

Chapter 4 INTEGRAL MORPHISMS

- 4.1 The Nakayama Lemma
- 4.2 Integral Extensions
- 4.3 Finiteness of the Integral Closure
- 4.4 Geometry of Integral Morphisms
- 4.5 Chevalley's Finiteness Theorem
- 4.6 Double Planes

The concept of an algebraic integer was one of the most important ideas contributing to the development of algebraic number theory in the 19th century. Then in the 20th century, through the work of Noether and Zariski, its analog became essential in algebraic geometry. We study this analog here. Some of the things we discuss are:

If $A \subset B$ are domains, an element of B is *integral over* A if it is the root of a *monic* polynomial with coefficients in A , and B is an *integral extension* of A if every element of B is *integral over* A . If A and B are finite-type domains and B is integral over A , then B is a finite A -module. The Noether Normalization Theorem asserts that every finite-type domain is an integral extension of a polynomial ring.

Let K be the fraction field of a finite-type domain A . The *normalization* of A is the set of all elements of K that are integral over A . The normalization is finite A -module.

A morphism $Y \xrightarrow{u} X$ is a *finite morphism* if the inverse image Y' of every affine open set X' of X is an affine open subset of Y that is integral over X' . Thus if $X' = \text{Spec } A$ and $Y' = \text{Spec } B$, B will be a finite A -module. Chevalley's Finiteness Theorem 4.5.2 asserts that if X and Y are projective and the fibres of u are finite sets, then u is a finite morphism.

We study double planes in the last section, and we relate a cubic surface to a double plane whose branch locus is a curve of degree 4. This allows us to determine the number of lines on a generic cubic surface in \mathbb{P}^3 .

nakayama

Section 4.1 The Nakayama Lemma

(Tadasi Nakayama (1912-1964))

It won't be surprising that eigenvectors are important, but the way that they are used to study rings and modules may be new to you.

Let P be an $n \times n$ matrix with entries in a ring A . As usual, the characteristic polynomial of P is $p(t) = \det(tI - P)$. The concept of an eigenvector for P makes sense when the entries of a vector are in an A -module. A vector $v = (v_1, \dots, v_n)^t$ with entries in a module is an *eigenvector* of P with *eigenvalue* λ if $Pv = \lambda v$. The requirement that an eigenvector must be nonzero, which is customary in linear algebra, isn't very useful when the entries are in a module, so we drop it.

eigenval

4.1.1. Lemma. *Let p be the characteristic polynomial of an $n \times n$ matrix P . If v is an eigenvector of P with eigenvalue λ , then $p(\lambda)v = 0$.*

The usual proof, in which one multiplies the equation $(\lambda I - P)v = 0$ by the cofactor matrix of $\lambda I - P$, carries over. □

Here is the most important application of this lemma.

nakaya-
malem

4.1.2. Nakayama Lemma. Let M be a finite module over a ring A , and let J be an ideal of A . If $M = JM$, there is an element z in J such that $m = zm$ for all m in M , or such $(1 - z)M = 0$.

Since the inclusion $M \supset JM$ is always true, the hypothesis $M = JM$ can be replaced by $M \subset JM$,

proof. Let $v = (v_1, \dots, v_n)^t$ be a vector with entries in M and whose entries generate M . The equation $M = JM$ tells us that there are elements p_{ij} in J such that $v_i = \sum p_{ij}v_j$. In matrix notation, $v = Pv$. So v is an eigenvector of P with eigenvalue 1, and $p(1)v = 0$. Since the entries of P are in J , inspection of the matrix $I - P$ shows that $p(1)$ has the form $1 - z$, with z in J . Then $(1 - z)v_i = 0$ for all i , and since v_1, \dots, v_n generate, $(1 - z)M = 0$. \square

idealzero

4.1.3. Corollary. Let A be a noetherian domain.

(i) If I and J are ideals of A and if $I = JI$, then either I is the zero ideal or J is the unit ideal.

(ii) Let J be an ideal of A that isn't the unit ideal. The intersection $\bigcap J^n$ of the powers of J is the zero ideal.

(iii) Let x and y be nonzero elements of a noetherian domain. The integers k such that x^k divides y are bounded.

proof. (i) Suppose that $I = JI$. Since A is noetherian, I is a finite A -module. The Nakayama Lemma tells us that there is an element z of J such that $zx = x$ for all x in I . If I isn't zero, we may choose a nonzero element x of I and cancel x from the equation $zx = x$, to obtain $z = 1$. Then 1 is in J , and J is the unit ideal.

(ii) The intersection $I = \bigcap J^n$ is an ideal, and it has the property that $I = JI$. Since J isn't the unit ideal, $I = 0$.

(iii) The intersection of the powers $x^k A$ of the ideal xA is the zero ideal. \square

extnotunit

4.1.4. Corollary. Let $A \subset B$ be finite-type domains such that B is a finite A -module, and let J be an ideal of A . If the extended ideal JB is the unit ideal of B , then J is the unit ideal of A .

proof. Suppose that $JB = B$. Since B is a finite A -module, the Nakayama Lemma applies. There is an element z in J such that $zb = b$ for all b in B . Since B is a domain, $z = 1$. So J is the unit ideal. \square

fracnotfinite

4.1.5. Corollary. Let A be a subring of a field K . If K is a finite A -module, then A is a field.

proof. Suppose that K is a finite A -module. Let x be nonzero element of A , and let J be the principal ideal xA . Since x is invertible in K , $JK = K$. Therefore J is the unit ideal, which shows that x is invertible in A . Every nonzero element of A is a unit, which means that A is a field. \square

Since there are many subrings of fields that aren't fields themselves, we see that, in the Nakayama Lemma, the hypothesis that one is dealing with a finite module cannot be dropped.

int

Section 4.2 Integral Extensions

An *extension* of a domain A is a domain B that contains A . An element β of an extension B is *integral over A* if it is a root of a monic polynomial with coefficients in A , say $f(\beta) = 0$, where

eqn (4.2.1)
$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0,$$

and a_i are in A . An extension of A is an *integral extension* if all of its elements are integral over A .

If $X = \text{Spec } A$ and $Y = \text{Spec } B$ are affine varieties, and if $A \subset B$ is an integral extension, we call the morphism $Y \xrightarrow{u} X$ defined by the inclusion $A \subset B$ an *integral morphism*.

The discussion of Section ??, is helpful for an intuitive understanding of the geometric meaning of integrality, so we review it here.

4.2.2. Example. Let X denote the affine line $\text{Spec } A$, $A = \mathbb{C}[x]$, and let Y be the plane affine curve defined by an irreducible polynomial $f(x, y)$. So $Y = \text{Spec } B$, $B = \mathbb{C}[x, y]/(f)$. The inclusion of A into B gives us a morphism $Y \xrightarrow{u} X$, the restriction of the projection from the plane $\mathbb{A}_{x,y}^2$ to the line X .

We write f as a polynomial in y whose coefficients are polynomials in x :

$$f(x, y) = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \dots + a_0(x).$$

integralovercx

Let x_0 be a point of X , and let $\bar{a}_i = a_i(x_0)$, so that $f(x_0, y) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \cdots + \bar{a}_0$. The fibre of Y over x_0 is the set of points (x_0, y_0) such that y_0 is a root of $f(x_0, y)$. Because f is irreducible, the discriminant of f with respect to the variable y isn't identically zero (??). So for most x_0 , $f(x_0, y)$ will have nonzero discriminant and therefore it will have n distinct roots.

If f is monic, the residue of y in B will be integral over A , and the polynomial $f(x, y)$ will have degree n for every x . The product of the roots, which is a_0 , is bounded near x_0 . Therefore either all roots are bounded near x_0 , or 0 is a root of $f(x_0, y)$. In the second case, we can substitute $y = y + c$ with a generic c . Then $f_1(x, y) = f(x, y + c)$ remains monic, and 0 is not a root of $f_1(x_0, y)$. Therefore the roots of $f_1(x_0, y)$ are bounded. So the roots of $f(x_0, y)$ are bounded in either case. As x approaches a point x_0 at which the discriminant vanishes, some roots come together, but the roots remain bounded.

On the other hand, if the leading coefficient $a_n(x)$ isn't constant and if x_0 is a root of a_n , then $f(x_0, y)$ will have degree less than n . Above x_0 , some roots are missing. What happens is that, as x approaches x_0 , at least one root tends to infinity. (In calculus, one says that the locus $f(x, y) = 0$ has a vertical asymptote at x_0 .) This is seen when one divides f by its leading coefficient. Let $c_i(x) = a_i(x)/a_n(x)$, and let

$$g(x, y) = y^n + c_{n-1}y^{n-1} + \cdots + c_n \quad (= f(x, y)/a_n)$$

The monic polynomial $g(x_0, y)$ has the same roots as $f(x_0, y)$ for all x_0 such that $a_n(x_0) \neq 0$. Suppose that $a_n(x_0) = 0$. Because f is irreducible, at least one coefficient of f , say a_i , doesn't have x_0 as root. Then the coefficient c_i tends to infinity as x approaches x_0 . Since c_i is a symmetric function in the roots, the roots don't remain bounded.

This is the general picture: The roots of a polynomial vary continuously, and they remain bounded when the leading coefficient isn't zero. If the leading coefficient vanishes at a point, some roots are unbounded near that point. □

figure

The next lemma shows that one can always clear the denominator in an algebraic element to obtain one that is integral.

4.2.3. Lemma. *Let A be a domain with fraction field K , let L be a field extension of K . and let β be an element of L that is algebraic over K . Say that β is a root of the polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, with $a_i \in K$. Then $\beta' = a_n \beta$ is integral over A .*

proof. We substitute $\beta = \beta'/a_n$ and multiply by a_n^{n-1} to clear the denominator: β' is a root of $x^n + a_{n-1}x^{n-1} + (a_n a_{n-2})x^{n-2} + \cdots + (a_n^{n-1} a_0)$. □

4.2.4. Lemma. *Let $A \subset B$ be domains.*

(i) *The ring extension $A[b]$ of A generated by an element b of B is a finite A -module if and only if b is integral over A .*

(ii) *The set of elements of B that are integral over A is a subring of B .*

(iii) *If B is generated by finitely many integral elements, it is a finite A -module.*

(iv) *Suppose that B is an integral extension of A . An element of an extension of B that is integral over B is also integral over A .* □

4.2.5. Corollary. *An extension $A \subset B$ of finite-type domains is an integral extension if and only if B is a finite A -module.* □

4.2.6. Example. If G is a finite group of automorphisms of a finite-type domain B , B is an integral extension of the ring of invariants B^G (see Theorem 2.9.2).

The next theorem is named after Max Noether (1844-1921), the father of Emmy Noether. We will make use of it often.

4.2.7. Noether Normalization Theorem. Let A be a finite-type algebra over an infinite field k . There exist elements y_1, \dots, y_n in A that are algebraically independent over k , and such that A is a finite module over the polynomial subalgebra $k[y_1, \dots, y_n]$.

The theorem can be stated by saying that every affine variety X admits an integral morphism $X \rightarrow \mathbb{A}^n$ to an affine space.

4.2.8. Lemma. *Let k be an infinite field, and let $f(x)$ be a nonzero polynomial of degree d in x_1, \dots, x_n , with coefficients in k . After a suitable linear change of variable, the coefficient of x_n^d in f will be nonzero.*

proof. Let f_d be the part of f of degree d . It suffices to choose coordinates x_1, \dots, x_n in \mathbb{P}^{n-1} so that the point $q = (0, \dots, 0, 1)$ isn't a zero of f_d . \square

proof of the Noether Normalization Theorem. Say that A is generated as algebra by the elements x_1, \dots, x_n . We use induction on n . If those elements are algebraically independent over k , A will be a polynomial ring, and we are done. If not, they will satisfy a polynomial relation $f(x) = 0$ of some degree d , with coefficients in k . The lemma tells us that, after a suitable change of variable, the coefficient of x_n^d in f will be nonzero. It can be normalized to 1. Then f will be a monic polynomial in x_n with coefficients in the subalgebra R generated by x_1, \dots, x_{n-1} . So x_n will be integral over R , and therefore A will be a finite R -module. By induction on n , we may assume that R is a finite module over a polynomial subalgebra P . Then A is a finite module over P too. \square

4.2.9. Nullstellensatz (version 4). Let K be a field extension of an infinite field k , and suppose that K is a finite-type k -algebra. Then K is a finite extension of k (a finite-dimensional K -vector space).

proof. The Noether Normalization Theorem tells us that K is a finite module over a polynomial subalgebra $P = k[y_1, \dots, y_d]$, and Corollary 4.1.5 shows that P is a field. This implies that $d = 0$. So K is a finite module over k . \square

Note. Theorems 4.2.7 and 4.2.9 are true when k is a finite field (see xxxx).

Section 4.3 Finiteness of the Integral Closure

Let A be a domain with fraction field K , and let L be a finite field extension of K .

The *integral closure of A in L* is the set of all elements of L that are integral over A . Lemma 4.2.4 (ii) shows that the integral closure is a domain, and it contains A .

The *normalization \bar{A}* of A is the integral closure of A in K – the set of all elements of the fraction field K that are integral over A . A *normal domain* A is a domain that is equal to its normalization. A *normal variety* X is a variety that has an affine covering $\{X_i = \text{Spec } A_i\}$ in which A_i are normal domains.

If \bar{A} is the normalization of a finite-type domain A , and if $X = \text{Spec } A$ and $\bar{X} = \text{Spec } \bar{A}$, we call \bar{X} the *normalization of X* .

The object of this section is to prove the next theorem:

4.3.1. Theorem. *Let A be a finite-type domain with fraction field K of characteristic zero, and let L be a finite field extension of K . The integral closure of A in L is a finite A -module, and therefore a finite-type domain. In particular, the normalization of A is a finite A -module and a finite-type domain.*

The theorem is also true for a finite-type k -algebra when k is a field of characteristic p , though the proof we give here doesn't work.

4.3.2. Example. (*normalization of a nodal cubic curve*) The algebra $R = \mathbb{C}[u, v]/(v^2 - u^3 - u^2)$ embeds into the one-variable polynomial algebra $S = \mathbb{C}[x]$ by $u = x^2 - 1$ and $v = x^3 - x$. Then $x = v/u$, so the fraction fields of the two algebras are equal, and the equation $x^2 - u - 1 = 0$ shows that x is integral over R . Here S is the normalization of R .

The curve $C = \text{Spec } R$ has a node at the origin, $\text{Spec } S$ is the affine line \mathbb{A}_x^1 , and the inclusion $S \subset R$ defines an integral morphism $\mathbb{A}_x^1 \rightarrow C$. The fibre of this morphism over the point $(0, 0)$ of C is the point pair $x = \pm 1$, and the morphism is bijective at all other points. One may regard C as the variety obtained from the affine line by gluing the points $x = \pm 1$ together. \square

##figure##

ufdnormal

4.3.3. Lemma. (i) A unique factorization domain is normal. In particular, a polynomial ring over a field is normal.

(ii) Let R be a normal domain, and let s be a nonzero element of R . The localization R_s is normal.

(iii) If s_1, \dots, s_k are elements of a domain R that generate the unit ideal, and if the localizations R_{s_i} are normal for every i , then R is normal.

proof. (i): Let R be a unique factorization domain, and let α be an element of its fraction field K that is integral over R . Say that

$$\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha + a_n = 0,$$

with a_i in R . We write $\alpha = r/s$, where r and s are relatively prime elements of R . Multiplying by s^n gives us the relation $r^n + a_1r^{n-1}s + \dots + a_ns^n = 0$, or

$$r^n = -s(a_1r^{n-1} + \dots + a_ns^{n-1}).$$

This equation shows that if a prime element p of R divides s , it also divides r . Since r and s are relatively prime, there is no such element. Therefore s is a unit, and α is in A .

We omit the verification of (ii) and (iii). □

abouttracetwo

4.3.4. Lemma. Let A be a normal noetherian domain with fraction field K of characteristic zero, and let β be an element of a field extension L of K that is integral over A . The coefficients of the (monic) irreducible polynomial f for β over K are elements of A .

proof. Since we may replace L by $K(\beta)$, we may assume that L is a finite extension of K . A finite extension embeds into a Galois extension, so we may assume that L is a Galois extension of K . Let G be its Galois group, and let $\{\beta_1, \dots, \beta_r\}$ be the G -orbit of β , with $\beta = \beta_1$. The irreducible polynomial for β over K is

orbitpoly

(4.3.5)
$$f(x) = (x - \beta_1) \cdots (x - \beta_r).$$

Its roots are the elements of the orbit, and its coefficients are symmetric functions in the roots. If β is integral over A , then all elements of the orbit are integral over A , and therefore the symmetric functions are integral over A . The symmetric functions are in K , and since A is normal, they are elements of A . So the coefficients of f are in A . □

Let L/K be a finite field extension, and let β be an element of L . When L is viewed as a vector space over K , multiplication by β becomes a linear operator on L . The trace of this operator will be denoted by $\text{tr}(\beta)$. The trace is a K -linear map, a linear transformation, $L \rightarrow K$.

abouttraceone

4.3.6. Lemma. Let β be an element of a finite field extension L of K , and let

$$f(x) = x^r + a_1x^{r-1} + \dots + a_r$$

be the irreducible polynomial for β over K . Let $n = [L : K]$ and $d = [L : K(\beta)]$, so that $n = dr$. Then $\text{tr}(\beta) = -da_1$. If β is an element of K , then $\text{tr}(\beta) = n\beta$.

proof. With respect to the basis $1, \beta, \dots, \beta^{r-1}$, the matrix of multiplication by β on $K(\beta)$ will have the form illustrated below for $n = 3$. Its trace is $-a_1$.

$$M_\beta = \begin{pmatrix} 0 & 0 & -a_3 \\ 1 & 0 & -a_2 \\ 0 & 1 & -a_1 \end{pmatrix}.$$

Next, let (u_1, \dots, u_d) be a basis for L over the intermediate field $K(\beta)$. Then $\{\beta^i u_j\}$, with $i = 0, \dots, r-1$ and $j = 1, \dots, d$, will be a basis for L over K . When this basis is listed in the order

$$(u_1, u_1\beta, \dots, u_1\beta^{r-1}; \dots; u_d, \dots, u_d\beta^{r-1}),$$

the matrix of multiplication by β will be made up of d blocks of the matrix M_β . □

formnondeg

4.3.7. Lemma. *Let A be a normal noetherian domain with fraction field K of characteristic zero, and let L be a finite field extension of K . The form $L \times L \rightarrow K$ defined by $\langle \alpha, \beta \rangle = \text{tr}(\alpha\beta)$ is K -bilinear, symmetric, and nondegenerate. If α and β are integral over A , then $\langle \alpha, \beta \rangle$ is an element of A .*

proof. The form is obviously symmetric, and it is bilinear because trace is linear. A form is nondegenerate if its nullspace is zero, which means that when α is nonzero, there is an element β such that $\langle \alpha, \beta \rangle \neq 0$. We let $\beta = \alpha^{-1}$. Then $\langle \alpha, \beta \rangle = \text{tr}(1)$, which is the degree $[L : K]$ of the field extension. It is here that the hypothesis on the characteristic of K enters: The degree is a nonzero element of K . Finally, if α and β are integral over A , so is their product $\alpha\beta$ (4.2.4)(ii). Lemmas 4.3.4 and 4.3.6 show that $\langle \alpha, \beta \rangle$ is an element of A . \square

proof of Theorem 4.3.1. Let A be a finite-type domain with fraction field K , and let L be a finite field extension of K . We are to show that the integral closure of A in L is a finite A -module.

Step 1: We may assume that A is normal.

We use the Noether Normalization Theorem to write A as a finite module over a polynomial subring $R = \mathbb{C}[y_1, \dots, y_d]$. Let F be the fraction field of R . Then K and L are finite extensions of F . An element of L will be integral over A if and only if it is integral over R (4.2.4)(iv). So the integral closure of A in L is the same as the integral closure of R in L . We may therefore replace A by the normal algebra R , and K by the field F .

Step 2: Bounding the integral extension.

Let (v_1, \dots, v_n) be a K -basis for L whose elements are integral over the normal domain A (see Lemma 4.2.3). We define a K -linear map

mapvector

$$(4.3.8) \quad T : L \rightarrow K^n$$

by $T(\beta) = (\langle \beta, v_1 \rangle, \dots, \langle \beta, v_n \rangle)$, where $\langle \cdot, \cdot \rangle$ is the form defined in Lemma 4.3.7. If $\langle \beta, v_i \rangle = 0$ for all i , then because (v_1, \dots, v_n) is a basis, $\langle \beta, \gamma \rangle = 0$ for all γ in L , and since the form is nondegenerate, $\beta = 0$. Therefore T is injective.

Let B be the integral closure of A in L . The basis elements v_i are in B , and if β is an element of B , the elements βv_i will be in B too. Therefore $\langle \beta, v_i \rangle$ will be in A , and $T(\beta)$ will be in A^n . When we restrict T to B , we obtain an injective map $B \rightarrow A^n$ that we denote by T_0 . Since T is K -linear, T_0 is A -linear. It maps B isomorphically to its image, an A -submodule of A^n . Since A is noetherian, every submodule of the finite A -module A^n is finitely generated. So the image is a finite A -module, and B is a finite A -module too. \square

prmint

Section 4.4 Geometry of Integral Morphisms

Let

finmorph

$$(4.4.1) \quad Y \xrightarrow{u} X$$

be an integral morphism of affine varieties, say $X = \text{Spec } A$ and $Y = \text{Spec } B$. The main facts about such a morphism are summarized below, in Theorem 4.4.3. That theorem shows that the geometry is as nice as could be expected for a map that, most often, isn't injective.

Corollary 4.1.4 shows that the extension IB of an ideal $I < A$ is not the unit ideal of B . The next lemma tells us something about the contraction of an ideal of B .

contrnotzero

4.4.2. Lemma. *Let $A \subset B$ be an integral extension of finite-type domains. If J is a nonzero ideal of B , its contraction $I = J \cap A$ is a nonzero ideal of A .*

proof. A nonzero element β of J will be integral over A , say $\beta^n + a_{n-1}\beta^{n-1} + \dots + a_0 = 0$, with $a_i \in A$. If $a_0 = 0$, then because B is a domain, we can cancel β from the equation. So we may assume $a_0 \neq 0$. The equation shows that a_0 is in J , and since it is also in A , it is a nonzero element of I . \square

Going back to the integral morphism $Y \xrightarrow{u} X$, we say that a closed subvariety D of Y lies over a closed subvariety C of X if C is the image of D , and we say that a prime ideal Q of B lies over a prime ideal P of A if P is the contraction $Q \cap A$ of Q . For example, if a point y of $Y = \text{Spec } B$ has image x in X , then y lies over x , and maximal ideal \mathfrak{m}_y lies over the maximal ideal \mathfrak{m}_x .

closedimage

4.4.3. Theorem. Let $Y \xrightarrow{u} X$ be an integral morphism of affine varieties.

- (i) u is surjective, and its fibres have bounded cardinality.
- (ii) The image of a closed subset of Y is closed in X .
- (iii) If $D' \subset D$ are closed subvarieties of Y that lie over the same closed subvariety C of X , then $D' = D$.
- (iv) The set of closed subvarieties D of Y that lie over a closed subvariety C of X is finite and nonempty.

proof of Theorem 4.4.3 (i). (bounding the fibres)

Let \mathfrak{m}_x be the maximal ideal at point x of X . Corollary 4.1.4 shows that the extended ideal $\mathfrak{m}_x B$ is not the unit ideal of B , so it is contained in a maximal ideal of B , say \mathfrak{m}_y , where y is a point of Y . Then x is the image of y (??), so u is surjective.

Let $k(x)$ be the residue field of A at x . Then $\overline{B} = B/\mathfrak{m}_x B$ is a $k(x)$ -algebra. Its maximal ideals correspond to the maximal ideals of B that contain $\mathfrak{m}_x B$, the ones that correspond to points y such that $u(y) = x$. Since B is a finite A -module, \overline{B} is a finite-dimensional complex vector space. Proposition 2.2.3 tells us that \overline{B} has finitely many maximal ideals. So there are finitely many points of Y that lie over x . \square

We make a digression before proving the remaining parts of Theorem 4.4.3. Say that $X = \text{Spec } A$ and $Y = \text{Spec } B$, as above, let Q be a prime ideal of B , and let $P = Q \cap A$ be its contraction. Further, let $\overline{B} = B/Q$ and $\overline{A} = A/P$. Because the kernel of the composed map $A \subset B \rightarrow \overline{B}$ is P , we obtain an injective map $\overline{A} \rightarrow \overline{B}$. If (b_1, \dots, b_k) span B as A -module, the residues $(\overline{b}_1, \dots, \overline{b}_k)$ span \overline{B} as \overline{A} -module. So \overline{B} is a finite \overline{A} -module.

Let $D = \text{Spec } \overline{B}$ and $C = \text{Spec } \overline{A}$. So $D \subset Y$ and $C \subset X$. Part (i) of the theorem shows that the map $D \rightarrow C$ is surjective. Therefore D lies over C .

QoverP

4.4.4. Corollary. With notation as above, let $C \subset X$ and $D \subset Y$ be subvarieties defined by prime ideals P and Q of A and B , respectively. Then D lies over C if and only if Q lies over P . \square

This will allow us to replace X and Y by the closed subvarieties C and D in some situations.

proof of Theorem 4.4.3 (ii). (the image of a closed set is closed)

It suffices to show that the image C of a closed subvariety D is closed. We replace Y and X by D and C . Then (i) applies. \square

proof of Theorem 4.4.3 (iii). ($D' \subset D$ lie over C)

We replace Y and X by D and C . Then what we must show is that if D' is a proper closed subset of Y , its image C' is a proper closed subset of X , or, if Q' is a nonzero prime ideal of B , then, then its contraction $P' = Q' \cap A$ is nonzero. This is Lemma 4.4.2.

proof of Theorem 4.4.3. (iv) (subvarieties that lie over a closed subvariety)

The inverse image $Z = u^{-1}C$ of a closed subvariety C is closed in Y . It is the union of finitely many irreducible closed subsets, say $Z = \bigcup D_i$. Let C_i be the image of D_i . Part (ii) tells us that C_i closed in X . Since u is surjective, $C = \bigcup C_i$, and since C is irreducible, it is equal to at least one C_i . The components D_i of Z such that $C_i = C$ are the ones that lie over C .

Next, any subvariety D' that lies over C will be contained in $Z = \bigcup D_i$, and since it is irreducible, it will be contained in D_i for some i . Part (iii) shows that $D' = D_i$. \square

Section 4.5 Chevalley's Finiteness Theorem

finmorph

A morphism of varieties $Y \xrightarrow{u} X$ is a *finite morphism* if the inverse image Y' of every affine open subset $X' = \text{Spec } A$ of X is affine, say $Y' = \text{Spec } B$, and B is a finite A -module. Integral morphisms of affine varieties and inclusions of closed subvarieties into a variety X are examples of finite morphisms.

onecov-
erfinite

4.5.1. Lemma. Let $Y \xrightarrow{u} X$ is a morphism of varieties, let $\{X^i\}$ be an open covering of a variety X , and let $Y_i = f^{-1}X_i$. If the restricted morphism $Y_i \xrightarrow{u_i} X_i$ is a finite morphism for each i , then u is a finite morphism.

proof. When we restrict a finite morphism $Y \rightarrow X$ to an open subvariety X' of X , the resulting map $Y' \rightarrow X'$ will be a finite morphism. Let $Y \xrightarrow{u} X$ be given, and suppose that there is a covering of X by open sets X^i

to which the restrictions of u are finite morphisms. Any open subset of X can be covered by open subsets, each of which is a subset of the sets X^i , so any open subset of X can be covered by open subsets to which the restriction of u is a finite morphism.

Let L denote the function field of Y . We are to show that the restriction of u to any affine open subset of X is a finite morphism. So we may assume that X is affine, say $X = \text{Spec } A$. Let $Y' = \text{Spec } B'$ be a (nonempty) affine open subset of Y . The morphism u restricts to a morphism $Y' \rightarrow X$, which is defined by a ring homomorphism $A \xrightarrow{\varphi} B'$, and the kernel of φ is independent of Y' because it is also the kernel of the composed map $A \rightarrow B' \subset L$. If \bar{A} is the image of A in L , the morphism u will send every affine open set Y' to $\bar{X} = \text{Spec } \bar{A}$. So u has image in \bar{X} . We may therefore replace X by \bar{X} , which reduces us to the case that φ is injective.

Since the simple localizations of X form a basis for the topology, we may cover X by simple localizations to which the restriction of u is finite. Thus there will be nonzero elements s_1, \dots, s_k that generate the unit ideal of A , such that, if $A_i = A_{s_i}$, $X^i = \text{Spec } A_i$, and $u^{-1}(X^i) = Y^i$, then Y^i is affine, say $Y^i = \text{Spec } B_i$, and B_i is a finite A_i -module. Let $B = \bigcap B_j$.

The plan is to show that $Y = \text{Spec } B$. Let $A_{ij} = A_{s_i s_j}$, and $X^{ij} = \text{Spec } A_{ij}$. Then $Y^{ij} = u^{-1}(X^{ij})$ is a localization of Y^i and of Y^j , the spectrum of the ring $B_{ij} = B_i[s_j^{-1}] = B_j[s_i^{-1}]$. The localization $B[s_i^{-1}]$ of B is equal to the intersection of the localizations $B_j[s_i^{-1}]$, all of which contains B_i , and one of which, namely $B_i[s_i^{-1}]$ is equal to B_i . So the intersection of the localizations $B_j[s_i^{-1}]$ is B_i .

We choose a finite set b_1, \dots, b_n of elements of B that generates B_i as A_i -module for every i . We can do this because B_i is a finite A_i -module. Let C be the cokernel of the map $A^n \rightarrow B$ that sends $e_\nu \rightsquigarrow b_\nu$. The localization C_i of C is the cokernel of the map $A_i^n \rightarrow B_i$ (0.7.6), and is zero for every i . Therefore $C = 0$. So B is a finite A -module. According to Proposition 3.5.5, there is a morphism $Y \xrightarrow{u} \text{Spec } B$. Because the localization of u is an isomorphism for every i , u is an isomorphism. \square

chevfin **4.5.2. Chevalley's Finiteness Theorem.** *Let Y be a closed subvariety of a product $\mathbb{P}^n \times X$ of a projective space with a variety X , and let π be the projection from Y to X . If the fibres of π are finite sets, then π is a finite morphism.*

projchevfin **4.5.3. Corollary.** *A morphism $Y \xrightarrow{u} X$ of projective varieties whose fibres are finite sets is a finite morphism.*

This corollary follows from the theorem when one replaces Y by the graph of the morphism u . \square

proof of the Chevalley Finiteness Theorem.

This is Schelter's proof. Descending induction on Y (2.7.4) allows us to assume that for every proper closed subvariety V of Y , the restriction of π to V is a finite morphism. Lemma 4.5.1 shows that we may assume X affine, say $X = \text{Spec } A$.

Let y_0, \dots, y_n be coordinates in \mathbb{P}^n , and let U^i be the standard affine open set $\{y_0 \neq 0\}$. To simplify notation, we replace the symbol $\times X$ by a tilde, writing $\tilde{\mathbb{P}}$ for $\mathbb{P}^n \times X$, and \tilde{U} for $U \times X$, etc.

We first consider a special case, that there exists a hyperplane H in \mathbb{P}^n such that Y is disjoint from $\tilde{H} = H \times X$. We adjust coordinates so that H is the hyperplane H^0 , and we let $Z = \tilde{H}^0$. Then $Y \cap Z = \emptyset$ and Y is contained in \tilde{U}^0 .

Let $u_i = y_i/y_0$ and $v_i = y_i/y_1$ be coordinates in U^0 and U^1 , respectively, with

$$u_0 = 1, \quad v_1 = 1, \quad \text{and} \quad v_0 u_1 = 1$$

So $\tilde{U}^0 = \text{Spec } A[u_0, \dots, u_n]$ and $\tilde{U}^1 = \text{Spec } A[v_0, \dots, v_n]$. Since Y is closed in $\tilde{\mathbb{P}}$, it is closed in \tilde{U}^0 . Therefore it is an affine variety, the zero set of a prime ideal P_0 of $A[u]$, and its coordinate algebra will be $B = A[u]/P_0$.

Next, we look on the standard affine open set U^1 . Let Y^1 and Z^1 denote the closed subvarieties $Y \cap \tilde{U}^1$ and $Z \cap \tilde{U}^1$ of \tilde{U}^1 , respectively. Then Y^1 is the zero set of a prime ideal P_1 of $A[v]$, and Z^1 is the zero set of the principal ideal of $A[v]$ generated by v_0 . The intersection $Y^1 \cap Z^1$ is empty because $Y \cap Z$ is empty, so the sum $P_1 + (v_0)$ is the unit ideal. There is an equation in $A[v]$ of the form

fplusg (4.5.4)
$$f_1(v) + g_1(v)v_0 = 1$$

with $f_1(v)$ in P_1 and $g_1(v)$ in $A[v]$.

This equation is also valid in the coordinate algebra of the intersection $\tilde{U}^0 \cap \tilde{U}^1$, which is the spectrum of the common localization $A[u, v] = A[v][v_0^{-1}] = A[u][u_1^{-1}]$. In $A[u, v]$, we may write the equation (4.5.4) in terms of u , using the relation

$$v_j = u_j u_1^{-1}$$

When we do this, and multiply by a large power u_1^k to clear denominators, we will obtain an equation in $A[u]$ of the form

$$F_1(u) + G_1(u) = u_1^k$$

where $F_1(u) = f_1(v)u_1^k$ and $G_1(u) = (g_1(v)v_0)u_1^k$. The ideals P_0 of $A[u]$ and P_1 of $A[v]$ generate the same ideal in $A[u, v]$. Since $f_1(v)$ is in P_1 , $F_1(u)$ will be in P_0 if k is large enough.

Now the important point is this: As functions of u , the variables v_j have degree zero. Therefore $F_1(u)$ will be a polynomial of degree k , but because $v_0 u_1 = 1$, $G_1(u)$ will have degree $k - 1$. When we restrict to Y , the term F_1 drops out, and we obtain the equation in B :

$$u_1^k = G_1(u)$$

in which G_1 has degree $k - 1$.

We can replace U^1 by U^i for every index $i = 1, \dots, n$, using the same large exponent k . Thus there will be relations in B of the form

uhatk (4.5.5)
$$u_i^k = G_i(u)$$

with G_i of degree $k - 1$.

Suppose that an element β of B is represented by a polynomial $p(u)$ in $A[u]$. If a monomial m that appears in p is divisible by u_i^k for some i , say $m = u_i^k z$, then β is also represented by the polynomial obtained by substituting $G_i(u)z$ for m into $p(u)$, and $G_i(u)z$ has lower degree than m . By making such substitutions finitely often, we will be left with a polynomial $\tilde{p}(u)$ that still represents β , and in which no monomial that appears is divisible by any u_i^k . Any monomial of degree $\geq nk + 1$ will be divisible by u_i^k or at least one i , so the polynomial \tilde{p} will have degree at most nk . Therefore the monomials in u of degree $\leq nk$ span B as A -module. So B is a finite A -module.

This takes care of the case in which there exists a hyperplane H such that Y is disjoint from \tilde{H} . The next lemma shows that we can cover the given variety X by open subsets to which this special case applies. Then Lemma 4.5.1 completes the proof.

avoidhplane **4.5.6. Lemma.** *Let hypotheses be as in the statement of Chevalley's Theorem. For every point p of X , there is a hyperplane H in \mathbb{P}^n and an affine open neighborhood X' of p whose inverse image Y' in Y is disjoint from \tilde{H} .*

proof. The fibre of Y over a point p of X will be finite a finite set of points $\tilde{q}_1, \dots, \tilde{q}_r$. Since $Y \subset \mathbb{P}^n \times X$ we can project these points to \mathbb{P}^n , obtaining a finite set q_1, \dots, q_r . We choose a hyperplane \tilde{H} in \mathbb{P}^n that avoids this finite set. Then \tilde{H} avoids the fibre of Y over p . Let V denote the closed subset $Y \cap \tilde{H}$ of Y . Since V is a proper closed subset of Y , every component of V is finite over X , and therefore has a closed image (Theorem 4.4.3). This is our induction hypothesis. Thus the image W of V in X is closed, and it doesn't contain p . Then $X' = X - W$ is the required neighborhood of p : If q' is a point of its inverse image Y' , then $q' \notin V$, and therefore $q' \notin \tilde{H}$. So $Y' \cap \tilde{H} = \emptyset$. \square

dplane Section 4.6 Example: Double Planes

affdplanes (4.6.1) affine double planes

Let A be the polynomial algebra $\mathbb{C}[x, y]$, and let X be the affine plane $\text{Spec } A$. An *affine double plane* is a locus of the form $w^2 = f(x, y)$ in affine 3-space, where f is a square-free polynomial – a nonconstant polynomial with no square factor. Let $B = \mathbb{C}[w, x, y]/(w^2 - f)$, so that the double plane is $Y = \text{Spec } B$. We denote by w, x, y both the variables and their residues in B .

dplanering-normal **4.6.2. Lemma** *The algebra B is a normal domain, and a free A -module with basis $(1, w)$. It has an automorphism σ of order 2, defined by $a + bw \rightsquigarrow a - bw$, and the algebra of σ -invariant elements is A . \square*

The inclusion $A \subset B$ gives us an integral morphism $Y \xrightarrow{u} X$ that sends (w, x, y) to (x, y) . Given a point $p = (x_0, y_0)$ of X , the equation $w^2 = f(x_0, y_0)$ determines the points of Y over p . When $f(x_0, y_0) = 0$, the only solution is $w_0 = 0$, and when $f(x_0, y_0) \neq 0$, there are two solutions that differ by sign. The reason that Y is called a *double plane* is that most points of the plane X are covered by two points of Y . Points of X correspond bijectively to σ -orbits of points of Y .

The curve $\{f = 0\}$ in X , which we denote by Δ , is the *branch locus* of the covering.

We study prime ideals of B that lie over principal prime ideals of A . A prime ideal Q that lies over a principal prime ideal P needn't be a principal ideal, but its zero set D in Y will lie over the plane curve C defined by P , and D will be called a curve too.

Since the fibres of the map $Y \rightarrow X$ have order at most two, there will be at most two closed subvarieties D that lie over C . If there are two such subvarieties, we say that C *splits* in Y .

circleex-
ample

4.6.3. Example. Let $f(x, y) = x^2 + y^2 - 1$. The double plane $Y = \{w^2 = x^2 + y^2 - 1\}$ is an affine quadric. Its branch locus Δ is the curve $\{x^2 + y^2 = 1\}$.

The line $C_1 : \{y = 0\}$ in X meets the branch locus Δ transversally at the points $(\pm 1, 0)$, and the prime ideal yA remains prime, because $B/yB \approx \mathbb{C}[w, x]/(w^2 - x^2 + 1)$ and $w^2 - x^2 + 1$ is an irreducible polynomial. On the other hand, the line $C_2 : \{y = 1\}$ is tangent to Δ at the point $(0, 1)$, and it splits. When we set $y = 1$ in the equation for Y , we obtain $w^2 = x^2$. The locus $\{w^2 = x^2\}$ is the union of the two lines $\{w = x\}$ and $\{w = -x\}$ that lie over C_1 .

##figure##

This example illustrates a general principle: A curve that intersects the branch locus transversally at some point doesn't split. We explain this now.

localanal

(4.6.4) local analysis

Let's suppose that a plane curve $C : \{g = 0\}$ and the branch locus $\Delta : \{f = 0\}$ of a double plane meet at a point p . We adjust coordinates so that p becomes the origin $(0, 0)$, and we write

$$f(x, y) = \sum a_{ij} x^i y^j = a_{10}x + a_{01}y + a_{20}x^2 + \dots$$

Since Δ contains p , the constant coefficient of f is zero. The line $\{a_{10}x + a_{01}y = 0\}$ is the tangent line to Δ at p . It is defined if the two linear coefficients aren't both zero. Similarly, writing $g(x, y) = \sum b_{ij} x^i y^j$, the tangent line to C , if defined, is the line $\{b_{10}x + b_{01}y = 0\}$.

Let's suppose that the two tangent lines are defined and distinct – that the curves intersect transversally at p . We change coordinates once more, to make the two tangent lines the coordinate axes. After adjusting by scalar factors, the polynomials f and g will have the form

$$f(x, y) = x + u(x, y) \quad \text{and} \quad g(x, y) = y + v(x, y),$$

where u and v are polynomials all of whose terms have degree at least 2.

Let $X_1 = \text{Spec } \mathbb{C}[x_1, y_1]$ be another affine plane. We consider the map $X_1 \rightarrow X$ defined by the substitution $x_1 = d + u, y_1 = y + v$.

Working in the classical topology, this map is invertible analytically, because the Jacobian matrix

jacob (4.6.5)
$$\left(\frac{\partial(x_1, y_1)}{\partial(x, y)} \right)_{(0,0)}$$

at p is the identity matrix. When we make this substitution, Δ becomes the locus $\{x_1 = 0\}$ and C becomes the locus $\{y_1 = 0\}$. In this local coordinate system, the equation $w^2 = f$ that defines the double plane becomes $w^2 = x_1$. When we restrict it to C by setting $y_1 = 0$, x_1 becomes a local coordinate function on C , and the restriction of the equation remains $w^2 = x_1$. The inverse image Z of C doesn't decompose, locally at p . Therefore it doesn't decompose globally either, and this shows that P remains prime.

splitnot-
transversal

4.6.6. Corollary. A curve C that meets the branch locus transversally at some point doesn't split in Y . \square

This isn't a complete analysis. When C and Δ are tangent at every point of intersection, C may split or not, and in most cases, which possibility occurs cannot be decided by a local analysis. However, there is one case in which a local analysis suffices to decide splitting, the case that C is a line. Say that $C \approx \text{Spec } \mathbb{C}[t]$. We restrict the polynomial f to C , obtaining a polynomial $\phi(t)$ in t . A root of ϕ corresponds to an intersection of the line C with Δ , and a multiple root corresponds to an intersection at which C and Δ are tangent, or at which Δ is singular. The line C will split if and only if $\phi(t)$ is a square in $\mathbb{C}[t]$. We factor: $\phi(t) = c(t-a_1)^{r_1} \cdots (t-a_k)^{r_k}$. Then $\phi(t)$ will be a square if and only if the multiplicity r_i of every root a_i is even.

tangentsplit

4.6.7. Corollary. *A line in the plane X splits if it has a simple tangency with the branch locus at every intersection point.* \square

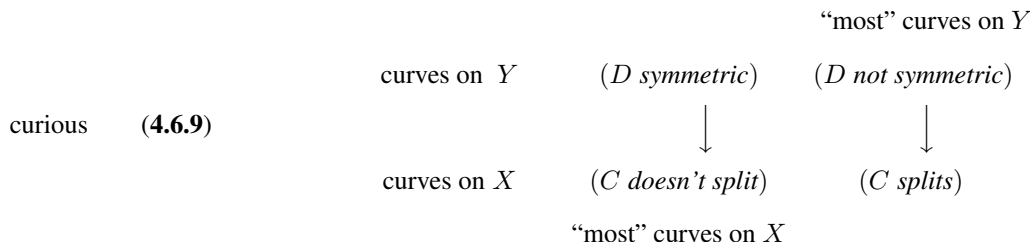
A *rational curve* is a curve whose function field is a rational function field $\mathbb{C}(t)$ in one variable. One may make a similar analysis for any rational plane curve, such as a conic, but one needs to examine its singular points and its points at infinity as well as its smooth points at finite distance.

curiouspoint

(4.6.8) a curious point.

Most curves C in the plane X will intersect a given branch locus $\Delta : \{f = 0\}$ transversally, and therefore won't split. In fact, at first glance it isn't obvious that there will be any curves in X that split, when f has high degree. However, every curve in Y lies over a curve in X , and most curves in Y won't be symmetric with respect to the symmetry σ that sends $(w, x, y) \rightsquigarrow (-w, x, y)$. For example, when we slice Y by a plane passing through a point $q = (w_0, x_0, y_0)$, the slice will most often not contain the point $q' = (-w_0, x_0, y_0)$. Then if D is the component of the slice that contains q , $D\sigma$ will contain q' , and it will be distinct from D . But the images in X of D and $D\sigma$ will be the same. The image will split. Curves that split do exist.

Here is the curious point: Let D be a curve in Y that lies over a curve C in X . Then C won't split if it has a transversal intersection with Δ , and this will be true for most curves in X . On the other hand, when C regarded as the image of the curve D on Y , C will split unless D is symmetric with respect to σ , and most curves in Y won't be symmetric.



One has to be careful about the meaning of the word “most”.

projdplane

(4.6.10) projective double planes

A *projective double plane* is a locus of the form

wtdplane

(4.6.11)
$$y^2 = f(x_0, x_1, x_2),$$

where f is a square-free homogeneous polynomial of even degree $2d$. To regard this as a homogeneous equation, we must assign *weight* d to the variable y . Then, since we have weighted variables, we must work in a *weighted projective space* \mathbb{WP} with coordinates x_0, x_1, x_2, y , where x_i have weight 1 and y has weight d . A point of this weighted space \mathbb{WP} is represented by a nonzero vector (x_0, x_1, x_2, y) with the relation that, for all $\lambda \neq 0$, $(x_0, x_1, x_2, y) \sim (\lambda x_0, \lambda x_1, \lambda x_2, \lambda^d y)$. The points of the weighted projective space \mathbb{WP} that solve the equation (4.6.11) are the points of the projective double plane Y .

If (x, y) solves (4.6.11) and $(x) = (0, 0, 0)$, then $y = 0$ too. The vector $(0, 0, 0, 0)$ doesn't represent a point of \mathbb{WP} . Therefore the projection $\mathbb{WP} \rightarrow \mathbb{P}^2 = X$ that sends $(x, y) \rightsquigarrow x$ is defined at all points of Y , and maps Y to the projective plane X . The fibre of Y over the point x of X consists of the points (x, y) and $(x, -y)$, which will be equal if and only if x lies on the *branch locus* of the double plane, the (possibly reducible) curve $\Delta : \{f = 0\}$ in X . The map $\sigma : (x, y) \rightsquigarrow (x, -y)$ is an automorphism of Y , and points of X correspond bijectively to σ -orbits in Y .

Since the double plane Y is embedded into a weighted projective space, it isn't presented to us as a projective variety in the usual sense. However, it can be embedded into a projective space in the following way: The projective plane \mathbb{P}_x^2 can be embedded by a Veronese embedding of higher order, using as coordinates the monomials m_1, m_2, \dots of degree d in x_0, x_1, x_2 . This embeds \mathbb{P}^2 into a projective space \mathbb{P}^N where $N = \binom{d+2}{2} - 1$. When we add one more coordinate y to this embedding, we obtain an embedding of the weighted projective space $\mathbb{W}\mathbb{P}$ into \mathbb{P}^{N+1} , that sends the point (x, y) to (m, y) . The double plane Y can be realized as a projective variety by this embedding.

If $Y \rightarrow X$ is a projective double plane then, as happens with affine double planes, a curve C in X may split in Y or not. If C has a transversal intersection with the branch locus Δ , it will not split, while if C is a line that has an ordinary tangent to the branch locus Δ at every intersection point, it will split (Corollary 4.6.7). For example, when the branch locus Δ is a generic quartic curve, the lines that split will be the bitangent lines (see Section ??).

homogdplan **(4.6.12) homogenizing an affine double plane**

We construct a projective double plane by homogenizing an affine double plane. Let's write an affine double plane as

relabelaffined-plane (4.6.13)
$$w^2 = F(u_1, u_2).$$

We suppose that F has even degree $2d$, and we homogenize F , setting $u_i = x_i/x_0$. To clear denominators, we must multiply by x_0^{2d} . When we set $y = x_0^d w$, we obtain an equation of the form (4.6.11), where f is the homogenization of F .

cubicsdplane **(4.6.14) cubic surfaces and quartic double planes**

Let X be the projective plane, with coordinates x_0, x_1, x_2 . We label coordinates in the 3-space \mathbb{P}^3 as $(x, z) = (x_0, x_1, x_2, z)$. Let S be the cubic surface in projective 3-space defined by an irreducible homogeneous cubic polynomial $g(x, z)$, and let $q = (0, 0, 0, 1)$ be a point of S . Let π be the projection $(x, z) \rightsquigarrow x$ $S \rightarrow X$.

Since q is a point of S , the coefficient of z^3 in g is zero. So g is quadratic in z :

projequation (4.6.15)
$$g(x, z) = a_1 z^2 + a_2 z + a_3,$$

The coefficients a_i are homogeneous, of degree i in x . The discriminant $a_2^2 - 4a_1 a_3$ is a homogeneous polynomial of degree 4 in x . Let Y be the double plane

quarticdplane (4.6.16)
$$y^2 = a_2^2 - 4a_1 a_3.$$

and let $\Delta : a_2^2 - 4a_1 a_3$ be its branch locus. As was remarked, the lines that split in Y will be bitangent lines, provided that the branch locus is generic.

Given a point (x, z) of S , we can pick out a square root y by defining

cubicand-plane (4.6.17)
$$y = 2a_1 z + a_2$$

This formula defines a map $S \xrightarrow{\varphi} Y$ at every point except q . The quadratic formula solves for z in terms of y :

quadrformula (4.6.18)
$$z = \frac{y - a_2}{2a_1}$$

which defines the inverse map $Y \xrightarrow{\psi} S$ when $a_1 \neq 0$.

4.6.19. Theorem. *A generic cubic surface contains precisely 27 lines.*

proof. Let S be a generic cubic surface in \mathbb{P}^3 , projected to the plane X from a generic point q of S , as above. We recall that a generic cubic surface contains finitely many lines. Therefore, when S and q are generic, q will not be contained in any line in S .

We inspect the projection $S \xrightarrow{\pi} \mathbb{P}_x^2$. Let ℓ be the line in X defined by a linear equation $b_0x_0 + b_1x_1 + b_2x_2 = 0$, and let P be the plane in $\mathbb{P}_{x,z}^3$ defined by the same equation. Then P contains q , and the points of P different from q project to ℓ . The intersection $Z = P \cap S$ will be a (possibly reducible) cubic curve in P that contains q . We distinguish three cases:

Case (a): q is a smooth point of Z , and Z is an irreducible cubic.

The complement of q in Z is a branched double covering of ℓ , with one missing point. The line ℓ doesn't split in Y .

Case (b): q is a smooth point of Z , and Z is a reducible cubic.

Since q is not contained in a line of S , Z is the union of a conic C and a line L , and q is a point of C . Then L maps bijectively to ℓ , and the complement of q in S maps injectively to ℓ . In this case ℓ does split in Y .

Case (c): q is a singular point of Z .

Since q is not contained in a line of S , Z is irreducible, and the map $Z' \rightarrow \ell$ is injective.

casec **4.6.20. Lemma.** *Case (c) occurs precisely once, and that is when P is the tangent plane to S at q .* □

We'll leave the proof of this lemma as an exercise.

The tangent plane to S is the plane orthogonal to the gradient ∇g at q of the defining equation $g(x, z)$ (4.6.15) of S . The partial derivative $\frac{\partial g}{\partial x_i}(q)$ is the coefficient of x_i in the linear polynomial $a_1(x)$, and $\frac{\partial g}{\partial z}(q) = 0$. Thus the tangent plane at q is the plane $a_1(x) = 0$. When we set $a_1 = 0$ in the equation (4.6.16) of Y , we get $y^2 = a_2^2$. The image $\ell : a_1(x) = 0$ of the tangent plane splits in Y . This doesn't contradict the fact that $Z' \rightarrow \ell$ is injective, because the projection from q is undefined at q .

Anyhow, there are 28 bitangents to a generic quartic, hence 28 lines ℓ that split in Y . Exactly one of these lines is the line $a_1(x) = 0$, and the 27 others are the ones in Case (b). Each of those gives us one line in S .

To complete the proof, we had better show that when S is a generic cubic surface, the associated double plane is also generic. We need this in order to justify the assertion that the quartic curve has 28 bitangents. The next lemma does this.

quarticis-
generic **4.6.21. Lemma.** *A generic homogeneous quartic $f(x_0, x_1, x_2)$ can be written in the form $a_2^2 - 4a_1a_3$, where a_i is a homogeneous polynomial of degree i .*

proof. We choose for a_1 a linear polynomial such that the line $C : \{a_1 = 0\}$ is a bitangent to the quartic curve $\{f = 0\}$. Then C splits in the double plane, so f is congruent to a square, modulo a_1 . Let a_2 be a quadratic polynomial such that $f \equiv a_2^2$ modulo a_1 . When we take this polynomial as a_2 , we will have $f = a_2^2 - 4a_1a_3$ for some cubic polynomial a_3 . □