MA4L7 Algebraic curves

Miles Reid

Part III. Applications of RR to the geometry of curves

7 Introduction

Part III takes on trust the Riemann–Roch theorem from Part II, and discusses at some length what it means and what it can do for us. The main purpose of RR is along the following lines: ensuring C has enough global functions with given poles allows us to embed C into projective space. In good cases, this takes us from the notion of an abstract curve of genus g to a subvariety $C \subset \mathbb{P}^n$ embedded in a known ambient space, and defined by equations that can be studied in explicit ways. For example, a curve of genus 1 is isomorphic to a plane cubic $C_3 \subset \mathbb{P}^2$. Or a nonhyperelliptic curve of genus 4 is embedded in $\mathbb{P}^3$ as a $(2,3)$ complete intersection $C = Q_2 \cap F_3$.

In complex analysis, RR is used to prove that every compact Riemann surface has global meromorphic functions that embed it in a projective space $\mathbb{P}^n$, where one sees that it is actually a projective algebraic curve, an object of algebraic geometry. These ideas open up new methods of study and have many applications.

7.1 Linear systems and projective embeddings

The RR spaces $\mathcal{L}(C,D)$ map C to projective space: a basis $f_{1\dots l}$ of $\mathcal{L}(C,D)$ gives the rational map $\varphi_D\colon C \dashrightarrow \mathbb{P}^r$ (with $r = l-1$), that takes a point $P \in C$ to the ratio $\bigl(f_1(P) : \cdots : f_l(P)\bigr)$. Here I study how to establish whether φ_D is an embedding (an isomorphism of C to its image), and if so, what the divisor D has to do with the geometry of $\varphi_D(C) \subset \mathbb{P}^r$.

First, some traditional terminology that goes back to antiquity. For C a nonsingular projective curve and $D = \sum d_P P$ a divisor, write

$$|D| = \bigl\{\operatorname{div} f + D \bigm| f \in \mathcal{L}(C,D)\bigr\} \tag{7.1}$$

for the *linear system* of D (the Italian tradition uses *linear series*). By construction, the divisors $D_f = \operatorname{div} f + D$ for $f \in \mathcal{L}(C,D)$ run through the effective divisors linearly equivalent to D. The set $|D|$ is parametrised by $\mathbb{P}^r = \bigl(\mathcal{L}(C,D) \setminus 0\bigr)/k^\times$, the projective space of 1-dimensional subspaces of the vector space $\mathcal{L}(C,D)$ (here $\mathcal{L}(D) = 0$ corresponds to $|D| = \emptyset$, treated as having dimension -1). We picture the linear system $|D|$ as a bunch of points running around C, parametrised by the projective space $\mathbb{P}^r$, in much the same way as the pencil of plane conics $\lambda Q_1 + \mu Q_2 = 0$ is parametrised by $\mathbb{P}^1_{\langle\lambda:\mu\rangle}$. A common abuse of language is to speak of $D \in |D|$ to mean a divisor $D_f \in |D|$.

It may happen that for some reason, rational functions $f \in k(C)$ are unable to take their full allocation of poles D, so all the effective divisors $D_f \in |D|$ have a common part $A > 0$. This means that each $f \in \mathcal{L}(C,D)$ satisfies $\operatorname{div} f + D \geq A$, or in other words, $\mathcal{L}(C,D) = \mathcal{L}(C, D - A)$. The biggest such A is the *fixed part* of $|D|$. We write $|D| = A + |D - A|$, where A is the fixed part and $|D - A|$ the *free part*.

I say that $|D|$ is *free* (or *fixed-point free*) if it has no fixed part. Then for every $P \in C$, some $f \in \mathcal{L}(C,D)$ has valuation $v_P(f) = -d_P$, so locally at P, this f is $z_P^{-d_P}$ times a unit of $\mathcal{O}_{C,P}$. In terms of the sheaf $\mathcal{O}_C(D)$, the global section $f \in \Gamma(C, \mathcal{O}_C(D)) = \mathcal{L}(C,D)$ bases $\mathcal{O}_C(D)$ locally as an $\mathcal{O}_C$-module at P. Thus $|D|$ free is synonymous with $\mathcal{O}_C(D)$ *generated by its global sections*.

Remark 7.1 A free linear system $|D|$ of degree d with $\dim \mathcal{L}(C,D) = r + 1$ is traditionally called a g^r_d, meaning that $|D|$ consists of effective divisors of degree d moving in an r-dimensional family. For example, the 2-to-1 morphism $C \to \mathbb{P}^1$ from a hyperelliptic curve to $\mathbb{P}^1$ is given by a g^1_2; for a plane curve $C_a \subset \mathbb{P}^2$ of degree a, the linear system $|H|$ cut out by the lines of $\mathbb{P}^2$ is a g^2_a.

There are two traditional sources of confusion: first, $r + 1 = l(C,D)$ is the dimension of $\mathcal{L}(C,D)$ as a vector space, whereas $r = l - 1$ refers to its projectivisation $\mathbb{P}^r = \bigl(\mathcal{L}(C,D) \setminus 0\bigr)/k^\times$, the parameter space of the linear system $|D|$.

Next, a point of $\mathbb{P}^r = |D|$ corresponds to $f \in \mathcal{L}(D)$ up to proportionality, that is, to a *line* of $\mathcal{L}(C,D)$ (a 1-dimensional vector subspace), whereas the target space of $\varphi_D \colon C \to \mathbb{P}^r$ has $\mathcal{L}(C,D)$ as its linear forms; thus a point of $\mathbb{P}^r$ corresponds to a *hyperplane* of $\mathcal{L}(C,D)$ (a codimension 1 vector subspace). The divisors $D \in |D|$ of a linear system correspond to hyperplanes of $\mathbb{P}^r$, that are parametrised by the dual projective space to $|D|$.

7.2 Strategy to prove embedding

How do I establish that a rational map $\varphi_D\colon C \dashrightarrow \mathbb{P}^r$ is an isomorphism to its image $\varphi(C) = \Gamma \subset \mathbb{P}^r$? An algebraic variety is a set of points X with locally defined functions $\mathcal{O}_X$ on it. Thus for $\varphi\colon C \to \Gamma$ to be an isomorphism needs three points:

(1) it is regular at every point of C;

(2) it is bijective as a map of point sets, and

(3) pullback of functions on Γ provide all the functions on C.

Definition 7.2 A divisor D is *very ample* if $\varphi_D\colon C \to \mathbb{P}^r$ is an isomorphism to its image $\varphi_D(C) = \Gamma \subset \mathbb{P}^r$, and the hyperplanes of $\mathbb{P}^r$ cut out the linear system $|D|$ on C.

First of all, if $|D|$ has a fixed part A then D and $D - A$ define the same morphism $\varphi_D = \varphi_{D-A}\colon C \dashrightarrow \mathbb{P}^r$. Thus the map φ_D only sees the free part $|D - A|$ of D, and ignores A completely. This follows as in the resolution of indeterminacies of Proposition 4.1: for rational functions $f_1, \dots, f_l, g \in k(C)$ the two expressions $f_1 : \cdots : f_l$ and $gf_1 : \cdots : gf_l$ define the same rational map to $\mathbb{P}^{l-1}$. Removing a removable singularity by cancelling a common factor $(z-c)f_1/(z-c)f_2 \mapsto f_1/f_2$ is part of the equivalence relation defining a rational function, so does nothing.

The main result is the following theorem.

Theorem 7.3 *Let D be a divisor on a nonsingular projective curve C. Then D is very ample if and only if the RR spaces of D on C satisfy the conditions:*

(1) *$l(D-P) = l(D) - 1$ for every $P \in C$; equivalently, $\mathcal{L}(D-P) \subsetneq \mathcal{L}(D)$. In other words, $|D|$ is free.*

(2) *$l(D-P-Q) = l(D) - 2$ for every pair of distinct point $P, Q \in C$; that is, $\mathcal{L}(D-P-Q) \subsetneq \mathcal{L}(D-P) \subsetneq \mathcal{L}(D)$. We say that $|D|$ is free and* separates points.

(3) *$l(D-2P) = l(D) - 2$ for every $P \in C$; equivalently, $\mathcal{L}(D-2P) \subsetneq \mathcal{L}(D-P) \subsetneq \mathcal{L}(D)$. We say that D* separates tangent directions *or in traditional language* "separates infinitely near points".

I start by relating the assumptions of the theorem to the above discussion. (1) is the statement that $|D|$ has no fixed part.

(2) is the condition that $\mathcal{L}(D-P-Q) \subset \mathcal{L}(D)$ has codimension 2, so that there is an $f \in \mathcal{L}(D)$ that vanishes at P and not at Q. In other words, there is a hyperplane of $\mathbb{P}^{l-1}$ through $\varphi_D(P)$ and not through $\varphi_D(Q)$, and vice-versa. Thus (2) gives directly that φ_D is injective on point sets.

To discuss (3), suppose that $P \in C$ appears in D with coefficient d_P, and that z_P is a local parameter of the DVR $\mathcal{O}_{C,P}$. Then by (1) we know that some $f_1 \in \mathcal{L}(D)$ has valuation $v_P(f_1) = -d_P$, so is a basis of $\mathcal{O}_C(D)$ on an affine neighbourhood U of P. Assumption (3) asserts that there is some $f_2 \in \mathcal{L}(D)$ with $v_P(f_2) = -(d_P - 1)$. Then f_2/f_1 is a regular function on U, and is a regular parameter of the local ring $\mathcal{O}_{C,P}$.

Proof in complex analysis Over $\mathbb{C}$, a nonsingular projective curve with its usual complex metric topology is a compact Riemann surface $C = \Sigma$ (compact because it is closed in projective space). Then $\varphi_D \colon \Sigma \to \Gamma \subset \mathbb{P}^r$ is a continuous map, and is bijective by condition (ii). A simple argument in point set topology shows that φ is then a homeomorphism: the image of a compact set under a continuous map is compact. In a compact metric topological space, compact is closed, so that $\varphi\colon \Sigma \to \Gamma$ is bijective and also a closed map, hence a homeomorphism.

In complex analysis, this completes the proof – we have regular map that is a homeomorphism, and functions on the image include a local analytic parameter at each point P, so the map is an embedding by the implicit function theorem.

The Zariski topology is too weak for this to work. Algebraic geometry replaces it with the following definition: a morphism $X \to Y$ is *proper* if it is universally closed. Closed means simply that the image of a closed subvariety is closed; universally closed is the condition that the product morphism $X \times Z \to Y \times Z$ is closed for all Z. The proof of Theorem 7.3 is based on the fact that a finite morphism $X \to Y$ is proper.

Example 7.4 The polynomial map $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^2$ given by

$$(u(v^2-u^2) : v(v^2-u^2) : u^3) \tag{7.2}$$

parametrises the cubic

$$\Gamma : y^2 z = x^2 z + x^3 \subset \mathbb{P}^2 \tag{7.3}$$

with the node $N = (0:0:1)$. Both points $P_{\pm 1} = (1 : \pm 1) \in \mathbb{P}^1$ map to N, corresponding to the two nodal branches $y = \pm x$.

Now φ restricted to the open curve $C_0 = \mathbb{P}^1 \setminus \{P_{-1}\}$ gives a bijective map, that only follows one of the two branches through the node N. The Zariski topology of C_0 has few closed sets, and one checks at once that φ is closed. However, it is not *universally* closed: in fact, the graph of the inclusion $C_0 \hookrightarrow \mathbb{P}^1$ (a kind of punctured diagonal $\{P, P\}$ with $P \neq P_{-1}$) is Zariski closed in $C_0 \times \mathbb{P}^1$, but its image in $\Gamma \times \mathbb{P}^1$ does not contain the point (N, P_{-1}) of its closure.

Proof of the theorem In algebraic geometry, write $\Gamma \subset \mathbb{P}^{l-1}$ for the Zariski closure of the image $\Gamma_0 = \varphi_D(C)$. It is an irreducible subvariety, and by (2), the morphism $\varphi_D \colon C \to \Gamma$ is injective on points. I have to prove that φ_D is surjective to Γ, and that pullback defines an isomorphism of local rings $\varphi_D^* \colon \mathcal{O}_{\Gamma,Q} \cong \mathcal{O}_{C,P}$ for every $P \in C$, where $Q = \varphi(P)$.

The proof consists of three steps: (1) Reduction to a finite morphism $\varphi_x \colon C_x \to \Gamma_x$ on affine pieces $C_x \subset C$ and $\Gamma_x \subset \Gamma$, with the induced homomorphism on the coordinate rings $\varphi_x^* \colon k[\Gamma_x] \subset k[C_x]$ making $k[C_x]$ into a finite module over $k[\Gamma_x]$. (2) Reduction to local commutative algebra with $\varphi_Q^* \colon \mathcal{O}_{\Gamma,Q} \cong \mathcal{O}_{C,P}$ a finite morphism of local rings. (3) Conclusion of the argument by Nakayama's lemma.

Remark 7.5 My treatment fits $\varphi_D \colon C \to \Gamma$ into a diagram $C \to \Gamma \to \mathbb{P}^1$. Then, as in the resolution of singularities of Chapter I, I reinpret C in terms of the integral closure of the affine rings $k[x]$ and $k[x^{-1}]$ of $\mathbb{P}^1$ in the field extension $k(\mathbb{P}^1) \subset k(C)$.

Reduction to affine Write $\Gamma_0 = \varphi_D(C) \subset \mathbb{P}^{l-1}$ and let $\Gamma \subset \mathbb{P}^{l-1}$ be its Zariski closure. Then $\Gamma_0 = \varphi_D(C)$ is an irreducible curve, and Γ adds at most finitely many points $Q \in \Gamma$ (actually none, but that is still to prove). The RR space $\mathcal{L}(C, D)$ gives the linear forms on $\mathbb{P}^{l-1}$, so choosing homogeneous coordinates $t_{1\dots l}$ for $\mathbb{P}^{l-1}$ is the same thing as choosing a basis $f_{1\dots l}$ of $\mathcal{L}(C, D)$.

Since Γ is a curve, for general coordinates on $\mathbb{P}^{l-1}$, it is disjoint from the codimension 2 subspace $t_1 = t_2 = 0$. The first two elements f_1, f_2 of the corresponding basis of $\mathcal{L}(C, D)$ give effective divisors $\operatorname{div} f_i + D$ with disjoint support.

Write $x = t_1/t_2$ for an affine coordinate on $\mathbb{P}^1$.

Given t_1, t_2 chosen as above, for any $Q \in \Gamma$, I can replace them with appropriate linear combinations so that Q is in the hyperplane $t_1 = 0$ and not in $t_2 = 0$, so that $x = t_1/t_2$ is regular and 0 at Q, that is $x \in \mathcal{O}_{\Gamma,Q}$. Or, for any given point $P \in C$, I can replace the corresponding f_1, f_2 with appropriate linear combinations so that $f_2 \in \mathcal{L}(C, D) \setminus \mathcal{L}(C, D - P)$ and $f_1 \in \mathcal{L}(C, D - P)$ and $x = f_1/f_2 \in \mathcal{O}_{C,P}$.

Now consider the commutative triangle

$$\begin{array}{ccc} C & \xrightarrow{\varphi_D} & \Gamma \\ & \searrow & \downarrow \\ & & \mathbb{P}^1 \end{array}$$

with $C \to \mathbb{P}^1$ the morphism defined by the ratio $(f_1 : f_2)$, and $\Gamma \to \mathbb{P}^1$ the morphism induced by the linear projection $\mathbb{P}^{l-1} \dashrightarrow \mathbb{P}^1_{\langle t_1, t_2 \rangle}$.

I now reduce to the construction of Part 1. Set $x = f_1/f_2 \in k(C)$. It is a nonconstant rational function on C, so that $k(x) \subset k(C)$ is a finite field extension. As in Part 1, write A_x for the integral closure of $k[x]$ in $k(C)$ and $C_x = \operatorname{Spec} A_x$ for the corresponding affine curve. I can do the same for $y = x^{-1} = f_2/f_1$, and identify C with the union $C_x \cup C_y$.

Since $\Gamma \subset \mathbb{P}^{l-1}$ is disjoint from $t_1 = t_2 = 0$, it is the union of two standard affine pieces Γ_{t_1} and Γ_{t_2} (with $t_i \neq 0$). The affine curve Γ_{t_2} has a finite morphism to $\mathbb{A}^1_x$ with parameter $x = t_1/t_2$ (respectively Γ_{t_1} to $\mathbb{A}^1_y$ with $y = x^{-1} = t_2/t_1$).

This gives affine varieties and morphisms $C_x \to \Gamma_x \to \mathbb{A}^1_x$, with coordinate rings $k[x] \subset k[\Gamma_x] \subset k[C_x]$. What I gain is that $k[C_x]$ is now finite as a module over $k[x]$, so a fortiori over $k[\Gamma_x]$.

At this point it clarifies the argument to separate the commutative algebra from the geometry.

Proposition 7.6 *Let $A \subset B$ be finitely generated k-algebras that are integral domains and $m \subset A$ a maximal ideal. Assume the following:*

(i) B is finite as A-module.

(ii) The ideal $I = mB$ is contained in a unique maximal ideal $n \subset B$ and $k = A/m = B/n$.

(iii) $m \to n/n^2$ is surjective.

Then on localising, the morphism of local rings $A_m \to B_n$ is surjective.

In the current case, $A = k[\Gamma_x]$ and $B = k[C_x]$. I have arranged that B is finite over A. Next $m = m_Q$ is the maximal ideal of a point $Q \in \Gamma_x$. The variety $V(I)$ of the ideal $I = mB$ consists of the points of C_x that map to Q. This consists of at most one point of C by (2), with $A/m = \mathcal{O}_{C,P}/m_p = k$. It is nonempty by the following lemma.

Lemma 7.7 *$mB \neq B$, so mB is contained in a maximal ideal of B.*

By contradiction, assume $B = mB$ and suppose b_i generate B. Then $b_i = \sum a_{ij} b_j$ with $a_{ij} \in m$, and the usual determinant trick gives $\Delta B = 0$ where $\Delta = \det(\delta_{ij} - a_{ij})$. Then $\Delta = 0$ because $1_A \in B$, but $\Delta \cong 1 \bmod m$, which is a contradiction.

So $C_x \to \Gamma_x$ is surjective, and since φ_D is injective then $Q = \varphi_D(P)$ for a unique P; this implies (b). Finally, (c) holds since (3) implies that some $f \in \mathcal{L}(C, D-P)$ has $v_P(f) = -(d_P - 1)$ which gives $v_P(f/f_2) = 1$.

Reduction to local Replace $A \subset B$ by their localisations $A_m \subset B_n$. One checks that the following still hold:

(i) B_n is finite as A_m module.

(ii) The ideal $I_n = mB_n$ is contained in nB_n and we still have $k = A/m = A_m/mA_m$ and $k = B/n = B_n/nB_n$.

(iii) $nB_n/n^2B_n = n/n^2$, so that $mA_m \to nB_n/n^2B_n$ remains surjective.

Proof of the local statement We have $I_n \subset n$, and by (3), the image of I_n generates n/n^2. This means that $n = I_n + n^2$, so that Nakayama's lemma (applied to the B-module n) implies that $I_n = n$.

Now B is a finitely generated k-algebra and n a maximal ideal, it follows by the weak NSS that $B/n = k$ (the same k). Therefore 1 generates $B/I = B/mB$, so that Nakayama's lemma (appplied to the A-module B) implies that 1 generates B. This proves Theorem 7.3.

8 Traditional applications of RR

8.1 Many characterisations of $g = 0$

I have already treated the statement of RR for $C = \mathbb{P}^1$ several times as remarks or exercises. There is a lot to say about it, in much the same way that there is a lot to say about the elements of the empty set.

Proposition 8.1 *Let C be a curve. Equivalent conditions*

(1) *There exists a divisor D of degree ≥ 1 such that $l(D) = 1 + \deg D$; or*

(1a) *the same for* every *divisor D of degree ≥ 1.*

(2) *There exist* $P \neq Q \in C$ *such that* $P \stackrel{\text{lin}}{\sim} Q$*; or*

(2a) *the same for* every $P, Q \in C$.

(3) $g(C) = 0$.

(4) $C \cong \mathbb{P}^1$.

This is all easy. If $l(D) = 1 + \deg D$ with $\deg D > 1$, the same continues to hold for $D - P$, and by induction we get a divisor of degree 1 with $l(D) = 2$. Then the linear system $|D|$ contains every $P \in C$ as a divisor, proving 2. The map $\varphi_D \colon C \to \mathbb{P}^1$ is an isomorphism by Theorem 7.3.

8.2 Treatment of $g = 1$

The ideas around RR provides practically the whole of the geometric theory and function theory of elliptic curves. First, to restate RR in the special case $g = 1$, it says that $l(D) = \deg D$ for every divisor D of degree ≥ 1. For D of degree 0, either $D \stackrel{\text{lin}}{\sim} 0 \stackrel{\text{lin}}{\sim} K_C$ or $l(D) = 0$.

A curve of genus 1 is isomorphic to a plane cubic $C \cong C_3 \subset \mathbb{P}^2$. Just choose any divisor D of degree 3. Then $l(D) = 3$, whereas $l(D - P) = 2$ and $l(D - P - Q) = 1$ for every $P, Q \in C$, so that $\varphi_D \colon C \to \mathbb{P}^2$ is an isomorphism to its image by Theorem 7.3. The linear system of lines of $\mathbb{P}^2$ pull back to the set $|D|$ of effective divisors linearly equivalent to D, so that the image $\varphi_D(C)$ is a nonsingular cubic curve.

Next, for the group law, the basic point is that a divisor D of degree 1 on C has $l(D) = 1$, so is linearly equivalent to a uniquely specified effective divisor of degree 1, necessarily a point $P \in C$. This makes the set of points of C into a coset of the group $\operatorname{Pic}^0 C$ of divisor classes of degree 0. We need to specify a point $O \in C$ as the neutral element to get out of the coset and into the subgroup.

This construction is important, so I spell it out: write $\operatorname{Div} C$ for the group of all divisors of C (the free Abelian group generated by the points $\{P \in C\}$), and $\deg \colon \operatorname{Div} C \to \mathbb{Z}$ for the degree map. Its kernel is the group $\operatorname{Div}^0 C$ of divisors of degree 0.

The principal divisors

$$\operatorname{PDiv} C = \{\operatorname{div} f \bigm| f \in k(C)^\times\} \tag{8.1}$$

also form a group, isomorphic to $k(C)^\times / k^\times$. This is a subgroup of $\operatorname{Div}^0 C$, because by Main Proposition (I) a principal divisor has degree 0.

Now define $\operatorname{Pic}^0 C$ as the quotient group

$$\operatorname{Pic}^0 C = \operatorname{Div}^0 C / \operatorname{PDiv} C = \operatorname{Div}^0 C / \overset{\text{lin}}{\sim}. \tag{8.2}$$

The group law on this is just addition of divisors mod linear equivalence, and the zero element is the class of the zero divisor.

Along with $\operatorname{Pic}^0 C$, consider its coset $\operatorname{Pic}^1 C$ formed by divisors of degree 1 up to linear equivalence. As we have seen, this is in bijection with C itself. Now choosing any point $O \in C$ provides a bijective map $\operatorname{Pic}^0 C \to \operatorname{Pic}^1 C \to C$ by $[D] \mapsto [D+O]$. That is, a divisor class D of degree 0 maps to the divisor class $D+O$, which is linearly equivalent to a unique $P \in C$; the inverse bijection $C \to \operatorname{Pic}^0 C$ takes P to the class of $P - O$. In conclusion, the group law on C is

$$(P, Q) \mapsto (P - O, Q - O) \mapsto (P + Q - 2O) \mapsto (P +_C Q),$$

where the middle step is addition in Pic^0, and $P +_C Q$ is the unique effective divisor linearly equivalent to $P + Q - O$.

There are a couple of exercises concerned with interpreting the traditional geometric $P + Q + R$ form of the group law on a nonsingular plane cubic curve (otherwise known as the secant-tangent construction) [UAG, Chap. 2] within the current treatment.

8.3 The hyperelliptic dichotomy for $g \geq 2$

A curve C of genus g has a canonical divisor K with $\deg K = 2g - 2$ and $l(K) = g$. In the main case $g \geq 2$, we have the following dichotomy.

Theorem 8.2 *Write $\varphi_K \colon C \to \mathbb{P}^{g-1}$ for the canonical map of C, defined by $|K_C|$. Then* either *φ_K is an isomorphism to its image $C \subset \mathbb{P}^{g-1}$ and the hyperplanes of $\mathbb{P}^{g-1}$ cut out the canonical system $|K|$ on C.* Or *C has a linear system g^1_2, and φ_K is obtained as the composite of the double covering $C \to \mathbb{P}^1$ given by the g^1_2, followed by the embedding $\mathbb{P}^1 \cong \Gamma_{g-1} \subset \mathbb{P}^{g-1}$ as the rational normal curve of degree $g - 1$.*

Every curve of genus $g = 2$ is hyperelliptic: the canonical system $|K_C|$ is itself a g^1_2.

Proof Equality $\mathcal{L}(K - P) = \mathcal{L}(K)$ holds only for $g = 0$ (when both spaces are zero). For RR would give $l(P) - g = 1 - g + \deg P$, that is, $l(P) = 2$, one of the characterisations of $\mathbb{P}^1$ of Proposition 8.1.

Next if $\mathcal{L}(K-P-Q) = g-2$ for every $P, Q \in C$, Theorem 7.3 guarantees that φ_K is an embedding, which is one leg of the dichotomy. It remains to analyse the other leg, when $\mathcal{L}(K-P-Q) = g-1$ for some $P+Q$. In this case RR gives

$$l(P+Q) - (g-1) = 1 - g + 2, \quad \text{that is,} \quad l(P+Q) = 2. \tag{8.3}$$

Thus $D = P + Q$ has $l(D) = 2$, so that $|D|$ is a g^1_2. It forms a pencil $|D|$, made up of moving pairs $P + Q \in |D|$ parametrised by $\mathbb{P}^1$, each of which also has $\mathcal{L}(K_C - P - Q) = g - 1$. When P, Q are distinct, they go to the same point under φ_{K_C}. When they coincide $\mathcal{L}(K_C - 2P) = \mathcal{L}(K_C - P)$ so that every $f \in \mathcal{L}(K_C - P)$ vanishes twice at P, so cannot provide a local parameter at P. Thus g^1_2 defines a 2-to-1 morphism $\varphi_D\colon C \to \mathbb{P}^1$, so that C is hyperelliptic. The final clause of the theorem is easy, and is discussed in the following section. $\square$

8.4 Special linear systems on a hyperelliptic curve

Hyperelliptic curves $y^2 = f_{2g+2}(x_1, x_2)$ provide the valuable portfolio of introductory examples discussed in introductory Lecture 3. They provide in particular curves of every genus g, and the topological picture of a Riemann surface of genus g. They also play a structural role in the theory of linear systems, starting with their role as counterexamples to canonical embedding as above, and at several points in what follows.

Every special linear system on a hyperelliptic curve C comes from its special pencil $|A| = g^1_2$. I discuss this in more detail: write t_1, t_2 for homogeneous coordinates on $\mathbb{P}^1$, corresponding to a basis $x_1, x_2 \in \mathcal{L}(A)$. For any $b \geq 1$, the homogeneous forms of degree b in t_1, t_2 form a vector space of dimension $b + 1$ based by

$$S^b(t_1, t_2) = \{t_1^b, t_1^{b-1}t_2, \ldots, t_2^b\}. \tag{8.4}$$

They are linearly independent because $(t_1 : t_2)$ is a nonconstant ratio on $\mathbb{P}^1$. The same goes for $(x_1 : x_2)$ on C, and x_1/x_2 is a transcendental generator of the function field $k(C)$.

The pullbacks $S^b(x_1, x_2)$ in $k(C)$ therefore base a $(b+1)$-dimensional vector subspace of $\mathcal{L}(bA)$. In the case $b = g - 1$, this means that $(g-1)A$ has degree $2g - 2$ and $l((g-1)A) = g$, so $(g-1)A \overset{\text{lin}}{\sim} K_C$ is a canonical divisor. It follows that $S^b(x_1, x_2)$ base $\mathcal{L}(bA)$ for $b = 1, \ldots, g-1$.

The divisor $gA = K_C + A$ has degree $2g$, so is regular, and has $l(gA) = g + 1$ by Proposition 5.7, (c). Thus $S^g(x_1, x_2)$ also base $\mathcal{L}(gA)$, so that the morphism φ_{K_C+A} is also composed of the double cover $\varphi_A\colon C \to \mathbb{P}^1$. It is only when we go to $(g+1)A$ that we find a function y on C that is not a rational function of x_1/x_2, and is capable of distinguishing the conjugate pairs $\varphi_A^{-1}(P)$ of C over $P \in \mathbb{P}^1$, and generating $k(C)$ as a quadratic extension of $k(\mathbb{P}^1)$.

Recall that a special linear system $|D|$ on a curve C is one for which $l(D) > 1 - g + \deg D$, so that $\mathcal{L}(K_C - D) \neq 0$ and $|K_C - D| \neq \emptyset$. The moving part of $|D|$ is a linear subsystem of $|K_C|$. For a hyperelliptic curve $|K_C| = |(g-1)A|$. It follows that every special linear system on C consists of a multiple of g^1_2 as its moving part, plus a fixed part.

8.5 Geometric form of RR

A main feature of the RR formula for a curve C

$$l(D) - l(K_C - D) = 1 - g + \deg D \tag{8.5}$$

is that, for given degree $\deg D \in [0, \dots, 2g-2]$, if $\mathcal{L}(D)$ is bigger than expected, then so is $\mathcal{L}(K_C - D)$. A geometer feels the desire to draw C in its canonical embedding as the picture of Figure 8.5.1.

Figure 8.5.1: Geometric Riemann–Roch: For a canonically embedded curve $C \subset \mathbb{P}^{g-1}$ of genus g, the hyperplanes through the linear span $\Pi = \langle D \rangle$ of a divisor D cut out the complete linear system $|K_C - D|$. The irregularity $l(K_C - D)$ of D equals $g - a$ where $\Pi = \mathbb{P}^{a-1}$, so corresponds to linear dependence relations between the points of D in $\mathbb{P}^{g-1}$.

The hyperplane sections of a canonically embedded curve $C \subset \mathbb{P}^{g-1}$ cut out the linear system $|K_C|$. For an effective divisor D, the hyperplanes through $\varphi_{K_C}(D)$ (with the appropriate local multiplicities) cut out the linear system $|K_C - D|$. Passing through $\varphi_{K_C}(D)$ is the same geometric condition as containing its linear span $\Pi = \langle \varphi_{K_C}(D) \rangle$. A projective linear system $\Pi = \mathbb{P}^{a-1}$ of dimension $a-1$ imposes a linear conditions on $\mathcal{L}(K_C)$, giving $l(K_C - D) = g - a$.

If the d points were linearly independent, they would of course span a linear subspace $\mathbb{P}^{d-1}$, and so impose d linearly independent conditions on $\mathcal{L}(K_C)$. Thus the difference $d - a$ is the number of linear dependencies between the d points.

Proposition 8.3 (Geometric RR) *The difference $d - a$ is equal to the dimension $r = \dim |D| = l(D) - 1$ of the linear system $|D|$. In other words, an effective divisor $D = P_1 + \cdots + P_d$ moves in a linear system g^r_d if and only if the points of D in $C \subset \mathbb{P}^{g-1}$ span a projective linear subspace $\Pi = \langle D \rangle$ of dimension $d - r - 1$.*

Proof Plug $l(K_C - D) = g - a$ into the RR formula. This gives

$$l(D) - (g - a) = 1 - g + d, \quad \text{hence} \quad r = l(D) - 1 = d - a. \quad \square \tag{8.6}$$

An important case is a *trigonal* linear system: three points of C map to collinear points of $\varphi_K(C) \subset \mathbb{P}^{g-1}$ if and only if $D = |P_1 + P_2 + P_3|$ moves in a g^1_3. Thus if C contains one triple of collinear points, these move in a family of collinear triples that is parametrised by $\mathbb{P}^1$.

9 Clifford's theorem and the free pencil trick

9.1 Multiplying RR spaces and the linear-bilinear problem

So far, the RR spaces $\mathcal{L}(C, D)$ have appeared as k-vector subspaces of the function field $k(C)$. This section introduces as a new ingredient the multiplication in $k(C)$, that defines a bilinear map $\mathcal{L}(D_1) \times \mathcal{L}(D_2) \to \mathcal{L}(D_1 + D_2)$ for any two divisors D_1, D_2. Lemma 9.3 and Proposition 9.8 give a first introduction to the *linear-bilinear problem*: if a bilinear map $V_1 \times V_2 \to W$ is nondegenerate in some sense, can we deduce a lower bound on the rank of the associated linear map $V_1 \otimes V_2 \to W$?

9.2 Clifford's theorem

The divisors D with degree in the range $(0, 2g-2)$ may be irregular. In this range, the maximum value of $l(D)$ is given by the hyperelliptic linear systems $|rA| = r|A|$ discussed in 8.4.

Theorem 9.1 (Clifford's theorem) *Let D be a divisor with $d = \deg D$ in the range $0 < d < 2g-2$, and set $l(D) = r+1$, so that $|D|$ is a g^r_d.*

Then $d \geq 2r$. Moreover equality holds only for $|D| = |rA|$ where A is a g^1_2 on a hyperelliptic curve, as in 8.4

Addendum 9.2 *In the range $-2 \leq d \leq 2g$, the inequality $d \geq 2r$ holds for any curve C. Moreover, equality $d = 2r$ holds only in the following cases:*

(1) *$d = -2$ and $r = -1$, or $d = 2g$ and $l(D) = g+1$, so $r = g$.*

(2) *$D \overset{\text{lin}}{\sim} 0$ and $r = d = 0$, or $D \overset{\text{lin}}{\sim} K_C$ and $r = g-1$, $d = 2g-2$.*

(3) *C is hyperelliptic with $A = g^1_2$, and $D = rA$ for $r = 1, \dots, g-2$, so that $d = 2r$ and $l(D) = r+1$.*

Here (1) and (2) are more or less vacuous, and hold for every curve C. Only case (3) has any content, and relates specifically to hyperelliptic curves. Strict inequality holds for every divisor D of degree -1, giving $l(D) = 0$, so $r = -1$, or degree $2g-1$, when $l(D) = g$, so $r = g-1$.

Proof This is based on the linear-bilinear inequality of the next lemma. Consider the multiplication map $\psi\colon \mathcal{L}(D) \times \mathcal{L}(K_C - D) \to \mathcal{L}(K_C)$. The two RR spaces $\mathcal{L}(D)$ and $\mathcal{L}(K_C - D)$ are k-vector subspaces of $k(C)$ and the map is multiplication in $k(C)$. It is clearly bilinear over k and *nondegenerate*, by which I mean that $f \neq 0$, $g \neq 0$ implies that $fg \neq 0$.

Lemma 9.3 *If $V_1 \times V_2 \to W$ is a nondegenerate bilinear map, the induced linear map*

$$\psi\colon V_1 \otimes V_2 \to W \tag{9.1}$$

has $\operatorname{rank} \psi \geq \dim V_1 + \dim V_2 - 1$.

Proof of Lemma Write $n = \dim V_1$ and $m = \dim V_2$. Recall that $V_1 \otimes V_2$ contains *primitive tensors* $v_1 \otimes v_2$ for $v_1 \in V_1$ and $v_2 \in V_2$. We can write $V_1 \otimes V_2$ as the space $\operatorname{Mat}(n \times m)$ of $n \times m$ matrices, and then the primitive tensors are the tensors of rank 1.

These are the $n \times m$ matrices of the form

$$(\text{column matrix with entries } x_i) \times (\text{row matrix with entries } y_j), \qquad (9.2)$$

so with (i,k)th entry $m_{ik} = x_i y_k$. Clearly, every 2×2 minor $\left|\begin{smallmatrix} m_{ik} & m_{il} \\ m_{jk} & m_{jl} \end{smallmatrix}\right|$ is zero. Moreover, if M is an $n \times m$ matrix of rank 1 and $m_{ik} \neq 0$, one sees from the rank 2 condition that the whole matrix is determined by the ith row and kth column, so M is of the form (9.2). These matrices form an affine subvariety of dimension $n+m-1$, since $v_1 \otimes v_2$ determines v_1, v_2 up to multiplying v_1 by $\lambda \in k^\times$ and v_2 by λ^{-1}.

The kernel of ψ in (9.1) is a vector subspace of $V_1 \otimes V_2$. The nondegeneracy assumption on ψ is that $\ker \psi$ intersects the primitive tensors only in 0. It follows that $\ker \psi \subset V_1 \otimes V_2$ has codimension $\geq n+m-1$, which proves the Lemma. □

An algebraic geometer expresses the argument in projective space: the projectivisation of $\ker \psi$ in (9.1) is the linear subspace

$$\mathbb{P}(\ker \psi) \subset \mathbb{P}^{nm-1} = \mathbb{P}(V_1 \otimes V_2). \qquad (9.3)$$

Nondegeneracy says it is disjoint from the projectivisation of the variety of $n \times m$ matrices of rank 1. This is the Segre embedding of $\mathbb{P}(V_1) \times \mathbb{P}(V_2) = \mathbb{P}^{n-1} \times \mathbb{P}^{m-1}$. It is a projective subvariety of dimension $n+m-2$. A projective linear subspace $\Pi \subset \mathbb{P}^{nm-1}$ is an intersection of c hyperplanes, where c is the codimension of Π in $\mathbb{P}^{nm-1}$. Now if $c \leq n+m-2$, the kernel subspace Π must[1] intersect $\mathbb{P}^{n-1} \times \mathbb{P}^{m-1}$. It follows that our kernel has codimension $\geq n+m-1$. This gives $\operatorname{rank} \psi \geq n+m-1$ as required. □

For the proof of Clifford's theorem, the nondegenerate bilinear multiplication ψ of the lemma has rank $\geq l(D) + l(K_C - D) - 1$ as a map to the g-dimensional space $\mathcal{L}(K_C)$. Putting this together with the RR formula give

$$l(D) + l(K_C - D) - 1 \leq g \qquad (9.4)$$
$$l(D) - l(K_C - D) = 1 - g + d. \qquad (9.5)$$

Adding the two gives $2l(D) \leq d+2$, that is, $d \geq 2r$. This proves the inequality.

It may not be obvious how to get started on the case of equality. The proof is the one-off idiosyncratic argument given below. With hindsight,

[1] This assumes basic properties of dimension theory. See, for example, Shafarevich, Basic Algebraic Geometry, Chapter 1, Section 6.

both $|D|$ and $|E| = |K_C - D|$ are made up of multiples of the g^1_2, and we play off one against the other to break off smaller multiples to establish the existence of the g^1_2. The argument depends on the following elementary fact from linear algebra concerning restriction to coprime divisors, that leads us into the Castelnuovo free pencil trick.

Coprime divisors An easy exercise in linear algebra shows that U_1, U_2 finite dimensional subspaces of a vector space V have

$$\dim U_1 + \dim U_2 - \dim(U_1 \cap U_2) = \dim(U_1 + U_2) \leq \dim V. \tag{9.6}$$

We say that two effective divisors B_1, B_2 on C with no points in common are *coprime*. That is, $B_1 = \sum a_P P$ and $B_2 = \sum b_P P$ have $a_P, b_P \geq 0$, and no P has both positive. Or equivalently, B_1 and B_2 have disjoint support. The following result is the key to what follows.

Lemma 9.4 *For coprime effective divisors B_1 and B_2, vanishing on both B_1 and B_2 is equivalent to vanishing on $B_1 + B_2$. That is*

$$\mathcal{L}(D - B_1) \cap \mathcal{L}(D - B_2) = \mathcal{L}(D - B_1 - B_2) \quad \textit{inside } \mathcal{L}(D). \tag{9.7}$$

There is nothing to prove: in the above notation, for $f \in \mathcal{L}(D)$, the conditions that $\operatorname{div}(f) + D \geq a_P$ for $P \in \operatorname{Supp} B_1$ and $\operatorname{div}(f) + D \geq b_P$ for $P \in \operatorname{Supp} B_2$ just says $\operatorname{div}(f) + D \geq a_P + b_P$ for every $P \in C$.

It is useful to write the conclusion as the following exact sequence:

Proposition 9.5 *For any divisor E, write $i_{B_i} \colon \mathcal{L}(E - B_i) \hookrightarrow \mathcal{L}(E)$ for the inclusion maps for $i = 1, 2$. These are just inclusion maps (the identity of $k(C)$). Then the sequence*

$$0 \to \mathcal{L}(E - B_1 - B_2) \xrightarrow{(i_{B_1}, i_{B_2})} \mathcal{L}(E - B_1) \oplus \mathcal{L}(E - B_2) \xrightarrow{\binom{i_{B_1}}{i_{B_2}}} \mathcal{L}(E). \tag{9.8}$$

is exact. Therefore $l(E) \geq l(E - B_1) + l(E - B_2) - l(E - B_1 - B_2)$. $\square$

Now for the case of equality $d = 2r$ in Clifford's theorem. The conclusion is that C is hyperelliptic, and that both D and $K - D$ are irregular, so the mobile parts of $|D|$ and $|K - D|$ are composed of the same g^1_2.

Suppose C has genus g, and that D is a divisor of degree $2r$ with $l(D) = r + 1$. Write $E = K_C - D$, so that $\deg E = 2g - 2 - 2r$ and the RR formula says that $l(E) = g - r$ and E also has equality in the Clifford inequality $\deg E = 2g - 2 - 2r = 2(l(E) - 1)$. The two divisors D and E appear symmetrically in the argument. There is nothing to prove if $r \le 1$ or $r \ge g - 2$: if $r = 1$ then $|D|$ is a g^1_2, whereas if $r = g - 2$ then $|E|$ is a g^1_2, so C is hyperelliptic and $|D| = |(g-2)E|$.

Suppose then that $2 \le r \le g - 3$. Both $|D|$ and $|E|$ are linear systems of (projective) dimension ≥ 2. The idea is to reduce $|D|$ to a smaller linear system $|D_0|$ that still has the equality $\deg D_0 = 2(l(D_0) - 1)$. To do this, choose any point $P \in C$, and consider the linear systems $|D-P|$ and $|E-P|$, each of which still has a positive dimensional mobile part. Choosing fairly general divisors $D' \in |D-P|$ and $E' \in |E-P|$ (and adding back the P) gives divisors $D \in |D|$ and $E \in |E|$ having P in common but neither contained in the other; fix such a D and E.

Write $D_0 = \gcd(D, E)$ for the greatest common divisor of D and E (that is, the greatest divisor with $D_0 \le D$ and $D_0 \le E$).

The two residual divisors $A = D - D_0$ and $B = E - D_0$ are effective and coprime, because we have subtracted off all the points they had in common. The divisor $E^0 = D_0 + A + B = E + A$ is the smallest divisor $E^0 \ge D$ and $\ge E$, so a kind of least common multiple.

Now we started from $D + E \overset{\text{lin}}{\sim} K_C$, and passed to $D_0 = D - A$ and $E^0 = E + A$, so that we still have $D_0 + E^0 \overset{\text{lin}}{\sim} K_C$.

On the other hand, we pass from E^0 down to D_0 by subtracting off A and B, which are coprime effective divisors. Thus applying the above Lemma 9.4 and Proposition 9.5 on coprime pairs gives

$$\begin{aligned} l(E^0) = l(D_0 + A + B) &\ge l(D_0 + A) + l(D_0 + B) - l(D_0) \\ &= l(D) + l(E) - l(D_0). \end{aligned} \tag{9.9}$$

By assumption, $|D|$ and $|E| = |K_C - D|$ are linear systems with the biggest RR spaces for their degree allowed by the Clifford inequality: namely D is a g^r_d with $d = 2r$ and E is a $g^{g-1-r}_{2(g-1-r)}$. The inequality $l(D_0) + l(E^0) \ge l(D) + l(E)$ of (9.9) implies that the same holds for $l(D_0)$ and $l(E^0)$.

To spell this out, the Clifford inequality applied to D_0 and E^0 gives $\deg D_0 \ge 2(l(D_0) - 1)$ and $\deg E^0 \ge 2(l(E^0) - 1)$. Taking sums and applying (9.9) gives

$$\begin{aligned} 2g - 2 = \deg D_0 + \deg E^0 &\ge 2(l(D_0) - 1) + 2(l(E^0) - 1) \\ &\ge 2(l(D) - 1) + 2(l(E) - 1) = 2g - 2. \end{aligned} \tag{9.10}$$

Thus equality holds throughout, and $|D_0|$ also has the equality $\deg D_0 = 2(l(D_0) - 1)$, so is a $g^{r'}_{2r'}$ but with $r' < r$. Induction on r proves that C

has a g^1_2, so is hyperelliptic. By the discussion of 8.4, all the divisors in the argument are special, so multiples of $A = g^1_2$. Q.E.D.

9.3 The Castelnuovo free pencil trick

The Castelnuovo free pencil trick applies Proposition 9.5 on coprime divisors to give a lower bound on the rank of multiplication maps

$$\mathcal{L}(E_1) \otimes \mathcal{L}(E_2) \to \mathcal{L}(E_1 + E_2) \tag{9.11}$$

given a suitable free pencil. The following result just rewrites the exact sequence of Proposition 9.5 for E any divisor and $|D-A|$ a free pencil. This means $s_1, s_2 \in \mathcal{L}(D-A)$ have $\operatorname{div} s_i + D - A = B_i$ with coprime $B_1, B_2 \in |D|$.

Corollary 9.6 (The free pencil trick) *Let E and $D - A$ be as above.*

$$0 \to \mathcal{L}(E - (D-A)) \xrightarrow{(i_{B_1}, i_{B_2})} \mathcal{L}(E)^{\oplus 2} \xrightarrow{\binom{-i_{B_2}}{i_{B_1}}} \mathcal{L}(E + D - A). \tag{9.12}$$

is exact. Here the inclusion maps are just the identity map of $k(C)$. The assumptions $\operatorname{div} s_i + D - A = B_i$ *they map between the stated RR spaces, and the sequence is exact by Proposition 9.5.*

Moreover, if the left-most divisor in (9.8) *is regular (that is, equality $l = 1 - g + d$ holds in RR), an easy dimension-counting proves the right-most map is surjective.* □

9.4 Max Noether's theorem

This is the typical application of the Castelnuovo free pencil trick. Let C be a nonhyperelliptic curve of genus g. Recall from Theorem 8.2 that K_C is very ample, and identify C with its canonical image $C = \varphi_{K_C}(C) \subset \mathbb{P}^{g-1}$.

Theorem 9.7 (Max Noether's theorem) *For each $d \geq 1$, the forms of degree d on $\mathbb{P}^{g-1}$ map surjectively to $\mathcal{L}(C, dK_C)$.*

By construction, saying that $C = \varphi_{K_C}(C) \subset \mathbb{P}^{g-1}$ means that the linear forms on $\mathbb{P}^{g-1}$ forms the RR space $\mathcal{L}(C, K_C)$. In other words, the hyperplanes of $\mathbb{P}^{g-1}$ cut out the complete canonical system $|K_C|$. The theorem states that, in the same way, the hypersurfaces of $\mathbb{P}^{g-1}$ of degree d cut out the complete linear system $|dK_C|$ for each

The basic case to work with is $d = 2$. The product $s_i s_j \in \mathcal{L}(C, 2K_C)$ because $\operatorname{div}(s_i s_j) = \operatorname{div} s_1 + \operatorname{div} s_2$. It is required to prove that the products $s_i s_j$ include $3g - 3$ elements that are linearly independent in $\mathcal{L}(C, 2K_C)$. The key to this is the Castelnuovo free pencil trick.

Linearly general position For $C \subset \mathbb{P}^n$ a nonsingular curve that spans $\mathbb{P}^n$, it is known that *a sufficiently general hyperplane $H \subset \mathbb{P}^n$ cuts C in d points that are linearly in general position.* This result is a curious backwater of the algebraic geometry literature, and I leave the proof to the Appendix below.

Choose g general points $P_1, \dots, P_g$ of $C \subset \mathbb{P}^{g-1}$, and assume the P_i map to the coordinate points $(0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{P}^{g-1}$. Applied to the hyperplane $V(s_1)$, linearly general position implies that s_1, s_2 both vanish on the divisor $A = P_3 + \cdots + P_g$ but not at any other point of C, so that $s_1, s_2 \in \mathcal{L}(C, K_C - A)$ form a free pencil as in 9.8.

Now $\mathcal{L}(A) = 1$. This follows (say) from Standard Trick (b): the points $P_3, \dots, P_g$ are general, so subtracting them one by one from K_C give irregularity $l(K_C - A) = 2$, therefore $l(A) - 2 = 1 - g + \deg A$.

The conclusion of the free pencil trick Proposition 9.8 is that the two subspaces $s_1\mathcal{L}(K_C)$, $s_2\mathcal{L}(K_C)$ intersect only in the 1 dimensional space $\mathcal{L}(A)$. This means that the $2g - 1$ monomials

$$s_1^2, \dots, s_1 s_g \quad \text{and} \quad s_2^2, s_2 s_3, \dots, s_2 s_g \tag{9.13}$$

are linearly independent in $\mathcal{L}(2K_C - A)$. They vanish at the $g - 2$ points of A by construction.

Now the $g - 2$ monomials $s_3^2, \dots, s_g^2$ are linearly independent modulo $\mathcal{L}(2K_C - A)$, because at each P_i, s_i^2 is nonzero, and the others zero. They thus form a complimentary basis of $\mathcal{L}(2K_C)$.

For $d \geq 3$, by the same argument, the two subspaces $s_1\mathcal{L}((d-1)K_C)$ and $s_2\mathcal{L}((d-1)K_C)$ intersect in $\mathcal{L}((d-2)K_C + A)$. Since $d \geq 3$ this is in the regular range, so there sum maps surjectively to $\mathcal{L}(dK_C - A)$, and the monomials $s_3^d, \dots, s_g^d$ again form a complementary basis of $\mathcal{L}(dK_C)$. QED

9.5 The free pencil trick

Let D be a divisor and $U = \langle s_1, s_2 \rangle \subset \mathcal{L}(C, D)$ a 2-dimensional vector subspace such that the linear subsystem $\mathbb{P}^1_U \subset |D|$, made up of the effective divisors

$$\operatorname{div}(\lambda s_1 + \mu s_2) + D = D_s \quad \text{for } s \in U, \tag{9.14}$$

is a free pencil. This just means that a basis s_1, s_2 of U gives divisors $B_1 = \operatorname{div} s_1 + D$ and $B_2 = \operatorname{div} s_2 + D$ that are coprime in the sense of Proposition 9.5. This is often a free g^1_d (see Remark 7.1), but the logic of the argument allows $U \subset \mathcal{L}(C, D)$ to be a strict subspace.

Proposition 9.8 *Let D and U be as above, and E any divisor. Consider the multiplication map $\mu_U\colon U \otimes \mathcal{L}(E) \to \mathcal{L}(D+E)$. Then*

$$\operatorname{rank}\mu = \dim(U \otimes \mathcal{L}(E)) - l(D-E) = 2l(E) - l(D-E). \tag{9.15}$$

Proof The assertion is a particular case of Proposition 9.5. In fact under μ_U, the two summands of

$$U \otimes \mathcal{L}(E) = s_1 \otimes \mathcal{L}(E) \oplus s_2 \otimes \mathcal{L}(E) \tag{9.16}$$

map to

$$s_1 \cdot \mathcal{L}(E) \quad \text{and} \quad s_2 \cdot \mathcal{L}(E) \subset \mathcal{L}(D+E), \tag{9.17}$$

which intersect in $\mathcal{L}(E - D_1 - D_2)$.

One traditionally expresses this as an exact sequence

$$0 \to \mathcal{L}(E-D) \to \mathcal{L}(E)^{\oplus 2} \to \mathcal{L}(D+E). \tag{9.18}$$

The argument for (9.18) can also be written intrinsically (with a small additional headache).

Most of the interesting consequences of the Castelnuovo free pencil trick relate to special divisors. However, if all the divisors in (9.18) are in the regular range (that is, $\deg(E-D) \geq 2g-1$), an easy calculation with the RR formula shows that the final map is surjective.

To do

Worked example for $g = 4$, $g = 5$: use Max Noether's theorem to get $Q_2 \cap F_3$ in $\mathbb{P}^3$ and $Q_1 \cap Q_2 \cap Q_3$ as plausible constructions the canonical models. Add a few hints looking forward to the Petri analysis.

To do The multiplication map $\mathcal{L}(D) \otimes \mathcal{L}(K_C - D) \to \mathcal{L}(K_C)$ is called the *Petri map*. There are favourable cases in which it is surjective, that has nice consequence.

I also use the Castelnuovo free pencil trick in Chapter 4, (page 6 in the 2020 notes) in the proof that s_1, s_2 in the complete sections ring $R(C, D)$ form a regular sequence.

10 Appendix on inseparability

10.1 Definitions

The material here is not really essential for algebraic curves (except for the easy part of the proof of linearly general position), but I hope eventually to put it all together as an appendix for the reader who needs it. Inseparable extensions are usually only mentioned in passing in a Galois theory course, mainly to get rid of them. However there is no special mystery or difficulty about what is going on, even if it is not specially familiar or congenial.

The first thing to discuss is the paradoxical geometry of an inseparable function or map. In analysis, or in geometry in characteristic 0, a function $f(x)$ that has zero derivative everywhere, or a map φ all of whose partial derivatives are identically zero is of course a constant. In characteristic p this does not hold. If a polynomial f has $f' \equiv 0$, the only thing one can say is that f only involves its variables to the pth power.

Separable Let $K \subset L$ be a field extension with $[L : K] < \infty$. The following equivalent conditions define what it means for $x \in L$ to be *separable* over K, or (with a minor change of wording) for the whole extension $K \subset L$ to be separable.

(1) The minimal polynomial $f_x \in k[X]$ of x splits into distinct factors in any extension of L.

(2) The minimal polynomial f_x has formal derivative $f' \neq 0$.

(3) The tensor product $L \otimes_K L$ has no nilpotents.

(4) The trace homomorphism $\mathrm{Tr}_{L/K} \colon L \to K$ is nonzero. Moreover the trace provides a nondegenerate bilinear pairing

$$\mathrm{Tr}_{L/K}(xy) \colon L \times L \to K. \tag{10.1}$$

Sample argument: if the extension $K \subset L$ is inseparable, then there is an a in K such that $x^p - a$ has a root in L. Then $L \otimes L$ has two such elements $x_1 = x \otimes 1$ and $x_2 = 1 \otimes x$ with $x_1^p = x_2^p$, therefore $(x_1 - x_2)^p = 0$, so it has nilpotents. At the same time, calculating the trace of any element of L by any method must involve sums of p identical terms, so the answer can only add to zero.

`TO DO. Discussion and proof of that.`

Purely inseparable The following equivalent conditions define what it means for $x \in L$ or the whole extension $K \subset L$ to be *purely inseparable.*

(1) The minimal polynomial f_x is $X^{p^n} - a = (X - \alpha)^{p^n})$ with $n \geq 1$.

(2) x has no other conjugates in any extension field $L \subset L'$.

(3) If $L \subset L'$ is any extension field and $\varphi\colon L \to L'$ a K-linear homomorphism then $\varphi_{|L} = \mathrm{Id}_L$.

(4) $K(x)/K$ is normal and $\mathrm{Aut}_K(K(x)) = \{\mathrm{Id}\}$.

Standard discussion from Galois theory Let L/K be finite field extension. Recall from Galois theory that the following conditions are equivalent, and L/K is *normal* if they hold.

(1) Every irreducible polynomial $f \in K[x]$ with a root in L has all its roots in L – in other words, if we view f as an element of $L[x]$, it splits into linear forms $f(x) = \prod(x - \xi_i)$ with $\xi_i \in L$.

(2) For every $\xi \in L$, the minimal polynomial $f \in k[x]$ of ξ splits as above.

(3) If L is contained in a bigger field extension $L \subset L'$ then any K-linear homomorphism $\varphi\colon L \to L'$ takes L to itself.

The following arguments are already in Part I of the 2022 notes.

Theorem 10.1 (Kaplansky) *Assume that L/K is normal. Then L is in a unique way the composite of a separable extension L^{sep} and a purely inseparable extension L^{insep}*

```
          L

L^sep     L^insep

          K
```

where

$$\begin{aligned} L^{\mathrm{sep}} &= \{x \in L \mid x \textit{ is separable}\} \quad \textit{and} \\ L^{\mathrm{insep}} &= \{x \in L \mid x \textit{ is purely inseparable}\}. \end{aligned} \tag{10.2}$$

Then L^{sep}/K is a Galois extension (that is, normal and separable) and L/L^{insep} is Galois with the same Galois group:

$$\mathrm{Gal}(L/L^{\mathrm{insep}}) = \mathrm{Gal}(L^{\mathrm{sep}}/K) = \mathrm{Aut}(L/K) \tag{10.3}$$

L^{insep}/K is the fixed subfield of $\mathrm{Aut}(L/K)$
L^{sep} is purely inseparable

Composite of the two disjoint field extensions L^{sep}/K and L^{insep}/K. As a K-algebra $L = L^{\text{sep}} \otimes_K L^{\text{insep}}$. The proof is a straightforward verification using the main results of Galois theory.

10.2 Finiteness of integral closure

The result for finiteness of integral closure works for finite field extensions (separable or not), depending on Kaplansky's theorem. This is already in the notes for Chapter 1, but it fits more logically here.

10.3 Frobenius morphism

The identity

$$(x + y)^p = x^p + y^p \quad \text{for all } x, y \in R \tag{10.4}$$

holds for R a commutative ring of characteristic p because the intermediate binomial coefficients $\binom{p}{i}$ are divisible by p. In other words, the map $\mathrm{Frob}_R = \varphi_R \colon R \to R$ defined by $x \mapsto x^p$ is an *endomorphism* (a homomorphism from a ring to itself). It is called the *Frobenius map.*

This idea already provides the whole of the Galois theory of finite fields: write $q = p^n$. Then the finite field $\mathbb{F}_q$ has the Frobenius homomorphism $\varphi_p \colon \mathbb{F}_q \to \mathbb{F}_q$ given by $x \mapsto x^p$. A homomorphisms of fields is always injective, and here it is also surjective, because the image and domain are finite sets with the same number of elements.

The equation $x^p = x$ has p roots that are the elements of $\mathbb{F}_p$ (by Fermat's little theorem). This implies that the fixed subfield of φ_p is $\mathbb{F}_p$. Also φ_p generates the Galois group, and is of order n, so that $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \mathbb{Z}/n$, and for $m \mid n$, the fixed subfield of φ_p^m is $\mathbb{F}_p^m$.

For an algebraic variety (or scheme) over a field of characteristic p, we have to distinguish the

```
  _absolute_ Frobenius  versus  _geometric_ Frobenius.
The point is that although phi is a ring homomorphism,
it is NOT a k-algebra homomorphism, since it messes
with the ground field k itself.
```

The absolute Frobenius (that takes $P = [x_1, \dots, x_n] \mapsto [x_1^p, \dots, x_n^p]$ can be twisted into a morphism of varieties by changing the target to be a variety over the field k', where k' is the same field, but acts on P by $a \cdot f = a^p \cdot f$ (that is, the pth power map.

Although not so much for this course, this is important in many other areas of algebra and number theory over a field of characteristic p, and was the key first step in the Weil–Grothendieck–Deligne treatment of the Riemann hypothesis over a finite field.

10.4 Theorem on linearly general position

Let $\Gamma \subset \mathbb{P}^n$ be an irreducible curve of degree d spanning $\mathbb{P}^n$. Assume either that we are over a field k of characteristic zero, or that C is nonsingular. Then a general hyperplane section of Γ consists of points in linearly general position. This means that Γ cut with a general hyperplane $H = \mathbb{P}^{n-1}$ is a set of d points such that every subset of n points spans H. For example, if $n \geq 3$, every general hyperplane section of Γ contains a secant line that is not a trisecant.

Step 1 Reduction from $C \subset \mathbb{P}^n$ for which the points of every hyperplane section have linear dependencies to a curve $C \subset \mathbb{P}^n$ with the same property.

Proof Take linear projection from a general linear subspace $\Pi = \mathbb{P}^{n-4}$ (or equivalently, from $n-3$ general points of $\mathbb{P}^n$) and follow your nose. We can assume that Π does not intersect any secant PQ or tangent line T_P for $P, Q \in C$, so that the image of C in $\mathbb{P}^3$ is isomorphic to C, so $C \subset \mathbb{P}^n$ nonsingular implies $C \subset \mathbb{P}^3$ remains so. The planes of $\mathbb{P}^3$ come from hyperplanes of $\mathbb{P}^n$ through Π.

Step 2 For $C \subset \mathbb{P}^3$, the assumption that the general secant PQ is a multisecant implies that the tangent lines T_P and T_Q at every two general points intersection.

Proof We assume that every secant line PQ contains a third point $R \in C$. If the point P moves infinitesimally to P', the secant line RP' must contain a point Q' infinitely near to Q. Therefore RPP' and QQ' are all coplanar, and the plane containing them contains both the tangent line to P and the tangent line to Q.

Step 3 Any two tangent lines to $C \subset \mathbb{P}^3$ intersect. Therefore they all pass through some point $A \in \mathbb{P}^3$. In other words, the projection from A is inseparable. (This is Samuel's *strange* curve. See below and the Appendix.)

Proof This is elementary projective geometry: three or more lines in $\mathbb{P}^3$ with any two meeting are either all coplanar or all concurrent. The tangent lines contain all points of C, so they are not all coplanar.

Samuel (and Hartshorne following him) define an irreducible projective curve Γ all of whose tangent lines at nonsingular points are concurrent at A to be *strange*.

In characteristic 0, no curves are strange (with the arguable exception of the straight line). Because the projection from A would give a rational map $\Gamma \dashrightarrow \mathbb{P}^{n-1}$ with differential everywhere zero. Then the map would have to be constant to a single point.

In characteristic p, the condition just means that the projection from A is inseparable. There are any number of such curves, but Samuel's argument proves that they are all singular, with the exception of the plane conic in characteristic 2.

For the proof and discussion, in this edition of the notes, I attach a typeset version of Samuel's appendix.

Remark 10.2 I have a number of current obsessions in this subject.

(I) Modern algebraic geometers have extraordinary difficulties in relating to language of the past – the 19th century, the Italian era, the Zariski and Weil period around WW2, the Serre and Grothendieck period. The literature of the 1960s is especially problematic: the people involved are brilliant researchers tackling hard problems. When they get a result they publish it, without the need to tidy up their arguments for others to understand.

(II) I have the distinct memory that Mumford told me around 1980 that the linearly general position statement for a singular irreducible curve is of course false in general, because there are curves for which every hyperplane section is a configuration of points with an action of $\mathbb{F}_p^+$. I'm not there yet, but I hope to understand his hint eventually. (Or maybe I just misunderstood it.)

(III) Samuel's notion of strange curve may be related to group schemes of order p or p^2. The projection from A is an inseparable morphism $C \to \Gamma$, and the functions on C are generated by a single new coordinate function x_1/x_0.

This presumably means that it factors via geometric Frobenius $C \to C^{(1)}$ (up to isomorphism: a priori we don't know what projective space $C^{(1)}$ is embedded in). This inseparable may be a μ_p or α_p torsor (or both). Then possibly the singularities of C relates to the zeros of p-closed vector fields. The correct treatment must navigate the counterexamples

$C =$ straight line and $C =$ plane conic in characteristic 2.

(IV) Big challenge: to find grown-up counterexamples to linearly general position for irreducible curve, or to prove they don't exist.

Appendix by Pierre Samuel
Lectures on old and new results on algebraic curves
Bombay, Tata Institute, 1966

Appendix to Chap. II, p. 76–78
Nonsingular strange curves

For proving the existence of a plane model of a function field with only nodes (Chap. II, Section 1), we had to avoid the *strange* curves of characteristic p, that is, the curves C in projective space all of whose tangents have a common point. A posteori (that is, using facts about divisors of differentials), one can prove that we were fighting against a phantom. More precisely:

Theorem 10.3 *The only nonsingular projective strange curves are lines, and in characteristic* 2*, also the plane conics.*

That a plane conic

$$ayz + bzx + cxy + dx^2 + ey^2 + fz^2 = 0$$

is strange in characteristic 2 is well known and easily proved. The equation of the tangent at (x, y, z) is

$$XF'_x + YF'_y + ZF'_z = X(bz + cy) + Y(cx + az) + Z(ay + bx) = 0,$$

and is satisfied by the point (a, b, c) (here $(a, b, c) \neq (0, 0, 0)$ because otherwise our conic is a double line).

Conversely, let $C \subset \mathbb{P}^n$ be a nonsingular strange curve, defined over an algebraically closed field k of characteristic $p > 0$. By a suitable choice of coordinates, we may assume that the point A common to all tangents to C has homogeneous coordinates $(1, 0, \dots, 0)$, and that C has no points at which two coordinates vanish (except perhaps for A).

Let $L = k(C)$ be the function field of C, and

$$(x, x_2, \dots, x_n) \quad \text{with } x \text{ and } x_i \in L.$$

the affine coordinate functions of C outside the hyperplane H (last coordinate $= 0$).[2]

Since all tangents to C pass through A, we have

$$D_{x_2} = \cdots = D_{x_n} = 0 \quad \text{for any } k\text{-derivation } D \text{ of } L.$$

That is,

$$x_2, \dots, x_n \in L^p. \tag{10.5}$$

We are going to compute the divisor $\operatorname{div}(dx)$. At a point $P \in C$ away from $C \cap H$, the curve C is transversal to the hyperplane $x_1 = 0$, whence $x - x(P)$ is a uniformizing parameter at P. Thus

$$v_P(dx) = 0 \quad \text{for } P \in C \setminus (C \cap H). \tag{10.6}$$

By hypothesis, all points of $C \cap H$ lie in the affine piece with coordinates $(1/x, x_2/x, \dots, x_n/x)$. We set $y = 1/x$ and $y_i = x_i/x$, so that $y \in L^p y_i$ for $i = 2, \dots, n$

Suppose first that $P \neq A$. We have $y(P) = 0$, and $y_i(P) \neq 0$ for $i = 2, \dots, n$. Since the maximal ideal of the local ring $\mathcal{O}_P$ (the valuation ring of v_P) is generated by $y, y_2 - y_2(P), \dots, y_n - y_n(P)$, there exists an index i for which $t = y_i - y_i(P)$ is a uniformizing parameter at P.

Since $y \in L^p y_i$ and since $v_P(y) > 0$, the expansion of y as a power series in t is

$$y = (y_i(P) + t)(\alpha_0 t^{pj_P} + \alpha_1 t^{p(j_P+1)} + \cdots) \quad \text{with } \alpha_0 \neq 0 \text{ and } j_P > 0.$$

This contains terms of degree pj_P and $pj_P + 1$ with nonzero coefficients. Therefore $v_P(y) = pj_P$ and $v_P(dy/dt) = pj_P$. Also, since $dx = -dy/y^2$, it follows that

$$v_P(dx) = -pj_P \quad \text{with } j_P > 0. \tag{10.7}$$

Finally, if $A \in C$, we have $y(A) = y_2(A) = \cdots = y_n = 0$. As above, one of the y_i is a uniformizing parameter at A, say $t = y_i$. From $y \in L^p y_i$ and $v_A(y) > 0$, we get the power series expansion

$$y = t(\alpha_0 t^{pj_A} + \alpha_1 t^{p(j_A+1)} + \cdots) \quad \text{with } \alpha_0 \neq 0 \text{ and } j_A \geq 0.$$

[2] I interpret this to mean that $\mathbb{P}^n$ has homogeneous coordinates $u_1, \dots, u_n, v$ with $v = 0$ the hyperplane at infinity, $x = x_1 = u_1/v$ and $x_i = u_i/v$. The point A is on the hyperplane at infinity. The choice of coordinates gives that $u_1 \neq 0$ at all such points.

Hence $v_A(y) = pj_A + 1$, and $v_A(dy/dt) = pj_A$. Since $dx = -dy/y^2$, we get

$$v_A(dx) = -pj_A - 2 \quad \text{with } j_A \geq 0. \tag{10.8}$$

From (10.6), (10.7) and (10.8), and from the fact that $C \cap H \neq \emptyset$, we see that the degree of $\operatorname{div}(dx)$ is < 0.

Since it is $2g - 2$ (where g denotes the genus of C), it is necessarily -2, and $g = 0$. Looking at (10.7) and (10.8), we see that only two cases may happen

(a) $C \cap H$ consists of only one point $P \neq A$. Then

$$v_P(dx) = -2, \quad p = 2, \quad j = 1, \quad \text{and } v_P(y) = 2.$$

This last relation shows that $C \cdot H = 2P$, whence C has degree 2. We get a conic in characteristic 2.

(b) $C \cap H$ contains only the point A. Then

$$v_A(dx) = -2, \quad j_A = 0, \quad \text{and } v_A(y) = 1,$$

so that $C \cdot H = A$; thus C has degree 1 and is a straight line. QED

Remark There exist, of course, many singular strange curves in charactistic p: take a function field L of transcendence degree 1 over k, functions $z_2, \dots, z_n \in L$ which generate L^p over k, and choose $z \in L \setminus L^p$. Then $L = k(z, z_2, \dots, z_n)$. The affine curve D with coordinate functions $(z, z_2, \dots, z_n)$ is a model of L. Take its projective closure $\overline{D}$. It is easily seen that all tangents to $\overline{D}$ at nonsingular points pass through the point $(1, 0, \dots, 0)$.

Bibliographic information

The book Pierre Samuel, *Lectures on old and new results on algebraic curves*, Bombay, Tata Institute, 1966 is in Univ. of Warwick library QA.565.S2 (reserve in Leamington) and in the Math Inst. Library, same QA.565.S2

The material is reworked in [Hartshorne, IV.3, pp. 310–316].

See also [Arbarello, Cornalba, Griffiths and Harris, III.1, pp. 109–113].

The main aim in all of these references is to prove that any curve projects birationally to a plane curve of degree d with δ nodes as the only singularity, so that they can use their favourite characterisation or definition of the genus as $\binom{d-1}{2} - \delta$ and of $\mathcal{L}(K_C)$ as adjoints of degree $d-3$ (forms of degree $d-3$ vanishing at the nodes). My treatment of K_C is quite different.

[ACGH] has an alternative and quite different idea: use Harris' Galois-monodromy argument to prove that the generic hyperplane section of C cannot have both linearly dependent and independent subsets of points. I have not yet understood whether this works in characteristic p.

Most seriously, I still have no idea whether there are any irreducible curves (necessarily in characteristic p, "strange" and singular) whose general hyperplane section is not in linearly general position.