THROUGH THE FIELDS AND FAR AWAY

JONATHAN TAYLOR

I'd like to thank Prof. Stephen Donkin for helping me come up with the topic of my project and also guiding me through its various complications.

Contents

Date: 12th May 2008.

1. Introduction

In this project we will be examining the relationship between field extensions and algebraic geometry. Specifically, we will be looking at how the *transcendence degree* of a field extension can be used to define the notion of dimension.

Field extensions, whose degrees are finite, are generally studied via Galois theory. However, when the degree of the extension is infinite, this tends to lie outside the scope of classical Galois theory. This second case is the one we will explore in greater depth during this project.

The main bulk of this project will be the discussion of field extensions. An important step to reaching our main goal will be to prove a theorem known as Hilbert's Nullstellensatz (roughly translated, 'theorem of zeros'). In fact this result will be a corollary of a much more general theorem dealing with the embedding of one field into another.

Our study of field extensions will be considered in three parts: algebraic extensions, integral ring extensions and transcendental extensions. By initially studying algebraic extensions we will be able to introduce some of the more basic concepts and fundamental results to the project. Then, we will concentrate for a substantial period of time on the discussion of integral ring extensions, which will benefit us later on in our study of algebraic geometry and affine varieties.

Throughout each section covering extensions, we will always have the underlying goal of proving our main theorem. Therefore each section will finish with the formulation and proof of this theorem for each of the special cases. As we approach the end of section 5, we will encounter the corollary that will benefit us in our discussion of algebraic geometry.

In section 6 we shall introduce the language of affine varieties, which we shall use to ground our study in section 7. In our final section we shall reformulate Hilbert's Nullstellensatz. There are, in fact, two forms of the Nullstellensatz in the language of affine varieties. They are referred to as the weak and strong form. It is the strong form of the Nullstellensatz that will be the restatement of our theorem from our discussion of field extensions. Finally in this section we shall show how the notion of dimension and transcendence degree are linked.

2. Basic Definitions and Theorems of Field Extensions

We note that all content from this section has been adapted from [1]. We start by introducing some of the basic definitions and facts that we will require for this project.

Definition. Let E and F be fields, then if $E \subseteq F$ is a subfield of F we say F is an *extension* of E. This can be denoted by F/E but throughout this project we will use the notation $E \subseteq F$.

Example 2.1. We have the fields $\mathbb{R} \subseteq \mathbb{C}$ and hence the complex numbers are a field extension of the real numbers.

We can view the field F as a vector space over the field E. We say that the extension is either finite or infinite, depending on whether the vector space has finite or infinite dimension. We denote the dimension of the vector space by $[F : E]$ and call it the *degree* of the extension. This is a very coarse measure as to the size of the extension.

Given any integral domain R we can define a ring $R[X]$ called the *polynomial ring* of R. In this project we will be interested in the polynomial ring of a field E. We can define an element of the polynomial ring in the following way:-

Consider a sum over all possible n-tuples $\nu = (\nu_1, \dots, \nu_n)$, then define

$$f(x_1, \dots, x_n) = \sum_{\nu} a_{(\nu)} x_1^{\nu_1} \cdots x_n^{\nu_n}$$

for some $a_{(\nu)} \in R$. Hence $R[X]$ is simply the set of all polynomials with coefficients in R.

Definition. Let F be a field and $p(X) \in F[X]$ such that $\deg(p) \geqslant 1$. We say that $p(X)$ is *reducible over F* if there exists $f(X), g(X) \in F[X]$, with $\deg(f), \deg(g) \geqslant 1$, such that $p(X) = f(X)g(X)$. If no such factorisation exists then we say $p(X)$ is *irreducible over F*.

We note that it is important to state which field the polynomial is irreducible over. Hardly any polynomials are universally irreducible over all fields.

Example 2.2. We can see that $x^2 + 1 \in \mathbb{R}[X]$ is not reducible over the field $\mathbb{R}$. However, we have that

$$x^2 + 1 = x^2 - ix + ix + 1 = (x + i)(x - i).$$

Thus it is reducible over $\mathbb{C}$.

Definition. Let $E \subseteq F$ be a field extension. Then any element $\alpha \in F$ is said to be *algebraic over E* if there exists a non-zero polynomial $p(X) \in E[X]$ such that $p(\alpha) = 0$. If no such polynomial exists then we say α is *transcendental over E*.

Now that we have set up some of the fundamental definitions of our topic of discussion we move on to prove our first main theorem. However, before we do this we need to prove a small lemma about irreducible polynomials, (this has been taken from [2]).

Lemma 2.1. *Let F be a field and $\lambda \in F$ where $\lambda \neq 0$. We have that f is an irreducible polynomial over F $\Leftrightarrow$ λf is an irreducible polynomial over F.*

Proof. Assume $f(X)$ is reducible over F, then there exists $g(X), h(X) \in F[X]$ such that $f(X) = g(X)h(X)$. Hence f is reducible over F if and only if λf is reducible over F, because

$$\lambda f(X) = \big(\lambda g(X)\big)h(X).$$

Thus we have f irreducible over F if and only if λf is irreducible over F. □

The following theorem allows us to create a relationship between algebraic elements of a field and the polynomial rings in which they reside. This theorem and proof have been taken from [2].

Theorem 2.1. *Let $E \subseteq F$ be a field extension and $\alpha \in F$ be algebraic over E. Then there exists a unique polynomial $p(X) \in E[X]$ such that p is monic, irreducible over E and has α as a root.*

Proof. Let $\alpha \in F$ be algebraic over E, then there exists a polynomial $f(X) \in E[X]$ such that $f(\alpha) = 0$. Assume $f(X)$ is the smallest polynomial in $E[X]$ such that α is a root, (i.e. f has the least degree of all such polynomials in $E[X]$). We have that f must be irreducible over E. If not, then there exists a non-trivial factorisation of f, such as

$$f(X) = g(X)h(X),$$

where $g(X), h(X) \in E[X]$ and $\deg(g), \deg(h) < \deg(f)$. However $f(\alpha) = 0 \Rightarrow g(\alpha) = 0$ or $h(\alpha) = 0$ but if this is true then this invalidates the choice of f as the smallest such polynomial. Hence f is irreducible over E. Let $a_n \in E$ be the coefficient of the highest term in f and define $p(X) = \frac{1}{a_n}f(X)$. By Lemma 2.1, f irreducible over E implies $p(X)$ is irreducible over E. Now we have shown that there exists a polynomial such that it is monic, irreducible over E and has α as a root.

Assume that there exist two polynomials $f_1, f_2 \in E[X]$ satisfying these conditions. Then we have that $f_1(\alpha) = 0$ and $f_2(\alpha) = 0 \Rightarrow (f_1 - f_2)(\alpha) = 0$. However, because f_1, f_2 are monic, we must have that the $\deg(f_1 - f_2)$ is strictly less than either $\deg(f_1)$ or $\deg(f_2)$. This means the only possibility is that $f_1 = f_2 \Rightarrow p(X)$ is unique. □

We call the polynomial in Theorem 2.1 the *minimum polynomial* of α over E because it has the smallest degree of any such polynomial. We refer to a sequence of field extensions as a *tower*. For example, we may have

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n.$$

The idea of a tower will be important to us throughout our discussion of extensions and so we prove a small Lemma to do with the degree of a tower of extensions, (this has been taken from [2]).

Lemma 2.2 (The Tower Law)**.** *Let $E \subseteq F \subseteq L$ be a tower of field extensions. Then we have that*

$$[L : E] = [L : F][F : E].$$

Proof. Let $\{x_1, \ldots, x_n\}$ be a basis for the vector space F over E and $\{y_1, \ldots, y_m\}$ be a basis for the vector space L over F. Let a be any element of L then, because L is a vector space over E, we can express a as

$$a = \sum_{i=1}^{m} \alpha_i y_i,$$

with the coefficients $\alpha_i \in F$. Now F forms a vector space over E, hence each element $\alpha_i \in F$ can be expressed as

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} x_j,$$

for some $\beta_j \in E$. Thus this gives us that a can be expressed as

$$a = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} x_j y_i.$$

Hence we have that the field L is spanned by the set $\{x_j y_i\}$. Are these elements linearly independent? Let $\gamma_{ij} \in E$, then we have

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \gamma_{ij} x_i y_j = 0 \Rightarrow \sum_{i=1}^{n} \gamma_{ij} x_i = 0 \Rightarrow \gamma_{ij} = 0$$

for all i, j because of the linear independence of $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$. Thus the set $\{x_i y_j\}$ form a basis for the vector space L over E, proving our result. □

We carry on with our discussion of basic theorems by developing more theory behind the polynomial ring. Specifically we wish to develop some special results for when R is a field. We are aiming to show that if f is an irreducible polynomial over F then $F[X]/\langle f \rangle$ is a field, where $\langle f \rangle$ is the *principal ideal* generated by f. The following Lemma and proof have been taken from [4].

Lemma 2.3. *Let F be a field, then every ideal in $F[X]$ is principal.*

Proof. Let $I \subseteq F[X]$ be an ideal. Take $f(X) \in I$ to be the polynomial with smallest degree in I. Then given any other $g(X) \in I$ we have by the division algorithm, (see Section 4, Chapter V of [1]), that there exists $q(X), r(X) \in F[X]$, with $\deg(r) < \deg(f)$ or $r(X) = 0$, such that

$$g(X) = q(X)f(X) + r(X).$$

If $r(X) = 0$ then we have $g(X) = q(X)f(X)$ and hence any element of I can be expressed as a multiple of f, which implies $I = \langle f \rangle$. If $r(X) \neq 0$ then we have

$$r(X) = g(X) - q(X)f(X) \in I,$$

by the ideal properties. However $\deg(r) < \deg(f)$ and this invalidates the choice of f as the polynomial in I with smallest degree. Thus I must be a principal ideal generated by the polynomial with smallest degree. □

Definition. Let R be a ring and $I \neq R$ an ideal of R. We say I is a *maximal ideal* if given any other ideal J of R such that $I \subseteq J \subseteq R$, then $J = I$ or $J = R$.

The following proof and Theorem have been taken from [4].

Theorem 2.2. *Take any ring R and let $I \subseteq R$ be an ideal. Then the quotient ring R/I is a field if and only if I is a maximal ideal.*

Proof. We have that R/I is a field if and only if the only ideals are $\{0 + I\}$ and R/I. By the correspondence theorem for ideals, (see Section 2.2.3 of [6]), we have R/I has no proper ideals if and only if there does not exist an ideal $J \neq R$ with $I \subseteq J \subseteq R$. This is equivalent to saying I is a maximal ideal. □

Now we have proved our result in the more general case of a ring, the result we desire comes out as a small corollary. The proof of the following Corollary has been taken from [2].

Corollary 2.1. *Given a field F and a polynomial $f \in F[X]$, we have that the quotient ring $F[X]/\langle f\rangle$ is a field $\Leftrightarrow$ f is irreducible over F. Consequently $F[X]/\langle f\rangle$ is a field extension of F.*

Proof. We start by showing that $\langle f\rangle$ is a maximal ideal if and only if f is irreducible over F. Assume $\langle f\rangle$ is maximal then if there exists $h(X) \in F[X]$ such that $h \mid f$ then we have that $\langle f\rangle \subseteq \langle h\rangle$ but by the maximality of $\langle f\rangle$ we must have $\langle h\rangle = \langle f\rangle$ or $\langle h\rangle = F[X]$, i.e. $h = f$, or h is a constant. Assume f is irreducible over F and that there exists an ideal $\langle g\rangle$, such that $\langle f\rangle \subseteq \langle g\rangle \subseteq F[X]$. We must have that $g \mid f$ but f is irreducible and so $g = \lambda$, a constant, or $g = \lambda f$. However $\langle \lambda f\rangle = \langle f\rangle$ and $\langle \lambda\rangle = F[X]$ and so $\langle f\rangle$ is a maximal ideal.

Hence by combining the above and Theorem 2.2 we get that $F[X]/\langle f\rangle$ is a field $\Leftrightarrow$ f is irreducible over F. Now we notice that there exists an isomorphic copy of F in $F[X]/\langle f\rangle$, because any element $a \in F$ can be expressed uniquely as $a + \langle f\rangle$ in $F[X]/\langle f\rangle$. Hence F is a subfield of $F[X]/\langle f\rangle$ and so is a field extension. □

Example 2.3. Consider the polynomial ring $\mathbb{R}[X]$ and the irreducible polynomial $x^2 + 1$ over $\mathbb{R}$. By our theorem we have that $\mathbb{R}[X]/\langle x^2 + 1\rangle$ is a field. Any element of this field will be of the form $g(X) + \langle x^2 + 1\rangle$, where $g(X) = ax + b$ with $a, b \in F$. If $g(X)$ has degree greater than or equal to 2, then use the division algorithm, (see Chapter 4, Section V of [1]), to divide through by $x^2 + 1$. Thus given any non-zero $(ax + b) + \langle x^2 + 1\rangle$ we claim the the element,

$$\left(-\frac{a}{a^2 + b^2}x + \frac{b}{a^2 + b^2}\right) + \langle x^2 + 1\rangle \in \mathbb{R}[X]/\langle x^2 + 1\rangle,$$

is its inverse. We check this using the standard multiplication in the quotient ring.

$$\begin{aligned}\Big(ax+b\Big)\Big(-\frac{a}{a^2+b^2}x+\frac{b}{a^2+b^2}\Big)+\langle x^2+1\rangle &= \frac{1}{a^2+b^2}(-a^2x^2+\cancel{abx}-\cancel{abx}+b^2)+\langle x^2+1\rangle,\\ &= \frac{1}{a^2+b^2}(-a^2x^2-a^2+a^2+b^2)+\langle x^2+1\rangle,\\ &= -\frac{a^2}{a^2+b^2}(x^2+1)+\frac{a^2+b^2}{a^2+b^2}+\langle x^2+1\rangle,\\ &= 1+\langle x^2+1\rangle.\end{aligned}$$

So, every non-zero element has an inverse and hence $\mathbb{R}[X]/\langle x^2+1\rangle$ is a field.

Looking at the above, we notice that the elements $ax+b$ and $\frac{1}{a^2+b^2}(-ax+b)$ bear a striking resemblance to the complex number $b+ai$ and its multiplicative inverse $\frac{1}{||b+ai||}(b-ai)$. In fact, this striking resemblance is not a coincidence. It is possible to prove that

$$\mathbb{R}/\langle x^2+1\rangle \cong \mathbb{C},$$

which can be seen in any book on classical Galois theory.

3. Algebraic Extensions

In this section we will develop the theory of algebraic extensions in order to prepare us for the section concerning transcendental extensions. Primarily, we will be dealing with the notion of algebraic closure. Please note, all elements of this section have been adapted from [1], unless otherwise stated. We start by defining some general terminology.

Definition. A field extension F of E is said to be *algebraic* if every element of the field F is algebraic over E.

Definition. Let $E \subseteq F$ be a field extension and α an element of F. Then we write $E(\alpha)$ to represent the smallest field containing both E and α. We say that α is *adjoined* to E.

The above definition is taken from [2]. It is important for us to consider how the property of being algebraic is maintained throughout a tower of extensions. To do this we consider the relationship between finite and algebraic extensions.

Proposition: *Let $E \subseteq F$ be a finite field extension. Then we must have that F is algebraic over E.*

Proof. We have that the dimension of F as a vector space over E is finite. Thus, the powers of β are linearly dependent, and hence there exists an equation

$$a_0 + a_1\beta + \cdots + a_n\beta^n = 0,$$

such that $a_i \in E$ and not all $a_i = 0$. Thus β is algebraic over E, and so F is algebraic over E. □

The following Lemma and proof have been taken from [2].

Lemma 3.1. *Let α be algebraic over a field E. Then we have that $E(\alpha) = E[\alpha]$ and $E(\alpha)$ is finite over E. The degree $[E(\alpha) : E]$ is equal to the degree of the minimum polynomial of α.*

Proof. Let $p(X) \in E[X]$ be the minimum polynomial of α. Pick any polynomial $f(X) \in E[X]$ such that $f(\alpha) \neq 0$ then we have $p(X) \nmid f(X)$. Hence by the division algorithm we have that there exists polynomials $g(X), h(X) \in E[X]$ such that

$$g(X)f(X) + h(X)p(X) = 1.$$

However because $p(\alpha) = 0$ we get $g(\alpha)f(\alpha) = 1$ and hence $f(\alpha)$ has an inverse in $E[\alpha]$. Thus $E[\alpha]$ is not only a ring but a field. We now want to show that $E[\alpha]$ is smallest among all such fields that contain E and α. Assume that $E[\alpha]$ is not the smallest field containing both E and α then we certainly have that $E(\alpha) \subseteq E[\alpha]$. Now $E(\alpha)$ contains α and all elements of E and because $E(\alpha)$ is a field it must contain any polynomial $f(\alpha)$ with coefficients in E. This gives us that $E[\alpha] \subseteq E(\alpha) \Rightarrow E(\alpha) = E[\alpha]$, as required.

Let $d = \deg(p)$ then the powers of α

$$1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$$

are linearly independent over E. If this is not so then we will have

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} = 0$$

for some non-zero $f(X) \in E[X]$. Because $p(X)$ is the minimum polynomial of α, we can see $p(X) \mid f(X)$ but $\deg(f) < \deg(p)$, which is a contradiction. We claim that the set $V = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ forms a basis for $E[\alpha]$ as a vector space over E. Let $g(X) \in E[X]$, then we have $g(\alpha) \in E[\alpha]$. By the division algorithm, there exist polynomials $q(X), r(X) \in E[x]$, with $\deg(r) < d$, such that

$$g(X) = q(X)p(X) + r(X).$$

However, this gives us that $g(\alpha) = r(\alpha)$ and hence every element in $E[\alpha]$ can be expressed using only the elements of V, because $\deg(r) < d$. Thus V forms a basis for $E[\alpha] = E(\alpha)$ as a vector space over E and hence $[E(\alpha) : E] = d$, as required. □

Lemma 3.2. *Let $F = E(a_1, \ldots, a_n)$ be a finitely generated extension of a field E. Assume that each a_j $(j = 1, \ldots, n)$ is algebraic over E, then we must have that F is algebraic over E.*

Proof. Consider the extension $E \subseteq F$ as a tower of extensions

$$E \subseteq E(a_1) \subseteq E(a_1, a_2) \subseteq \cdots \subseteq E(a_1, \ldots, a_n) = F.$$

Each step in this tower is generated by adjoining one extra element to the field before it. By Lemma 2.2 we have that the degree $[F : E]$ is

$$[F : E] = [F : E(a_1, \ldots, a_{n-1})][E(a_1, \ldots, a_{d-1}) : E(a_1, \ldots, a_{d-2})] \ldots [E(a_1) : E].$$

By Lemma 3.1 above we have that each one of these degrees is equal to the minimum polynomial of some a_i over the field $E(a_1, \ldots, a_{i-1})$, i.e. each degree is finite. Then this gives us that $[F : E]$ is finite and by the very first proposition of this section we have F is algebraic over E. □

Theorem 3.1. *Given a tower of field extensions $E \subseteq F \subseteq K$ we have that K is algebraic over $E \Leftrightarrow F$ is algebraic over E and K is algebraic over F.*

Proof. Start by assuming that K is algebraic over E, then given any element $\alpha \in K$ there exists a polynomial $p(X) \in E[X]$, such that $p(\alpha) = 0$. Now $F \subseteq K$ and hence F is algebraic over E. Also $E \subseteq F$, hence $p(X) \in E[X] \Rightarrow p(X) \in F[X]$ and so K is algebraic over F.

Now assume that K is algebraic over F and F is algebraic over E. We want to show that K is algebraic over E. Let $\alpha \in K$ then $0 \neq f(X) \in F[X]$ exists, such that

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0.$$

Consider the field $F' = F(a_n, \ldots, a_0)$. Then F' is a finitely generated extension of E and each a_j is algebraic over E. Thus by Lemma 3.2 we have F' is algebraic over E. We have a tower of extensions

$$E \subsetneq F' \subsetneq F'(\alpha),$$

where $F'(\alpha)$ is a finite extension of E and hence is algebraic over E. Hence α is algebraic over E and so any element of K is algebraic over E, as required. □

We note that we refer to an *embedding* as a ring homomorphism which induces an isomorphism on its image. Any injective homomorphism will do so, and hence when we refer to an embedding we think of an injective homomorphism. In this section we will primarily be developing theorems about algebraic closure by looking at embeddings from one field to another.

The major result that we are leading up to is to show that any field is in fact a subfield of an *algebraically closed* field. We say a field E is algebraically closed when given any polynomial $f(X) \in E[X]$ with $\deg(f) \geqslant 1$ then $f(X)$ has a root in E. On the road to this theorem we start with a small proposition, which has been taken from [2].

Proposition: *Let E be a field and $f(X)$ a polynomial in $E[X]$ with $\deg(f) \geqslant 1$. Then there exists a field extension F of E such that f has a root in F.*

Proof. Assume that f is an irreducible polynomial. If f is not an irreducible polynomial then factorise f as $f = gh$, where g is irreducible, and continue with g. Consider the field $E[X]/\langle f\rangle$, i.e. the field of left cosets of the ideal $\langle f\rangle$ in $E[X]$. Elements of this field take the form $g(X) + \langle f\rangle$, where $\deg(g) < \deg(f)$. Now let us assume $f(X)$ has the form

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

where each $a_i \in E$. Now $f(X)$ has an isomorphic copy of itself in the field $E[X]/\langle f\rangle$ and it takes the form

$$f(X) = (a_0 + \langle f\rangle) + (a_1 + \langle f\rangle)X + (a_2 + \langle f\rangle)X^2 + \cdots + (a_n + \langle f\rangle)X^n.$$

We want to show that $f(X)$ has a root in the field $E[X]/\langle f\rangle$, which is an extension of the field E. Consider $X + \langle f\rangle$ as a possible root of f. This gives us

$$\begin{aligned} f(X + \langle f\rangle) &= (a_0 + \langle f\rangle) + (a_1 + \langle f\rangle)(X + \langle f\rangle) + \cdots + (a_n + \langle f\rangle)(X + \langle f\rangle)^n, \\ &= (a_0 + \langle f\rangle) + (a_1X + \langle f\rangle) + \cdots + (a_nX^n + \langle f\rangle), \\ &= (a_0 + a_1X + \cdots + a_nX^n) + \langle f\rangle, \\ &= f + \langle f\rangle, \\ &= \langle f\rangle. \end{aligned}$$

We note that in the field $F[X]/\langle f\rangle$ the zero element is $\langle f\rangle$ and hence f has a root in $F[X]/\langle f\rangle$. □

Corollary 3.1. *Let E be a field and $f_1(X), \ldots, f_n(X)$ be polynomials in $E[X]$ with $\deg(f_i) \geqslant 1$. Then there exists a field extension $E \subseteq F$ such that every f_i has a root in F.*

Proof. We prove this by induction. We have that for one polynomial $f_1(X)$ that the result is true by the above proposition. Assume that there exists a field extension $E \subseteq F'$ such that the polynomials $f_1(X), \ldots, f_r(X)$ have a root in F'. Consider a polynomial $f_{r+1}(X) \in E[X]$, such that $f_{r+1} \notin \{f_1, \ldots, f_r\}$ and $\deg(f_{r+1}) \geqslant 1$. Then by the proof of the above proposition, we can see that f_{r+1} will have a root in the field $F'[X]/\langle f_{r+1}\rangle$. Clearly $E \subseteq F' \subseteq F'[X]/\langle f_{r+1}\rangle$ is a field extension of E, and so $F'[X]/\langle f_{r+1}\rangle$ contains a root for each f_i, (with $1 \leqslant i \leqslant r+1$). Hence our result is proved. □

Theorem 3.2. *Given any field E there exists a field extension $E \subseteq F$, such that F is algebraically closed.*

Proof. We wish to construct a field which is algebraically closed, i.e. given any $f(X) \in F[X]$ there exists an element $\alpha \in F$ such that $f(\alpha) = 0$. Now consider the polynomial ring $E[X]$ and the ideal generated by all polynomials $f(X) \in E[X]$ with $\deg(f) \geqslant 1$. Call this ideal I. We can see that $I \neq E[X]$. If $I = E[X]$ then there exists a finite number of elements $f_1, \ldots, f_n \in I$ and $g_1, \ldots, g_n \in E[X]$ such that $g_1 f_1 + \cdots + g_n f_n = 1$, which is not possible.

Hence there exists a maximal ideal $\langle h\rangle$ such that $I \subseteq \langle h\rangle$ and $E[X]/\langle h\rangle$ is a field extension of E. We can see that for any polynomial $f \in E[X]$, with $\deg(f) \geqslant 1$, we will have $\langle f\rangle \subseteq \langle h\rangle$. Hence, by the same reasoning as in our previous proposition, f will have a root in $E[X]/\langle h\rangle$. By repeating this argument we can inductively create a sequence of fields

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n \subseteq \cdots,$$

in which every polynomial $f(X) \in E_n[X]$, with $\deg(f) \geqslant 1$, has a root in E_{n+1}. Now let $F = \cup_{i=1}^{\infty} E_i$, which we can show produces a field. Take $x, y \in F$, then for some n sufficiently large we have $x, y \in E_n$. Performing the operations xy and $x + y$ in E_n then gives us $xy \in F$ and $x + y \in F$. Given any polynomial $f(X) \in F$ we must have, for some sufficiently large n, that $f(X) \in E_n[X]$, and hence $f(X)$ has a root in E_{n+1}, (which implies $f(X)$ has a root in F). Therefore, F is algebraically closed, as required. □

Corollary 3.2. *Let E be a field, then there exists a field extension $E \subseteq \overline{E}$, which is algebraically closed and algebraic over E.*

Proof. Start by constructing an extension $E \subseteq F$ which is algebraically closed. Now consider all extensions of E contained in F

$$E \subseteq F_i \subseteq F,$$

such that F_i is algebraic over E. Now define $\overline{E} = \cup_{i=1}^{\infty} F_i$, (i.e. the union of all algebraic subextensions of F). Let $\alpha \in \overline{E}$ then we have that α is algebraic over E, (because α resides in some F_i), and hence $\overline{E}$ is algebraic over E. We now want to show that $\overline{E}$ is algebraically closed. Let $f(X) \in \overline{E}[X] \subseteq F[X]$, then $f(X)$ has a root $\alpha \in F$ because F is algebraically closed. We have a tower of extensions $E \subseteq \overline{E} \subseteq F$ where α is algebraic over $\overline{E}$ and, by Theorem 3.1, α is algebraic over E. Now we must have $\alpha \in F_i$ for some i and so $\alpha \in \overline{E}$. Hence $\overline{E}$ is algebraically closed and algebraic over E. □

Example 3.1. If we consider the field of real numbers, then the complex numbers are an extension of $\mathbb{R}$ that contain a root for each $p(X) \in \mathbb{R}[X]$, by the Fundamental Theorem of Algebra. Also, given any complex number $xi + y$ we can find a polynomial $p(X) \in \mathbb{R}[X]$, such that $p(xi+y) = 0$. Hence $\mathbb{R} \subseteq \mathbb{C}$ is an algebraically closed extension which is algebraic over $\mathbb{R}$.

On reflection, we can appreciate that the above proofs required little input from fields and are, in fact, more set-theoretic in nature. All the results, that were used above had been proven in small Lemmas and Propositions earlier in the section.

In connection with this we now move on to proving a theorem about extending embeddings $\sigma : E \to L$ to algebraic extensions F of E. We will look to prove a similar result when considering transcendental extensions of a field.

Theorem 3.3. *Let E be a field and F an algebraic extension of E. Consider an embedding $\sigma : E \to L$ into some algebraically closed field L. Then there exists an extension of σ into an embedding F in L. If F is algebraically closed and L is algebraic over $\sigma(E)$, then any such extension of σ is an isomorphism of E into L.*

Proof. We wish to create a set S of totally ordered pairs. Start by considering all subfields of F which contain E, i.e. the tower of extensions

$$E \subseteq F_i \subseteq F.$$

With each of these subfields assign a corresponding embedding $\tau_i : F_i \to L$. We now take all such pairs (F_i, τ_i) and form a totally ordered set $S = \big\{(F_i, \tau_i)\big\}$. We say that $(F_i, \tau_i) \leqslant (F_j, \tau_j)$ if $F_i \subseteq F_j$ and $\tau_j|_{F_i} = \tau_i$. We can see that $S \neq \emptyset$ because by the initial statement of the theorem we have $(E, \sigma) \in S$.

Define $F' = \cup_{i=1}^{\infty} F_i$ and τ' such that for any F_j we have $\tau'|_{F_j} = \tau_j$. Now clearly (F', τ') is an upper bound of our set and so we have a chain of ordered pairs

$$(E, \sigma) \leqslant (F_1, \tau_1) \leqslant (F_2, \tau_2) \leqslant \cdots \leqslant (F', \tau').$$

By Zorn's Lemma there must exist a maximal element (K, λ) of S. We claim $K = F$ and hence there exists $\lambda : F \to L$, an extension of σ as required. If $K \neq F$ then there exists an element $\alpha \in F$ such that $\alpha \notin K$.

We consider the field $K(\alpha) = K[\alpha]$. Now F is algebraic over E and hence there exists a minimum polynomial $p(X) \in E[X]$ such that $p(\alpha) = 0$. We know L is algebraically closed and $\lambda(p) \in L[X]$ hence there exists a root $\beta \in L$ of $\lambda(p) = p^{\lambda}$. Note that we define $p^{\lambda}(X)$ in the following way

$$p^{\lambda}(X) = \lambda\big(p(X)\big) = \lambda(a_0 + a_1 X + \cdots + a_n X^n) = \lambda(a_0) + \lambda(a_1)X + \cdots + \lambda(a_n)X^n.$$

Let $f(\alpha)$ be an element of $K(\alpha)$ and define an extension of λ by mapping $f(\alpha) \to f^{\lambda}(\beta)$. We check that this is well defined. Let $g(\alpha) \in K(\alpha)$ then if $g(\alpha) = f(\alpha)$ we must have $g(\alpha) - f(\alpha) = 0 \Rightarrow p(X) \mid \big(g(X) - f(X)\big)$. This gives us that

$$p^{\lambda}(X) \mid (g-f)^{\lambda}(X) \Rightarrow g^{\lambda}(\beta) - f^{\lambda}(\beta) = 0 \Rightarrow g^{\lambda}(\beta) = f^{\lambda}(\beta).$$

Hence the extension of λ is well defined. We can see that the restriction of our extension to K is λ. However this pair $(K(\alpha), \lambda')$ is an element of S and so invalidates the maximality of (K, λ). Thus we must have $K = F$ and λ is an extension of σ to F.

Let F be algebraically closed and L be algebraic over $\sigma(E)$, then $\sigma(F)$ is algebraically closed and L is algebraic over $\sigma(F)$. Hence $L = \sigma(F)$. □

As a consequence of this theorem we have that any two algebraically closed and algebraic extensions of E are isomorphic, (see Section 2, Chapter VII of [1]). Thus, we consider the $\overline{E}$ in Corollary 3.2 to be unique up to isomorphism and refer to it as the *algebraic closure* of E.

4. Integral Ring Extensions

All rings in this section will be commutative and have a unit element 1.

Please note, all elements of this section have been adapted from [1], unless otherwise stated. Having spent time introducing algebraic field extensions, we now need to focus on a more general idea. By looking at the concept of integral ring extensions we can aim to generalise the result of Theorem 3.3 from the above section. Integral elements of rings are very similar to algebraic elements in field. We need this study of ring extensions to help prove our main result for transcendental field extensions and start by introducing the definition of an integral element.

Definition. Let B be a ring and A a subring of B. We say an element $\alpha \in B$ is *integral over A* if there exists a polynomial

$$p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X],$$

such that $p(\alpha) = 0$. The way that this definition differs from the notion of an algebraic element is that the polynomial $p(X)$ must be *monic*, i.e. the leading coefficient is 1.

We note that there are two equivalent statements of the definition of integrality. We say $\alpha \in B$ is integral over A if:

- the subring $A[\alpha]$ is a finitely generated A-module,
- there exists a finitely generated A-module M such that, for any $a \in A[\alpha]$, $aM = 0 \Rightarrow a = 0$.

(We will not prove the equality of these statements here but they can be found in Chapter 9, Section 1 of [1].)

If we let A be a subring of a ring B, then we say B is integral over A if every element of B is integral over A. By an *integral domain* we refer to a ring which has no zero divisors. So, if A is an integral domain and $a, b \in A$ such that $ab = 0$ then $a = 0$ or $b = 0$.

Proposition: *Let A be an integral domain and K its associated quotient field. If $\alpha \in A$ is algebraic over E then there exists a non-zero element $c \in A$, such that $c\alpha$ is integral over A.*

Proof. We have that α is algebraic over K and hence there exists some $p(X) \in K[X]$ such that

$$p(\alpha) = k_n\alpha^n + k_{n-1}\alpha^{n-1} + \cdots + k_0 = 0$$

and $k_n \neq 0$. We have that K is a field and thus k_n has an inverse element k_n^{-1}. Multiply $p(\alpha)$ through by k_n^{n-1} to get

$$k_n^{n-1}(k_n\alpha^n) + k_n^{n-1}(k_{n-1}\alpha^{n-1}) + \cdots + k_n^{n-1}k_0 = 0,$$
$$(k_n\alpha)^n + k_{n-1}(k_n\alpha)^{n-1} + \cdots + k_n^{n-1}k_0 = 0.$$

Each $k_i \in K$ is of the form $\frac{a_i}{b_i}$ for some $a_i \in A$ and non-zero $b_i \in A$. Consider the product $b = b_n \cdots b_0$, which is a non-zero element of A. Multiplying the above equation through by b^n gives us

$$(bk_n\alpha)^n + bk_{n-1}(bk_n\alpha)^{n-1} + \cdots + b^n k_n^{n-1} k_0 = 0.$$

Hence each coefficient of the above polynomial is in A and $c = bk_n$ is a non-zero element of A. So $c\alpha$ is integral over A as required. □

Lemma 4.1. *Let A be a subring of a ring B such that B is integral over A. If B is finitely generated as an A-algebra then B is finitely generated as an A-module.*

Proof. We note that given any subring A of a ring B we will always have that B is an A-algebra. So, if B is a finitely generated A-algebra then let $w_1, \dots, w_n$ be the generators of B. Now as $\{w_1, \dots, w_n\}$ is a subset of B we have that each w_i is integral over A. Consider the following tower

$$A \subseteq A[w_1] \subseteq A[w_1, w_2] \subseteq \cdots \subseteq A[w_1, \dots, w_n] = B.$$

We start by showing that if w_1 is integral over A then we have $A[w_1]$ is a finitely generated A-module. Let w_1 be integral over A then w_1 solves some monic polynomial $p(X) \in A[X]$, with $\deg(p) \geqslant 1$. Let p be such a polynomial with least degree in $A[X]$. Now consider any polynomial $f(X) \in A[X]$ with $\deg(f) \geqslant 1$. We have by the factor theorem that

$$f(X) = g(X)p(X) + r(X),$$

with $\deg(r) < \deg(p)$ or $r(X) = 0$. If $r(X) = 0$ then $f(w_1) = 0 \Rightarrow f(X) = p(X)$, otherwise $f(w_1) = r(w_1)$. If we have $\deg(p) = n$ then the elements $1, w_1, \dots, w_1^{n-1}$ clearly generate $A[w_1]$. Hence $A[w_1]$ is a finitely generated A module.

Now we can see from the tower above that B will be a finitely generated A-module. This is because each step of the tower is finitely generated. □

Proposition: *Let A, B be subrings of a ring C such that A is a subring of B. Now we have that C is integral over A if and only if C is integral over B and B is integral over A.*

Proof. Assume that C is integral over A. Now $\alpha \in C \Rightarrow \alpha \in B$ and hence B is clearly integral over A. Also $p(X) \in A[X] \Rightarrow p(X) \in B[X]$ and so C is clearly integral over B. Now assume C is integral over B and B is integral over A. Given an element $\beta \in C$ we have that there exists a monic polynomial in $B[X]$ such that

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_0 = 0.$$

Consider the ring $B' = A[b_{n-1}, \dots, b_0]$, then we have A is a subring of B' and hence B' forms a finitely generated A-algebra. Also each element of B' is integral over A and hence by Lemma 4.1 we have that B' is a finitely generated A-module. It's clear that given any element $a \in B'[\beta]$ then $aB' = 0$ only if $a = 0$.

Now $\beta B' \subseteq B'$ and so we must have that β is integral over A by the alternate definition of integrality. Thus C is integral over A, as required. □

We now consider ring-homomorphisms and the notion of integral elements. As homomorphisms are structure preserving functions we would like to assume that they would also preserve integral elements.

Lemma 4.2. *Let A be a subring of a ring B such that B is integral over A. If $\sigma : A \to B$ is a ring homomorphism then $\sigma(B)$ is integral over $\sigma(A)$.*

Proof. Let $\alpha \in B$ then we have that there exists some monic polynomial with coefficients $a_i \in A$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

Now applying the homomorphism to the above equation we have that

$$\begin{aligned} \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) &= 0, \\ \sigma(\alpha^n) + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \cdots + \sigma(a_0) &= 0, \\ \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(a_0) &= 0. \end{aligned}$$

Thus $\sigma(\alpha) \in \sigma(B)$ is integral over $\sigma(A)$ as each $\sigma(a_i) \in \sigma(A)$. So, ring homomorphisms preserve the property of being integral. □

In the light of ring homomorphisms, it is going to be useful for us to adapt our idea of being integral. If $f : A \to B$ is a ring homomorphism then we can consider B as an A-module by defining the map

$$a \cdot b = f(a)b.$$

Now we can see that this will allow us to satisfy the axioms of an A-module, which we detail below. Let $a, b \in A$ and $x, y \in B$, then we have

- $a \cdot (x + y) = f(a)(x + y) = f(a)x + f(a)y = a \cdot x + a \cdot y$,
- $(a + b) \cdot x = f(a + b)x = \big(f(a) + f(b)\big)x = f(a)x + f(b)x = a \cdot x + b \cdot x$,
- $(ab) \cdot x = f(ab)x = f(a)\big(f(b)x\big) = a \cdot (b \cdot x)$,
- $1 \cdot x = x$ (trivially).

In fact B will form an A-algebra if $f(A)$ lies in the centre of B, i.e. $f(a)b = bf(a)$ for all $a \in A$ and $b \in B$. However, all rings in this section are commutative and hence $f(A)$ does lie in the centre of B. This gives us that for $a \in A$ and $x, y \in B$ we have

$$\begin{aligned} x(a \cdot y) &= x\big(f(a)y\big) = f(a)(xy) = a \cdot (xy), \\ (a \cdot x)y &= \big(f(a)x\big)y = f(a)(xy) = a \cdot (xy). \end{aligned}$$

Hence given any two rings, A and B, together with a ring homomorphism $f : A \to B$, we see that B forms an A-algebra. Now we extend the definition of being integral by saying that f is integral if B is integral over $f(A)$.

From a previous proposition we know that a tower of ring extensions is integral if and only if every step in the tower is integral. Now assume $A \subseteq B \subseteq C$ is a tower of ring extensions.

Let $f : A \to B$ and $g : B \to C$ be integral ring homomorphisms then $g \circ f : A \to C$ is also integral. We note however that if $g \circ f$ is integral then this does not imply that f is integral.

Given any ring A and a submonoid, under multiplication, of A, (say S), we can form the *quotient ring* of A by S. We do this by defining an equivalence relation for pairs $(a, s) \in A \times S$. We say that if $(a, s) \sim (a', s')$ then there exists an element $t \in S$, such that

$$t(as' - a's) = 0. \tag{1}$$

We denote the equivalence class containing a pair (a, s) by $\frac{a}{s}$ and the quotient ring itself by $S^{-1}A$. We define multiplication and addition in the quotient ring by the standard notation of fractions

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'},$$
$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'}.$$

By defining $0_{S^{-1}A} = \frac{0}{1}$ and $1_{S^{-1}A} = \frac{1}{1}$ we can see that the above operations will give $S^{-1}A$ a ring structure. It can be shown using the relation above that these are, in fact, well-defined relationships.

If A is an integral domain and S is the set of all non-zero elements in A, then we have that $S^{-1}A$ is a field, which we refer to as the *quotient field* of A. For any given non-zero element $\frac{a}{s} \in S^{-1}A$ then

$$\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{sa} = 1.$$

We can see that this satisfies (1) because by letting $t = 1$ we have $as \cdot 1 - sa \cdot 1 = 0$. Also $\frac{s}{a} \in S^{-1}A$ because $a \neq 0$ and so $S^{-1}A$ is a field.

Example 4.1. Given our classic example of a ring $\mathbb{Z}$, we can clearly see that $\mathbb{Q}$ is its associated quotient field.

Our next step is to consider the integral relationship between two rings and their quotient rings. Let $f : A \to B$ be an integral ring homomorphism and S a multiplicative submonoid of A. We can define a homomorphism between $S^{-1}A$ and $S^{-1}B$, say $S^{-1}f : S^{-1}A \to S^{-1}B$ by letting

$$(S^{-1}f)\left(\frac{a}{s}\right) = \frac{f(a)}{f(s)}$$

for all $(a, s) \in A \times S$. When we refer to S in $S^{-1}B$ we strictly mean the image of S under f, i.e. $\big(f(S)\big)^{-1}B$. It is clear that the homomorphic property of f will endow $S^{-1}f$ with the same property. Thus we have a commutative diagram

$$\begin{tikzcd}
B \arrow[r, "\tau"] & S^{-1}B \\
A \arrow[u, "f"] \arrow[r, "\tau"'] & S^{-1}A \arrow[u, "S^{-1}f"']
\end{tikzcd}$$

where τ is the canonical transformation $\tau(x) = \frac{x}{1}$ for $x \in A$ or B. We now wish to show that the property of being integral is preserved by $S^{-1}f$.

Lemma 4.3. *Let $f : A \to B$ be an integral ring extension and S a multiplicative submonoid of A. Then $S^{-1}f : S^{-1}A \to S^{-1}B$ is also integral.*

Proof. We have f is integral and so given some $\alpha \in B$ we see that α solves a monic polynomial in $f(A)[X]$, say

$$\alpha^n + f(a_{n-1})\alpha^{n-1} + \cdots + f(a_0) = 0.$$

If we apply the map τ to the above equation we find that

$$\left(\frac{\alpha}{f(1)}\right)^n + \frac{f(a_{n-1})}{1}\left(\frac{\alpha}{f(1)}\right)^{n-1} + \cdots + \frac{f(a_0)}{1} = 0,$$

noting that $f(1) = 1$ because f is a ring homomorphism. Each coefficient of the above polynomial lies in $S^{-1}A$ and hence $\frac{\alpha}{1}$ is integral over $S^{-1}A$. Letting s be any element of S then we multiply the above equation by $\frac{1}{f(s)^n}$ to get

$$\left(\frac{\alpha}{f(s)}\right)^n + \frac{f(a_{n-1})}{f(s)}\left(\frac{\alpha}{f(s)}\right)^{n-1} + \cdots + \frac{f(a_0)}{f(s)^n} = 0.$$

Each coefficient in the above polynomial lies in $(S^{-1}f)(S^{-1}A)$ and so $\frac{\alpha}{f(s)} \in S^{-1}B$ is integral over $(S^{-1}f)(S^{-1}A)$. Thus, $S^{-1}f$ is an integral ring homomorphism as required. □

Lemma 4.4 (Nakayama's Lemma)**.** *Let A be a ring and I an ideal of A which is contained in all maximal ideals of A. If M is a finitely generated A-module and $IM = M$ then $M = 0$.*

Proof. We assume that M is finitely generated and $IM = M$. Let $\{w_1, \ldots, w_n\}$ be a set of generators for M. Now as $IM = M$ it follows that each of the generators, say w_1, has the following expression

$$w_1 = \alpha_1 w_1 + \cdots + \alpha_n w_n,$$

for some $\alpha_j \in I$. Rearranging gives us that

$$(1 - \alpha_1)w_1 = \alpha_2 w_2 + \cdots + \alpha_n w_n \tag{2}$$

and we argue that $1 - \alpha_1$ must be a unit. If $1 - \alpha_1$ is not a unit then it is contained in some maximal ideal J of A. As I is contained in all maximal ideals of A we have that

$\alpha_1 \in J \Rightarrow 1 \in J$ by the ideal property of J. This is a contradiction and so $1-\alpha_1$ is a unit, thus we can multiply (2) by the inverse of $1-\alpha_1$. This implies that M can be generated by $n-1$ elements and so $M = 0$. □

Throughout this section, our aim has been to generalise Theorem 3.3 from the previous section to integral ring extensions. We need to look now at prime ideals and see how they affect integral rings. By looking at prime ideals of rings, we can consider local rings and then reduce some of our problems. We say an ideal $\mathfrak{p} \neq A$ is a prime ideal of a ring A if $A/\mathfrak{p}$ is an integral domain. Equivalently we say $\mathfrak{p} \neq A$ is a prime ideal of A if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We can see this is true, as $A/\mathfrak{p}$ is an integral domain

$$\begin{aligned}
&\Leftrightarrow (a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p},\\
&\Leftrightarrow (a+\mathfrak{p}) = \mathfrak{p} \text{ or } (b+\mathfrak{p}) = \mathfrak{p},\\
&\Leftrightarrow\ a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.
\end{aligned}$$

Now let A be a ring and $\mathfrak{p}$ a prime ideal of A. Define S to be the set complement of $\mathfrak{p}$ in A, i.e. $S = A \setminus \mathfrak{p}$. This is clearly a multiplicative submonoid of A. Take $s, s' \in S$ then if $ss' \in \mathfrak{p}$ we must have $s \in \mathfrak{p}$ or $s' \in \mathfrak{p}$ but this is a contradiction and so S is closed under multiplication. We note that $1 \notin \mathfrak{p}$ otherwise $\mathfrak{p}$ is trivially the whole ring and so $1 \in S$.

Example 4.2. Let $3\mathbb{Z} \subseteq \mathbb{Z}$ be an ideal of $\mathbb{Z}$. It is easy to see that $3\mathbb{Z}$ is prime. Given $ab \in 3\mathbb{Z}$ then $ab = 3z$ for some $z \in \mathbb{Z} \Rightarrow 3 \mid 3z$ and $3 \mid ab$. As 3 is a prime number we must have $3 \mid a$ or $3 \mid b$ and hence $a \in 3\mathbb{Z}$ or $b \in 3\mathbb{Z}$. Taking the set complement of $3\mathbb{Z}$ in $\mathbb{Z}$ we have $S = \mathbb{Z} \setminus 3\mathbb{Z} = \{z \in \mathbb{Z} \mid 3 \nmid z\}$. Clearly $3 \mid 0$ and so $0 \notin S$, which means S forms a multiplicative submonoid of $\mathbb{Z}$. Let $\mathfrak{p} = 3\mathbb{Z}$, then we have

$$\mathbb{Z}_{\mathfrak{p}} = \left\{ \frac{z}{s} \,\middle|\, z \in \mathbb{Z} \text{ and } s \in S \right\},$$

which is a set of equivalence classes.

Let $f : A \to B$ be a ring homomorphism, (i.e. B is an A-algebra), and consider the sets $S^{-1}A$ and $S^{-1}B$. We denote these sets by $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ respectively and can consider $B_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$-module. We make the following definition.

Definition. Let A be a subring of a ring B and $\mathfrak{p}$, $\mathfrak{q}$ be prime ideals of A and B respectively. We say that $\mathfrak{q}$ *lies above* $\mathfrak{p}$ if $\mathfrak{q} \cap A = \mathfrak{p}$.

Now let A be a subring of a ring B and $\mathfrak{p}$, $\mathfrak{q}$ be prime ideals of A and B respectively such that $\mathfrak{q}$ lies above $\mathfrak{p}$. If $\lambda : A \to B$ is an injective homomorphism between the rings then we can induce an injective homomorphism $\tilde{\lambda} : A/\mathfrak{p} \to B/\mathfrak{q}$ between the factor rings. Explicitly, this map will be $\tilde{\lambda}(a+\mathfrak{p}) = \lambda(a) + \mathfrak{q}$ for all $a \in A$. This gives us a commutative diagram of injective homomorphisms.

$$\begin{tikzcd}
B \arrow[r] & B/\mathfrak{q} \\
A \arrow[u, "\lambda"] \arrow[r] & A/\mathfrak{p} \arrow[u, "\tilde{\lambda}"']
\end{tikzcd}$$

The horizontal mappings in the diagram are just the canonical homomorphisms. For a simple example of λ we can consider λ to be the inclusion map. Now if B is integral over A then we have, by Lemma 4.2, that $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$.

Lemma 4.5. *Let A be a subring of a ring B such that B is integral over A. Let $\mathfrak{p}$ be a prime ideal of A then we have that $\mathfrak{p}B \neq B$ and there exists a prime ideal of B, say $\mathfrak{q}$, lying above $\mathfrak{p}$.*

Proof. We start by proving the first part of the statement, namely that $\mathfrak{p}B \neq B$. We have that B is integral over A and so $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ by Lemma 4.3. The ideal $\mathfrak{p}$ is prime and so $A_\mathfrak{p}$ is a local ring of A with unique maximal ideal $\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p}$, for $S = A \setminus \mathfrak{p}$, (see Section 3, Chapter II of [1] for details). We notice that, by the ideal property of $\mathfrak{p}$, we have

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}B_\mathfrak{p}.$$

From this we can see that it will be enough to show that $\mathfrak{p}B \neq B$ when A is a local ring. By the existence of a prime ideal in A we note that we must have $1 \neq 0$. It is also apparent that $\mathfrak{p}B = B$ if and only if $1 \in \mathfrak{p}B$. Now assume for a contradiction that $\mathfrak{p}B = B$, then $1 \in \mathfrak{p}B$ and so

$$1 = \alpha_1 b_1 + \cdots + \alpha_n b_n,$$

for some $\alpha_i \in \mathfrak{p}$ and $b_i \in B$. Consider the ring $B' = A[b_1, \ldots, b_n]$ we note that A is a subring of B' and so B' is a finitely generated A-algebra. By Lemma 4.1 we have that B' is a finitely generated A-module. Given any $q(b_1, \ldots, b_n) \in B'$ and $p \in \mathfrak{p}$ it's clear that $pq(b_1, \ldots, b_n) \in B'$ because the coefficients will still lie in $A_\mathfrak{p}$. Thus $\mathfrak{p}B' = B'$ and so by Nakayama's Lemma $B' = 0$, however this is a contradiction, so $\mathfrak{p}B \neq B$.

Let f represent the homomorphism $S^{-1}f : S^{-1}A \to S^{-1}B$ and consider the following commutative diagram:

$$\begin{tikzcd}
B \arrow[r] & B_\mathfrak{p} \\
A \arrow[u] \arrow[r] & A_\mathfrak{p} \arrow[u, "f"']
\end{tikzcd}$$

All other homomorphisms in the above diagram are the canonical homomorphisms. We have shown in the first part of this proof that $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$ and so $\mathfrak{m}_\mathfrak{p}$ is contained in some maximal ideal M of B. Consider the pre-image of M in $A_\mathfrak{p}$

$$f^{-1}(M) = \{a \in A_\mathfrak{p} \mid f(a) \in M\}.$$

Now we have that $f^{-1}(M)$ is an ideal in $A_\mathfrak{p}$ and in fact will be a maximal ideal containing $\mathfrak{m}_\mathfrak{p}$. We know that $\mathfrak{m}_\mathfrak{p}$ is a maximal ideal in $A_\mathfrak{p}$ and so $f^{-1}(M) = \mathfrak{m}_\mathfrak{p}$, i.e. $M \cap A_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$. Consider the canonical mapping $\tau : B \to B_\mathfrak{p}$ and the pre-image of M under this map

$$\tau^{-1}(M) = \{b \in B \mid \tau(b) \in M\}.$$

Now this will be an ideal in B and in fact will be a prime ideal. Let $bc \in \tau^{-1}(M)$ then we have that $\tau(bc) \in M \Rightarrow \tau(b)\tau(c) \in M$. Any maximal ideal is also a prime ideal and so we must have either $\tau(b) \in M$ or $\tau(c) \in M$, which gives us $b \in \tau^{-1}(M)$ or $c \in \tau^{-1}(M)$. Hence $\tau^{-1}(M)$ is a prime ideal of B, say $\mathfrak{q}$.

We note that the pre-image of $\mathfrak{m}_\mathfrak{p}$ in A is just $\mathfrak{p}$. Now consider the pre-image of M going both directions in the commutative diagram. We can see that $B \cap \mathfrak{q} = \mathfrak{p}$ and so $\mathfrak{q}$ lies above $\mathfrak{p}$, as required. □

We now progress to the final and main theorem of this section, the generalisation of Theorem 3.3. We want to look at extending a homomorphism from an integral ring into an algebraically closed field.

Theorem 4.1. *Let A be a subring of a ring B such that B is integral over A. Consider L to be an algebraically closed field and $\varphi : A \to L$ to be a homomorphism. Then we can extend φ into a homomorphism from B to L.*

Proof. We start by reducing this problem to one of local rings. Let $\mathfrak{p}$ be the kernel of φ, then $\mathfrak{p}$ is a prime ideal of A. This is because if $bc \in \operatorname{Ker}(\varphi)$ then $\varphi(bc) = 0 \Rightarrow \varphi(b)\varphi(c) = 0$. Now $\varphi(b), \varphi(c) \in L$ and L is a field, which is an integral domain and so $\varphi(b) = 0$ or $\varphi(c) = 0 \Rightarrow b \in \operatorname{Ker}(\varphi)$ or $c \in \operatorname{Ker}(\varphi)$. Consider the set complement $S = A \setminus \mathfrak{p}$ then we can describe a commutative diagram

$$\begin{tikzcd}
B \arrow[r] & S^{-1}B \\
A \arrow[u] \arrow[r] & S^{-1}A \arrow[u]
\end{tikzcd}$$

as we have done before. In fact $S^{-1}A$ is just the local ring $A_\mathfrak{p}$. Now we have that $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ by Lemma 4.3. We extend the definition of φ such that for any $\frac{a}{s} \in A_\mathfrak{p}$

$$\varphi\left(\frac{a}{s}\right) = \frac{\varphi(a)}{\varphi(s)}.$$

Hence we can factor φ into a mapping $A \to A_\mathfrak{p} \to L$. We now wish to show that this can be extended to a homomorphism $B_\mathfrak{p} \to L$.

We consider $\psi : A_\mathfrak{p} \to L$ such that if $\tau : A \to A_\mathfrak{p}$ is the canonical homomorphism, then $\varphi = \psi \circ \tau$. Let $\mathfrak{m}$ be the unique maximal ideal of $A_\mathfrak{p}$ and assume $\operatorname{Ker}(\psi) = \mathfrak{m}$. By Lemma 4.5 we know that there exists a maximal ideal, (because $\mathfrak{m}$ is maximal - see Section 1, Chapter IX of [1]), say M, of $B_\mathfrak{p}$ that lies above $\mathfrak{m}$. Clearly $B_\mathfrak{p}/M$ and $A_\mathfrak{p}/\mathfrak{m}$ are fields and in fact $A_\mathfrak{p}/\mathfrak{m} \subseteq B_\mathfrak{p}/M$ is an algebraic extension. By the first isomorphism theorem, (see Section 2.2.3 of [6]), we have $A_\mathfrak{p}/\mathfrak{m} \cong \psi(A_\mathfrak{p})$.

It is possible to find an isomorphism from $A_{\mathfrak{p}}/\mathfrak{m}$ to $\psi(A_{\mathfrak{p}})$ such that the factored homomorphism $A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{m} \to L$ is the same as ψ. Now we choose an embedding of $B_{\mathfrak{p}}/M$ into L such that the following diagram is commutative.

$$\begin{tikzcd}
B_{\mathfrak{p}} \arrow[r] & B_{\mathfrak{p}} \backslash M \arrow[dr] & \\
A_{\mathfrak{p}} \arrow[u] \arrow[r] & A_{\mathfrak{p}} \backslash \mathfrak{m} \arrow[u] \arrow[r] & L
\end{tikzcd}$$

This has allowed us to extend our homomorphism $\psi : A_{\mathfrak{p}} \to L$ to a homomorphism from $B_{\mathfrak{p}} \to L$. Thus by composing this with the canonical homomorphism from $B \to B_{\mathfrak{p}}$ we have extended our original homomorphism φ and so our theorem is proved. □

5. Transcendental Extensions

Please note, all elements of this section have been adapted from [1], unless otherwise stated. Now we have developed some of the theory of field extensions, we can move on to the discussion of transcendental extensions. We currently have a very coarse measure of size in a field extension, called the degree of the extension. To improve on this we introduce the idea of dimension in a field extension, much like dimension in a vector space.

To create a basis in a vector space we look at the linearly independent elements of the space. We do a similar thing for a field extension by looking at the *algebraically independent* elements of the extension. We start by defining what is meant for elements to be algebraically independent.

Definition. Let $E \subseteq F$ be a field extension and $S = \{x_i\}$ a subset of F, with $|S| = n$. We say that S is *algebraically independent* over E if, summing over all possible n-tuples $\nu = (\nu_1, \dots, \nu_n)$, we have

$$0 = \sum_{\nu} a_{(\nu)} \prod_{i} x_i^{\nu_i}$$

with $a_{(\nu)} \in E \Rightarrow a_{(\nu)} = 0$. Another way of putting this is that there exists no non-zero polynomial $q(X) \in E[X]$ such that $q(x_1, \dots, x_n) = 0$.

Example 5.1. We have that i and $\sqrt{2}$ are algebraically dependent over $\mathbb{R}$, because given the polynomial

$$q(x_1, x_2) = \sqrt{2}x_1^2 + x_2 \in \mathbb{R}[X],$$

it's clear to see that $q(i, \sqrt{2}) = -\sqrt{2} + \sqrt{2} = 0$. Hence the set $\{i, \sqrt{2}\}$ is not algebraically independent over $\mathbb{R}$.

Example 5.2. Using well known results from number theory we know that e and π are transcendental over $\mathbb{Q}$, and hence neither satisfy a polynomial equation in $\mathbb{Q}[X]$. Thus we have that $\{e\}$ and $\{\pi\}$ are algebraically independent subsets of $\mathbb{R}$ over $\mathbb{Q}$. It's important to note, however, that this set is *not* algebraically independent over $\mathbb{R}$. It is currently unknown whether the subset $\{e, \pi\}$ of $\mathbb{R}$ is algebraically independent over $\mathbb{Q}$, but it has been proved that the set $\left\{\pi, e^{\pi}, \Gamma(\frac{1}{4})\right\}$ is algebraically independent over $\mathbb{Q}$.

These algebraically independent subsets can be ordered by inclusion, with F an upper bound of the inclusion. Clearly by Zorn's Lemma these sets have maximal elements, i.e. sets with largest cardinality. Let $E \subseteq F$ be a field extension and M be a subset of F such that M is algebraically independent over E. If M has maximum cardinality with respect to such subsets, then we call the cardinality of M the *transcendence degree* or *dimension* of F over E.

A subset M of F, which is algebraically independent over E and maximal amongst all such subsets, shall be referred to as a *transcendence base* of F over E. We can see that if $M = \{m_1, \dots, m_i\}$ is a transcendence base, then F is algebraic over $E(M)$. This is because if $\alpha \in F$ then we must have that α is algebraically dependent upon the set M over E because M is maximal. Therefore there exist some non-zero $f(X) \in E[X]$ where

$$f(\alpha, m_1, \ldots, m_i) = 0.$$

If we define $g(x) = f(x, m_1, \ldots, m_i)$ then $g(x) \in E(M)[X]$ and $g(\alpha) = 0$, then we can see F is algebraic over $E(M)$. These transcendence bases shall be the focus of our discussion in this section. To start, we will show that the cardinality of a transcendence base is unique.

Theorem 5.1. *Let $E \subseteq F$ be a field extension. If X and Y are two transcendence bases for F over E then we must have that $|X| = |Y|$.*

Proof. We start by dealing with the case when the transcendence base is finite. Let X be a finite transcendence base of F over E such that $X = \{x_1, \ldots, x_m\}$, $m \geqslant 1$. We want to show that any other transcendence base must also have m elements. Let $Y = \{y_1, \ldots, y_n\}$ be another transcendence base of F over E with $n \geqslant 1$. By the definition of the transcendence base X is the largest algebraically independent subset of F over E. Following in our previous logic there exists a non-zero $f(X) \in E[X]$, in $m+1$ variables, where

$$f(y_1, x_1, \ldots, x_m) = 0.$$

We have that X and Y are maximal algebraically independent subsets of F. Hence we must have at least one x_i which is algebraically dependent on $(y_1, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m)$. After a suitable renumbering of the elements say this element is x_1. Now x_1 and y_1 must both occur in f and thus x_1 is algebraic over $E(y_1, x_2, \ldots, x_m)$.

Assume for an inductive argument that after a finite application of the above process we can find $\{y_1, \ldots, y_\ell\}$ ($\ell < n$), such that F is algebraic over $E(y_1, \ldots, y_\ell, x_{\ell+1}, \ldots, x_m)$. Then there must exist a non-zero polynomial $g(X) \in E[X]$, in $m+1$ variables, where

$$g(y_{\ell+1}, y_1, \ldots, y_\ell, x_{\ell+1}, \ldots, x_m) = 0$$

and $y_{\ell+1}$ occurs in $g(X)$. Now the $\{y_1, \ldots, y_{\ell+1}\}$ and $\{x_{\ell+1}, \ldots, x_m\}$ are two algebraically independent sets over E. Due to the algebraic independence of the y_i, some x_j must also occur in g. After a suitable renumbering of $\{x_{\ell+1}, \ldots, x_m\}$, if we assume that $x_{\ell+1}$ occurs in g, then we have that $x_{\ell+1}$ is algebraic over $E(y_1, \ldots, y_{\ell+1}, x_{\ell+2}, \ldots, x_m)$.

From the above arguments we have developed a tower of extensions,

$$E \subseteq E(x_1, \ldots, x_m) \subseteq E(y_1, x_2, \ldots, x_m) \subseteq \cdots \subseteq E(y_1, \ldots, y_{\ell+1}, x_{\ell+2}, \ldots, x_m) \subseteq F.$$

By Theorem 3.1, a tower of algebraic extensions is algebraic. Hence we must have F is algebraic over $E(y_1, \ldots, y_{\ell+1}, x_{\ell+2}, \ldots, x_m)$. If $n \geqslant m$, then we can replace all the x_js by y_is and obtain F is algebraic over $E(y_1, \ldots, y_m)$. If $n \leqslant m$ then we can start this procedure with the basis Y and replace each of the y_is by x_js. This would give us F is algebraic over $E(x_1, \ldots, x_m)$, and hence we must have that $n = m$, i.e. $|X| = |Y|$.

Now consider the case when $|X|$ is infinite. If $|Y|$ is finite then we can use a finite application of the above argument to replace each y_i by an x_j. However, this new set of

x_js will not be maximal as it will be strictly contained in X. Hence Y cannot form a transcendence base for the extension, which gives us that $|Y|$ must be infinite. □

Theorem 5.2. *Let $E \subseteq F$ be a field extension and Γ a set of generators of the extension, such that $F = E(\Gamma)$. If $S \subseteq \Gamma$ is an algebraically independent subset, then S can be extended to a transcendence base M.*

Proof. If S is maximal with respect to the inclusion ordering of algebraically independent subsets, then it is a transcendence base already and we are done. If we assume S is not maximal then $S = \{s_1, \dots, s_k\}$ resides in some transcendence base $X = \{x_1, \dots, x_n\}$ of $E \subseteq F$. Now the elements of S are algebraically independent and because $S \subset X$ there must exist some $x_i \neq s_j$ for all $j = 1, \dots, k$. Now after a sufficient renumbering of the elements of X, we can say this element is x_{k+1}. Then we have that x_{k+1} is not algebraic over

$$E(s_1, \dots, s_k)$$

and so $M = \{s_1, \dots, s_k, x_{k+1}\}$ is algebraically independent over E. Repeat this argument until $|M| = n$ and hence M is a transcendence base of $E \subseteq F$. □

Lemma 5.1. *Let $E \subseteq F \subseteq L$ be a tower of field extensions. Then if n is the transcendence degree of $E \subseteq F$ and m is the transcendence degree of $F \subseteq L$ we have $n + m$ is the transcendence degree of $E \subseteq L$.*

Proof. Let $X = \{x_1, \dots, x_n\}$ be a transcendence base for the extension $E \subseteq F$ and $Y = \{y_1, \dots, y_m\}$ be a transcendence base for the extension $F \subseteq L$. We want to show that the set $M = \{x_1, \dots, x_n, y_1, \dots, y_m\}$ is a transcendence base for the extension $E \subseteq L$. Now given any element $\alpha \in L$ it must be algebraically dependent upon the transcendence base Y. Hence there exists a non-zero polynomial $p(X) \in F[X]$, such that

$$p(y_1, \dots, y_m, \alpha) = 0.$$

Each coefficient of $p(X)$ is an element of F, which is algebraic over $E(x_1, \dots, x_n)$. Hence we can replace each coefficient of $p(X)$ with a non-zero polynomial of $E[X]$ dependent upon $x_1, \dots, x_n$. We can then consider $p(X)$ to be the non-zero polynomial $q(X) \in E[X]$, such that

$$q(x_1, \dots, x_n, y_1, \dots, y_m, \alpha) = 0.$$

Renaming this polynomial $g(x) = q(x_1, \dots, x_n, y_1, \dots, y_m, x)$ we have $g(x) \in E(M)[X]$ and $g(\alpha) = 0$. Thus α is algebraic over $E(M) \Rightarrow L$ is algebraic over $E(M)$.

To show that M is a transcendence base we have to show that it is maximal. If M is not maximal then there exists some M' that contains M, which is algebraically independent over E. This suggests that there is some $\beta \in M'$ where $\{x_1, \dots, x_n, y_1, \dots, y_m, \beta\}$ is an algebraically independent set. However, this gives us that $\{y_1, \dots, y_m, \beta\}$ is an algebraically independent subset of L over F, which invalidates the maximality of Y. Hence M is maximal and forms a transcendence base for $E \subseteq L$ with $|M| = n + m$. □

Now we have developed some of the basic results concerning transcendence bases, we want to move towards an important theorem called Hilbert's Nullstellensatz. Given any field E the Nullstellensatz allows us to relate zeros of polynomials in $E[X]$ with the ideals of $E[X]$. This will prove very useful in our study of algebraic geometry, as we will primarily be concerned with zeros of polynomials.

However, before we can prove the Nullstellensatz we need to return to a theorem in the previous section. We now aim to revisit Theorem 3.3 to prove it in a more specialised form, which mainly concerns finitely generated polynomial rings of a field E.

Theorem 5.3. *Let E be a field and consider the finitely generated polynomial ring $E[X] = E[X_1, \dots, X_n]$. Now consider $\varphi : E \to L$ an embedding of E into an algebraically closed field L. If such a φ exists then there exists an extension of φ to a homomorphism of $E[X]$ into L.*

Proof. Let $\langle g \rangle$ be a maximal ideal of $E[X]$ and consider the canonical homomorphism $\sigma : E[X] \to E[X]/\langle g \rangle$. We can see that $\sigma(E)\big[\sigma(X)\big]$ is a field, which is in fact an extension of the field $\sigma(E)$. Now if we can show that there exists a homomorphism $\psi : E[X]/\langle g \rangle \to L$ then by taking the composition $\psi \circ \sigma$ we can show that φ extends to $E[X]$.

So, we assume that $E[X]$ is a field. If $E[X]$ is algebraic over E then by Theorem 3.3 we have φ extends to $E[X]$ and we're done. If we assume $E[X]$ is not algebraic, then there exists a transcendence base $t_1, \dots, t_r$, with $r \geqslant 1$, for the extension $E \subseteq E[X]$. Each element of $E[X]$ is algebraic over the field $E(t_1, \dots, t_r) = E(t)$. Hence each X_i has a minimum polynomial $p_i(X_i) \in E(t)[X]$, which we express as

$$\frac{a_i^n(t)}{b_i^n(t)}X^n + \frac{a_i^{n-1}(t)}{b_i^{n-1}(t)}X^{n-1} + \dots + \frac{a_i^0(t)}{b_i^0(t)}.$$

for some $a_i^j(t) \in E[t]$ and non-zero $b_i^j(t) \in E[t]$. Now we consider $b_i(t) = b_i^n(t) \cdots b_i^0(t)$, which we note is a non-zero element of $E[t]$. By multiplying $p_i(X_i)$ by $b_i(t)$ we will get a polynomial $q_i(X_i) = b_i(t)p_i(X_i)$ which has coefficients in $E[t]$.

Consider the product of the leading coefficients of these polynomials $a(t) = a_1(t) \cdots a_n(t)$, where we simply refer to $a_i^n(t)$ as $a_i(t)$. We have that $a_i(t) \neq 0$ and so $a(t)$ is also non-zero. As $a(t) \neq 0$ there must exist elements $s_1, \dots, s_r$ in $\overline{E}$ such that $a(s) \neq 0$. If $a(s) \neq 0$ then we must have each $a_i(s) \neq 0$. Now by multiplying each $q_i(X_i)$ by $\frac{1}{a_i(t)}$ every X_i is integral over the ring

$$E\left[t_1, \dots, t_r, \frac{1}{a_1(t)}, \dots, \frac{1}{a_n(t)}\right].$$

Let $\lambda : E[t] \to \overline{E}$ be a homomorphism such that $\lambda(E) = E$ and $\lambda(t_j) = s_j$. Let $\mathfrak{p}$ be the kernel of λ, which will be an ideal in $E[t_1, \dots, t_r]$. By arranging λ in this way we have that $\lambda\big(a(t)\big) = a(s) \neq 0$ and hence $a(t) \notin \mathfrak{p}$. It is clear that $\mathfrak{p}$ is a prime ideal of $E[t]$ and so we can reduce this problem to the local ring $E[t]_{\mathfrak{p}}$. We remark that because $a(t) \notin \mathfrak{p}$ then we must have that $\frac{1}{a(t)} \in A_{\mathfrak{p}}$.

By considering the canonical homomorphism from $E[t] \to E[t]_{\mathfrak{p}}$ we can extend λ to a homomorphism of $E[t]_{\mathfrak{p}} \to \overline{E}$. Now $E[t]_{\mathfrak{p}}[X]$ is a ring containing $E[t]_{\mathfrak{p}}$ and is in fact integral over $E[t]_{\mathfrak{p}}$ by our above remarks. So, by Theorem 4.1 we have that λ extends to a homomorphism of $E[t]_{\mathfrak{p}}[X] \to \overline{E}$, which proves our theorem. □

We can finally now prove the main result that we have been leading up to. In fact this result is just one of the many corollarys of the above theorem. It is referred to as Hilbert's Nullstelensatz, which roughly translated means theorem of zeros.

Definition. Let E be a field, S a subset of the ring $E[X] = E[X_1, \ldots, X_n]$ and $E \subseteq F$ a field extension. By a *zero* of S in F we refer to an n-tuple $c = (c_1, \ldots, c_n)$, such that $f(c) = 0$ for all $f \in S$.

Corollary 5.1 (Hilbert's Nullstellensatz)**.** *Let E be a field and $E[X] = E[X_1, \ldots, X_n]$ a finitely generated ring with ideal I. If we let f be a polynomial such that $f(c) = 0$ for all zeros $c = (c_1, \ldots, c_n)$ of I in $\overline{E}$. Then there exists an integer $m \geqslant 0$ such that $f^m \in I$.*

Proof. If $I = E[X]$ then we are done, as $f^1 \in E[X]$. Assume for a contradiction that no power of f lies in I and define a multiplicative submonoid $S = \{f^m \mid m \in \mathbb{N}^0\}$ of $E[X]$. Let M be a maximal ideal in the set of all ideals that contain I such that $M \cap S = \emptyset$. Then we have M is a prime ideal (see Chapter 6, Section 4 of [1]). We can now create an isomorphism

$$E[X_1, \ldots, X_n]/M \to E[x_1, \ldots, x_n].$$

Now $f(X) \notin M$ because f is an element of S and hence $f(X) + M \neq M$. Thus under our isomorphism we will have $f(x) \neq 0$. Let $\lambda : E[x] \to \overline{E}$ be a homomorphism over E such that $\lambda\big(f(x)\big) \neq 0$. Then by the homomorphic property of λ we get

$$\lambda\big(f(x)\big) = f\big(\lambda(x)\big) = f\big(\lambda(x_1), \ldots, \lambda(x_n)\big) \neq 0.$$

This, however, contradicts the fact that f vanishes on all zeros of I in $\overline{E}$ and so $f^m \in I$ for some $m \geqslant 0$. □

6. Affine Varieties

All fields in this section will be algebraically closed.

Please note, all elements of this section have been adapted from [5], unless otherwise stated. In this section we will be introducing the algebraic structure known as an affine variety. To study algebraic geometry effectively we want to look at sets of points in which more than one polynomial vanish. When we move into more complicated space, i.e. projective or affine space, we will find that our geometric objects can be defined by multiple polynomials. Thus it is important for us to be able to look at the points where multiple polynomials, in multiple unknowns, will vanish. The affine variety structure will give us the language to do precisely this.

At this moment in time it may not seem apparent how this structure will relate to what we have just discussed. However, we will see that our important result from the previous section, Hilbert's Nullstellensatz, can actually be reformulated in the language of affine varieties.

Before we introduce the definition of an affine variety, we need to familiarise ourselves with some of the terminology that we will use. If E is a field, then by $\mathrm{Map}(V, E)$ we refer to the set of all functions $f : V \to E$. We can then consider $\mathrm{Map}(V, E)$ to be an E-algebra, by defining the operation point-wise. For example, given $f, g \in \mathrm{Map}(V, E)$ then $(gf)(x) = g(x)f(x)$. Now we define a map $\varepsilon_x : \mathrm{Map}(V, E) \to E$, called the *evaluation map*, such that for any $f \in \mathrm{Map}(V, E)$ we have $\varepsilon_x(f) = f(x)$.

Finally, given two E-algebras, A and B, we define $\mathrm{Hom}_{E-\mathrm{alg}}(A, B)$ to be the set of all E-algebra homomorphisms from A to B. We will often refer to this just as $\mathrm{Hom}(A, B)$ when the field is apparent.

Definition. Let E be a field, V a set and A a finitely generated E-subalgebra of $\mathrm{Map}(V, E)$. Then we define an *affine variety* to be a pair (V, A) such that the map

$$\begin{aligned} V &\to \mathrm{Hom}_{E-\mathrm{alg}}(A, E); \\ x &\mapsto \varepsilon_x, \end{aligned}$$

is a bijection.

Our classic example of an affine variety is affine n-space, denoted $\mathbb{A}^n$. We consider $\mathbb{A}^n = E^n$ and the subalgebra $A = E[X_1, \ldots, X_n]$, where X_i are the coordinate functions defined to be $X_i(x_i) = x_i$ for $(x_1, \ldots, x_n) \in \mathbb{A}^n$. As an example we show that $(\mathbb{A}^n, A)$ is in fact an affine variety.

Example 6.1. We clearly have that A is a finitely generated E-subalgebra as there are finitely many $X_1, \ldots, X_n$. We are now left to show that the map from $V \to \mathrm{Hom}(A, E)$ is a bijection. We start by showing that the map is injective. Let x, y be elements of $\mathbb{A}^n$ such that $\varepsilon_x = \varepsilon_y$. Then for any X_i we have

$$\varepsilon_x(X_i) = \varepsilon_y(X_i) \Rightarrow X_i(x) = X_i(y) \Rightarrow x_i = y_i$$

for all $1 \leqslant i \leqslant n$ and so $x = y$. Thus our map is injective.

We now just need to show that the map is surjective. Let φ be any homomorphism in $\mathrm{Hom}(\mathbb{A}^n, A)$ then we wish to show there exists an x such that $\varphi = \varepsilon_x$. Let $x_i = \varphi(X_i)$ for $1 \leqslant i \leqslant n$ and $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$. Now $x_i = X_i(x) = \varepsilon_x(X_i)$ and so $\varphi(X_i) = \varepsilon_x(X_i)$. We will prove below that because $X_1, \ldots, X_n$ generate A then $\varphi = \varepsilon_x$ and so our map is a bijection.

Proposition: *Let $\varphi, \psi : A \to B$ be two E-algebra homomorphisms and suppose A is a finitely generated E-algebra, such that $A = E(a_1, \ldots, a_r)$. Then if $\varphi(a_i) = \psi(a_i)$ for all $1 \leqslant i \leqslant n$ then $\varphi = \psi$.*

Proof. As $a_1, \ldots, a_r$ generate A as an E-algebra, then any element $a \in A$ can be expressed as

$$a = \sum_{\nu} \alpha_{(\nu)} \prod_{i=1}^{n} a_i^{\nu_i},$$

for a finite number of n-tuples $\nu = (\nu_1, \ldots, \nu_n)$. Now using the homomorphic properties of φ and ψ we can see that

$$\begin{aligned}\varphi(a) &= \varphi\left(\sum_{\nu} \alpha_{(\nu)} \prod_{i=1}^{n} a_i^{\nu_i}\right), \\ &= \sum_{\nu} \alpha_{(\nu)} \prod_{i=1}^{n} \varphi(a_i)^{\nu_i}, \\ &= \sum_{\nu} \alpha_{(\nu)} \prod_{i=1}^{n} \psi(a_i)^{\nu_i}, \\ &= \psi\left(\sum_{\nu} \alpha_{(\nu)} \prod_{i=1}^{n} a_i^{\nu_i}\right), \\ &= \psi(a).\end{aligned}$$

So $\varphi(a) = \psi(a)$ for all $a \in A \Rightarrow \varphi = \psi$ as required. □

We recall the definition of a Noetherian ring. A ring A is called *Noetherian* if given any ascending chain of ideals

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

in A, then there exists an r such that $I_r = I_j$ for all $j \geqslant r$. In other words there exists no infinite ascending chain of ideals in A. Equivalently, we can say that A is Noetherian if every ideal $I \subseteq A$ is finitely generated. This definition has been taken from Section 7.2.2 of [6]. We now prove an important theorem, which has been adapted from Section 1.1 of [7].

Theorem 6.1 (Hilbert's Basis Theorem). *If A is a Noetherian ring then $A[X]$, the polynomial ring in one variable, is also Noetherian.*

Proof. We aim to prove this result by contradiction. We assume that there is a non-zero ideal $I \subseteq A[X]$ such that I is not finitely generated, and let $I_0 = I \setminus \{0\}$. Let f_1 be the polynomial in I_0 such that f_1 has least degree amongst all polynomials in I_0. Now I is not finitely generated and so $I_1 = I \setminus \langle f_1 \rangle$ is not empty. Let f_2 be the polynomial in I_1 such that f_2 has least degree amongst all polynomials in I_1. We note that $\deg(f_2) \geqslant \deg(f_1)$ and because I is not finitely generated we have $I_2 = I \setminus \langle f_1, f_2 \rangle$ is non-empty.

We can repeat this argument indefinitely until we have a series of polynomials $f_1, f_2, f_3, \ldots$ in I such that $\deg(f_1) \leqslant \deg(f_2) \leqslant \deg(f_3) \leqslant \ldots$ and $f_{r+1} \in I_r = I \setminus \langle f_1, \ldots, f_r \rangle$ for all r. Consider the leading coefficients, say a_i, of each of the polynomials f_i for $i \geqslant 1$. Now the ideal $\langle a_i \rangle \subseteq A$ is clearly finitely generated, as A is Noetherian, and hence $\langle a_i \rangle = \langle a_1, \ldots, a_n \rangle$ for some n. All leading coefficients of each f_i are in $\langle a_i \rangle$, including a_{n+1}, which implies that $a_{n+1} = \sum_{j=1}^{n} x_j a_j$ for some $x_j \in A$, not all zero.

Now let us define a new polynomial

$$g = f_{n+1} - \sum_{j=1}^{n} x_j X^{\deg(f_{n+1-j})} f_j \in I_n.$$

We can see that we will have $\deg(g) \leqslant \deg(f_{n+1})$ by design of g. However, if we examine the coefficient of X^{n+1} in g we see that

$$a_{n+1}X^{n+1} - x_1 a_1 X^{n+1} - \cdots - x_n a_n X^{n+1} = \left[a_{n+1} - \sum_{j=1}^{n} x_j a_n j \right] X^{n+1} = 0.$$

Therefore we must have $\deg(g) < \deg(f_{n+1})$. However we chose f_{n+1} to be the polynomial with least degree in I_n and hence this is a contradiction. So, I is finitely generated, as required. □

At this point we would like to introduce the notion of algebraic sets and then put forward a topology, known as the Zariski topology, that will be very useful to us. Oscar Zariski was incredibly influential in the field of algebraic geometry. He was born in Poland, but spent most of his life studying in the USA. He did, however, begin his time by studying algebraic geometry with the Italians in Rome. He began to grow increasingly distressed with the lack of rigor in the Italian approach and decided to ground the field in commutative algebra. Although many others have influenced the subject greatly, the work of Zariski was incredibly important to the sustained study of this field, (this information has been taken from [11]).

Definition. Let (V, A) be an affine variety and $S \subseteq A$ any subset of A. Then we refer to the following set

$$\mathcal{V}(S) = \{x \in V \mid f(x) = 0 \text{ for all } f \in S\}$$

as the *algebraic set* defined by S on V.

We now aim to show that the sets $\mathcal{V}(S)$ form the closed sets of a topology on V. We have that

$$\mathcal{V}\big(\{1\}\big) = \{x \in V \mid 1(x) = 0\} = \emptyset,$$

as 1 is the function such that $1(x) = 1$ for all $x \in V$. Also it is clear to see that $\mathcal{V}\big(\{0\}\big) = V$ as $0(x) = 0$ for all $x \in V$ and so $\emptyset, V$ are both algebraic sets on V. Let J be an indexing set and consider a collection of subsets $S_j \subseteq A$, then

$$\mathcal{V}\left(\bigcup_{j\in J} S_j\right) = \left\{x \in V \,\middle|\, f(x) = 0 \text{ for all } f \in \bigcup_{j\in J} S_j\right\}.$$

Now $x \in \mathcal{V}(\cup_{j\in J} S_j) \Leftrightarrow x \in \mathcal{V}(S_j)$ for all $j \in J \Leftrightarrow x \in \mathcal{V}(\cap_{j\in J} S_j)$. Therefore the intersection of subsets in A forms an algebraic set on V. Finally, if S, T are two subsets of a ring R then we write $ST = \{st \mid s \in S, t \in T\}$. Instead, if we let S, T be subsets of our algebra A, then we have

$$\begin{aligned}
\mathcal{V}(ST) &= \{x \in V \mid f(x) = 0 \text{ for all } f \in ST\},\\
&= \{x \in V \mid (gh)(x) = 0 \text{ for all } g \in S, h \in T\},\\
&= \{x \in V \mid g(x)h(x) = 0 \text{ for all } g \in S, h \in T\},\\
&= \{x \in V \mid g(x) = 0 \text{ or } h(x) = 0 \text{ for all } g \in S, h \in T\},\\
&= \{x \in V \mid g(x) = 0 \text{ for all } g \in S\} \cup \{x \in V \mid h(x) = 0 \text{ for all } h \in T\},\\
&= \mathcal{V}(S) \cup \mathcal{V}(T).
\end{aligned}$$

Hence the subsets $\mathcal{V}(S) \subseteq V$, $S \subseteq A$, form the closed sets of a topology on V, which we refer to as the *Zariski topology.*

Before progressing further, it is necessary to prove the tools that will help us later on. Primarily we would like to prove a result known as *Noether normalization.* Our main area of interest will be finitely generated algebras over a field, so we will find this result incredibly useful. The following theorem and proof has been adapted from Section 2.1 of [7].

Theorem 6.2 (Noether Normalization). *Let E be a field and $A = E[a_1, \ldots, a_n]$ a finitely generated E-algebra. Then there exists algebraically independent elements $x_1, \ldots, x_d \in A$ such that A is integral over the ring $E[x_1, \ldots, x_d]$.*

Proof. We prove this result by induction on the number of generators n. If $n = 0$ then $A = E$ and certainly, as E is a field, E is integral over itself, so we assume $n \geqslant 1$. If $a_1, \ldots, a_n$ are algebraically independent elements then we are done. If we assume these elements are algebraically dependent then there exists a non-zero polynomial $f \in E[X_1, \ldots, X_n]$ such that $f(a_1, \ldots, a_n) = 0$. After a suitable relabeling of the variables we can assume X_n occurs in f. Thus we express f as

$$f(X_1,\dots,X_n)=\sum_{\nu}a_{(\nu)}\prod_{j=1}^{n}X_j^{\nu_j}$$

for some finite number of n-tuples $\nu=(\nu_1,\dots,\nu_n)$. Now using this polynomial, we aim to construct a finitely generated polynomial ring of E such that each of the generators of A is integral over this ring.

Let r be an integer such that $r>\nu_j$ $(j=1,\dots,n)$ for all ν such that $a_{(\nu)}\neq 0$. Then we define $N(\nu)$ to be

$$N(\nu)=\nu_n+\nu_{n-1}r+\cdots+\nu_1 r^{n-1}=\sum_{i=0}^{n-1}\nu_{n-i}r^i.$$

We show that given any ν,μ such that $a_{(\nu)},a_{(\mu)}\neq 0$ then $N(\nu)=N(\mu)\Rightarrow\nu=\mu$. If we assume $N(\nu)=N(\mu)$ then

$$\begin{aligned}
&\sum_{i=0}^{n-1}\nu_{n-i}r^i=\sum_{i=0}^{n-1}\mu_{n-i}r^i,\\
\Rightarrow\quad &\sum_{i=0}^{n-i}(\nu_{n-i}-\mu_{n-i})r^i=0,\\
\Rightarrow\quad &\nu_{n-i}=\mu_{n-i}, &&\text{for all } i=0,\dots,n-1\\
\Rightarrow\quad &\nu_j=\mu_j, &&\text{for all } j=1,\dots,n\\
\Rightarrow\quad &\nu=\mu.
\end{aligned}$$

We set $r_i=r^{n-i}$ and define a new term $Y_i=X_i-X_n^{r_i}$, then consider the product $X_1^{\nu_1}\cdots X_n^{\nu_n}$. We want to show that this product can be expressed as $X_n^{N(\nu)}+$ lower order terms. So, we have

$$X_1^{\nu_1}\cdots X_n^{\nu_n}=(Y_1+X_n^{r_1})^{\nu_1}\cdots(Y_{n-1}+X_n^{r_{n-1}})^{\nu_{n-1}}X_n^{\nu_n}.$$

If we expand the brackets in this expression we note that the highest power of X_n takes the form

$$\nu_n+\nu_{n-1}r_{n-1}+\cdots+\nu_1 r_1=\nu_n+\nu_{n-1}r+\cdots+\nu_1 r^{n-1}=N(\nu).$$

So we can see that the product will have the following expression

$$X_1^{\nu_1}\cdots X_n^{\nu_n}=X_n^{N(\nu)}+\sum_{j=0}^{N(\nu)-1}h_jX_n^j,$$

for some $h_j\in E[Y_1,\dots,Y_{n-1}]$. We let $N=\max\{N(\nu)\mid a_{(\nu)}\neq 0\}$ and in light of the above remark suggest that our polynomial f has an expression of the form

$$f(X_1, \dots, X_n) = \lambda X_n^N + \sum_{j=0}^{N-1} h_j X_n^j,$$

for some $h_j \in E[Y_1, \dots, Y_{n-1}]$ and $0 \neq \lambda \in E$.

We now wish to construct a ring R such that each element of A will be integral over R. Define $y_i = a_i - a_n^{r_i}$ for $i = 1, \dots, n-1$ and consider the finitely generated subring $R = E[y_1, \dots, y_{n-1}]$. Define $g(X_n) = f(y_1, \dots, y_n, X_n) \in R[X_n]$, which is a non-zero polynomial such that $g(a_n) = 0$. By multiplying g by $\frac{1}{\lambda}$ we have a_n is integral over R and by rearranging, we have $a_i = y_i + a_n^{r_i}$ is integral over R for each $i = 1, \dots, n$. It is clear from the proof of Lemma 4.1 that as each a_i is integral over R, and the a_i generate A, we will have A is integral over R.

Using induction we can find an algebraically independent subset $\{r_1, \dots, r_m\}$ of R such that R is integral over $E[r_1, \dots, r_m]$. So, we have a tower of ring extensions $E[r_1, \dots, r_m] \subseteq R \subseteq A$ such that A is integral over R and R is integral over $E[r_1, \dots, r_m]$. By a proposition from section 4, A is integral over $E[r_1, \dots, r_m]$ and we are done. □

Although we have introduced the affine variety structure, we have yet to show how two varieties can be related. First, we must make a comment on a particular notation that we will use throughout the rest of this section. Often when we consider a pair (V, A) as an affine variety we already have an E-subalgebra in mind. Thus, when we refer to V as an affine variety we consider A to be the coordinate algebra on V, so $A = E[V]$. Now with this notation in place, we are able to introduce the concept of a *morphism* between two varieties.

Definition. Let V and W be two affine varieties. We say that a map $\phi : V \to W$ is a *morphism of varieties* if $g \circ \phi \in E[V]$ for every $g \in E[W]$. If $\phi : V \to W$ is a morphism we write $\phi^\sharp : k[W] \to k[V]$ for the map $\phi^\sharp(g) = g \circ \phi$ for all $g \in k[W]$. The map $\phi^\sharp$ is called the *comorphism* of ϕ.

Proposition: *Let $\phi : V \to W$ be a morphism of varieties. We have ϕ is an isomorphism if and only if $\phi^\sharp$ is an E-algebra isomorphism.*

Proof. Start by assuming that ϕ is an isomorphism, then there exists an inverse map $\phi^{-1} : W \to V$ such that $\phi \circ \phi^{-1} = \text{id}$. Now consider the homomorphism $\phi^\sharp$. If we can construct a $\theta : E[V] \to E[W]$ such that $\theta \circ \phi^\sharp = \text{id}_{E[W]}$ then $\phi^\sharp$ is a bijection and hence an isomorphism. Define θ to be the function, such that for any $h \in E[V]$ we have

$$\theta(h) = h \circ \phi^{-1}.$$

Now given any $g \in E[W]$ we have that

$$(\theta \circ \phi^\sharp)(g) = \theta\big(\phi^\sharp(g)\big) = \theta(g \circ \phi) = (g \circ \phi) \circ \phi^{-1} = g \circ (\phi \circ \phi^{-1}) = g.$$

So, θ is in fact an inverse of $\phi^\sharp$ and hence $\phi^\sharp$ is an isomorphism.

Now assume that $\phi^\sharp$ is an isomorphism, then we hope to show that there exists an inverse mapping $\lambda : W \to V$ for ϕ. Let $\tau : E[V] \to E[W]$ be the inverse map of $\phi^\sharp$ such that $\tau \circ \phi^\sharp = \mathrm{id}_{E[W]}$. Now, for any $g \in E[W]$ we will have

$$(\tau \circ \phi^\sharp)(g) = \tau(g \circ \phi) = \tau \circ (g \circ \phi) = g.$$

In particular this will be true when $g = \mathrm{id}_{E[W]}$ and so we have $\tau \circ \phi = \mathrm{id}_{E[W]}$ and so ϕ is a bijection and hence an isomorphism, as required. □

Lemma 6.1. *Let V and W be affine varieties and $\phi : V \to W$ a morphism of varieties. Suppose $\phi^\sharp : E[W] \to E[V]$ is surjective, then the image of ϕ is closed in W and the restriction $\phi_0 : V \to \mathrm{Im}(\phi)$ is an isomorphism.*

Proof. We start first by showing that $\mathrm{Im}(\phi)$ is a closed set in W, i.e. there exists some $I \subseteq E[W]$ such that $\mathrm{Im}(\phi) = \mathcal{V}(I)$. In fact we conjecture that $I = \mathrm{Ker}(\phi^\sharp)$ and set $Z = \mathrm{Im}(\phi)$. We have that $\phi^\sharp$ induces an isomorphism $\bar{\phi}^\sharp : E[W]/I \to E[V]$, by the first isomorphism theorem, and so there exists an inverse map $\theta : E[V] \to E[W]/I$, say, such that $\bar{\phi}^\sharp \circ \theta = \mathrm{id}$.

Let $g \in I$ and $x \in V$ then we have $\phi(x) \in Z$ and $g\big(\phi(x)\big) = (g \circ \phi)(x) = \phi^\sharp(g)(x) = 0$, which gives us $\phi(x) \in \mathcal{V}(I) \Rightarrow Z \subseteq \mathcal{V}(I)$. We now wish to show the reverse inclusion, that $\mathcal{V}(I) \subseteq Z$. So, let $y \in \mathcal{V}(I)$ and consider the evaluation map $\varepsilon_y : E[W] \to E$, which is clearly zero on I. This, therefore, induces an isomorphism $\bar{\varepsilon}_y : E[W]/I \to E$. By composing this function with our inverse function θ we get a homomorphism $\bar{\varepsilon}_y \circ \theta : k[V] \to E$.

Now V is an affine variety and hence all homomorphisms from $E[V] \to E$ take the form of an evaluation map ε_x for some $x \in V$. Thus we have $\bar{\varepsilon}_y \circ \theta = \varepsilon_x$ for some $x \in V$, which gives us $\bar{\varepsilon}_y = \varepsilon_x \circ \bar{\phi}^\sharp$ because $\theta \circ \bar{\phi}^\sharp = \mathrm{id}$. We are aiming to show that $y = \phi(x)$ for some $x \in V$. To do this we take $g \in E[W]$ and apply $\bar{\varepsilon}_y$ to get

$$\bar{\varepsilon}_y(g + I) = (\varepsilon_x \circ \bar{\phi}^\sharp)(g + I).$$

However, this gives us that

$$\varepsilon_y(g) = (\varepsilon_x \circ \phi^\sharp)(g) = \phi^\sharp(g)(x) = (g \circ \phi)(x) = g\big(\phi(x)\big) = \varepsilon_{\phi(x)}(g).$$

So, $\varepsilon_y(g) = \varepsilon_{\phi(x)}(g)$ for all $g \in E[W]$ and so $\varepsilon_y = \varepsilon_{\phi(x)} \Rightarrow y = \phi(x)$. Finally, this gives us that $\mathcal{V}(I) \subseteq Z \Rightarrow Z = \mathcal{V}(I)$, as required.

Now we can prove our second statement, that the restriction of ϕ is an isomorphism. If we recall the inclusion function ι, then we have that $\phi = \iota \circ \phi_0$. Thus we must have $\phi^\sharp = \phi_0^\sharp \circ \iota^\sharp$ and since $\phi^\sharp$ is surjective, and clearly ι is surjective, then we have $\phi_0^\sharp$ is surjective. Suppose $h \in E[V]$ such that $h \in \mathrm{Ker}(\phi_0^\sharp)$ then we have $h = g|_Z$ for some $g \in E[W]$. We can see that

$$\phi_0^\sharp(h) = h \circ \phi_0 = g \circ \phi = \phi^\sharp(g) = 0,$$

which gives us $g \in I$ and so $h = g|_Z = 0$ because $Z = \mathcal{V}(I)$. Thus $\mathrm{Ker}(\phi_0^\sharp) = 0$ and so $\phi_0^\sharp$ is injective $\Rightarrow$ $\phi_0^\sharp$ is an isomorphism. By our previous proposition we must have that ϕ_0 is an isomorphism and, finally, we are done. □

7. Algebraic Geometry

All fields in this section will be algebraically closed.

The information in the following introduction has been adapted from [8, 9]. Algebraic geometry is a subject with a deep history which has been transformed by new techniques and insight. Originally promoted by the Italian school of mathematics, the classical study of algebraic geometry made great advances, only later being held back by the restrictions of the language. Even the most proficient in the subject struggled to show more advanced results. Although the Italian approach has been superseded by more advanced theory, it is not without merit. It allows great insight to the problems and has a beautifully intricate theory in its own right.

Many mathematicians, including Zariski, who spent most of their time studying in America, saw the problems in the classical approach and the need to put the subject on a firm grounding in algebra. It is from such pioneering work by Zariski, and the German school of mathematics, that later works benefited so much. After Zariski came the work of Weil, who introduced the notion of algebraic varieties and then the work of Serre, who introduced the fundamental tool of Sheaf theory. Finally came the work of Alexander Grothendieck, whose work helped to unify the subject. He, aided by many others, introduced the concept of a scheme, which is the modern language in which algebraic geometry is studied today.

It is important to note that algebraic geometry can be studied over arbitrary fields. In fact it can even be studied over rings. However, this approach requires increased technical accuracy and the development of a greater degree of theory. For the purposes of this section we shall consider all fields to be algebraically closed. This will allow us to avoid minor technical difficulties and progress to more interesting results.

Unfortunately it is beyond the scope of this project to discuss the many different approaches from which algebraic geometry can be studied. If the reader is interested in exploring the modern language of schemes in more detail, I would recommend [9]. One aim in this section will be to finally show the definition of dimension using the transcendence degree. Another, after a brief discussion of topological spaces, will be to show the reformulation of Hilbert's Nullstellensatz in the language of affine varieties.

Please note, all elements of this section have been adapted from [5], unless otherwise stated. Given any affine variety, we have already introduced a topological space, which we refer to as the Zariski topology. Now any topological space X is said to be *Noetherian* if every ascending chain of open sets $U_1 \subseteq U_2 \subseteq \cdots$ is such that there exists an n with $U_r = U_n$, for all $r \geqslant n$. So, much like the condition of a Noetherian ring, there exist no infinite ascending chain of open sets. However, we are much more likely to deal with the closed sets of a topology, and we can see that X will be Noetherian if every descending chain $Z_1 \supseteq Z_2 \supseteq \cdots$ is finite.

Consider an affine variety V and let Z be a subset of V. Then we define a subset

$$\mathcal{N}(Z) = \{f \in E[V] \mid f(x) = 0 \text{ for all } x \in Z\}$$

of the coordinate algebra $E[V]$. Suppose Z is a closed subset of V, then there exists a subset $S \subseteq E[V]$ such that $Z = \mathcal{V}(S)$. We conjecture that $S = \mathcal{N}(Z)$. Certainly, given any $f \in S$, we have $f(x) = 0$ for all $x \in Z$, which implies $f \in \mathcal{V}(Z)$, and hence $S \subseteq \mathcal{N}(Z)$. Due to this inclusion it is reasonable to see that $\mathcal{V}\big(\mathcal{N}(Z)\big) \subseteq \mathcal{V}(S) = Z$. Certainly, given any $x \in Z$, we have $x \in \mathcal{V}\big(\mathcal{N}(Z)\big)$ and so $Z \subseteq \mathcal{V}\big(\mathcal{N}(Z)\big) \Rightarrow Z = \mathcal{V}\big(\mathcal{N}(Z)\big) \Rightarrow S = \mathcal{N}(Z)$.

We check that $\mathcal{N}(Z)$ is in fact an ideal of $E[V]$. Given any $f, g \in \mathcal{N}(Z)$ and $x \in Z$ we have $(f+g)(x) = f(x) + g(x) = 0$ and so $f + g \in I$. Let $x \in V$ and $h \in E[V]$, then $(hf)(x) = h(x)f(x) = 0$ and so $hf \in \mathcal{N}(Z)$, which implies $\mathcal{N}(Z)$ is an ideal of $E[V]$. Thus, suppose $Z_1 \supseteq Z_2 \supseteq \cdots$ is a descending chain of closed sets in V. Then we have an ascending chain of ideals $\mathcal{N}(Z_1) \subseteq \mathcal{N}(Z_2) \subseteq \cdots$ in $E[V]$.

Any field E will definitely be Noetherian, as the only ideals of E are $\{0\}$ and E itself. Thus, by Theorem 6.1 we have $E[V]$ will be Noetherian if $E[V]$ is finitely generated. In any affine variety, say V, we have $E[V]$ is finitely generated and so $E[V]$ is Noetherian. Hence, there exists an r such that $\mathcal{N}(Z_r) = \mathcal{N}(Z_n)$, for all $n \geqslant r$. However, for any Z_i we have $Z_i = \mathcal{V}\big(\mathcal{N}(Z_i)\big)$, and so

$$Z_r = \mathcal{V}\big(\mathcal{N}(Z_r)\big) = \mathcal{V}\big(\mathcal{N}(Z_n)\big) = Z_n$$

for all $n \geqslant r$. Hence, any affine variety V will be a Noetherian topological space.

Definition. Let X be a topological space. Then X is *irreducible* if it is impossible to write $X = Y \cup Z$ for proper closed subsets Y, Z of X. If X is not irreducible then we say X is *reducible.*

Proposition: *Let X be a topological space. Then X is* irreducible $\Leftrightarrow$ *given any two open subsets U, V of X we have $U \cap V$ is non-empty.*

Proof. Let U, V be two open subsets of X, then there exist two closed subsets Z, W of X, such that $U = \overline{Z}$ and $V = \overline{W}$. We consider the intersection of these sets and see

$$U \cap V = \overline{Z} \cap \overline{W} = \overline{Z \cup W},$$

by DeMorgan's laws. We have $U \cap V \neq \emptyset \Leftrightarrow Z \cup W \neq X \Leftrightarrow X$ is irreducible. □

This poses a natural question. "Can all Noetherian topological spaces be expressed as a finite union of closed irreducible sets?" If we assume not, then there exists a topological space X, which does not have a finite expression. Let $Y \subseteq X$ be the smallest closed subset which cannot be expressed in this way. We can see that Y cannot be irreducible and so $Y = M \cup N$ for some closed subsets M, N of V. We proposed that Y was the least amongst all subsets that could not be expressed in this way, and so both M and N are a finite union of closed irreducible sets. However, this gives us Y is a finite union but this is a contradiction. Hence, any Noetherian topological space X can be written as a finite union of closed irreducible sets.

Definition. Let X be a set and $X_1, \ldots, X_n$ be subsets of X such that $X = X_1 \cup \cdots \cup X_n$. We say X is *irredundant* if, for any $i \neq j$ we have $X_i \nsubseteq X_j$.

Theorem 7.1. *Let X be a Noetherian topological space. Then, X can be written as an irredundant finite union of irreducible closed subsets of X. Furthermore, this expression is unique up to the ordering of the sets.*

Proof. By our previous remark we have that X must be a finite union of closed irreducible subsets of X, say

$$X = X_1 \cup X_2 \cup \cdots \cup X_n.$$

If we write this expression with n as small as possible, then each X_i is distinct and hence X is irredundant. Assume X has a second expression as an irredundant finite union of irreducible closed sets, say

$$X = X'_1 \cup X'_2 \cup \cdots \cup X'_m.$$

Now we can see that, for any X_i, $(1 \leqslant i \leqslant n)$, we have

$$X_i = X_i \cap X = X_i \cap (X'_1 \cup \cdots \cup X'_m) = (X_i \cap X'_1) \cup \cdots \cup (X_i \cap X'_m).$$

However, each X_i is an irreducible set and so there must exist a $1 \leqslant j \leqslant m$ such that $X_i = (X_i \cap X'_j)$. Clearly, we can see that $X_i \subseteq X'_j$ and $X'_j \subseteq X_k$ for some $1 \leqslant k \leqslant n$. Thus, we have $X_i \subseteq X_k$ but X is irredundant and so $i = k$. We can now define a map $\sigma : \{1, \dots, n\} \to \{1, \dots, m\}$ between the indices of our subsets such that $X_i = X'_{\sigma(i)}$. However, we also have a map $\tau : \{1, \dots, m\} \to \{1, \dots, n\}$ such that $X'_j = X_{\tau(j)}$. Thus, we have for any $1 \leqslant i \leqslant n$ that

$$X_i = X'_{\sigma(i)} = X_{\tau(\sigma(i))} = X_{(\tau\circ\sigma)(i)}.$$

Hence, $\tau \circ \sigma = \mathrm{id}_{\{1,\dots,n\}} \Rightarrow \sigma$ and τ are bijections, which means $n = m$. Thus the expression of X is unique up to the ordering of the subsets. □

Now we have expanded our understanding of topological spaces, we can reformulate Hilbert's Nullstellensatz in the language of affine varieties. There are in fact two versions of the Nullstellensatz that we will state and prove. They are referred to as the weak and strong forms of the Nullstellensatz. The strong form is the version that infers the statement of Corollary 5.1.

Theorem 7.2 (Hilbert's Nullstellensatz - weak form)**.** *Let E be a field and (V, A) be an affine variety.*

(i) *Let A be a finitely generated E-algebra. Then every maximal ideal of A has codimension 1.*

(ii) *Let I be an ideal of A such that $I \neq A$ then $\mathcal{V}(I) \neq \emptyset$.*

Proof.

(i) Let M be a maximal ideal of A, then we have A/M is a field by Theorem 2.2. We can view $E \subseteq A/M$ as a field extension, and so

$$\mathrm{codim}(M) = [A/M : E],$$

(i.e. the dimension of A/M as a vector space over A). By Noether normalization we have that A/M is integral over some polynomial algebra $E[X_1, \dots, X_n]$, where $X_1, \dots, X_n$ are algebraically independent. Now, as A/M is a field we have $E[X_1, \dots, X_n]$ is a field, (see Corollary of Proposition 1, Appendix A3 of [5]). We can see that $E \subseteq E[X_1, \dots, X_n]$ and therefore $E = E[X_1, \dots, X_n]$. So, $E \subseteq A/M$ is an algebraic extension of E. However, E is algebraically closed and so we must have $A/M = E$, and hence $\operatorname{codim}(M) = 1$.

(ii) Consider M' to be the maximal ideal of A such that $I \subseteq M'$. Now, consider an E-algebra map $\lambda : A \to E$, such that $\operatorname{Ker}(\lambda) = M'$. We have that (V, A) is an affine variety, hence there exists an $x \in V$ such that $\lambda = \varepsilon_x$. For any $f \in I$ we have $f(x) = \varepsilon_x(f) = \lambda(f) = 0$ and so $x \in \mathcal{V}(I)$, as required. □

Definition. Let (V, A) be an affine variety and I an ideal of A, then we define the *radical* of I to be

$$\sqrt{I} = \{f \in A \mid f^n \in I \text{ for some } n \geqslant 0\}.$$

Proposition: *Let (V, A) be an affine variety and I an ideal of A. Then the radical of I is also an ideal of A.*

Proof. Let $f, g \in \sqrt{I}$, then there exist integers $s, t \geqslant 0$ such that $f^s, g^t \in I$. Now, we wish to show that $f + g \in \sqrt{I}$, i.e. there exists an integer $p \geqslant 0$ such that $(f + g)^p \in I$. Consider $p = s + t$, then by the binomial theorem we have

$$(f + g)^{s+t} = \sum_{i=0}^{s+t} \binom{s+t}{i} f^{s+t-i} g^i.$$

We have two cases to consider. If $i \leqslant t$ then we have $f^{s+t-i} \in I$ and so any term containing f^{s+t-i} will be in I by the ideal property. If $i \geqslant t$ then $g^i \in I$ and hence any term containing g^i will be in I by the ideal property. Thus, all terms of the expansion are in I and so $(f + g)^{s+t} \in I$. Hence, we have $f + g \in \sqrt{I}$.

Let $h \in A$ and f as above. Then we have $hf^s \in I \Rightarrow (hf)^s \in I$ and so $hf \in \sqrt{I}$. Clearly we have $0 \in \sqrt{I}$ and so $\sqrt{I}$ is an ideal of A. □

We finally introduce the reformulation of our original statement of Hilbert's Nullstellensatz from section 5. By considering the affine variety $(E^n, E[X_1, \dots, X_n])$ it is clear that the second statement below infers Theorem 5.1. Theorem 5.1 only gives us that $\mathcal{N}(\mathcal{V}(I)) \subseteq \sqrt{I}$, whereas the formulation below gives us equality between these sets.

Theorem 7.3 (Hilbert's Nullstellensatz - strong form)**.** *Let E be a field and (V, A) an affine variety.*

(i) *Let A be a finitely generated E-algebra. Then the intersection of the maximal ideals of A is the nilradical of A.*

(ii) *Let I be an ideal of A, then $\mathcal{N}(\mathcal{V}(I)) = \sqrt{I}$.*

Proof.

(i) We have that the nilradical of A is the intersection of the prime ideals of A, (see Appendix A1 of [5]). Therefore, all we have to show is that each prime ideal, (say P), of A is in fact the intersection of the maximal ideals which contain it. It will be fine to replace A by the quotient A/P, and therefore we can assume A is an integral domain. Let $f \in A$ be a non-zero element. By Noether normalization we have A is integral over a polynomial algebra $B = E[Y_1, \dots, Y_n]$, for some algebraically independent elements $Y_1, \dots, Y_n$. Thus, there exists a monic polynomial in $B[X]$ such that

$$f^m + b_1 f^{m-1} + \cdots + b_m = 0, \tag{3}$$

where $b_i \in B$ and $b_m \neq 0$. We consider b_m to be a polynomial $g = g(Y_1, \dots, Y_n) \in B$. We regard g as a non-zero function $g : E \to B$ and hence there must exist $y_1, \dots, y_n \in E$, such that $g(y_1, \dots, y_n) \neq 0$. Hence, g does not belong to the maximal ideal $M = \langle Y_1 - y_1, \dots, Y_n - y_n \rangle$ of B.

Now A is integral over B. By Lemma 4.5 there exists a prime ideal Q of A, such that Q lies above M, (i.e. $Q \cap B = M$). Consider $I \neq A$ to be an ideal of A, such that $Q \subseteq I$, then $M \subseteq I \cap (Q \cap B) = I \cap B$. However, by the maximality of M this must give us $M = I \cap B$. If f is an element of Q, then by (3) we have that $g \in Q$ and hence $g \in M$, but this is a contradiction. So we have $f \notin Q$. Thus every non-zero element of A has a corresponding maximal ideal Q of A, such that $f \notin Q$. Hence the intersection of all maximal ideals of A is 0, and we are done.

(ii) Given any $f \in \sqrt{I}$ we have $f^m \in I$ for some $m \geqslant 0$. Now, if $f^m \in I$ then surely $f^m(x) = 0$, for all $x \in \mathcal{V}(I)$, and so $f^m \in \mathcal{N}(\mathcal{V}(I))$. However, f^m is also in $\sqrt{I}$ and so $\sqrt{I} \subseteq \mathcal{N}(\mathcal{V}(I))$. We wish to show the reverse inclusion, that $\mathcal{N}(\mathcal{V}(I)) \subseteq \sqrt{I}$. Suppose, for a contradiction, that there exists an element $f \in C = \mathcal{N}(\mathcal{V}(I)) \setminus \sqrt{I}$. By applying part (i) of this theorem to A/I, we have there exists a maximal ideal M', (such that $I \subseteq M'$), with $f \notin M'$. By part (i) of the weak form of the Nullstellensatz we have $\operatorname{codim}(M') = 1$. Consider $\lambda : A \to E$ to be the E-algebra homomorphism, such that $\operatorname{Ker}(\lambda) = M'$. Then, because (V, A) is an affine variety, we have $\lambda = \varepsilon_x$ for some $x \in V$. However, we have $x \in \mathcal{V}(I)$ and so $f(x) = \varepsilon_x(f) = \lambda(f) \neq 0 \Rightarrow f \notin \mathcal{N}(\mathcal{V}(I))$, which is a contradiction. □

Having introduced the Nullstellensatz in the language of affine varieties, we bring our discussion of algebraic geometry to a close by considering the dimension of a variety. To do so we need to introduce a number of definitions.

Definition. Let X be a topological space. We say X has *dimension* n if, given any strictly ascending chain of closed irreducible subsets of X

$$X_0 \subset X_1 \subset X_2 \subset \cdots \subset X_r,$$

the largest possible value of r is n. Equivalently, there exists no strictly ascending chain of closed irreducible subsets of X longer than n. If there is no bound on the length of these chains then we say the dimension of X is ∞. We refer to the dimension of X as $\dim X$.

Definition. Let E be a field, then we define the *free polynomial algebra* over E, which we write $E[X_1,\dots,X_n]$. This algebra consists of all linear combinations of the $X_1,\dots,X_n$ with coefficients in E. This is considered to be the noncommutative analogue of the polynomial ring as the difference in this case is that the X_i do not commute [12].

If A is a ring, then we define a topology, (known as the spectral topology), on A as the set of all prime ideals in A. For any subset $S \subseteq A$ we define the closed sets of the spectral topology to be

$$\mathcal{V}(S) = \{P \in \operatorname{Spec}(A) \mid S \subseteq P\}.$$

We can see that this will form a topological space over A, by the properties of prime ideals. Hence our above definition of dimension for a topological space applies to the spectral topology. We refer to the dimension of spec(A) by $\dim(A)$.

Proposition: *Let E be a field and B an E-algebra, such that B is integral over the free polynomial algebra $A = E[X_1,\dots,X_n]$. Then we have the dimension of* $\operatorname{Spec}(B)$ *is n.*

Proof. We prove this by showing that the inequalities, $\dim(B) \leqslant n$ and $\dim(B) \geqslant n$, both hold. We start by showing $\dim(B) \leqslant n$. To do this we must show that any strictly ascending chain of prime ideals

$$P_0 \subset P_1 \subset \cdots \subset P_r$$

in $\operatorname{Spec}(B)$ is such that $r \leqslant n$. By factoring out P_0, (i.e. the prime $\{0\}$), we can assume that B is an integral domain. We create an induction argument on n. If $n = 0$ then we have that B is a field, (see Corollary, Appendix A3 in [5]), and so $\dim(B) = 0$. Now assume that $n \geqslant 1$ and that the assumption holds for E-algebras, which are integral over a polynomial algebra in m variables, such that $m < n$.

Now let $0 \neq f \in P_1$. We have that there exists a monic polynomial in $A[X]$, such that

$$f^k + a_0 f^{k-1} + \cdots + a_k = 0$$

and $a_k \neq 0$. Think of a_k as a polynomial $g = g(X_1,\dots,X_n)$. We have B/P_1 is integral over $\bar{A} = A/(P_1 \cap A)$. So $\bar{A} = E[x_1,\dots,x_n]$, where each $x_i = X_i + P_1 \cap A$. We can see that these elements will not be algebraically independent because $g(x_1,\dots,x_n) = 0$. By Noether normalization we have $\bar{A}$ is integral over a polynomial algebra $E[y_1,\dots,y_m]$ for some algebraically independent $y_1,\dots,y_m$, such that $m < n$. Now, by a proposition from section 4, we have B/P_1 is integral over $E[y_1,\dots,y_m]$ because $\bar{A}$ is integral over $E[y_1,\dots,y_m]$. By the inductive hypothesis we have $\dim B/P_1 \leqslant m$, and so the chain

$$P_1/P_1 \subset P_2/P_1 \subset \cdots \subset P_r/P_1$$

has, at most, length m. Thus we have $r - 1 \leqslant m < n \Rightarrow r \leqslant n$, as required.

We now show the reverse inequality. In A we have a natural strictly ascending chain of prime ideals

$$\langle 0\rangle \subset \langle X_1\rangle \subset \langle X_1, X_2\rangle \subset \cdots \subset \langle X_1, \ldots, X_n\rangle,$$

which gives us that $\dim(A) \geqslant n$. We have $\dim(B) \geqslant \dim(A)$, (see Lemma, Appendix A5 in [5]), and so $\dim(B) \geqslant n \Rightarrow \dim(B) = n$, as required. □

Let V be an affine variety and

$$X_0 \subset X_1 \subset \cdots \subset X_m$$

a chain of closed irreducible subsets in V. Then $\mathcal{V}(X_i)$, for $0 \leqslant i \leqslant m$, will be a prime ideal of $E[V]$. Therefore, the above chain gives us a strictly ascending chain of prime ideals in $E[V]$

$$\mathcal{V}(X_0) \subset \mathcal{V}(X_1) \subset \cdots \subset \mathcal{V}(X_m).$$

Conversely, any strictly ascending chain of prime ideals $P_0 \subset \cdots \subset P_t$ of V will give us a strictly ascending chain of closed irreducible subsets

$$\mathcal{V}(P_0) \subset \cdots \subset \mathcal{V}(P_t).$$

Therefore, we can see that the dimension of V will be the dimension of the spectral topology of the ring $E[V]$. As a consequence of the above proposition, we will have the dimension of V is finite and, if V is an irreducible topological space, then the dimension of V will be equal to the transcendence degree of $E[V]$ over E.

8. Conclusion

The most significant outcome of this project is the proof that the dimension of an affine variety is equal to the transcendence degree of its field of fractions. In our journey to this point we have encountered many useful tools in the areas of commutative ring theory and field theory. One theorem of major importance to us has been Hilbert's Nullstellensatz. This allowed us to show that the set of polynomials, which vanish on all zeros of an ideal I, is equal to the radical of I – an equality which was only achieved, however, when we reformulated the result in the language of affine varieties.

This study of dimension could be taken further by introducing a local notion of dimension, that of the dimension of the tangent space $T_x(V)$, for any x in an affine variety V. This notion of local dimension is useful as it forms the basis of many inductive arguments in algebraic geometry.

The theory of algebraic geometry is linked very closely with the theory of *algebraic groups*. We say a group G is an *algebraic group* if G is also an affine variety, such that multiplication and inversion of elements are morphisms of varieties. These can lead to many interesting theorems, such as Borel's Fixed Point Theorem, (I refer the reader to [5] for further details).

Algebraic Groups also play a vital role in the classification of finite simple groups. By working with algebraic groups over finite fields of characteristic $p > 0$ we can classify nearly all the finite simple groups. The only groups that evade classifying in this manner are the alternating groups and 26 sporadic simple groups.

The transcendence degree of a field of fractions is in fact an invariant and hence the dimension of an affine variety is an invariant. One of the major open problems in algebraic geometry is to classify all the algebraic varieties, up to isomorphism. The seeking out of numerical invariants, such as dimension, is therefore of great importance. Clearly dimension alone is not going to be enough to distinguish an algebraic variety but it is a starting point.

What we have not shown here is the interrelation of the different technical languages of algebraic geometry. In particular the language of schemes, developed by Alexander Grothendieck. This is a fascinating area of mathematics with endless possibilities for discovery and, given time, we would have been able to show that the alternate definition of dimension, under schemes, is in fact equivalent to the definition introduced in this project.

References

[1] Serge Lang, *Algebra.* Addison Wesley Publishing Company, Massachusetts, 1965.

[2] Brent Everitt, *Symmetries of Equations: An Introduction to Galois Theory.* Lecture course, University of York (2007).

[3] Wikipedia Article on Algebraically Independent Elements. `http://en.wikipedia.org/wiki/Algebraically_independent`. 17th April 2008 - 18:47.

[4] Stephen Donkin, *Advanced Algebra (Ring Theory).* Lecture course, University of York (2007).

[5] Stephen Donkin, *Five Lectures on Algebraic Groups.* Lecture course, University of Alberta (2000).

[6] Peter J. Cameron, *Introduction to Algebra.* Oxford University Press, 1998.

[7] Meinolf Geck, *An Introduction to Algebraic Geometry and Algebraic Groups.* Oxford University Press, 2003.

[8] Joe Harris, *Algebraic Geometry: A First Course.* Springer-Verlag, 1992.

[9] Robin Hartshorne, *Algebraic Geometry.* Springer-Verlag, 1977.

[10] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag, 1995.

[11] Wikipedia Article on Oscar Zariski. `http://en.wikipedia.org/wiki/Oscar_Zariski`. 7th May 2008 - 18:41.

[12] Wikipedia Article on the Free Algebra. `http://en.wikipedia.org/wiki/Free_algebra`. 9th May 2008 - 13:24.