MATH 6122: Algebra II

Joe Tran

Winter 2025

Preface

These are the first edition of these lecture notes for MATH 6122 (Algebra II). Consequently, there may be several typographical errors, missing exposition on necessary background, and more advanced topics for which there will not be time in class to cover. Future iterations of these notes will hopefully be fairly self-contained provided one has the necessary background. If you come across any typos, errors, omissions, or unclear expositions, please feel free to contact me so that I may continually improve these notes.

Contents

Chapter 1

Fields and Galois Theory

This chapter contains the most important results for this chapter: The Fundamental Theorem of Algebra and the Unsolvability of the Quintic. Hungerford's treatment of Galois theory is based on the approach of Irving Kaplansky who extended the ideas of Emil Artin. In Galois theory, we consider field F an extension of field K; that is, K is a subfield of F. The Galois group of extension F of K is the group of all automorphisms of F that fix K elementwise. The Fundamental Theorem of Galois Theory states that there exists a bijection between the intermediate fields of a finite-dimensional Galois field extension and the subgroups of the Galois group of the extension. The fundamental theorem allows us to translate problems involving fields, polynomials, and field extensions into group theoretic terms (thus making group theory the central part of abstract algebra as well as classical algebra–particularly, the algebraic solvability of a polynomial equation).

1.1 Field Extension

The basic facts needed for the study of field extensions are presented first, followed by a discussion of simple extensions. Finally, a number of essential properties of algebraic extensions are proved.

Definition 1.1.1

A field F is said to be an *extension field* of K (or simply an extension of K) provided that K is a subfield of F.

If F is an extension of K, then it is easy to note that $1_K = 1_F$. Furthermore, F is a vector space over K. Throughout this chapter, the dimension of the vector space F over K will be denoted by $[F : K]$ rather than $\dim_K(F)$.

Definition 1.1.2

If F is a field and K is a subfield of F, then F is said to be a *finite-dimensional extension* if $[F : K]$ is finite. If $[F : K]$ is not finite, then we say that F is an *infinite-dimensional extension* if $[F : K]$ is infinite.

Theorem 1.1.3

Let F be a field extension of E, and E be an extension field of K. Then

$$[F:K] = [F:E][E:K]$$

i.e. F is a field extension of K. Furthermore, $[F:K]$ is finite if and only if $[F:E]$ and $[E:K]$ are finite.

Proof.

The proof is very easy; to see that F is a field extension of K, then note since we have F is a field extension of E, then we have $[F:E]$, and similarly, since E is a field extension of K, then we have $[E:K]$, and therefore,

$$[F:K] = [F:E][E:K]$$

Therefore, F is a field extension of K.

To prove the second assertion, first note that if $[F:E]$ and $[E:K]$ are finite, then $[F:K]$ is also finite. Conversely, if $[F:E]$ and $[E:K]$ are infinite, then so is $[F:K]$. ■

Definition 1.1.4

If F is a field extension of E and E is a field extension of K, i.e. $K \leq E \leq F$, then we call E an *intermediate field.*

Definition 1.1.5

If F is a field and $X \subset F$, then the *subfield* (resp. *subring*) *generated by* X is the intersection of all subfields (resp. subrings) of F that contain X. If F is a field extension of K and $X \subset F$, then the subfield (resp. subring) generated by $K \cup X$ is called the *subfield* (resp. *subring*) *generated by* X *over* K and is denoted by $K(X)$ (resp. $K[X]$). Note that $K[X]$ is necessarily an integral domain.

Definition 1.1.6

If $X = \{x_1, ..., x_n\}$, then the subfield $K(X)$ (resp. subring $K[X]$) of F is denoted by $K(x_1, ..., x_n)$ (resp. $K[x_1, ..., x_n]$). The field $K(x_1, ..., x_n)$ is said to be *finitely generated extension* of K (but it need not be finite-dimensional over K). If $X = \{x\}$, then $K(x)$ is said to be a *simple extension of* K.

Theorem 1.1.7

If F is an extension field of a field K, $x, x_1, ..., x_n \in F$, and $X \subset F$, then

(i) The subring $K[x]$ consists of all elements of the form $f(x)$, where f is a polynomial with coefficients in K.

(ii) The subring $K[x_1, ..., x_n]$ consists of all elements of the form $f(x_1, ..., x_n)$ where f is a polynomial in n indeterminates with coefficients in K.

(iii) The subring $K[X]$ consists of all elements of the form $f(x_1, ..., x_n)$, where each $x_i \in X$, $n \in \mathbb{N}$, and f is a polynomial in n indeterminates with coefficients in K.

(iv) The subfield $K(x)$ consists of all elements of the form $f(x)g^{-1}(x)$ where $f, g \in K[x]$ and $g(x) \neq 0$.

(v) The subfield $K(x_1, ..., x_n)$ consists of all elements of the form $f(x_1, ..., x_n)g^{-1}(x_1, ..., x_n)$ where $f, g \in K[x_1, ..., x_n]$ and $g(x_1, ..., x_n) \neq 0$.

(vi) The subfield $K(X)$ consists of all elements of the form $f(x_1, ..., x_n)g^{-1}(x_1, ..., x_n)$ where $n \in \mathbb{N}$, $f, g \in K[x_1, ..., x_n]$, $x_1, ..., x_n \in X$ and $g(x_1, ..., x_n) \neq 0$.

(vii) For each $v \in K(X)$ (resp. $K[X]$), there exists a finite subset Y subset of X such that $v \in K(Y)$ (resp. $K[Y]$).

Proof.

We will only prove (vi) and (vii).

To see that (vi) holds, note that every field that contains K and X must contain the set

$$E = \left\{ \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)} : n \in \mathbb{N}, f, g \in K[x_1, ..., x_n], x_1, ..., x_n \in X, g(x_1, ..., x_n) \neq 0 \right\}$$

and so $E \subset K(X)$. For the other inclusion, if $f, g \in K[x_1, ..., x_m]$ and $f_1, g_1 \in K[x_1, ..., x_n]$, then define $h, k \in K[x_1, ..., x_{m+n}]$ by

$$h(x_1, ..., x_{m+n}) = f(x_1, ..., x_m)g_1(x_{m+1}, ..., x_{m+n}) - g(x_1, ..., x_m)f_1(x_{m+1}, ..., x_{m+n})$$

and $k(x_1, ..., x_{m+n}) = g(x_1, ..., x_m)g_1(x_{m+1}, ..., x_{m+n})$. Then for any $x_1, ..., x_m$, $y_1, ..., y_n \in X$ such that $g(x_1, ..., x_m) \neq 0$ and $g(y_1, ..., y_n) \neq 0$,

$$\frac{f(x_1, ..., x_m)}{g(x_1, ..., x_m)} - \frac{f_1(y_1, ..., y_n)}{g_1(y_1, ..., y_n)} = \frac{h(x_1, ..., x_m, y_1, ..., y_n)}{k(x_1, ..., x_m, y_1, ..., y_n)} \in E$$

Therefore, E is an additive subgroup of F. Similarly,

$$\frac{\frac{f(x_1, ..., x_m)}{g(x_1, ..., x_m)}}{\frac{f_1(y_1, ..., y_n)}{g_1(y_1, ..., y_n)}} = \frac{f_2(x_1, ..., x_m, y_1, ..., y_n)}{g_2(x_1, ..., x_m, y_1, ..., y_n)} \in E$$

and so $E \setminus \{0\}$ is a multiplicative subgroup. So E is a field. Since $K(X)$ is the intersection of all fields containing $K \cup X$, then $K(X) \subset E$. Therefore, $K(X) = E$.

To see that (vii) holds, if $x \in K(X)$, then by (vi),

$$x = \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)}$$

for some $n \in \mathbb{N}$ and $f, g \in K[x_1, ..., x_n]$. So with $X' = \{x_1, ..., x_n\}$, we have $x \in K(X')$. ■

Definition 1.1.8

If K and L are subfields of a field F, the *composite* of K and L in F, denoted by KL, is the subfield generated by the set $X = K \cup L$.

We now distinguish between two types of elements of an extension field. This is fundamental to all that follows.

Definition 1.1.9

Let F be an extension field of K.

(i) An element $\alpha \in F$ is *algebraic* over K if α is a root of some polynomial $p \in K[x]$.

(ii) If α is not a root of any nonzero $p \in K[x]$, then α is *transcendental* over K.

(iii) F is an *algebraic extension* of K if every element of F is algebraic over K.

(iv) F is a *transcendental extension* if at least one element of F is transcendental over K.

Example 1.1.10

The most common example of an algebraic extension field is

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

Another useful algebraic extension is

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} \simeq \mathbb{C}$$

The list of known transcendental real numbers is brief, but includes π and e. A readable account of transcendental numbers is *Making Transcendence Transparent: An Intuitive Approach to Classical Transcendental Number Theory* by E. Burger and R. Tubbs, Springer (2004).

Example 1.1.11

If K is a field, then the polynomial ring $K[x_1, ..., x_n]$ is an integral domain. The field of quotients of $K[x_1, ..., x_n]$ is denoted $K(x_1, ..., x_n)$. The elements of field $K(x_1, ..., x_n)$ consist of all fractions fg^{-1} where $f, g \in K[x_1, ..., x_n]$ and $g \neq 0$. The field $K(x_1, ..., x_n)$ is the *field of rational functions* in indeterminates $x_1, ..., x_n$ over K.

In the following two theorems, we classify simple extensions (first, extending by a transcendental and second extending by an algebraic).

Theorem 1.1.12

If F is an extension field of K and $\alpha \in F$ is transcendental over K, then there exists an isomorphism of fields $K(\alpha) \simeq K(x)$ which is the identity when restricted to K.

Proof.

Assume that α is transcendental. Then $f(\alpha), g(\alpha) \neq 0$ for all nonzero $f, g \in K[x]$. Let $\phi : K(x) \to F$ by the map $fg^{-1} \mapsto f(\alpha)g(\alpha)^{-1}$. "Clearly", ϕ is a homomorphism. Now for $f_1g_1^{-1} \neq f_2g_2^{-1}$ then $f_1g_2 \neq f_2g_1$ and $f_1g_2 - f_2g_1 \neq 0$ (not the zero polynomial). Now,

$$f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha) \neq 0$$

and so

$$\phi(f_1g_1^{-1}) = f_1(\alpha)g_1(\alpha)^{-1} \neq f_2(\alpha)g_2(\alpha)^{-1} = \phi(f_2g_2^{-1})$$

Therefore, ϕ is an injection. Also, ϕ is the identity on K (treating K as a subfield of $K(x)$; think of K as the constant rational functions in $F(x)$). Therefore, by Theorem 1.1.7 (iv), the image of ϕ is $K(\alpha)$, so ϕ is an isomorphism from $K(x)$ to $K(\alpha)$ which is the identity on K. ■

Theorem 1.1.13

If F is an extension field of K and $\alpha \in F$ is algebraic over K, then

(i) $K(\alpha) = K[\alpha]$.

(ii) $K(\alpha) \simeq K[x]/\langle f \rangle$, where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(\alpha) = 0$ and $g(\alpha) = 0$, where $g \in K[x]$, if and only if $f \mid g$.

(iii) $[K(\alpha) : K] = n$

(iv) $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis of the vector space $K(\alpha)$ over K.

(v) Every element of $K(\alpha)$ can be written uniquely of the form

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

where each $a_i \in K$.

Theorem 1.1.13 tells us what elements of the algebraic extension $K(\alpha)$ of K "look like". That is, there exists a fixed $n \in \mathbb{N}$ such that every element of $K(\alpha)$ is of the form

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

for some $a_i \in K$. Notice that Theorem 1.1.12 and Theorem 1.1.7 (iv) tell us what elements of the transcendental extension $K(\alpha)$ of K "look like":

$$\frac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_m\alpha^m}$$

where $a_1, ..., a_n, b_1, ..., b_m \in K$ and $b_0 + b_1\alpha + \cdots + b_m\alpha^m \neq 0$.
Proof.

We first prove (i) and (ii). Define $\phi : K[x] \to K[\alpha]$ by $g \to g(\alpha)$. It is easy to see that ϕ is a ring homomorphism. By Theorem 1.1.7 (i), ϕ is onto. Since K is a field, then $K[x]$ is a principal ideal domain. Now, $\ker(\phi)$ is an ideal, so $\ker(\phi) = \langle f \rangle$ for some $f \in K[x]$. Notice that $\phi(f) = f(\alpha) = 0$. Since α is algebraic, $\ker(\phi) \neq \{0\}$. Also, $\ker(\phi) \neq K[x]$ (for example, nonzero constant polynomials are not mapped to zero). So $f \neq 0$ and $\deg(f) \geq 1$. Furthermore, if c is the leading coefficient of f, then c is a unit in $K[x]$, and so $c^{-1}f$ is monic. Consequently, without loss of generality, assume that f is monic. Then by the First Isomorphism Theorem of Rings, $K[x]/\langle f \rangle = K[x]/\ker(\phi) \simeq \text{Range}(\phi) = K[\alpha]$. Since $K[\alpha]$ is an integral domain, since K is a field, the ideal of $\langle f \rangle$ is prime. Since $\langle f \rangle$ is a prime ideal, then f itself is a prime element of $K[x]$ and so, f is irreducible in $K[x]$ (notice that $K[x]$ is a principal ideal domain as explained above), and thus, $\langle f \rangle$ is a maximal ideal in $K[x]$. Consequently, $K[x]/\langle f \rangle$ is a field. Now, since $K(\alpha)$ is the smallest subfield of F containing $K \cup \{\alpha\}$ (since $K(\alpha)$ is the intersection of all subfields of F containing $K \cup \{\alpha\}$), and $K[\alpha]$ is a ring containing $K \cup \{\alpha\}$, but $K[\alpha]$ is a subfield since $K[\alpha] \simeq K[x]/\langle f \rangle$, then $K(\alpha) \subset K[\alpha]$. However, in general, the ring $K[\alpha]$ is a subset of the field $K(\alpha)$, so $K(\alpha) \supset K[\alpha]$, so we must have $K(\alpha) = K[\alpha]$, and (i) follows. We have established (ii), except for the uniqueness claim. Suppose $g(\alpha) = 0$ for $g \in K[x]$. Then $\phi(g) = g(\alpha) = 0$, and so $g \in \ker(\phi) = \langle f \rangle$. Since the principal ideal $\langle f \rangle$ consists of all multiples of f, then g is a multiple of f, that is, f divides g, so (i) follows.

We next prove (iv). By Theorem 1.1.7 (i), every element of $K[\alpha] = K(\alpha)$ is of the form $g(\alpha)$ for some $g \in K[x]$. By the Division Algorithm, we know that $g(x) = q(x)f(x) + r(x)$ with $q, r \in K[x]$, and $\deg(r) < \deg(f)$. Therefore,

$$g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = 0 + r(\alpha) = b_0 + \cdots + b_m\alpha^m$$

with $m < n = \deg(f)$. Thus, every element of $K(\alpha)$ can be written as a linear combination of $1_K, \alpha, \alpha^2, ..., \alpha^{n-1}$. That is, $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ spans $K(\alpha)$. Now, to see that $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is linearly independent over K, assume

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

for some $a_0, ..., a_{n-1} \in K$. Then

$$g = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in K[x]$$

has α as a root and has a degree of at most $n-1$. Then by (ii), $f \mid g$ and $\deg(f) = n$, so it must be that $g = 0$; i.e. $a_i = 0$ for all i, and so $\{1_K, ..., \alpha^{n-1}\}$ is linearly independent and hence is a basis of $K(\alpha)$.

Next, we prove (iii). Note that $[K(\alpha) : K]$ denotes the dimension of $K(\alpha)$ as a vector space. So by (iv), we have

$$K[(\alpha) : K] = n$$

Now we prove (v). By (iv), every element of $K(\alpha)$ can be written in the form

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

for some $a_0, ..., a_{n-1} \in K$, since $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis. For uniqueness, suppose

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

Then

$$(a_0 - b_0) + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0$$

and since $\{1_K, \alpha, ..., \alpha^{n-1}\}$ is linearly independent, so

$$a_0 - b_0 = \cdots = a_{n-1} - b_{n-1} = 0$$

and thus, $a_i = b_i$ for all $0 \leq i \leq n-1$, and the representation is unique. ■

Definition 1.1.14

Let F be an extension field of K and $\alpha \in F$ algebraic over K. The monic irreducible polynomial f of Theorem 1.1.13 (ii) is the *irreducible polynomial of* α. The *degree of* α *over* K is $\deg(f) = [K(\alpha) : K]$.

Example 1.1.15

The polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, since the only possible rational roots are ± 1, neither of which is a root (we have also used the Factor Theorem here). By the Intermediate Value Theorem, there exists a real root α. Now, $x^3 - 3x - 1$ is irreducible polynomial of α, so α has degree 3 over $\mathbb{Q}$, and $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ by Theorem 1.1.13 (iv). Now, $\alpha^4 + 2\alpha^3 + 3 \in \mathbb{Q}(\alpha)$ and so must be some linear combination of $1, \alpha, \alpha^2$. The division algorithm in $\mathbb{Q}[x]$ gives

$$x^4 + 2x^3 + 3 = (x+2)(x^3 - 3x - 1) + (3x^2 + 7x + 5)$$

and so

$$\begin{aligned}\alpha^4 + 2\alpha^3 + 3 &= (\alpha+2)(\alpha^3 - 3\alpha - 1) + (3\alpha^2 + 7\alpha + 5)\\ &= (\alpha+2)(0) + (3\alpha^2 + 7\alpha + 5)\\ &= 3\alpha^2 + 7\alpha + 5\end{aligned}$$

In notation of linear algebra, we would say that $\alpha^4 + 2\alpha^3 + 3$ has coordinate representation $[5, 7, 3]_B$ with respect to the ordered basis $B = \{1, \alpha, \alpha^2\}$.

Suppose we have the fields $K \leq E$ and $L \leq F$ and $\sigma : K \to L$ is an isomorphism between E and F. The following result addresses this for simple extensions.

Theorem 1.1.16

Let $\sigma : K \to L$ be an isomorphism of fields, α be an element of some extension field of K and β be an element of some extension field of L. Assume either

(i) α is transcendental over K and β is transcendental over L.

(ii) α is a root of an irreducible polynomial $f \in K[x]$ and β is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(\alpha) \simeq L(\beta)$ which maps α onto β.

Proof.

Assume that (ii) does not hold. We will show that (i) holds. Since $\sigma : K \to L$ is an isomorphism, then the mapping $K[x] \to L[x]$ given by

$$\sum_{i=0}^{n} r_i x^i \mapsto \sum_{i=0}^{m} \sigma(r_i) x^i$$

is an isomorphism. By Theorem 1.1.7 (iv), every element of $K(x)$ is of the form hg^{-1} for some $h, g \in K[x]$ and every element of $L(x)$ is of the form $k\ell^{-1}$, for some $k, \ell \in L(x)$. Since the mapping above, (which we also denote as σ), is a bijection, then σ extends to a bijection mapping of $K(x)$ to $L(x)$ as $g\ell^{-1} \mapsto \sigma(g)\sigma(\ell)^{-1}$. It is easy to verify that this extended σ is an isomorphism. Then since α is transcendental, then by Theorem 1.1.12, we have

$$K(\alpha) \simeq K(x) \simeq L(x) \simeq L(\beta)$$

The isomorphism from $K(\alpha)$ to $K(\beta)$ is an extension of σ, so the extension still maps K to L. Since the isomorphism of $K(\alpha)$ to $K(x)$ maps α to x, the isomorphism of $K(x)$ to $L(x)$ maps x to x, and the isomorphism of $L(x)$ to $L(\beta)$ maps x to β, then the extension of σ maps α to β. This proves (i).

Now assume that (i) does not hold, and we will show that (ii) holds. Without loss of generality, assume that f is monic (since the extended isomorphism $\sigma : K[x] \to L[x]$ maps polynomial kf to $\sigma(kf) = k\sigma(f)$ for all $k \in K$) and the roots of f and kf coincide. Since $\sigma : K[x] \to L[x]$ is an isomorphism, then $\sigma f \in L[x]$ is monic and irreducible. In the proof of Theorem 1.1.13 (ii), the mappings $\phi : K[x]/\langle f \to K[\alpha] = K(\alpha)$ and $\psi : L[x]/\langle \sigma f \rangle \to L[\beta] = L(\beta)$ given respectively by

$$\phi(g + \langle f \rangle) = g(\alpha)$$

and

$$\psi(h + \langle \sigma f \rangle) = h(\beta)$$

are isomorphisms. Then, the mapping $\theta : K[x]/\langle f \to L[x]/\langle \sigma f \rangle$ given by $\theta(g + \langle f \rangle) = \sigma g + \langle \sigma f \rangle$ is an isomorphism. Therefore, the composition

$$K(\alpha) \xrightarrow{\phi^{-1}} K[x]/\langle f \rangle \xrightarrow{\theta} L[x]/\langle \sigma f \rangle \xrightarrow{\psi} L(\beta)$$

is an isomorphism of fields $K(\alpha)$ and $L(\beta)$ such that $g(\alpha) \mapsto g(x) + \langle f \rangle \mapsto \sigma g(x) + \langle \sigma f \rangle + \sigma g(\beta)$. Also, $\psi\theta\phi^{-1}$ agrees with σ on K (the "constant" rational functions of α in $K(\alpha)$) and maps $\alpha \mapsto x + \langle f \rangle \mapsto x + \langle \sigma f \rangle \mapsto \beta$. This proves (ii). ∎

Corollary 1.1.17

Let E and F be extension fields of K and let $\alpha \in E$ and $\beta \in F$ be algebraic over K. The following assertions are equivalent:

(a) α and β are roots of the same irreducible polynomial $f \in K[x]$.

(b) there exists an isomorphism of fields $K(\alpha) \simeq K(\beta)$ which sends α onto β and it is the identity on K.

Proof.

(a) $\Rightarrow$ (b) First assume that α and β are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem 1.1.16 (ii) with $\sigma = 1_K$, we have $\sigma f = f$, and so α (a root of f) and β (a root of $f = \sigma f$) and $K(\alpha) \simeq K(\beta)$, where the isomorphism between $K(\alpha)$ and $K(\beta)$ sends α onto β.

(b) $\Rightarrow$ (a) Now assume that $\sigma : K(\alpha) \to K(\beta)$ is an isomorphism with $\sigma(\alpha) = \beta$ and $\sigma(k) = k$ for all $k \in K$. Let $f \in K[x]$ be the irreducible monic polynomial for which algebraic α is a root. If $f = \sum_{i=0}^{n} k_i x^i$, then

$$0 = f(\alpha) = \sum_{i=0}^{n} k_i \alpha^i$$

Since $\sigma(0) = 0$, then

$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^{n} k_i\alpha^i\right) = \sum_{i=0}^{n} \sigma(k_i\alpha^i) = \sum_{i=0}^{n} \sigma(k_i)\sigma(\alpha^i) = \sum_{i=0}^{n} k_i\sigma(\alpha)^i = \sum_{i=0}^{n} k_i\beta^i = f(\beta)$$

So β is a root of f as well. ∎

So far, we have dealt with a field K and some element α which is algebraic over K and is an element of some (mysterious) given extension field of F. The following result shows that for any polynomial $f \in K[x]$, there exists some field extension F such that F contains a root of f. This is a step towards the Fundamental Theorem of Algebra in that we now know of the existence of an extension field containing a root of a given polynomial. Of course, the Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed. The next result is commonly called Kronecker's Theorem.

Theorem 1.1.18: Kronecker's Theorem

If K is a field and $f \in K[x]$ is a polynomial of degree n, then there exists a unique simple extension $F = K(\alpha)$ of K such that

(i) $\alpha \in F$ is a root of f.

(ii) $[K(\alpha) : K] \leq n$ with equality holding if and only if f is irreducible in $K[x]$.

(iii) If f is irreducible in $K[x]$, then $K(\alpha)$ is unique up to an isomorphism which is the identity on K.

Proof.

Without loss of generality, we may assume that f is irreducible (if not, we replace f by one of its irreducible factors). Then the ideal $\langle f\rangle$ is maximal in $K[x]$, and so $F = K[x]/\langle f\rangle$ is a field. Furthermore, the canonical projection $\pi : K[x] \to K[x]/\langle f\rangle$ given by the mapping $g \mapsto g + \langle f\rangle$ when restricted to K (the constant polynomials in $K[x]$) is a one-to-one homomorphism (the canonical projection is a homomorphism, the only "constant" in $\langle f\rangle$ is the zero function since $\langle f\rangle$ contains all multiples of f by elements in $K[x]$, and so the kernel of the canonical projection is one-to-one). Then since π is one-to-one, $\pi(K) \simeq K$ can be considered as a subfield of a field F; that is, F is an extension field of K (provided that K is identified with $\pi(K)$). For $x \in K[x]$, let $\alpha = \pi(x) = x + \langle f\rangle = K[x]/\langle f\rangle$. Then by Theorem 1.1.13 (ii) and since coset addition and multiplication is performed on representatives, then

$$f(\alpha) = f(x + \langle f\rangle) = f(x) + \langle f\rangle = 0 + \langle f\rangle$$

since $0 + \langle f\rangle$ is the additive identity in $K[x]/\langle f\rangle = F$, so (i) follows.

To see that (ii) holds, note that Theorem 1.1.13 shows that $[K(\alpha) : K] = n$ for irreducible f of degree n. As commented above, if f is not irreducible, then we consider an irreducible factor of f (of degree less than n) and (ii) follows.

Finally, to see that (iii) holds, Corollary 1.1.17 implies (iii) and that the extension field does not depend on which root of f is used. ∎

We now establish some "basic facts" about algebraic extension fields.

Theorem 1.1.19

If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.

Proof.

If F is a finite-dimensional extension of K, say $[F : K] = n$. Let $\alpha \in F$ be arbitrary. Then the set of $n+1$ elements $\{1_K, \alpha, ..., \alpha^n\}$ must be linearly dependent over F. So there exists $a_0, ..., a_n \in K$ not all zero such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

which implies that α is algebraic over K. Since α was arbitrary, F is an algebraic extension of K. If $\{x_1, ..., x_n\}$ is a basis of F over K, then by Theorem 1.1.7 (v) that $F = K(x_1, ..., x_n)$. This completes the proof. ■

Theorem 1.1.20

If F is a field extension of K, and $X \subset F$ such that $F = K(X)$, and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite-dimensional over K.

Proof.

If $\alpha \in F$, then by Theorem 1.1.7 (iv),

$$\alpha = \frac{f(u_1, ..., u_n)}{g(u_1, ..., u_n)}$$

for some $n \in \mathcal{N}$ and $f, g \in F[x_1, ..., x_n]$ and some $u_1, ..., u_n \in X$. So $x \in K(u_1, ..., u_n)$. So there exists a tower of subfields

$$K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, ..., u_n)$$

For fixed $i \geq 2$, u_i is algebraic over K and so u_i is algebraic over $K(u_1, ..., u_{i-1})$, say u_i is of degree r_i over $K(u_1, ..., u_{i-1})$. Since

$$K(u_1, ..., u_{i-1})(u_i) = K(u_1, ..., u_i)$$

we have

$$[K(u_1, ..., u_i) : K(u_1, ..., u_{i-1})] = r_i$$

by Theorem 1.1.13 (iii). Now let r_1 be the degree of u_1 over K (we had $i \geq 2$ above), then by an inductive application of Theorem 1.1.3, shows that

$$[K(u_1, ..., u_n) : K] = r_1 \cdots r_n$$

By Theorem 1.1.19, $K(u_1, ..., u_n)$ (since the dimension $r_1 \cdots r_n$ is finite) is algebraic over K, and so $\alpha \in K(u_1, ..., u_n)$ is algebraic over K. Since α was arbitrary, then F is algebraic over K.

If X was a finite set, say $X = \{u_1, ..., u_n\}$, then as argued above,

$$[F(u_1, ..., u_n) : K] = r_1 \cdots r_n$$

is finite. This completes the proof. ■

Theorem 1.1.21

If F is an algebraic extension field of E, and E is an algebraic extension field of K, then F is an algebraic extension of K.

Proof.

Let $\alpha \in F$ be arbitrary. Since F is an algebraic extension of E, then α is algebraic over E, and so

$$b_n\alpha^n + \cdots + b_0 = 0$$

for some $b_0, ..., b_n \in E$ with $b_n \neq 0$. Therefore, α is algebraic over the subfield $K(b_0, ..., b_n)$ of E. Consequently, there is a tower of fields

$$K \subset K(b_0, ..., b_n) \subset K(b_0, ..., b_n)(\alpha)$$

where $[K(b_0, ..., b_n)(u) : K(b_0, ..., b_n)]$ is finite by Theorem 1.1.13 (iii) since α is algebraic over $K(b_0, ..., b_n)$, and $[K(b_0, ..., b_n) : K]$ is finite by Theorem 1.1.13 (iii) since α is algebraic over $K(b_0, ..., b_n)$, and $[K(b_0, ..., b_n) : K]$ is finite by Theorem 1.1.20 since there is a finite number of b_i and each is algebraic over K. Therefore, $[K(b_0, ..., b_n)(\alpha) : K]$ is finite by Theorem 1.1.3. Hence, by Theorem 1.1.19, α is algebraic over K. Since $\alpha \in F$ is arbitrary, F is algebraic over K. ■

Theorem 1.1.22

Let F be an extension field of K and E the set of all elements of F which are algebraic over K. Then E is a subfield of F.

Proof.

For any $\alpha, \beta \in E$, $K(\alpha, \beta)$ is an algebraic extension of K by Theorem 1.1.20. Since $K(\alpha, \beta)$ is a field, then $\alpha - \beta \in K(\alpha, \beta)$ and $\alpha\beta^{-1} \in K(\alpha, \beta)$ for $\beta \neq 0$. Hence, $\alpha - \beta \in E$ and $\alpha\beta^{-1} \in E$ and so E is an additive group and $E \setminus \{0\}$ is a multiplicative group. Therefore, E is a field. ■

Theorem 1.1.22 justifies the claim that the algebraic real numbers $\mathcal{A}$ are a field:

$$\mathcal{A} = \{r \in \mathbb{R} : p(r) = 0 \text{ for some } p \in \mathbb{Q}[x]\}$$

1.2 The Fundamental Theorem of Galois Theory

In this section, we define the Galois group of an arbitrary field extension. We prove the Fundamental Theorem of Galois Theory. The Fundamental Theorem allows us to translate problems involving fields, polynomials, and extensions into group theoretical terms.