MRQ 2017

School of Mathematics and Statistics

MT5836 Galois Theory

Handout II: Field Extensions: Algebraic elements, minimum polynomials, and simple extensions

2 Field Extensions

Definition 2.1 Let F and K be fields such that F is a subfield of K. We then say that K is an *extension* of F. We also call F the *base field* of the extension.

In particular, note that every field is an extension of its prime subfield. The point of this definition, though, is a change of perspective. We are not viewing a field extension $F \subseteq K$ as being the situation where we start with a field K and then pass to a subfield F. Instead, the philosophy here will be much more starting with a base field F and then creating a bigger field K containing F that is the extension.

The degree of an extension

The first observation to make in this setting is that if the field K is an extension of the field F, then K, in particular, satisfies the following conditions:

- K forms an abelian group under addition;
- we can multiply elements of K by elements of F;
- $a(x + y) = ax + ay$ for all $a \in F$ and $x, y \in K$;
- $(a + b)x = ax + bx$ for all $a, b \in F$ and $x \in K$;
- $(ab)x = a(bx)$ for all $a, b \in F$ and $x \in K$;
- $1x = x$ for all $x \in K$.

Thus, we can view K as a *vector space* over the field F.

Definition 2.2 Let the field K be an extension of the field F.

(i) The *degree* of K over F is the dimension of K when viewed as a vector space over F. We denote this by $|K : F|$. Thus
$$|K : F| = \dim_F K.$$

(ii) If the degree $|K : F|$ is finite, we say that K is a *finite extension* of F.

Warning: Note that saying K is a finite extension of F does *not* mean that K is a finite field. There are many situations where both fields have infinitely many elements in them. It refers precisely to the dimension of the bigger field over the smaller field.

Theorem 2.4 (Tower Law) *Let $F \subseteq K \subseteq L$ be field extensions. Then L is a finite extension of F if and only if L is a finite extension of K and K is a finite extension of F. In such a case,*
$$|L : F| = |L : K| \cdot |K : F|.$$

Comment: In the course of the proof of the theorem we observe that if $F \subseteq K \subseteq L$ are field extensions, $\{v_1, v_2, \dots, v_m\}$ is a basis for L over K and $\{w_1, w_2, \dots, w_n\}$ is a basis for K over F, then $\{\, v_i w_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n \,\}$ is a basis for L over F.

Algebraic elements and algebraic extensions

Definition 2.5 Let the field K be an extension of the field F.

(i) An element $\alpha \in K$ is said to be *algebraic* over F if there exists a non-zero polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$. When this holds, we shall say that α satisfies the polynomial equation $f(X) = 0$.

(ii) We say that K is an *algebraic extension* of F if every element of K is algebraic over F.

Thus to say that an element $\alpha \in K$ is algebraic over the subfield F is to say that there are coefficients b_0, b_1, …, b_n in F such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

Lemma 2.6 *Every finite extension is an algebraic extension.*

The example at the end of this chapter shows that the converse does not hold: there are algebraic extensions that are not finite extensions.

Simple extensions

Definition 2.7 Let the field K be an extension of the field F and α_1, α_2, …, α_n be elements of K. We write

$$F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

for the smallest subfield of K that contains both F and the elements α_1, α_2, …, α_n.

It is straightforward to verify that the intersection of a collection of subfields of K is again a subfield. Consequently, the "smallest subfield" containing F and the elements α_1, α_2, …, α_n makes sense: it is the intersection of all the subfields of K that contain this collection of elements.

Definition 2.8 We say that the field K is a *simple extension* of the field F if $K = F(\alpha)$ for some $\alpha \in K$. We then also say that K is obtained by *adjoining the element* α to F.

Example 2.9 Let F be a field and X be an indeterminate. The field $F(X)$ of rational functions is a simple extension of F.

The indeterminate X is *not* an algebraic element over F. We use the term *transcendental* for an element that is not algebraic over the base field. It turns out that if α is any transcendental element over the base field F, then the simple extension $F(\alpha)$ is isomorphic to the field $F(X)$ of rational functions.

Minimum polynomials

Definition 2.10 Let F be a field and α be an element in some field extension of F such that α is algebraic over F. The *minimum polynomial* of α over F is the monic polynomial $f(X)$ of least degree in $F[X]$ such that $f(\alpha) = 0$.

Recall that a polynomial is *monic* if its leading term has coefficient 1.

Lemma 2.11 *Let F be a field and α be an element in some field extension of F such that α is algebraic over F. Then*

(i) *the minimum polynomial of α over F exists;*

(ii) *the map $\phi\colon F[X] \to F(\alpha)$ given by $g(X) \mapsto g(\alpha)$ (that is, evaluating each polynomial at α) is a ring homomorphism with kernel $\ker\phi = \big(f(X)\big)$;*

(iii) *the minimum polynomial $f(X)$ of α over F is irreducible over F;*

(iv) *if $g(X) \in F[X]$, then $g(\alpha) = 0$ if and only if the minimum polynomial $f(X)$ of α over F divides $g(X)$;*

(v) *the minimum polynomial $f(X)$ of α over F is unique;*

(vi) *if $g(X)$ is any monic polynomial over F such that $g(\alpha) = 0$, then $g(X)$ is the minimum polynomial of α over F if and only if $g(X)$ is irreducible over F.*

Comment: Note that the minimum polynomial of an algebraic element α depends upon the particular base field. For example, $\sqrt{2}$ has minimum polynomial over $X^2 - 2$ over $\mathbb{Q}$, whereas its minimum polynomial over $\mathbb{R}$ is $X - \sqrt{2}$.

If we concentrate our efforts on simple extensions $F(\alpha)$ with α algebraic over the base field F, there are two questions that naturally arise and whose answers will enable us to make progress:

(i) Given an irreducible polynomial $f(X)$ over the field F, can we construct a simple extension $F(\alpha)$ such that the minimum polynomial of α over F is $f(X)$?

(ii) If α is algebraic over F, what is the structure of the simple extension $F(\alpha)$ and in what way is this determined by the minimum polynomial of α over F?

These questions essentially boil down to the existence of simple extensions and to then investigating their properties (and essentially establishing uniqueness as a consequence). Note that in answering the first question in the affirmative, as we do in the following theorem, we are showing that we can always *adjoin a root α of an irreducible polynomial to a field F* to construct some simple extension $F(\alpha)$.

Theorem 2.13 *Let F be a field and $f(X)$ be a monic irreducible polynomial over F. Then there exists a simple extension $F(\alpha)$ of F such that α is algebraic over F with minimum polynomial $f(X)$.*

Comments: In the proof of the above theorem, we construct $F(\alpha)$ as the quotient ring $K = F[X]/I$, where $I = (f(X))$ is the ideal generated by the polynomial $f(X)$. There are two comments to make placing the above existence result for simple extensions in context.

(i) The Correspondence Theorem for rings tells us that there is a one-one correspondence between ideals in the quotient ring $F[X]/I$, where $I = (f(X))$, and ideals in the polynomial ring $F[X]$ that contain I. We have shown that when $f(X)$ is irreducible, the quotient $K = F[X]/I$ is a field; that is, it has only two ideals $\mathbf{0}$ and K itself. Therefore, via the correspondence, $I = (f(X))$ is a maximal ideal of the polynomial ring: there are no ideals J satisfying $I < J < F[X]$. Consequently, we are observing above that $(f(X))$ is a maximal ideal when $f(X)$ is irreducible. (The implication also reverses, as follows quite easily, but we omit the proof.)

(ii) Recall that the prime subfields are constructed from the ring of integers $\mathbb{Z}$. We observed, in Theorem 1.12, that the prime subfield of any field is either isomorphic to $\mathbb{Q}$ (which is the field of fractions of the Euclidean domain $\mathbb{Z}$) or to a finite field $\mathbb{F}_p$ (which occurs as the quotient $\mathbb{Z}/(p)$ by the ideal generated by some prime p, the primes being the irreducible elements in $\mathbb{Z}$). An analogous observation is being made here. If F is a field, the simple extensions of F are constructed from the Euclidean domain $F[X]$ as follows:

- If α is transcendental, then $F(\alpha)$ is isomorphic to the field of fractions, $F(X)$, of $F[X]$.
- If α is algebraic, then $F(\alpha)$ can be constructed as the quotient $F[X]/(f(X))$ by an ideal generated by an irreducible polynomial $f(X)$.

Theorem 2.14 *Let F be a field and α be an element in some extension of F. The simple extension $F(\alpha)$ over F is a finite extension if and only if α is algebraic over F. Moreover, in this case,*

$$|F(\alpha) : F| = \deg f(X),$$

the degree of the minimum polynomial $f(X)$ of α over F. Furthermore,

$$F(\alpha) \cong \frac{F[X]}{(f(X))}$$

(as rings).

Corollary 2.15 *Suppose that α is algebraic over F with minimum polynomial of degree n. Then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for the simple extension $F(\alpha)$ over F.*

Theorem 2.17 *Let K be an extension of a field F. Then K is a finite extension of F if and only if $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ for some finite collection α_1, α_2, ..., α_n of elements of K each of which is algebraic over F.*

Example 2.19 Let us write $\mathbb{A}$ for the set of all elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. We call $\mathbb{A}$ the *field of algebraic numbers* over $\mathbb{Q}$. In this example, we show that $\mathbb{A}$ is indeed a subfield of $\mathbb{C}$ and determine the degree $|\mathbb{A} : \mathbb{Q}|$.