Thus ϕ is unramified at P iff $v_P(\phi^*dt) = 0$ for any local parameter t at Q. Since ϕ^*dt is a non-zero rational differential on V (cf. §3), we deduce that ϕ has only finitely many ramification points. By analysing the order of poles and zeros of $\phi^*\omega$ for a rational differential ω on W, and using the fact that the degree of the divisor (ω) is $2g(W) - 2$ and that of $(\phi^*\omega)$ is $2g(V) - 2$, it is straightforward to deduce the following precise relation, the Riemann–Hurwitz Formula. Recall that we are assuming $\mathrm{char}(k) = 0$, although the formula (and proof) remains valid in characteristic p, so long as p does not divide the degree n or any of the ramification indices.

Riemann–Hurwitz Formula. *If $\phi : V \to W$ is a non-constant morphism of degree n between smooth projective curves, then*

$$2g(V) - 2 = n(2g(W) - 2) + \sum_{P \in V} (e_P - 1) \ .$$

This result enables us to interpret the genus topologically (non-examinable). A smooth complex projective curve is also a compact Riemann surface, which in turn is a compact orientable 2-manifold. Topologically, these are spheres with a certain number of handles (see Algebraic Topology course), and the *topological genus* is just the number of such handles. Note the complex projective line corresponds to the Riemann sphere and so has topological genus zero. One can however prove the Riemann–Hurwitz Formula in the same form but with the topological genus (this is essentially done in Kirwan's book - see Remark 4.23 there). Given any smooth complex projective curve V, we can choose a non-constant rational function on V, which therefore exhibits V as a branched cover of $\mathbf{P}^1(\mathbf{C})$. From the two forms of Riemann–Hurwitz, we deduce that, over the complex numbers, the genus that we have been using in this course is precisely the same as the topological genus.

Returning now to the case of $\pi : V \to \mathbf{P}^1$ a double cover (e.g. V hyperelliptic), it follows from Riemann–Hurwitz that π is branched over $2g(V) + 2$ points of $\mathbf{P}^1$.

Proposition 4.2. *Suppose $\pi : V \to \mathbf{P}^1$ is a morphism of degree 2 from a smooth projective curve of genus $g(V) > 0$. If $P \in V$ is a ramification point of π, then up to a (linear) automorphism of $\mathbf{P}^1$, we have $\pi = \phi_{2P}$.*

Proof. Let $\pi(P) = Q = (q_0 : q_1) \in \mathbf{P}^1$. Choose any non-constant $t \in \mathcal{L}(Q)$, e.g. $t = (r_1x_0 - r_0x_1)/(q_1x_0 - q_0x_1)$ with $(r_0 : r_1) \neq (q_0 : q_1)$. Then $1/t$ is a local parameter at Q, and hence $v_P(\pi^*(1/t)) = 2$, and hence $\pi^*(t) \in \mathcal{L}(2P)$. Since $l(2P) \leq 2$ (Example Sheet II, Question 5), we have a basis $\{1, \pi^*(t)\}$ for $\mathcal{L}(2P)$. Setting $\phi_{2P} = (1 : \pi^*(t))$, we deduce that $\phi_{2P} = \psi_t \circ \pi$, where $\psi_t = (1 : t) = (q_1x_0 - q_0x_1 : r_1x_0 - r_0x_1) : \mathbf{P}^1 \to \mathbf{P}^1$ is a (linear) automorphism of $\mathbf{P}^1$.

We return to the case of elliptic curves and smooth plane cubics.

Lemma 4.3. *Let $V \subset \mathbf{P}^2$ be a smooth plane cubic, and $R \in V$ a fixed point. The map $V \to V$ given by sending each point P to the third point of intersection of the line RP with V (with obvious interpretations when $R = P$, etc.) is an morphism ψ of the projective curve V to itself.*

Proof. It is easily checked that there is an explicit rational map, and hence morphism, ψ, such that the image of $P \neq R$ is in fact $\psi(P)$. Let Q denote the third point of intersection of the tangent line at R with V; it then follows that $\psi(V \setminus \{R\}) = V \setminus \{Q\}$. Since however the morphism ψ is surjective (Finiteness Theorem), we deduce that $\psi(R) = Q$ also.

The morphism ψ in (4.3) is its own inverse, and in particular is an isomorphism of V to itself, i.e. an *automorphism* of V. It then follows easily, from the geometric description of the group law on an elliptic curve V, that the map from V to itself given by adding a fixed point Q is an automorphism of V. Hence the group of automorphisms of V is transitive. This contrasts with the case when $g(V) > 1$, in which case it can be shown that the automorphism group is always finite.

Proposition 4.4. *Given an elliptic curve V and two double covers $\pi_1 : V \to \mathbf{P}^1$ and $\pi_2 : V \to \mathbf{P}^1$, there is an automorphism σ of V and a (linear) automorphism τ of $\mathbf{P}^1$ such that $\pi_2 \circ \sigma = \tau \circ \pi_1$.*

Proof. Let P_1 be a ramification point for $\pi_1 : V \to \mathbf{P}^1$, and P_2 a ramification point for $\pi_2 : V \to \mathbf{P}^1$. Now choose an automorphism σ of V with $\sigma(P_1) = P_2$. Thus $\pi_2 \circ \sigma : V \to \mathbf{P}^1$ is also a double cover, with P_1 a ramification point. Since, by (4.2), a ramification point determines the double cover $V \to \mathbf{P}^1$ up to a (linear) automorphism of $\mathbf{P}^1$, there are (linear) automorphisms τ_1 and τ_2 of $\mathbf{P}^1$ with $\tau_1 \pi_1 = \phi_{2P_1} = \tau_2 \pi_2 \sigma$. Hence the existence of a (linear) automorphism τ of $\mathbf{P}^1$ such that $\pi_2 \circ \sigma = \tau \circ \pi_1$.

From this, we show that the number $\lambda \in k$ appearing in the Legendre normal form for V is determined up to the well-known action of S_3 on $k \setminus \{0, 1\}$; namely, if $\alpha \in \mathrm{S}_3$ and $\lambda \in k \setminus \{0, 1\}$, permute $0, 1, \lambda$ according to α and then apply the unique linear transformation of k sending the first number to 0 and the second to 1, and define $\alpha(\lambda)$ to be the image of the third number. We show (Lemma 5.5) that the orbit of λ is then $\{\lambda, 1/\lambda, 1-\lambda, 1/(1-\lambda), \lambda/(\lambda-1), (\lambda-1)/\lambda\}$. If we define

$$j(\lambda) = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

we observe that $j(\lambda)$ is invariant under the above action of S_3. The content of the next result is that this procedure determines an invariant $j(V)$ of the elliptic curve V, called the *j-invariant*, parametrizing isomorphism classes of elliptic curves.

Theorem 4.6. *(a) $j(\lambda)$ defined above from a Legendre normal form depends only on V.*
(b) Two elliptic curves V_1 and V_2 are isomorphic if and only if $j(V_1) = j(V_2)$.
(c) Every element of k is the j-invariant of some elliptic curve.

Proof. (a) Suppose we have two different choices of base point P_1 and P_2 on V; we then obtain double covers $\pi_i : V \to \mathbf{P}^1$, with $\pi_i(P_i) = \infty$ $(i = 1, 2)$. As in (4.4), we choose an

automorphism σ of V with $\sigma(P_1) = P_2$, and deduce the existence of a linear automorphism τ of $\mathbf{P}^1$ such that $\pi_2 \circ \sigma = \tau \circ \pi_1$. Thus $\tau(\infty) = \infty$ and τ sends the other branch points $\{0, 1, \lambda_1\}$ of π_1 to the points $\{0, 1, \lambda_2\}$ of π_2 (in *some* order). As τ is an affine linear transformation, we deduce that λ_2 is related to λ_1 via the action of S_3 defined above, and so in particular that $j(\lambda_1) = j(\lambda_2)$ depends only on V.
(b) For $\lambda \neq 0, 1$, an easy calculation shows that $j(\lambda_1) = j(\lambda_2)$ if and only if λ_1 and λ_2 differ by the above action of S_3. Now given V_1 and V_2, we can take Legendre normal forms $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda_i X_0)$ for the curves $(i = 1, 2)$. If V_1 is isomorphic to V_2, then it is clear that we may take Legendre normal forms with $\lambda_1 = \lambda_2$, and hence $j(V_1) = j(V_2)$. Conversely, if $j(V_1) = j(V_2)$, then λ_1 and λ_2 are related by an element of S_3, and so after a linear change of variable in the affine coordinate x, we may assume $\lambda_1 = \lambda_2$; hence V_1 and V_2 are isomorphic to the same projective plane cubic.
(c) Observe that for any $j \in k$, we can solve for λ $(\lambda \neq 0, 1)$. Therefore $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda X_0)$ is an elliptic curve with the required j-invariant.

We have seen therefore that the isomorphism classes of elliptic curves are parametrized by k. So having specified the genus as $g = 1$, we still have a one-dimensional variety parametrizing isomorphism classes of smooth projective curves. For genus $g > 1$, it can be shown that such a parametrizing variety still exists, but in these cases its dimension is $3g - 3$.

If now V is a smooth projective curve of genus $g \geq 2$, we can consider the morphism $\phi_{K_V} : V \to \mathbf{P}^{g-1}$, called the *canonical map* on V. Using the embedding criterion from §2, we see that the canonical map is an embedding of V if $l(K_V - P - Q) = g - 2$ for all $P, Q \in V$. But Riemann–Roch tells us that $l(P + Q) = 3 - g + l(K_V - P - Q)$, and hence the canonical map is an embedding if $l(P + Q) = 1$ for all $P, Q \in V$. This latter condition is however precisely the condition that V is non-hyperelliptic. If on the other hand V is hyperelliptic of genus $g > 1$, then the canonical map is a double cover of $\mathbf{P}^1$ embedded as a twisted $(g - 1)$-ic in $\mathbf{P}^{g-1}$ (see Example Sheet III, Question 6). We have therefore shown:

Theorem 4.7. *If V is a smooth projective curve of genus $g > 1$, the canonical map $\phi_{K_V} : V \to \mathbf{P}^{g-1}$ is an embedding of V as a curve of degree $2g - 2$ in $\mathbf{P}^{g-1}$ if and only if V is non-hyperelliptic.*

Thus, for example, any curve V of genus $g = 2$ is hyperelliptic, with the canonical map being a double cover of $\mathbf{P}^1$. For $g = 3$ however, we see that a curve V is either hyperelliptic

or it is embedded by the canonical map as a smooth plane quartic (which by our genus formula from §3 does have genus 3). Moreover, (3.3) implies that for a smooth plane quartic in $\mathbf{P}^2$, the canonical class is the class of a hyperplane section, and so the canonical map is an embedding, i.e. V cannot be hyperelliptic. This bifurcation into distinct cases, the hyperelliptic and non-hyperelliptic cases, occurs for all genera $g \geq 3$, and enables us to provide a classification for all curves of low genus. For $g = 4$ for instance, we have that either V is hyperelliptic, or it is isomorphic to the intersection of an irreducible quadric and an irreducible cubic in $\mathbf{P}^3$. As mentioned above, the isomorphism classes of curves of genus $g > 1$ are parametrized by a quasi-projective variety M_g of dimension $3g - 3$ (the complement of some subvariety in a projective variety $\overline{M}_g$). Inside this variety M_g, there is a subvariety of dimension $2g - 1$ parametrizing the hyperelliptic curves (where of course this subvariety is the whole of M_2 when $g = 2$). For further reading on the classification of curves, the reader is recommended Mumford's book, *Curves and their Jacobians*, University of Michigan Press 1975.