MA4L7 Algebraic curves

Miles Reid

Part 1. Definition and nonsingular projective model

Nonsingular projective curves relate closely to field extension $k \subset K$ where K is finitely generated as a field extension, and $\operatorname{tr}\deg = 1$. When we have all the fairly straightforward definitions and properties lined up, we show in Theorem 2.1 that they are in bijection up to the appropriate notions of isomorphism.

Over $k = \mathbb{C}$, a nonsingular projective curve is also the same thing as a compact Riemann surface; however, the proof that a compact Riemann surface is algebraic depends on results from analysis that are beyond the scope of this course.

From a technical point of view, my treatment depends on the relation between algebraic varieties and commutative rings – many different rings are associated with an algebraic variety X. These include

1. The affine coordinate ring $k[X]$ of an affine variety $X \subset \mathbb{A}^n$.
2. The function field of X, the field of fraction $k(X) = \operatorname{Frac}(k[X])$, which is a finitely generated field extension $k \subset k(X)$ with $\operatorname{tr}\deg = \dim X$.
3. The local ring $\mathcal{O}_{X,P}$ at a point $P \in X$, that is, the subring of $k(X)$ consisting of functions that are regular at P.
4. The homogeneous coordinate ring of projective variety $X \subset \mathbb{P}^n$ (which depends on the embedding in $\mathbb{P}^n$).
5. The integral closure of any of the above.

After a colloquial style introductory discussion of the material to lay out the prerequisites in algebraic geometry, the next aim is to give the definitions and properties of these objects, to recall some results from Galois theory and commutative algebra, and to point to a small number of future results that will be important in my subsequent treatment.

1 Basics and the NSS

Let k be a field. Throughout the course, either we assume that k is algebraically closed, or we accept $\overline{k}$-valued points as points of our varieties. In other words "for all $P \in X$" means "for all $P \in X(\overline{k})$)". The general advice is to take $k = \overline{k}$ or even $k = \mathbb{C}$ for a simple life; if you actually need more general k, you can eventually figure out how to modify the arguments over $\overline{k}$. I work with the polynomial ring $k[x_{1...n}]$ not as a construction of abstract algebra, but as a set of functions on $\mathbb{A}^n$. That is, $f \in k[x_{1...n}]$ is the function $\mathbb{A}^n \to k$ defined by $P = (a_{1...n}) \mapsto f(P) = f(a_{1...n})$.

Then an affine variety $X \subset \mathbb{A}^n$ has an associated ideal $I_X \subset k[x_{1...n}]$ consisting of functions $f \in k[x_{1...n}]$ such that $f(P) = 0$ for all $P \in X$. When X is irreducible I_X is prime. This sets up a bijection

$$\{\text{irreducible subvariety } X \subset \mathbb{A}^n\} \longleftrightarrow \{\text{prime ideal } I_X \subset k[x_{1...n}]\}. \quad (1.1)$$

The theory is mostly just definitions and tautological consequences. See [UAG, Chap. 3] or Christian Boehning's notes. Many points in what follows simplify when we assume that X is irreducible and 1-dimensional.

However, the NSS is a nontrivial result. If you haven't seen this, please look it up and remember the statement as a first priority. The main point is that a nontrivial ideal

$$J \subsetneq k[x_{1...n}] \quad (1.2)$$

(here $J \neq k[x_{1...n}]$ is equivalent to saying $1 \notin J$) has zeros forming a *nonempty* variety $V(J) \subset \mathbb{A}^n(\overline{k})$. (I give a joke proof of this in the exercises to this section.) In fact $V(J)$ has *so many zeros* that any polynomial $f \in k[x_{1...n}]$ that is identically zero on $V(J)$ has some power $f^N \in J$. There are lots of minor variants on the proof, for which see the literature.

1.1 Coordinate ring $k[X]$

For $X \subset \mathbb{A}^n$ as above, the coordinate ring $k[X]$ is defined as $k[X] = k[x_{1...n}]/I_X$. This is just the set of polynomial functions on X, or the restriction of polynomial functions $f \in k[x_{1...n}]$ to X. The main result is [UAG, Prop. 4.5], that says that a polynomial map $f\colon X \to Y$ between affine varieties $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ induces a k-algebra homomorphism $\Phi = f^*\colon k[Y] \to k[X]$ and conversely: the map f is given by polynomial functions $f_{1...m} \in k[X]$, so that knowing f is the same as knowing the composite of f with the coordinate functions $y_{1...m} \in k[Y]$. Please read the material around [UAG, Prop. 4.5] if you are confused by any of this.

1.2 Function field $k(X)$, rational maps and morphisms

The *function field* any affine variety is just the field of fractions $k(X) = \mathrm{Frac}(k[X])$ of its coordinate ring (see [UAG, Chap. 3–4]). $f \in k(X)$ can be written $f = \frac{g}{h}$ with $g, h \in k[X]$ and $h \neq 0$, in significantly different ways if $k[X]$ is not a UFD.

The *domain* of f is the open subset $\operatorname{dom} f \subset X$ consisting of points P for which *there exists* an expression $f = \frac{g}{h}$ with $h(P) \neq 0$. The NSS implies that $\operatorname{dom} f = X$ if and only if $f \in k[X]$: that is, everywhere regular rational maps are polynomial maps. This is an important step in passing between birational geometry (geometry up to birational equivalence) to biregular (geometry up to isomorphism).

Also for $g \in k[X]$, if a rational function $f \in k(X)$ is regular at every point $P \in X$ with $g(P) \neq 0$ then $g^N f \in k[x]$. This establishes the principal open set $V_g = \{P \in X \bigm| g(P) \neq 0\}$ as an affine variety with coordinate ring the partial ring of fractions $k[X][\frac{1}{g}]$.

2 The first main aim: nonsingularity

I describe the first group of results, involving normalisation and nonsingular models. This depends on several ingredients from algebra that I treat later. k is an algebraically closed field.

Let C be an irreducible algebraic variety of dimension 1 over k. Its function field $k(C)$ has the properties

1. $k \subset k(C)$ is a finitely generated field extension.
2. $\operatorname{tr}\deg_k k(C) = 1$.

Theorem 2.1 *Conversely, if $k \subset K$ is a field extension satisfying 1 and 2, then there exists a nonsingular projective curve C for which $K \cong k(C)$.*

Moreover this C is unique up to isomorphism: if C_1 and C_2 are two nonsingular projective curves over k, an isomorphism $\varphi\colon k(C_1) \to k(C_2)$ over k of their function fields determines an isomorphism $C_2 \to C_1$.

Summary Along with the basic notions of algebraic geometry, the key ingredients in the proof are the notions of discrete valuation ring (DVR) and normalisation (that is, integral closure) and their properties. These are developed in the next few sections. In slightly more detail, given a point $P \in X$ of an algebraic variety, X is a nonsingular curve near P if and only if the local ring $\mathcal{O}_{X,P}$ is a DVR. (This is practically the definition of nonsingular.) If K satisfies 1 and 2, let $x \in K$ be any element that is transcendental over k (that is, not algebraic). Then by assumptions 1 and 2, K is obtained as the field extension $k \subset k(x) \subset K$, where the first step $k \subset k(x)$ is the function field in one variable, so relates to $\mathbb{P}^1$ with affine coordinate x, and the second step $k(x) \subset K$ is a finite field extension. The nonsingular curve C is obtained from the integral closure of $\mathbb{P}^1$ in K; see below for the detailed development.

2.1 Prerequisites

Noetherian conditions: All rings here are commutative with a 1. A ring is Noetherian if every ideal is finitely generated. In the same way, an A-module M is Noetherian if every submodule $N \subset M$ is finitely generated as A-module. If A is Noetherian and M is a finite A-module then M is Noetherian, so any of its submodule is again finite. If you don't already have this onboard, please see any commutative algebra textbook, for example [UCA, Chap. 2].

2.2 Discrete valuation rings

Recall the definition of local 1-dimensional domain A: the only prime ideals of A are 0 and m, with $0 \subsetneq m \subsetneq A$. A *DVR* is a Noetherian integral domain A satisfying:

$$A \text{ is 1-dimensional local, with principal maximal ideal } m = Az.$$

A generator z of m is called a *local parameter* of A.

It follows that every nonzero element $f \in A$ is of the form $f = z^v \cdot f_0$ where $f_0 \in A^\times$ is a unit, and $v = v_A(f)$ is a nonnegative integer. Indeed, if $f \notin m$ then f is a unit; else $f = z \cdot f_1$ and we continue. If $f = z^n \cdot f_n$ and $f_n = z \cdot f_{n+1}$ then the principal ideal (f_{n+1}) is strictly bigger than (f_n), so this process must terminate by the Noetherian assumption.

In the same way, every nonzero element $f \in K = \operatorname{Frac} A$ has a valuation $v(f) \in \mathbb{Z}$ such that $f \cdot z^{-v}$ is a unit: just apply the above argument to numerator and denominator of f. The valuation $f \mapsto v(f)$ defines a map $v \colon K^\times \to \mathbb{Z}$ (or $v \colon K \to \mathbb{Z} \cup \infty$ with $v(0) = \infty$) that satisfies

1. $v(fg) = v(f) + v(g)$;
2. $v(f + g) \geq \min(v(f), v(g))$.

It is this valuation that defines the zeros and poles of $f \in K$: if $v(f) > 0$ we say *zero of order* v, if $v(f) < 0$ then f has a *pole of order* $-v$, and if $v(f) = 0$ then f is invertible.

I come back to this after discussing integral closure, to give the important criterion: a DVR A is a local 1-dimensional integral domain that is integrally closed.

2.3 Integral extension and finiteness properties

Let $A \subset B$ be integral domains. An element $y \in B$ is *integral* over A if it satisfies a relation

$$y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 \quad \text{with } a_i \in A$$

that is *monic* (leading coefficient 1).

We say an A-module M is a *finite* A-module to mean that it is finitely generated as A-module, that is $M = \sum_{i=1}^{n} A e_i$. (Every element is a *linear combination* of finitely many of them. This is s much stronger condition than finitely generated as A-algebra, where we allow polynomial combinations of the generators.)

If y is integral over A, the subring $A[y] \subset B$ is finite as A-module (generated by $1, y, \dots, y^{n-1}$). Moreover if B is finitely generated as A-algebra, and is integral over A, then it is also finite as A-module.

Proof If $B = A[y_1, \dots, y_n]$, set $B_i = A[y_1, \dots, y_i]$, so that $A = B_0 \subset B_1 \subset \cdots \subset B_n = B$. Then prove as a straightforward exercise that if $A \subset B_1 \subset B_2$ with B_1 finite over A and B_2 finite over B_1 then also B_2 is finite over A. The rest follows by induction.

There is a converse that is not quite trivial.

Proposition 2.2 *If $A \subset B$ is finite as A-module then it is integral.*

The proof takes a finite generating set e_i of B and considers, for any $y \in B$, the multiplication map $b \mapsto yb \in B$. Then ye_i is a particular element of B, so can be written $ye_i = \sum a_{ij} e_j$. Rewrite this as

$$\sum (y\delta_{ij} - a_{ij}) e_j = 0 \quad \text{for all } j,$$

and consider the matrix $Y = (y\delta_{ij} - a_{ij})_{ij}$.

I claim that $(\det Y) e_i = 0$ all i. Then $\det Y = 0$, because $1 \in A \subset B$ is a linear combination of the e_i. To prove the claim, just multiply our set of relations $\sum(y\delta_{ij} - a_{ij})e_j = 0$ on the left by the adjoint matrix $Y^\dagger$ of Y (the matrix of cofactors, with $Y^\dagger Y = (\det Y)I_n$).

The following addendum is proved by the same method (the *determinant trick*). For an A-module M, say that A acts *faithfully* if multiplication by any nonzero a is injective on M.

Proposition 2.3 *Let M be a finite A-module on which A acts faithfully and $\varphi\colon M \to M$ a homomorphism. Then φ satisfies a monic equation over A.*

This says that if we view M as a module over the (commutative) ring $A[z]$, with z acting by φ, then z is integral over A.

Lemma 2.4 (Nakayama's lemma) *Let M be a finite A-module over a local ring A, m. Then $mM = M$ implies that $M = 0$.*

Proof Suppose $e_1, \dots, e_n$ is some minimal basis of M. If $n = 0$ then we are done. Otherwise, consider $e_n \in M = mM$. Then $e_n = \sum_{j=1}^{n} a_{nj}e_j$ with $a_{ij} \in m$. Take the component in e_n to the left, to get $(1 - a_{nn})e_n = \sum_{j=1}^{n-1} a_{nj}e_j$. However, $(1-a_{nn}) \notin m$, so is invertible, and e_n is a combination of $e_1, \dots, e_{n-1}$. This is a contradiction.

2.4 Characterisation of DVR by normality

A domain A is *normal* if it is integrally closed in its field of fractions $K = \mathrm{Frac}(A)$.

Theorem 2.5 *Let A, m be a Noetherian integral domain that is local and 1-dimensional (that is, $0 \subset m \subset A$ are the only prime ideals).*

Then A is a DVR if and only if A is normal.

Proof A DVR is a UFD, and it is an exercise to see that a UFD is normal.

To prove the converse, first $m \neq m^2$ by Nakayama's lemma, so choose $x \in m \setminus m^2$. I claim that $m = (x)$.

By contradiction, assume that $M = m/(x) \neq 0$.

For nonzero $z \in M$, write $\mathrm{Ann}(z)$ for the *annihilator* of z, the set of $f \in A$ such that $fz = 0$ in M. This is an ideal, and clearly $x \in \mathrm{Ann}(z)$. Consider all the ideals of A of the form $\mathrm{Ann}(z)$ for $0 \neq z \in M$. There must be an $\mathrm{Ann}(z)$ that is maximal among this set; this $\mathrm{Ann}(z)$ is then prime: in fact for $f, g \notin \mathrm{Ann}(z)$, we know $fz \neq 0$, and certainly $\mathrm{Ann}(z) \subset \mathrm{Ann}(fz)$, so maximality gives $\operatorname{Ann}(z) = \operatorname{Ann}(fz)$, therefore (because $g \notin \operatorname{Ann}(z)$), also $fgz \neq 0$, and the product $fg \notin \operatorname{Ann}(z)$.

Now $\operatorname{Ann}(z)$ is a prime ideal of A, and contains x, so $\operatorname{Ann}(z) = m$.

Choose a lift $y \in A$ so that $y \bmod (x)$ is $z \in M$. Then $y \notin (x)$ (because $z \neq 0$), but $my \subset (x)$ (because $mz = 0$).

Consider $y/x \in K = \operatorname{Frac} A$. Then $\frac{y}{x}m \subset A$. There are two cases:

1. Either $\frac{y}{x}m$ contains a unit of A. Then $x \in ym$, so $x \in m^2$, contradicting the choice of x.

2. Or $\frac{y}{x}m \subset m$. Now multiplication by $\frac{y}{x}$ is an endomorphism $\varphi\colon m \to m$ of the finite faithful A-module m, so that the determinant trick (Proposition 2.3) says that $\frac{y}{x}$ is integral over A, so in A by the normal assumption. This contradicts $y \notin (x)$, so $M = 0$ and $m = (x)$ as required. $\square$

3 Integral closure is finite

Theorem 3.1 *Write $k[X]$ for the coordinate ring of an irreducible affine variety X, and let $k(X) \subset L$ be a finite separable field extension. Then the integral closure of $k[X]$ in L is finite as a $k[X]$-module.*

This holds for any finite extension $k(X) \subset L$, but separable is the essential case. I treat the inseparable case as addendum Theorem 3.4.

Many results in commutative algebra work for general Noetherian rings. This is not the case for finiteness of integral closure, much as one might regret it, and the proof of the theorem involves a couple of sidesteps. The treatment here is mostly taken from [UCA, 8.12–8.13].

Proposition 3.2 (Noether normalisation) *Let $k[X]$ be the coordinate ring of an irreducible affine variety X. Then there exist algebraically independent elements $y_1, \dots, y_m \in k[X]$ (so that $k[y_1, \dots, y_m] \subset k[X]$ is just the polynomial ring), $k[X]$ is a finite module over $k[y_1, \dots, y_m]$, and the field extension $k(y_1, \dots, y_m) \subset k(X)$ is separable.*

For the proof, see [UAG, Theorem 3.13 and Addendum 3.16].

Write $A = k[y_1, \dots, y_m] \subset K = k(y_1, \dots, y_m)$ and let $K \subset L$ be a finite separable extension. An element $a \in L$ is the root of a uniquely defined minimal polynomial

$$f_a(T) = T^d + c_{d-1}T^{d-1} + \cdots + c_1T + c_0 \in K[t].$$

That is, $f_a(T)$ is irreducible and $f_a(a) = 0$, so that $K[a] \cong K[T]/(f_a)$.

The *trace* of a is defined as $-c_{d-1} \cdot [L : K(a)]$.

Proposition 3.3 $\mathrm{Tr}_{L/K} \colon L \to K$ *is a* K*-linear map. If* $a \in L$ *is integral over* A *then* $\mathrm{Tr}(a) \in A$*. Assume (as here) that* $K \subset L$ *is separable. Then* $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ *is a nondegenerate bilinear pairing on* L *over* K*.*

See [UCA, 8.13] and Example sheet 2 for details.

Proof of the theorem Write $A = k[y_1, \dots, y_m] \subset K$, and B for the integral closure of A in L.

An element $u \in L$ has a minimal polynomial over K. Multiplying u through by a suitable common denominator in A of its coefficients, I can arrange that u is integral over A. It follows that I can choose a K-basis $u_1, \dots, u_n$ of L made of elements u_i that are integral over A. Let $B_0 = \sum_{i=1}^n Au_i \subset B$.

In the K-vector space L let $v_1, \dots, v_n$ be the dual basis to $u_1, \dots, u_n$ with respect to the nondegenerate bilinear form $\mathrm{Tr}_{L/K}$. Then

$$B_0 = \sum_{i=1}^n Au_i \subset B \quad \text{implies that} \quad B \subset B_0^\vee = \sum_{i=1}^n Av_i.$$

In fact for $y \in B$ write $y = \sum_j a_j v_j$ with $a_j \in K$. Then $yu_i \in B$ for each i, so $\mathrm{Tr}(yu_i) \in A$, but (since $\{u_i\}$ and $\{v_j\}$ are dual bases), I can calculate the coefficients a_i from

$$\mathrm{Tr}(yu_i) = \mathrm{Tr}\Bigl(\sum_j a_j u_i v_j\Bigr) = \sum_j a_j \mathrm{Tr}(u_i v_j) = a_i$$

and therefore $a_i \in A$.

Thus B is an A-submodule of a finitely generated module, and over the Noetherian ring A this implies that B is a finite A-module.

3.1 Same result also holds for inseparable extension

Theorem 3.4 *For* k *algebraically closed, consider* $k \subset k[x] \subset k(x) = K$*, and let* $K \subset L$ *be a finite field extension (possibly inseparable).*

Set A_x *to be the integral closure of* $k[x]$ *in* L*. Then* A_x *is finite as* $k[x]$*-module.*

Step 1 Reduce to L/K normal in the sense of Galois theory. (That is, if an irreducible $f \in K[t]$ has a root, then it splits completely into linear factors.)

This is not hard: as usual in Galois theory, pass to a normal closure L' of L, which is still finite over K. Then $A_x \subset L$ is a submodule of the integral closure $A'_x \subset L'$, so that the result for L' implies the result for $L \subset L'$ by the usual Noetherian stuff.

Step 2. Proposition A normal field extension L/K is the composite of a separable and a purely inseparable extension that are linearly disjoint.

This is known, for example [Kaplansky]. It means that there is a tower of field extensions

$$\begin{array}{ccc} & L & \\ K^{\text{insep}} & & K^{\text{sep}} \\ & K & \end{array} \tag{3.1}$$

with both northwest inclusions inseparable of the same degree, and both northeast inclusions Galois with the same G. Here K^{sep} is the maximal separable extension, that is, the subfield of all $y \in L$ that are separable over K. This is normal and separable, so Galois with group $G = \operatorname{Gal}(K^{\text{sep}}/K)$, and L is purely inseparable over K^{sep} so that $\operatorname{Aut}(L/K^{\text{sep}}) = \{\text{Id}\}$, because the minimal polynomial of any $y \in L$, has only one root y with multiplicity.

On the other hand the group $\operatorname{Aut}(L/K)$ of K-automorphisms of L equals G. In fact it must take K^{sep} to itself, and an automorphism that is the identity on K^{sep} is the identity in $\operatorname{Aut}(L/K)$.

Step 3 It is enough to prove the theorem first for the purely inseparable part then the separable part.

This just follows from definition of integral closure and the tower law $A \subset B_1 \subset B_2$ for finite algebras.

Step 4 If k is algebraically closed of characteristic p, the only purely inseparable extensions of $k(x)$ are of the form $k(x) \subset k(x^{1/q})$ for some $q = p^n$. Moreover, the integral closure of $k[x]$ in $k(x^{1/q})$ is simply $k[x^{1/q}]$.

Consider first the case $q = p$. An inseparable extension $K \subset K_1$ of degree p is necessarily primitive with minimal polynomial $T^p - a$. Now $a \in k[x]$ factorises as $\prod(x - a_i)$ because k is algebraically closed. Moreover

$$(x - a_i)^{1/p} = x^{1/p} + a_i^{1/p} \quad \text{with } a_i^{1/p} \in k.$$

It follows from this that $T^p - a$ has a root in $K(x^{1/p})$, so $K_1 = K(x^{1/p})$.

An element of $K_1 = k(x^{1/p})$ that is integral over $k[x]$ has pth power in $k[x]$, which gives that the integral closure of $k[x]$ in K_1 is $k[x^{1/p}]$.

The result for $q = p^n$ follows by induction.

Step 5 Now the general result follows by applying Theorem 3.1 to the top left inclusion in (3.1).

3.2 Conclusion

If C is an affine curve and $k[C]$ is normal then C is nonsingular: in fact normal is a local property, so $k[C]$ normal if and only if $\mathcal{O}_{C,P}$ is normal, which means each $\mathcal{O}_{C,P}$ is a DVR.

Normalisation provides an automatical way of resolving the singularities of an irreducible affine curve Γ. Just take the integral closure $\widetilde{k[\Gamma]}$ of its coordinate ring $k[\Gamma]$, then replace Γ by the curve $C = \widetilde{\Gamma} = \operatorname{Spec} \widetilde{k[\Gamma]}$, with the finite morphism $\nu\colon C \to \Gamma$ given by the inclusion $k[\Gamma] \subset k[C] = \widetilde{k[\Gamma]}$.

3.3 Resolution as a projective curve

I want to do something similar to construct the normalisation of a projective curve Γ, and hence its resolution of singularities $C \to \Gamma$. For this, start from the function field $L = k(\Gamma)$, and choose a transcendental generator x. I could take x to be a *separable* transcendental generator for an easy life, but this is not essential by Theorem 3.4.

Then construct an affine curve C_x with coordinate ring the integral closure $A_x = k[C_x]$ of $k[x]$ in L. I view C_x as a finite cover of $\mathbb{A}^1_x$. Now take $y = x^{-1}$ and construct in the same way an affine curve C_y whose coordinate ring $A_y = k[C_y]$ is the integral closure of $k[y]$ in L.

The two curves both have the same function field $L = \operatorname{Frac}(A_x) = \operatorname{Frac}(A_y)$, so are birational. In fact, much more than that: we can equally well take the integral closure A_0 of $k[x, x^{-1}]$ in L; then $A_0 = A_x[x^{-1}] = A_y[y^{-1}]$. This means that the two nonsingular affine curves $C_x = \operatorname{Spec} A_x$ and $C_y = \operatorname{Spec} A_y$ have $C_0 = \operatorname{Spec} A_0$ as a common open set, with isomorphisms

$$C_x \setminus (x = 0) \cong C_0 \cong C_y \setminus (y = 0).$$

In particular, for any $f \in A_x$, we have $y^N f \in A_y$ for some power y^N, and vice versa.

In the rest of this section I show how to glue these two nonsingular affine curves into a nonsingular projective curve C. At a more basic level, the construction should be viewed as glueing the finite $k[x]$-algebra A_x and the $k[y]$ algebra A_y into an algebra over $\mathbb{P}^1$.

Take generators

$$\{1, x, u_{2\dots n}\} \quad \text{of } A_x \text{ as } k[x]\text{-module}, \tag{3.2}$$

starting with the redundant choice $u_0 = 1$, $u_1 = x$ (see below). The multiplication in A_x gives relations

$$u_i u_j = \sum c_{ijk} u_k \quad \text{with } c_{ijk} \in k[x]. \tag{3.3}$$

In the same way, take generators

$$\{y, 1, v_{2\dots m}\} \quad \text{of } A_y \text{ as } k[y]\text{-module}, \tag{3.4}$$

with multiplication

$$v_i v_j = \sum d_{ijk} u_k \quad \text{with } d_{ijk} \in k[y]. \tag{3.5}$$

I choose N large enough so that all the $x^N v_i \in A_x$ and $x^N d_{ijk} \in k[x]$, and similarly $y^N u_i \in A_y$ and $y^N c_{ijk} \in k[y]$ (at present it would not do any harm to choose a larger N).

I intend to embed the curve $C_x \cup C_y$ into a projective space as a closed subvariety, and have chosen generators so that I own $x^N, x^{N-1}, x, 1$ and $1, y, y^{N-1}, y^N$, that will distinguish points of C_x and C_y over different points of the base $\mathbb{P}^1$.

Now take $p_{0\dots n}, q_{0\dots m}$ as homogeneous coordinates on $\mathbb{P}^{n+m+1}$, and consider the two maps

$$i_x\colon C_x \hookrightarrow \mathbb{P}^{n+m+1} \quad \text{by} \quad (1 : x : u_{2\dots n} : x^{N-1} : x^N : x^N u_{2\dots m})$$

and

$$i_y\colon C_y \hookrightarrow \mathbb{P}^{n+m+1} \quad \text{by} \quad (y^N : y^{N-1} : y^N u_{2\dots n} : y : 1 : u_{2\dots m}).$$

Each is an embedding: in fact x and $u_{2\dots n}$ generate the affine coordinate ring of C_x, so that i_x is a polynomial map of C_x into the standard affine piece $p_0 \neq 0$ of $\mathbb{P}^{n+m+1}$, the graph of the function $x^{N-1}, x^N, x^N u_{2\dots m}$.

Moreover, in view of $xy = 1 \in L$, the two maps coincide on the overlap $C_0 = C_x \setminus (x = 0) = C_y \setminus (y = 0)$.

Using (3.3) and (3.5), one sees[1] that one can write down homogeneous equations that determine the union of the two images as a projective curve $C \subset \mathbb{P}^{n+m+1}$ having two affine pieces isomorphic to C_x and C_y.

Example 3.5 (Hyperelliptic curve $C : z^2 = f(x)$) I assume here that k has characteristic $\neq 2$, so that $\frac{1}{2} \in k$. A hyperelliptic curve is (the nonsingular model of) an affine curve $C_x \subset \mathbb{A}^2_{\langle x,z\rangle}$ given by $z^2 = f(x)$, where

$$f(x) = a_{2g+2}x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_1x + a_0$$

is a polynomial of degree $2g+2$ or $2g+1$ in x without repeated roots. The coefficient a_{2g+2} may be zero, that I interpret as f having a simple root at $x = \infty$.

For clarity, consider $z^2 = f(x) = x^5+1$, which is a nonsingular curve (put in more general coefficients as desired). To make C_x into a projective curve, one might consider its closure in the usual $\mathbb{P}^2_{\langle x,z,w\rangle}$ given by $z^2w^3 = x^5 + w^5$. However, the drawback is the unpleasant singularity $x^5 = w^3 - w^5$ "at infinity" at the point $(0, 1, 0)$.

Instead of this, write $y = x^{-1} \in k(C_x)$ and consider the integral closure of $k[y]$ in $k(C_x)$. One checks that this is the curve $C_y \subset \mathbb{A}^2_{\langle y,t\rangle}$ given by $t^2 = y + y^6$. The birational map $C_x \dashrightarrow C_y$ takes (x, z) to $y = x^{-1}$, $t = \frac{z}{x^3}$. It is instructive to note that the projective closure of C_y in $\mathbb{P}^2_{\langle y,t,u\rangle}$ is $t^2u^4 = u^5y + y^6$, with the singularity $y^6 = u^4(1 - uy)$ at $(0, 1, 0)$ that looks like two cusps $y^2 = \pm y^3$ head-to-head.

The projective embedding of $C_x \cup C_y$ that I used above boils down in this case to

$$i_x \colon C_x \hookrightarrow \mathbb{P}^5 \quad \text{by} \quad (1 : x : z : x^2 : x^3 : z)$$

and

$$i_y \colon C_y \hookrightarrow \mathbb{P}^5 \quad \text{by} \quad (y^3 : y^2 : t : y : 1 : t).$$

The two expressions differ only by multiplication by y^3. If I write the coordinates of $\mathbb{P}^5$ as $p_0, p_1, p_2, q_0, q_1, q_2$, the equations of the image are

$$\bigwedge^2 \begin{pmatrix} p_0 & p_1 & q_0 \\ p_1 & q_0 & q_1 \end{pmatrix} = 0, \quad p_2 = q_2, \quad p_2^2 = p_0^2 + q_0q_1.$$

The variables p_0, p_1, q_0, q_1 correspond to the twisted cubic $\Gamma_3 \subset \mathbb{P}^3_{\langle p_0,p_1,q_0,q_1\rangle}$ parametrised by $(1, x, x^2, x^3)$, and $p_2 = q_2$ is a new variable in $\mathbb{P}^4$ giving the cone over Γ_3. The first block of equations are the 3 quadrics defining Γ_3, and the final equation renders the right-hand side of $z^2 = 1 + x^5$ or $t^2 = y + y^6$ as quadratic functions in the coordinates p_0, p_1, q_0, q_1 of Γ_3.

[1] I omit some details in the current draft.

4 The nonsingular projective model is unique

Proposition 4.1 (Resolution of indeterminacies) *A rational map*

$$\varphi\colon C \dashrightarrow \mathbb{P}^n$$

from a nonsingular curve C to $\mathbb{P}^n$ (or to any projective subvariety $X \subset \mathbb{P}^n$) extends to a morphism.

Proof A rational map φ is given by $f_0 : \cdots : f_n$ with rational functions $f_i \in k(C)$. At the same time, $gf_0 : \cdots : gf_n$ defines the same rational map for any $g \in k(C)$. The point is now to use the fact that the local ring $\mathcal{O}_{C,P}$ of any $P \in C$ is a DVR. Let t_P be a local parameter. By multiplying the f_i by a common power of t_P, I can assume that all f_i are regular at P; if they all vanish at P, I can take out a common factor while leaving them regular at P. In other words, if $m = \min v_P(f_i)$ then all the $t_P^m f_i$ are regular at P, and at least one of them is a unit. Then $(t_P^m f_0 : \cdots : t_P^m f_n)$ is regular at P, and extends the rational map φ as a morphism at P.

Corollary 4.2 *Let $C_1 \subset \mathbb{P}^n$ and $C_2 \subset \mathbb{P}^n$ be two nonsingular algebraic curves and $\varphi\colon C_1 \dashrightarrow C_2$ be a birational map. The φ is an isomorphism.*

This establishes the one-to-one correspondence of Theorem 2.1 between function fields in one variable over k (up to isomorphism) and nonsingular algebraic curves over k (up to isomorphism).

One of the main ways that I intend to use this result is as follows: if I start from any irreducible curve Γ (possibly singular and nonprojective), the nonsingular model C of its function field has a morphism $f\colon C \to \overline{\Gamma}$ to any projective completion of Γ.

Over any affine piece $\Gamma_0 \subset \Gamma$, the inverse image $C_0 = f^{-1}(\Gamma_0) \subset C$ is affine, with coordinate ring $k[C_0]$ finite as Γ_0-module.

MA4L7 Algebraic curves. First example sheet

Exercise in Nakayama's lemma Let A be a local ring and M a finite A-module (the same assumptions as in Lemma 2.4), suppose that $m_1, \dots, m_n \in M$ generate M mod m (in other words, $M = mM + \sum Am_i$). Then $m_1, \dots, m_n \in M$ generate M.

Integrally closed is a local condition If $A \subset L$ is an integral domain contained in a bigger field L (that is L is an extension field of $K = \mathrm{Frac}(A)$)

The first week's lectures talked around the prerequisites. (Many students who did Christian Boehning's lecture course MA4A5 will find this too easy.)

1. Affine varieties $X \subset \mathbb{A}^n$

Reread UAG, Chap. 2 up to the proof of NSS. Don't worry too much about the Zariski topology, because it is just the cofinite topology if X irreducible and 1-dimensional.

2. Affine coordinate ring

and function field $k(X)$ from UAG, Chap. 3.

The coordinate ring is defined as $k[X] = k[x_{1\dots n}]/I_X$.

Exercise 4.3 *Use the NSS to establish the bijections*

$$\Big\{\textit{maximal ideals of } k[X]\Big\} \longleftrightarrow \Big\{\textit{maximal ideal of } k[x_{1\dots n}] \textit{ containing } I_X\Big\}$$
$$\longleftrightarrow \Big\{m_P = (x_i - a_i \bigm| i \in [1..n]),\ \textit{where } P = (a_{1\dots n}) \in X\Big\}.$$

and

$$\Big\{\textit{prime ideals of } k[X]\Big\} \longleftrightarrow \Big\{\{\textit{prime ideal of } k[x_{1\dots n}] \textit{ containing } I_X\}\Big\}$$
$$\longleftrightarrow \Big\{\ I_Y \textit{ with } Y \subset X \textit{ irreducible subvariety.}\Big\}$$

These have the flavour "the ring $k[X]$ knowns everying about X", and will justify writing $X = \operatorname{Spec} X$ (with a small abuse of terminology concerning the single prime ideal $0 \subset k[X]$).

Exercise 4.4 *X affine irreducible with affine coordinate ring $k[X]$ and function field $k(X)$. Prove that if $f \in k(X)]$ is regular at every $P \in X$, then $f \in k[X]$. That is rational plus everywhere regular implies polynomial.*

Moreover for $0 \neq g \in k[X]$, if $f \in k(X)]$ is regular at every $P \in X$ with $g(P) \neq 0$ then $f \in k[X][\frac{1}{g}]$.

In either case, you need to use NSS. This will be used later as a step in going from birational (geometry up to birational equivalence) to biregular (geometry up to isomorphism).

3. DVR

Recall the definition of DVR from lectures or one of the textbooks.

Exercise 4.5 *Prove that $P \in X$ is a nonsingular point of a curve if and only if the local ring $\mathcal{O}_{X,P}$ is a DVR.*

This is more or less the definition, but you have to get all the words right.

4. Integral closure.

Exercise 4.6 *Show that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. More generally, if A is a UFD, prove that A is integrally closed. (That is, any element of $K = \operatorname{Frac} A$ that satisfies a monic polynomial equation over A is actually in A.)*

Deduce that a DVR is integrally closed.

I will prove later that a 1-dimensional Noetherian local ring A that is integrally closed in its field of fractions $K = \operatorname{Frac} A$ is a DVR.

Exercise 4.7 *Prove the following lemma: consider $A \subset A[x]/f$ where A is a ring and $f \in A[x]$ a monic polynomial. Then*

$$A \text{ is a field} \iff A[x]/f \text{ is a field.}$$

5. Rational functions on $\mathbb{P}^1$ and the "baby case"' of RR.

Let u, v be homogeneous coordinates on $\mathbb{P}^1$, and write $x = v/u$ for the affine coordinate on $\mathbb{A}^1 \subset \mathbb{P}^1$, and write $P = (1:0)$ and $Q = (0:1) \in \mathbb{P}^1$. The vector space $k[x]_{\leq d}$ has dimension $1+d$ (with a basis you can easily guess). If we view it as the space of rational fuctions with pole $\leq dQ$, it is the ideal first case of RR space $\mathcal{L}(\mathbb{P}^1, dQ)$. The equality $l(\mathbb{P}^1, dQ) = 1 - g + d$ (with $g = 0$) holds for all $d \geq -1$, and fails by 1 for $d = -2$.

By considering $(x-a)/(x-b)$, show that $k(\mathbb{P}^1)$ contains a function with $\operatorname{div} f = P_1 - P_2$ for any $P_1, P_2 \in \mathbb{P}^1$. More generally, if $\sum m_i P_i$ and $\sum n_j Q_j$ have $\sum m_i = \sum n_j$, then there exists $f \in k(\mathbb{P}^1)$ with $\operatorname{div} f = \sum m_i P_i - \sum n_j Q_j$.

Prove that $l(\mathbb{P}^1, D) = 1 - g + \deg D$ for any $D = \sum m_i P_i$ of degree $d = \sum m_i$.

MA4L7 Algebraic curves. Example sheet 2

Week 2 of lectures were on integral extensions, finite A-modules, normalisation, characterisation of DVR. The material is standard, covered in many commutative algebra textbooks. I mostly follow [UCA, esp. Chap. 8].

Recall that *finite A-module* means finitely generated as A-module: every element can be written as a *linear combination* of finitely many generators $e_1, \dots, e_n$. (As opposed to a finitely generated A-algebra $A \subset B$, when every $b \in B$ is a *polynomial* combination of generators $x_1, \dots, x_n$.)

1. Tower law. Let $A \subset B_1 \subset B_2$ are integral domains. If B_1 is finite as A-module and B_2 is finite as B_1-module prove that B_2 is finite as A-module.

Given the determinant trick [UCA, 2.7], modify the argument to prove the same statement for integral extensions.

2. Standard open sets X_g. If X is an affine algebraic variety with coordinate ring $k[X]$ and $g \in k[X]$, it is known that the open subvariety $X_g = \{P \in X \bigm| g(P) \neq 0\}$ is also affine, and has coordinate ring $k[X_g] = k[X][\frac{1}{g}]$. The X_g, called *standard open sets*, form a basis of the Zariski topology of X.

Prove that $k[X_g]$ is a finite $k[X]$-module if and only if $1/g$ is integral over $k[X]$. If $k[X]$ is already normal (integrally closed in $k(X)$), this happens only if g is a unit of $k[X]$, so that $X_g = X$. Thus the inclusion $X_g \subset X$ is usually not a finite morphism.

3. Finite and nonfinite extension. The nodal cubic $C \subset \mathbb{A}^2$ given by $y^2 = x^2(x+1)$ has the usual parametrisation $f \colon \mathbb{A}^1 \to C \subset \mathbb{A}^2$ given by $x = t^2 - 1$, $y = t(t^2-1)$. Show that f is finite, that is, $k[\mathbb{A}^1]$ is a finite $k[C]$-module. [Hint: $k[C] \cdot 1_{k[t]}$ contains x, y; what more do you need to get $k[\mathbb{A}^1]$? You might start by finding a basis of the vector space $k[t]/k[x,y]$.]

Now replace $\mathbb{A}^1$ by the hyperbola $H : s(t-1) = 1 \subset \mathbb{A}^2_{\langle t,s \rangle}$ and consider the polynomial map $f : H \to C$ given by $x = t^2 - 1$, $y = t(t^2-1)$. Show that f is a bijective map. Show that it is not finite (that is, $k[H]$ is not a finite $k[C]$-module).

4. Similar exercise. The cuspidal cubic $\Gamma : y^2 = x^3$ has parametrisation $x = t^2$, $y = t^3$. Show that it is finite. On the other hand $H = \mathbb{A}^1 \setminus 0$ defined by $st = 1$ is a nonsingular curve, and $x = t^2$, $y = t^3$ maps H isomorphically to $\Gamma \setminus (0,0)$. Show that $H \to \Gamma$ is not finite. (It misses the singular point, so we don't allow it as a resolution of singularities.)

5. Explicit normalisation. Let A be a UFD with field of fractions $K = \operatorname{Frac} A$, and assume $1/2 \in A$. For square-free $a \in A$, consider the quadratic field $K(\alpha)/K$ where $\alpha = \sqrt{a}$. Show that $A[\alpha] \subset K(\alpha)$ is integrally closed. [Hint: find the minimal polynomial of $c + d\alpha$ and show $d \in A$.]

Let A be a UFD with $K = \operatorname{Frac} A$, and assume $1/3 \in A$. Let $a, b \in A$ be square-free coprime elements. Consider the cubic extension field $L = K(\sqrt[3]{a^2b})$ generated by y with minimal polynomial $y^3 = a^2b$. Prove that y and $z = y^2/a$ are integral over A, and show that the ideal of all relations holding between y, z is generated by 3 quadratic relations in y, z. [Hint: $y^3 = a^2b$ is a linear combination of these 3.] Now given that $X = e + cy + dz \in L$ has minimal polynomial $(X - e)^3 - 3abcd(X - e) - ab(ac^3 + bd^3)$, deduce that $A[y, z]$ is the integral closure of A in L.

If $a = (x - 1)(x - 2)$ and $b = x(x + 1)$, determine the normalisation of the affine plane curve $y^3 = ab^2$.

6. Normalisation of monomial curve. Following on from the cuspidal cubic $y^2 = x^3$, determine the normalisation of $k[x, y]/(y^2 - x^5)$. Same question for $k[x, y]/(y^3 - x^7)$. More generally, if a, b are coprime, find the normalisation of $x^a = y^b$. [Hint: If you want to write $x = t^a$ and $y = t^b$ you are on the right track. However, for this to be a normalisation, you still have to establish that $t \in \operatorname{Frac}(A)$ where $A = k[x, y]/(x^a - y^b)$. In other words, express t in terms of x and y.]

7. Trace in a finite field extension. Let $K \subset L$ be a finite field extension. Recall from Galois theory that any $y \in L$ has a *minimal polynomial*, an irreducible polynomial

$$p(T) = T^d + c_{d-1}T^{d-1} + \cdots + c_1T + c_0 \in K[T]$$

such that $p(y) = 0$, so that $K[y] = K[T]/(p(T))$; it follows that $K[y] = K(y)$ is a field, since $(p(T))$ is a maximal ideal. We say that L/K is a *primitive extension* with generator y if $L = K(y)$.

Consider the multiplication map $\mu_y \colon L \to L$ consisting of multiplication by y. If L/K is a primitive extension, write out the matrix of μ_y in the basis $1, y, \ldots, y^{d-1}$, and deduce that its trace is $\operatorname{Tr}_{L/K} \mu_y = -c_{d-1}$.

In general, prove that the trace of μ_y equals $-c_{d-1}[L : K(y)]$. [Hint: let b_j for $j = 1, \ldots, [L : K(y)]$ be any basis of $L/K(y)$, and calculate the trace of μ_y in the basis y^ib_j of L/K.