Zariski's Main Theorem

Anand P. Sawant
School of Mathematics
Tata Institute of Fundamental Research, Mumbai, India.

16th June, 2010

Abstract

Zariski's main theorem is a theorem proved by Zariski (1943, 1949) which implies that fibers over normal points of birational projective morphisms of varieties are connected. The theorem can be stated in several ways which at first sight seem to be quite different. In particular, the name "Zariski's main theorem" is also used for a closely related theorem of Grothendieck that describes the structure of quasi-finite morphisms of schemes, which implies Zariski's original main theorem. In this article, we give an account of different versions of Zariski's main theorem and give an algebraic proof of Grothendieck's version of Zariski's main theorem.

1 Introduction

Throughout the article, by a *variety* we mean an irreducible affine algebraic set over an *algebraically closed* field k. Recall that if X and Y are varieties, a *rational map* $\varphi : X \to Y$ is an equivalence class of pairs $\langle U, \varphi_U \rangle$, where U is a nonempty open set of X and φ_U is a morphism from U to Y, and where $\langle U, \varphi_U \rangle$ and $\langle V, \varphi_V \rangle$ are equivalent if $\varphi_U = \varphi_V$ on $U \cap V$. φ is said to be *dominant* if for some open set U in X, $\varphi_U(U)$ is dense in Y. Note that a rational map is not in general a map of the set X to Y. Also note that dominant rational maps can be composed and hence, we can consider the category of varieties with morphisms as dominant rational maps. Isomorphisms in this category are called *birational maps*.

Definition 1.1. Let X and Y be varieties. A *birational map* $\varphi : X \to Y$ is a rational map which admits an inverse, that is, a rational map $\psi : Y \to X$ such that $\psi \circ \varphi = \mathrm{id}_X$ and $\phi \circ \psi = \mathrm{id}_Y$ as rational maps.

If there is a birational map from X to Y, we say that X and Y are *birationally equivalent*, or simply *birational*. We recall that to give a birational morphism φ from X to Y is to give an open set $U \subseteq X$ and a morphism $f : U \to Y$ which induces an isomorphism of function fields $k(Y) \xrightarrow{\sim} k(X)$. If we have another open set $V \subseteq X$ and another morphism $g : V \to Y$ representing φ, then f and g agree on $U \cap V$, so we can glue them to obtain a morphism $U \cup V \to Y$. In this way, we obtain a largest open set $U \subseteq X$ on which φ is represented by a morphism $U \to Y$. We say that φ is *defined* at the points of U and tht the points of $X \backslash U$ are *fundamental points* of φ.

If $\varphi : X \to Y$ is a birational transformation defined on U, represented by a morphism $f : U \to Y$, let $\Gamma_0 \subseteq U \times Y$ be the graph of f, and let $\Gamma \subseteq X \times Y$ be its closure. Γ is called the *graph* of φ. For any subset $Z \subseteq X$, we define $\varphi(Z) := p_Y(p_X^{-1}(Z))$, where $p_X : \Gamma \to X$, $p_Y : \Gamma \to Y$ are the projections. $\varphi(Z)$ is called the *total transform* of Z. If φ is defined at a point $P \in X$, then $\varphi(P)$ is just the point $\varphi(P)$. But if P is a fundamental point of φ, then its total transform will consist of more than one point in general.

2 Zariski's Main Theorem - Smooth Case

In this section, we prove Zariski's main theorem in case of the fibre of a smooth point. We shall use a result about the dimension of intersection of an affine variety with an algebraic set, proof of which follows directly from Krull's principal ideal theorem.

Theorem 2.1. *If X is an r-dimensional affine variety and $f_1, \ldots, f_k$ are polynomial functions on X, then every irreducible component of $X \cap V(f_1, \ldots, f_k)$ has dimension $\geq r - k$.*

Theorem 2.2 (Zariski's Main Theorem - smooth case)**.** *Let $\varphi : X \to Y$ be a birational regular map of r-dimensional affine varieties. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ denote the affine coordinates on X and Y respectively. Let $p \in X$ and $q = \varphi(p) \in Y$ be a smooth point. Then either*
(i) φ^{-1} is a regular correspondence at q; more precisely, there exists a polynomial $d(y_1, \ldots, y_m)$ such that $d(q) \neq 0$ and an inverse $\psi : Y' = \{y \in Y \mid d(y) \neq 0\} \to X$ to φ, which is given by $x_i = \dfrac{a_i(y_1, \ldots, y_m)}{d(y_1, \ldots, y_m)}$, for some polynomials a_i, or
(ii) there exists a subvariety $E \subseteq X$ of dimension $r - 1$ such that $\dim \overline{\varphi(E)} \leq r - 2$.(Such an E is called an exceptional divisor. In particular, the fibre $\varphi^{-1}(q)$ has a positive-dimensional component through p.)

Proof. Since φ is birational, it induces an isomorphism $\varphi^* : k(Y) \to k(X)$ on the function fields. Hence, each function x_i on X equals $b_i(y_1, \ldots, y_m)/c_i(y_1, \ldots, y_m) \circ \varphi$, for some polynomials b_i, c_i such that $c_i \neq 0$ on Y (for simplicity, we are not specifying the open sets on which the representatives are defined). Since $q \in Y$ is a smooth point, the local ring $\mathcal{O}_{q,Y}$ is regular local, and consequently, a UFD. We can therefore write $x_i = b_i(y_1, \ldots, y_m)/c_i(y_1, \ldots, y_m) \circ \varphi$, where b_i and c_i are relatively prime in $\mathcal{O}_{q,Y}$. We now have two possibilities: either $c_i(q) \neq 0$ for all i, or $c_i(q) = 0$ for some i. In the former case, take $d = \prod_{i=1}^{n} c_i$ and define $\psi : Y' \to X$, where $Y' = \{y \in Y \mid d(y) \neq 0\}$, by

$$\psi(y_1, \ldots, y_m) := \left(\frac{a_1(y)}{d(y)}, \ldots, \frac{a_n(y)}{d(y)} \right),$$

where $a_i(y) = b_i(y) \prod_{j \neq i} c_j(y)$.

In the latter case, let us assume that $c_1(q) = 0$. Let $\gamma_1(y)$ be a polynomial that represents an irreducible factor of $c_1(y)$ in $\mathcal{O}_{q,Y}$ such that $\gamma_1(q) = 0$. Let E be an irreducible component of $X \cap V(\gamma_1 \circ \varphi)$ passing through p. By Theorem 2.1, $\dim E = r - 1$. But if $c_1 = c_1' \cdot \gamma_1$, then on X, we have $b_1 \circ \varphi = x_1 \cdot (c_1' \circ \varphi) \cdot (\gamma_1 \circ \varphi)$; whence $b_1 \circ \varphi = 0$ on E. Therefore, b_1 and γ_1 vanish on $\varphi(\overline{E})$. Now, γ_1, being irreducible, generates a prime ideal of $\mathcal{O}_{q,Y}$. Therefore, the ideal

$$I := \{f \in k[Y] \| f \in \gamma_1 \cdot \mathcal{O}_{q,Y}\}$$

is a prime ideal of $k[Y]$. Observe that $b_1 \notin I$, since b_1 and c_1 are relatively prime. (*Reason*: If $b_1 \in I$, then $b_1 = \gamma_1 \cdot \dfrac{f}{g}$ in $\mathcal{O}_{q,Y}$ with $g(q) \neq 0$. Thus, we have $g b_1 = f \gamma_1$. Now, γ_1 cannot divide g since $g(q) \neq 0$, so γ_1 divides b_1.) Hence, $b_1 \neq 0$ on $V(I)$. Therefore, we see that

$$Y \supsetneq V(I) \supsetneq \varphi(E),$$

which implies that $\dim \overline{\varphi(E)} \leq r - 2$. □

The stronger version of the Zariski main theorem assumes only that the local ring $\mathcal{O}_{q,Y}$ is integrally closed in $k(Y)$. Then either φ^{-1} is a regular correspondence at q, or $\varphi^{-1}(q)$ has a positive dimensional component through p. We give an algebraic proof of this stronger version of the Zariski main theorem in the last section.

3 Various Versions of Zariski's Main Theorem

Zariski, in [7], first stated and proved his main theorem. In modern language, the statement takes the following forms:

Version 1 (Original form - I)**.** Let $T : X \to Y$ be a birational transformation of projective varieties over k, and assume that X is normal. If P is a fundamental point of T, then the total transform $T(P)$ is connected and of dimension ≥ 1.

Version 2 (Original form - II)**.** Let X be a normal variety over k and let $f : X' \to X$ be a birational morphism with finite fibres from a variety X'. Then f is an isomorphism of X' with an open subset $U \subseteq X$.

Zariski also gave a version which could be deduced from pure local algebra and power series techniques.

Version 3 (Power series form)**.** Let X be a normal variety over k and let $x \in X$ be a normal point (not necessarily closed), that is, the local ring $\mathcal{O}_x$ is normal. Then the completion $\hat{\mathcal{O}}_x$ is an integral domain which is normal.

Grothendieck (1966) observed that Zariski's main theorem could easily be deduced from a more general theorem about the structure of quasi-finite morphisms (that is, morphisms having finite fibres), and "Zariski's main theorem" is sometimes used to refer to this generalization. It is well known that open immersions and finite morphisms are quasi-finite. Zariski's main theorem for quasifinite morphisms, which is much harder than these facts is a kind of converse statement.

Version 4 (Grothendieck's form)**.** Let $f : X' \to X$ be a morphism of varieties over k with finite fibres. Then there exists a diagram

$$\begin{array}{ccc} X' & \hookrightarrow & Y \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle g} & \\ X & & \end{array}$$

where Y is a variety, X' is an open set in Y and g is a finite morphism.

Observe that Version 4 immediately implies Version 2. A direct appliction of Version 4 with the hypotheses of Version 2 gives a variety Y such that X' is a dense open set in Y. Then it follows that g is a birational finite morphism. Since X is normal, it must be an isomorphism. This proves that X' is an open subset of X, as desired.

Version 5 (Connectedness theorem - I)**.** Let X be a variety over k, normal at a closed point $x \in X$. Let $f : X' \to X$ be a birational proper morphism. Then the fibre $f^{-1}(x)$ is connected (in the Zariski topology).

Version 6 (Connectedness theorem - II)**.** Let $f : X' \to X$ be a birational projective morphism of noetherian integral schemes. Assume that X is normal. Then the fibre $f^{-1}(x)$ is connected (in the Zariski topology).

The most powerful approach to Zariski's main theorem is via Version 3. Zariski proved Version 3 and deduced the original Versions 1 and 2 from it. Versions 4, 5 and 6 are very deep. Version 5 is a very global statement, since properness of f is involved. There are cohomological proofs of Versions 5 and 6 due to Grothendieck and proofs using projective techniques and completions due to Zariski. There is a proof of Version 4 heavily depending upon Version 3 due to Grothendieck. Zariski, in [8], reformulated his main theorem in terms of commutative algebra. Algebraic version of Grothendieck's generalization (1961) of Zariski's formulation, which will be proved in the next section, is as follows:

Version 7 (Algebraic form)**.** Let B be a finitely generated A-algebra. If $\mathfrak{q}$ is a prime ideal of B isolated over $\mathfrak{p} = \mathfrak{q} \cap A$, then there exists a finite A-algebra R contained in B and an element $s \in R \backslash \mathfrak{q}_R$, where $\mathfrak{q}_R = \mathfrak{q} \cap R$, such that $R_s = B_s$.

4 Zariski's Main Theorem - Grothendieck's Version

The aim of this section is to give an algebraic proof of Grothendieck's version of Zariski's main theorem. We need a result in the proof below, which is a consequence of the following version of Hilbert's Nullstellensatz:

Theorem 4.1 (Nullstellensatz)**.** *Let k be a field and A be a finite type k-algebra. If $\mathfrak{m}$ is a maximal ideal in A, then $A/\mathfrak{m}$ is a finite extension of k.*

The corollary of Theorem 4.1 which will be used in the proof of Grothendieck's stronger version of Zariski's main theorem is the following.

Corollary 4.2. *Let $R \subseteq S \subseteq T$ be commutative rings such that T is integral over a finite type R-algebra. If a prime ideal $\mathfrak{q}_T$ of T is maximal in its fibre above $\mathfrak{q}_R := \mathfrak{q}_T \cap R$, then $\mathfrak{q}_S := \mathfrak{q}_T \cap S$ is maximal in its fibre over $\mathfrak{q}_R$.*

Proof. First, we may assume that R is local by localizing at $\mathfrak{q}_R$. By going modulo $\mathfrak{q}_T$, we may assume that R, S, T are integral domains, that $\mathfrak{q}_T = 0$, and that R is a field. Since $\mathfrak{q}_T$ is isolated over the maximal ideal $\mathfrak{q}_R$ of R, it is itself maximal. This makes T a field. Let T' be a finite type sub-R-algebra of T such that T is integral over T'. Since T is a field, the lying-over theorem implies that T' must be field. By Theorem 4.1, T' must finite algebraic over R, which implies that T is algebraic over R. Therefore, S has to be a field, since $R \subseteq S \subseteq T$. □

Let $f : A \to B$ be a homomorphism of commutative rings. f induces a map $f^\sharp : \operatorname{Spec} B \to \operatorname{Spec} A$, which is given by $f^\sharp(\mathfrak{q}) = f^{-1}(\mathfrak{q})$, for all prime ideals $\mathfrak{q}$ of B. Let $\mathfrak{p}$ be a prime ideal of A. The prime ideals of B in the fibre of $f^\sharp$ over $\mathfrak{p}$ are in one to one correspondence with the prime ideals of the ring $B \otimes_A \kappa(\mathfrak{p})$, where $\kappa(\mathfrak{p})$ denotes the residue field of $\mathfrak{p}$ ($\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$).

Definition 4.3. Let $f : A \to B$ be a homomorphism of rings. A prime ideal $\mathfrak{q}$ of B is said to be *isolated in its fibre* if $\mathfrak{q}$ is maximal as well as minimal (with respect to inclusion) in $f^{-1}(\mathfrak{p})$, where $\mathfrak{p} = A \cap \mathfrak{q}$.

Before going on to prove the main theorem, we first prove a couple of lemmas which will be required. In what follows, all the rings are assumed to be commutative with unity and noetherian.

Lemma 4.4. *Let $A \subseteq B$ be integral domains such that A is local with maximal ideal $\mathfrak{p}$ and that A is integrally closed in B. Suppose that there exists $t \in B$, which is transcendental over A, such that B is integral over $A[t]$. Then no prime $\mathfrak{q}$ of B is isolated in its fibre over $\mathfrak{p} = \mathfrak{q} \cap A$.*

Proof. Let us first assume that A is integrally closed. Then $A[t]$ is also integrally closed. Let $\mathfrak{q}$ be a prime ideal of B and set $\mathfrak{p} = \mathfrak{q} \cap A$, $\mathfrak{r} = \mathfrak{q} \cap A[t]$. We claim that $\mathfrak{r}$ is not isolated over $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{r} \cap A$. Indeed, since $A[t]$ is a polynomial ring over A, the prime ideal $\mathfrak{p}A[t]$ lying over $\mathfrak{p}$ is not maximal; also, the maximal ideal of $A[t]$ containing $\mathfrak{p}A[t]$ also lies over $\mathfrak{p}$. From this it follows that $\mathfrak{r}$ is not isolated in its fibre over $\mathfrak{p}$. By applying the going-up or the going-down theorem, depending on whether $\mathfrak{r}$ is minimal or maximal among the prime ideals in the fibre over $\mathfrak{p}$, it can be seen that $\mathfrak{q}$ is not isolated in its fibre over $\mathfrak{p}$.

If A is not integrally closed, let A' and B' denote the integral closures of A and B respectively. Clearly, t is transcendental over A' and B' is integral over $A'[t]$, B being integral over $A[t]$. If $\mathfrak{q}'$ is a prime ideal of B' such that $\mathfrak{q}' \cap B = \mathfrak{q}$, then it is not isolated over $\mathfrak{p}' = \mathfrak{q}' \cap A'$, by the special case proved above. Therefore, there exists a prime ideal $\mathfrak{q}'_1$ in B' such that $\mathfrak{q}'_1 \cap A' = \mathfrak{p}'$ and either $\mathfrak{q}' \subsetneqq \mathfrak{q}'_1$ or $\mathfrak{q}'_1 \subsetneqq \mathfrak{q}'$. We shall work out the case $\mathfrak{q}' \subsetneqq \mathfrak{q}'_1$; the other case follows similarly. If $\mathfrak{q}' \subsetneqq \mathfrak{q}'_1$, then if set $\mathfrak{q}_1 = \mathfrak{q}'_1 \cap B$, we have $\mathfrak{q} \subsetneqq \mathfrak{q}_1$, in view of the going-up theorem. We thus have $\mathfrak{q}_1 \cap A = \mathfrak{q}'_1 \cap B \cap A = \mathfrak{q}'_1 \cap A' \cap A = \mathfrak{q}' \cap A' \cap A = \mathfrak{q}' \cap B \cap A = \mathfrak{p}$. Therefore, $\mathfrak{q}$ cannot be isolated in its fibre over $\mathfrak{p} = \mathfrak{q} \cap A$. This completes the proof. □

Define the *conductor* from B to $A[t]$ to be

$$I := \{v \in A[t] \mid vB \subseteq A[t]\}.$$

Note that I is an ideal of B.

Lemma 4.5. *Let $A \subseteq B$ be integral domains with the same quotient field such that A is integrally closed in B. Suppose that there exists $t \in B$ such that B is integral over $A[t]$. If the conductor from B to $A[t]$ contains an element of the form $F(t)$ for a monic polynomial $F \in A[X]$, then $B = A[t]$.*

Proof. If $\deg(F) = 0$, then $F(X) = 1$ and clearly, $B = A[t]$. If $F(t) = 0$, then t is integral over A. Since A is integrally closed in B and B is integral over $A[t]$, it follows that $A = A[t] = B$. Thus, we assume that $\deg(F) > 0$ and that $F(t) \neq 0$. Let $b \in B$. There exists $G \in A[X]$ such that $F(t)b = G(t)$. Using division algorithm, write $G = QF + R$, where $\deg R < \deg F$. Set $s = b - Q(t)$. Then we have

$$F(t) - \frac{1}{s}R(t) = 0$$

in the localization B_s. Hence, t is integral over the subring $A[\frac{1}{s}]$ of B_s. But $s \in B$ is integral over $A[t]$ by hypothesis, whence s is also integral over $A[\frac{1}{s}]$. Therefore, we can find $\alpha_i \in A[\frac{1}{s}]$ such that

$$s^n + \alpha_{n-1}s^{n-1} + \cdots + \alpha_0 = 0.$$

Write $\alpha_i = a_i/s^{r_i}$, where $a_i \in A$. Then mutiplying the above equation by a sufficiently high power of s, we see that s is integral over A, and consequently, in A. Therefore, $b = s + Q(t) \in A[t]$, completing the proof that $B = A[t]$.

□

Grothendieck's version of Zariski's main theorem follows from the following theorem.

Theorem 4.6. *Let $A \subseteq B$ be integral domains with A integrally closed in B such that there exist $t_1, \ldots, t_n \in B$ with B integral over $A[t_1, \ldots, t_n]$. Assume further that A and B have the same quotient field and that A is local with maximal ideal $\mathfrak{p}$. If a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{p} = \mathfrak{q} \cap A$ is isolated in its fibre, then $A = B$.*

Proof. The proof is divided into three steps.

Step 1 : Reduction to the case $n = 1$.

The case $n = 0$ is obvious. Assume the result for $n = 1$. The proof in general case is by induction on n. Let C denote the integral closure of $A[t_1, \ldots, t_{n-1}]$ in B. We are given a prime ideal $\mathfrak{q}$ of B isolated in its fibre over $\mathfrak{p} = \mathfrak{q} \cap A$. Set $\mathfrak{q}_C = \mathfrak{q} \cap C$. $\mathfrak{q}_C$ is maximal above $\mathfrak{p}$ by Corollary 4.2. To see that $\mathfrak{q}_C$ is also minimal over $\mathfrak{p}$, look at $C \subseteq C[t_n] \subseteq B$. $\mathfrak{q}$ is isolated in its fibre over $\mathfrak{q}_C$, since it is so over $\mathfrak{p}$. We therefore have $C = B$. Minimality of $\mathfrak{q}_C$ in its fibre is now immediate. Hence, $\mathfrak{q}_C$ is isolated in its fibre, whence by the induction hypothesis, we obtain $A = C$.

Thus, it is enough to consider the case where we have $A \subseteq A[t] \subseteq B$, with B integral over $A[t]$ and A integrally closed in B. Let

$$I = \{v \in A[t] \mid vB \subseteq A[t]\}$$

denote the conductor from B to $A[t]$. We treat separately the cases $\mathfrak{q} \not\supseteq I$ and $\mathfrak{q} \supseteq I$.

Step 2 : The case $\mathfrak{q} \not\supseteq I$.

We first settle the case when $B = A[t]$. Set $k = \kappa(\mathfrak{p}) = A/\mathfrak{p}$. Now, $B \otimes k = B \otimes_A A/\mathfrak{p} = B/\mathfrak{p}B = A[t]/\mathfrak{p}A[t] \cong k[t]$. If t is an indeterminate over k, then $k[t] \cong k[X]$, and it is easy to see that no prime of the polynomial ring $k[X]$ is isolated. Hence, we assume that t is algebraically dependent over k; in that case, there exists a polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

with $a_i \in A$, not all in $\mathfrak{p}$ such that $f(t) = 0$. We claim that $t \in A$. We prove this by induction on $\deg(f) = n$. If $n = 1$, then $a_1 t + a_0 = 0$. If a_1 is a unit, we are through; otherwise, since $a_1 \in \mathfrak{p} \subseteq \mathfrak{q}$, so $a_1 t \in \mathfrak{q}$. But this implies that $a_0 \in \mathfrak{q} \cap A = \mathfrak{p}$, a contradiction since a_0 has to be a unit. Assume the result for all positive integers $< n$. Observe that

$$0 = a_n^{n-1} f(t) = (a_n t)^n + a_{n-1}(a_n t)^{n-1} + \cdots + a_0 a_n^{n-1},$$

whence $a_n t$ is integral over A, and consequently, in A, A being integrally closed in B. If a_n is a unit, we are through; otherwise, we have $(a_n t + a_{n-1})t^{n-1} + a_{n-2}t^{n-2} + \cdots + a_0 = 0$, and the claim follows from the induction hypothesis. Thus, we have $A = B$, as desired.

Coming back to the general case, let I denote the conductor from B to $A[t]$. We have assumed that $\mathfrak{q} \not\supseteq I$. Set $\mathfrak{r} = \mathfrak{q} \cap A[t]$. We have an injection $A[t]_{\mathfrak{r}} \hookrightarrow B_{\mathfrak{r}}$. By assumption, there exists a $v \in A[t] \backslash \mathfrak{r}$ such that $vB \subseteq A[t]$. This implies that $B_{\mathfrak{r}} = B_{\mathfrak{q}}$ and that $A[t]_{\mathfrak{r}} \xrightarrow{\sim} B_{\mathfrak{r}} = B_{\mathfrak{q}}$. This makes $\mathfrak{r}$ isolated in its fibre above $\mathfrak{p}$, and by applying the result proved above in the special case, we have $A = A[t]$. Now, B is integral over $A[t] = A$ and A is integrally closed in B. Therefore, we have $A = B$.

Step 3 : The case $\mathfrak{q} \supseteq I$.

We prove that no prime $\mathfrak{q}$ of B is isolated in its fibre over $\mathfrak{p} = \mathfrak{q} \cap A$. Let $\mathfrak{n}$ be a minimal prime ideal of B/I, where I denotes the conductor from B to $A[t]$. We claim that the image of t in $B/\mathfrak{n}$ is transcendental over $A/\mathfrak{m}$, where $\mathfrak{m} = \mathfrak{n} \cap A$. Replacing A by $A_{\mathfrak{m}}$, its localization at $\mathfrak{m}$, we may assume that A is local and $\mathfrak{m}$ is a maximal ideal. The conductor I need not be preserved under localization, but it is still contained in $\mathfrak{n}$. We prove the claim by contradiction. If t is algebraic over $B/\mathfrak{n}$, then there exists a monic polynomial $F \in A[X]$ such that $F(t) \in \mathfrak{n}$. Since $\mathfrak{n}$ is a minimal prime of I, the ring $B_{\mathfrak{n}}/I_{\mathfrak{n}}$ has a single prime ideal, namely $\mathfrak{n}_{\mathfrak{n}}$. Hence, $F(t)$ is nilpotent in $B_{\mathfrak{n}}/I_{\mathfrak{n}}$, so there exists $d \in \mathbb{N}$ such that $F(t)^d \in I_{\mathfrak{n}}$. This means that $vF(t)^d \in I$, for some $v \in B\backslash\mathfrak{n}$. Now, we apply Lemma 4.5, taking $A[t] + vB$ for B and F^d to be the monic polynomial in the conductor from $A[t] + vB$ to $A[t]$ to obtain $A[t] + vB = A[t]$, that is, v belongs to the conductor from $A[t] + vB$ to $A[t]$. Hence, $v \in I \subseteq \mathfrak{n}$, a contradiction. This proves the claim.

We now return to the original situation $A \subseteq A[t] \subseteq B$ with B integrally closed in $A[t]$ and A integrally closed in B. In view of the above claim, to prove that no prime ideal $\mathfrak{q}$ of B is isolated in its fibre, we take a minimal prime $\mathfrak{n}$ over I contained in $\mathfrak{q}$ and set $\mathfrak{m} = \mathfrak{n} \cap A$. Since the image of t in $B/\mathfrak{n}$ is transcendental over $A/\mathfrak{m}$, it suffices to prove that no prime of $B/\mathfrak{n}$ is isolated in its fibre. This follows immediately from Lemma 4.4, applied to the situation $A/\mathfrak{m} \subseteq \frac{A}{\mathfrak{m}}[t] \subseteq B/\mathfrak{n}$. This finishes the proof of Step 3 and proves the theorem. □

We are now ready to prove Grothendieck's version of Zariski's main theorem.

Theorem 4.7 (Zariski's Main Theorem - Grothendieck's version)**.** *Let B be a finitely generated A-algebra. If $\mathfrak{q}$ is a prime ideal of B isolated over $\mathfrak{p} = \mathfrak{q} \cap A$, then there exists a finite A-algebra R contained in B and an element $s \in R\backslash\mathfrak{q}_R$, where $\mathfrak{q}_R = \mathfrak{q} \cap R$, such that $R_s = B_s$.*

Proof. Assume that B is generated by $x_1, \ldots, x_n$ as an A-algebra. Let C be the integral closure of A in B. Clearly, $x_1, \ldots, x_n$ generate B as a C-algebra also. Note that $\mathfrak{q}$ is isolated over $\mathfrak{r} = \mathfrak{q} \cap C$. Set $S = C\backslash\mathfrak{r}$. By Theorem 4.6, we conclude that $C_{\mathfrak{r}} = S^{-1}B$. Hence, there exist $y_1, \ldots, y_n \in C$ and $s_1, \ldots, s_n \in S$ such that $x_i = y_i/s_i$. Put $s = \prod_i s_i$. It is now clear that $R = A[y_1, \ldots, y_n, s]$ is a finite A-algebra with $s \notin \mathfrak{q}_R$ such that $B_s = R_s$. □

References

[1] Bourbaki, N., *Elements of mathematics. Commutative algebra*, Translated from the French. Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972.

[2] Hartshorne, Robin, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[3] Iversen, Birger, *Generic local structure of the morphisms in commutative algebra*, Lecture Notes in Mathematics, Vol. 310. Springer-Verlag, Berlin-New York, 1973.

[4] Mumford, David, *Algebraic geometry. I. Complex projective varieties*, Grundlehren der Mathematischen Wissenschaften, No. 221. Springer-Verlag, Berlin-New York, 1976.

[5] Mumford, David, *The red book of varieties and schemes*, Lecture Notes in Mathematics, 1358. Springer-Verlag, Berlin, 1999.

[6] Peskine, Christian, *An algebraic introduction to complex projective geometry. 1. Commutative algebra.*, Cambridge Studies in Advanced Mathematics, 47, Cambridge University Press, Cambridge, 1996.

[7] Zariski, Oscar, *A simple analytical proof of a fundamental property of birational transformations*. Proc. Nat. Acad. Sci. U. S. A. 35, (1949), p.62-66.

[8] Zariski, Oscar, *Foundations of a general theory of birational correspondences*. Trans. Amer. Math. Soc. 53, (1943). p.490-542.