Part IIB Algebraic Curves Course 1995 PMHW

Abbreviated Lecture Notes

§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 $\mathbf{P}^n$. 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 $\lambda \in k^*$.

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. We say that V is *irreducible* if it cannot be written as the union $V = V_1 \cup V_2$ of two proper subvarieties. Can show that V is irreducible iff $I^h(V)$ is a prime ideal.

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.

In this course we shall take $k = \mathbf{C}$. 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. We say that V is a *complex projective curve* if $\dim(V) = 1$, i.e. $\mathbf{C}(V)$ is a finite extension of the field $\mathbf{C}(t)$ of rational functions in one variable.

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 $\mathbf{A}^n_0$, 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. Easily seen that for V irreducible, the function field $k(V)$ can be defined purely in terms of a (non-empty) affine piece. As an example, consider $V \subset \mathbf{P}^2$ 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 1.2. *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). From this lemma, it follows that if F is irreducible, then the only proper subvarieties of V are finite sets of points , and so V must be irreducible. 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.

A local ring 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 a complex 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. Otherwise we say that P is a *singularity* of V. For plane curves, these definitions are easily seen to be equivalent to the usual definitions

in terms of vanishing of partial derivatives of an irreducible defining polynomial.

Lemma 1.4. *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 $f = f_1 + f_2 + \ldots$, 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 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 $f_1 \neq 0$, contrary to assumption.

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 (1.2), 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 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 $k(V)$ 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. Interpretting 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; 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 $\psi : W \to V$. An isomorphism induces isomorphisms of the local rings (given by composition with ϕ), and intrinsic properties of the variety are not affected. Example of twisted cubic in $\mathbf{P}^3$ being isomorphic to $\mathbf{P}^1$. 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 (clear denominators and cancel out any common factors of t in the f_i).

Given a surjective (or in fact a morphism whose image is not contained in a subvariety of W) morphism $\phi : V \to W$ between projective curves, composition with ϕ induces an injective homomorphism of function fields $\phi^* : k(W) \hookrightarrow k(V)$. The *degree* $\deg(\phi)$ of ϕ is by definition the degree of the field extension $[k(V) : \phi^*k(W)]$. Morphisms between smooth projective curves have the additional property of *finiteness* : if $\phi : V \to W$ is a 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 $\sum_{P \in \phi^{-1}(Q)} v_P(\phi^*(t)) = \deg(\phi)$ (proof omitted). This says that, counting multiplicities, the number of points in each fibre is a constant finite number, equal to the degree of the morphism.

§2. We now introduce some tools for the study of smooth complex 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 $D = \sum n_iP_i$ with $P_i \in V$ and $n_i \in \mathbf{Z}$. The *degree* of D is just $\deg(D) = \sum n_i$.

For V a smooth projective curve and $f \in k(V)^*$, it is clear that $v_P(f) = 0$ for all but finitely many points $P \in V$ - consider the morphism ϕ defined below from f and apply

the finiteness property. 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*. 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 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

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

i.e. any principal divisor has degree 0.

For a smooth projective curve $V \subset \mathbf{P}^n$, any hyperplane not containing V cuts out a divisor on V in an obvious way, and any two such divisors are linearly equivalent and so have the same degree; we call this the *degree* of V in $\mathbf{P}^n$. If $V \subset \mathbf{P}^2$ is defined by an irreducible homogeneous polynomial of degree d, then easily seen that $\deg(V) = d$. The twisted cubic $V \subset \mathbf{P}^3$ has degree 3.

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, 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. $D' \sim D$. Using the fact that $\mathcal{O}_{V,P}$ is a DVR, it is an easy check that $l(D-P) \geq l(D)-1$ (define an obvious injective homomorphism $\mathcal{L}(D)/\mathcal{L}(D-P) \to k$).

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 may take a basis $1, X_1/X_0, \ldots, X_n/X_0, h_1, \ldots, h_r$ of $\mathcal{L}(D)$ and then $\phi_D : V \to \mathbf{P}^{n+r}$ is an embedding of V (since composing with projection $\pi : \mathbf{P}^{n+r} - \to \mathbf{P}^n$, we just get the original inclusion given by $(X_0 : \ldots : X_n)$). The hyperplane section D of V given by $X_0 = 0$ is therefore also a hyperplane section of V embedded by ϕ_D into $\mathbf{P}^{n+r}$, and so the degree of V under either embedding is just $\deg(D)$. For D a hyperplane section as above, it is clear that for any $P, Q \in V$ (not necessarily distinct), $l(D - P - Q) \leq l(D) - 2$, and hence from above calculation we have equality. In the case $P = Q$, we are saying here that the general hyperplane through P determines a local parameter on V at P (exercise for reader).

Theorem. *(stated only). 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 whose image has degree* $\deg(D)$.

As an example, 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.

§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, we know that for some $s \in k(V)$ non-constant, $k(V)$ is a finite extension of $k(s)$. Given any other non-constant element $t \in k(V)$, we have that t satisfies an equation over $k[s]$

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

with $a_i \in k[s]$, not all the a_i being in $k = \mathbf{C}$. This may also be regarded as an equation for s over $k[t]$, and so $k(s,t)$ is finite over $k(t)$. It follows then that $\Omega^1_{k(V)/k}$ is 1-dimensional over $k(V)$ with generator dt for any non-constant $t \in k(V)$ (any $g \in k(V)$ satisfies a separable 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 $\omega = f dt$, 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.

In particular, we deduce that $v_P(\omega)$ does not depend on the choice of t, for if $t' = ut$ with $u \in U(\mathcal{O}_{V,P})$, we have

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

for some $h \in \mathcal{O}_{V,P}$. 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.*

For the proof, reduce to the affine case and consider the differential dx_1 for x_1 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 $k(V)/k(x_1)$.

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 $k = \mathbf{C}$ 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 (invariant under isomorphism). A closely related basic invariant is the degree of the canonical class (well defined since

principal divisors have degree zero, and clearly also 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. The smooth plane curve V with equation $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda X_0)$ $(\lambda \neq 0, 1)$ is seen to have (up to constant multiples) only one global regular differential, namely dx/y, where $x = X_1/X_0$ and $y = X_2/X_0$; hence $g(V) = 1$. A curve of genus 1 will be called *elliptic*, and 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 above curve admits a degree 2 morphism $\pi : V \to \mathbf{P}^1$ (viz. $\pi(x_0 : x_1 : x_2) = (x_0 : x_1)$) 'branched' over the four points $0, 1, \lambda, \infty$.

More generally, a smooth curve V is called *hyperelliptic* if there is a degree 2 morphism $\pi : V \to \mathbf{P}^1$; equivalently, $k(V)$ is a degree 2 extension of $k(\mathbf{P}^1) \cong k(t)$ or that V has an affine piece with equation $y^2 = f(x)$ with f a square free polynomial. It will follow from the Riemann-Hurwitz formula in §4 that π is 'branched' over $2n$ points of $\mathbf{P}^1$ (*aliter* f has degree $2n$ or $2n - 1$) 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. A calculation we'll perform in lectures shows that $\deg(K_V) = d(d - 3)$. 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 $X_0X_2^2 = X_1^2(X_1 + X_0)$ and the cuspidal cubic $X_0X_2^2 = X_1^3$). The above formula translates into the statement that the genus $g(V) = \frac{1}{2}(d - 1)(d - 2)$.

§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 only through lack of time), the proof of this theorem is rather 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 R–R, we obtain $\deg(K_V) = 2g - 2$, a highly useful alternative characterization of the genus.

As an immediate consequence of R–R, 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 $\phi^* : k(W) \hookrightarrow k(V)$ induced by composition with ϕ 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 $\mathbf{C}$; 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. By R–R we deduce that for D a divisor of degree 0 on V, there is a unique point P with $D \sim P - P_0$. Thus the map $V \to \mathrm{Cl}^0(V)$ (divisor classes of degree 0) given by $P \mapsto \mathrm{class}(P - P_0)$ 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 R–R 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 R–R 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* $X_0X_2^2 = X_1(X_1 - X_0)(X_1 - \lambda X_0)$ $(\lambda \neq 0, 1)$ (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 $\pi = \phi_{2P_0} = (1 : x)$.

It follows easily from the above description of the group law on V that the map from V to itself given by adding a fixed point Q is a rational map, and hence a morphism. It clearly has an inverse and is therefore an isomorphism. Hence the group of *automorphisms* of V is transitive. From this it follows that given two double covers $\pi_1 : V \to \mathbf{P}^1$ and $\pi_2 : V \to \mathbf{P}^1$, determined by bases of $\mathcal{L}(2P_1)$ and $\mathcal{L}(2P_2)$, we have an automorphism σ of V with $\sigma(P_1) = P_2$, and then that both π_1 and $\pi_2 \circ \sigma$ are given by (possibly different) choices of bases for $\mathcal{L}(2P_1)$; in other words, there is an automorphism τ of $\mathbf{P}^1$ such that $\pi_1 \circ \sigma = \tau \circ \pi_2$. From this, we show that the complex number λ 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 $\alpha \in S_3$ and $\lambda \in k \setminus \{0, 1\}$, permute $0, 1, \lambda$ according to α and then apply the unique linear transformation of $k = \mathbf{C}$ sending the first number to 0 and the second to 1, and define $\alpha(\lambda)$ to be the image of the third number. 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, and hence defines an invariant $j(V)$ of the elliptic curve V, called the *j-invariant.* It is now a simple application of Galois Theory to show that two elliptic curves V_1 and V_2 are isomorphic iff $j(V_1) = j(V_2)$. Moreover, any complex number is the j-invariant of some elliptic curve, and so the isomorphism classes of elliptic curves are parametrized by $\mathbf{C}$.

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 iff $l(K_V - P - Q) = g - 2$ for all $P, Q \in V$. But R–R tells us that $l(P + Q) = 3 - g + l(K_V - P - Q)$, and hence the canonical map is an embedding iff $l(P + Q) = 1$ for all $P, Q \in V$. This latter condition is however precisely the condition that V is non-hyperelliptic. Thus for $g = 2$, we see that any curve V is hypelliptic 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, examination of the proof of the genus formula shows 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 $g \geq 3$. 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 promised, we now return to the case of a non-constant morphism $\phi : V \to W$ of smooth complex 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 $\phi^* dt$ 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.

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

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

Finally, we 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 (see Differentiable Manifolds). 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 $\mathbf{P}^1$. From the two forms of Riemann–Hurwitz, we deduce that the genus that we have been using in this course is precisely the same as the topological genus.

Example 2 from §3

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 $x = w(w - z)(w - \lambda z)$. 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 $g(V) = n - 1$.