Section V.1. Field Extensions

Note. In this section, we define extension fields, algebraic extensions, and transcendental extensions. We treat an extension field F as a vector space over the subfield K. This requires a brief review of the material in Sections IV.1 and IV.2 (though if time is limited, we may try to skip these sections). We start with the definition of vector space from Section IV.1.

Definition IV.1.1. Let R be a ring. A (left) *R-module* is an additive abelian group A together with a function mapping $R \times A \to A$ (the image of (r, a) being denoted ra) such that for all $r, a \in R$ and $a, b \in A$:

(i) $r(a + b) = ra + rb$;

(ii) $(r + s)a = ra + sa$;

(iii) $r(sa) = (rs)a$.

If R has an identity 1_R and

(iv) $1_R a = a$ for all $a \in A$,

then A is a *unitary R-module*. If R is a division ring, then a unitary R-module is called a (left) *vector space*.

Note. A right R-module and vector space is similarly defined using a function mapping $A \times R \to A$.

Definition V.1.1. A field F is an *extension field* of field K provided that K is a subfield of F.

Note. With $R = K$ (the ring [or field] of "scalars") and $A = F$ (the additive abelian group of "vectors"), we see that F is a vector space over K.

Definition. Let field F be an extension field of field K. The dimension of F as a vector space over K is denoted $[F : K]$. F is a *finite dimensional extension* or an *infinite dimensional extension* of K according as $[F : K]$ is finite or infinite.

Note. We defined the product of two cardinal numbers in Definition 0.8.3. The following is a restatement of Theorem IV.2.16 and, if we skipped Chapter IV, we simply accept this without proof. The case for finite dimensional extensions is proved in Fraleigh (see Theorem 31.4 of the 7th edition).

Theorem V.1.2. Let F be an extension field of E and E an extension field of K. Then $[F : K] = [F : E][E : K]$. Furthermore $[F : K]$ is finite if and only if $[F : E]$ and $[E : K]$ are finite.

Definition. If field F is an extension field of field E and E is an extension field of field K (so that $K \subset E \subset F$) then E is an *intermediate field* of K and F. For field F and set $X \subset F$, then *subfield* (respectively, *subring*) *generated by* X is the intersection of all subfields (respectively, subrings) of F that contain X. If F is an extension field of K and $X \subset F$ then the subfield (respectively, subring) generated by $K \cup X$ is the *subfield* (respectively, *subring*) *generated by* X *over* K and is denoted $K(X)$ (or, respectively, in the case of rings, $K[X]$).

Definition. If $X = \{u_1, u_2, \ldots, u_n\}$ then the subfield $K(X)$ (respectively, subring $K[X]$) of F is denoted $K(u_1, u_2, \ldots, u_n)$ (respectively, $K[u_1, u_2, \ldots, u_n]$). The field $K(u_1, u_2, \ldots, u_n)$ is a *finitely generated extension* of K. If $X = \{u\}$ then $K(u)$ is a *simple extension* of K.

Note. The field $K(u_1, u_2, \ldots, u_n)$ is a finitely generated extension of K but it may not be a finite dimensional extension over K (see Exercise V.1.2—it uses a transcendental extension; for example, $\mathbb{Q}(\pi)$).

Note. In Exercise V.1.4 it is shown that neither $K(u_1, u_2, \ldots, u_n)$ nor $K[u_1, u_2, \ldots, u_n]$ depends on the order of the u_i and that $K(u_1, u_2, \ldots, u_{n-1})(u_n) = K(u_1, u_2, \ldots, u_n)$ and $K[u_1, u_2, \ldots, u_{n-1}][u_n] = K[u_1, u_2, \ldots, u_n]$.

Theorem V.1.3. If F is an extension field of a field K, $u, u_i \in F$, and $X \subset F$, then

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

(ii) the subring $K[u_1, u_2, \ldots, u_n]$ consists of all elements of the form $g(u_1, u_2, \ldots, u_m)$, where g is a polynomial in m indeterminates with coefficients in K (that is, $g \in K[x_1, x_2, \ldots, x_m]$);

(iii) the subring $K[X]$ consists of all elements of the form $h(u_1, u_2, \ldots, u_n)$ where each $u_i \in X$, $n \in \mathbb{N}$, and h is a polynomial in n indeterminates with coefficients in K (that is, $n \in \mathbb{N}$ and $h \in K[x_1, x_2, \ldots, x_n]$);

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

(v) the subfield $K(u_1, u_2, \ldots, u_m)$ consists of all elements of the form

$$h(u_1, u_2, \ldots, u_m)/k(u_1, u_2, \ldots, u_m) = h(u_1, u_2, \ldots, u_m)k(u_1, u_2, \ldots, u_m)^{-1}$$

where $h, k \in K[x_1, x_2, \ldots, x_m]$ and $k(u_1, u_2, \ldots, u_m) \neq 0$;

(vi) the subfield $K(X)$ consists of all elements of the form

$$f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n) = f(u_1, u_2, \ldots, u_n)g(u_1, u_2, \ldots, u_n)^{-1}$$

where $n \in \mathbb{N}$, $f, g \in K[x_1, x_2, \ldots, x_n]$, $u_1, u_2, \ldots, u_n \in X$, and $g(u_1, u_2, \ldots, u_n) \neq 0$.

(vii) For each $v \in K(X)$ (respectively, $K[X]$) there is a finite subset X' of X such that $v \in K(X')$ (respectively, $K[X']$).

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

Note. Several of the exercises deal with composites of fields (Exercises V.1.5, V.1.20, and V.1.21).

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

Definition V.1.4. Let F be an extension field of K. An element $u \in F$ is *algebraic* over K if u is a root of some nonzero polynomial $f \in K[x]$. If u is not a root of any nonzero $f \in K[x]$ then u is *transcendental* over K. F is an *algebraic extension* of K if every element of F is algebraic over K. F is a *transcendental extension* if at least one element of F is transcendental over K.

Example V.1.A. The most common example of an algebraic extension field is

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

Another useful algebraic extension field is

$$\mathbb{R}(i) = \{a + ib \mid a, b \in \mathbb{R}\} \cong \mathbb{C}.$$

Note. 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. If K is a field, then the polynomial ring $K[x_1, \ldots, x_n]$ is an integral domain by Theorem III.5.3. The field of quotients of $K[x_1, \ldots, x_n]$ is denoted $K(x_1, \ldots, x_n)$. The elements of field $K(x_1, \ldots, x_n)$ consist of all fractions f/g where $f, g \in K[x_1, \ldots, x_n]$ and $g \neq 0$ (by Theorem III.4.3—though we may have skipped Section III.4). The field $K(x_1, \ldots, x_n)$ is the *field of rational functions* in indeterminates $x_1, x_2, \ldots, x_n$ over K In Exercise V.1.6, it is shown that every element of $K(x_1, \ldots, x_n)$ not in K itself is transcendental over K.

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

Theorem V.1.5. If F is an extension field of K and $u \in F$ is transcendental over K, then there is an isomorphism of fields $K(u) \cong K(x)$ which is the identity when restricted to K.

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(i) $K(u) = K[u]$;

(ii) $K(u) \cong K[x]/(f)$ where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0$ (where $g \in K[x]$) if and only if f divides g;

(iii) $[K(u) : K] = n$;

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

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1}$ where each $a_i \in K$.

Note. Theorem V.I.6 tells us what elements of the algebraic extension $K(u)$ of K "look like." That is, there exists a (fixed) $n \in \mathbb{N}$ such that every element of $K(u)$ is of the form $a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$ for some $a_i \in K$. Notice that Theorem V.1.5 and Theorem V.1.3(iv) tell us what elements of the transcendental extension $K(u)$ of K "look like":

$$\frac{a_0 + a_1u + \cdots + a_nu^n}{b_0 + b_1u + \cdots + b_mu^m} \text{ where } a_i, b_i \in K \text{ and } b_0 + b_1u + \cdots + b_mu^m \neq 0.$$

Definition V.1.7. Let F be an extension field of K and $u \in F$ algebraic over K. The monic irreducible polynomial f of Theorem V.1.6(ii) is the *irreducible polynomial of* u. The *degree of* u *over* K is $\deg(f) = [K(u) : K]$.

Example. The polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, since by Proposition III.6.8 the only possible rational roots are ± 1, neither of which is a root (we have also used the Factor Theorem, Theorem III.6.6, here). By the Intermediate Value Theorem of Calculus 1, there is some real root u. Now $x^3 - 3x - 1$ is the irreducible polynomial of u, so u has degree 3 over $\mathbb{Q}$ and $\{1, u, u^2\}$ is a basis of $\mathbb{Q}(u)$ over $\mathbb{Q}$ by Theorem V.1.6(iv). Now $u^4 + 2u^3 + 3 \in \mathbb{Q}(u)$ and so must be some linear combination of $1, u, u^2$. The Division Algorithm (Theorem III.6.2) gives in $\mathbb{Q}[x]$:

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

whence

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

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

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

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(i) u is transcendental over K and v is transcendental over L; or

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

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Corollary V.1.9. Let E and F each be extension fields of K and let $u \in E$ and $v \in F$ be algebraic over K. Then u and v are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is an isomorphism of fields $K(u) \cong K(v)$ which sends u onto v and it is the identity on K.

Note. Fraleigh (in his Definition 48.1) calls two roots of the same irreducible polynomial over K, "conjugates." This terminology is inspired by the fact that roots of irreducible second degree polynomials over $\mathbb{R}$ come in complex conjugates pairs.

Note. So far we have dealt with a field K and some element u which is algebraic over K and is an element of some (mysterious) given extension field F. The following result shows that for any polynomial $f \in K[x]$ there exists some extension field 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. In Section V.3 we will show that every field has an algebraic closure (that is, an extension field that contains all roots of all polynomials over both the original field and the extension field)—see Theorem V.3.6. Of course, the Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed (as we'll see in the appendix to Section V.3). The next result is commonly called Kronecker's Theorem (see Fraleigh's Theorem 29.3—Fraleigh makes this result the "basic goal" of his book).

Theorem V.1.10. Kronecker's Theorem.

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

(i) $u \in F$ is a root of f;

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

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

Note. In the proof of Kronecker's Theorem part (i), one might be interested in *how* Kronecker find the root u. Notice that is is dealt with very symbolically; namely, $u = x + (f)$ in $K[x]/(f) = F$.

Note. The "Kronecker" of "Kronecker's Theorem" is Leopold Kronecker (1823–1891) who was born in Poland and did most of his work in Germany.

He is well-known for the quote "God made the integers; all else is the work of man." Kronecker's philosophical view of math is that every object of mathematics should be constructible and constructed in a finite number of steps. In 1882 he published "Foundations of an Arithmetic Theory of Algebraic Numbers" in which he introduced the idea of an extension field created by adjoining a single element (a root of a polynomial) to the field of rational numbers. Quoting from *A History of Abstract Algebra* by Israel Kleiner: "Kronecker rejected irrational numbers as bona fide entities since they involve the mathematical infinite. For example, the algebraic number field $Q(\sqrt{2})$ was defined by Kronecker as the quotient field of the polynomial ring $Q[x]$ relative to the ideal generated by $x^2 - 2$, though he would have put it in terms of congruences rather than quotient rings. These ideas contain the germ of what came to be known as *Kronecker's Theorem*, namely that every polynomial over a field has a root in some extension field." Kronecker's rival in this "finitest" view was Richard Dedekind (1831–1916). Dedekind used an axiomatic approach, including an acceptance of the axiomatized infinite. Whereas Kronecker would start with the natural numbers, build the integers, the rationals, and then finite extensions of the rationals, Dedekind treats the real numbers as a complete ordered field from the start. Dedekind's version of completeness (and hence his approach to irrationals) is dealt with using "Dedekind cuts." A Dedekind cut of $\mathbb{R}$ is two nonempty sets $A, B \subset \mathbb{R}$ such that: $a < b$ for all $a \in A$ and $b \in B$, $A \cap B = \varnothing$, and $A \cup B = \mathbb{R}$. The claim (the "Axiom of Completeness" for $\mathbb{R}$) is that either A has a largest element or B has a smallest element. This can be stated in everyday language as the following. Suppose an airplane taxis down a runway and takes off. Is there a last point in time the plane is on the ground or a first

point in time that the plane is off the ground? (The answer: There is a last point in time the plane is on the ground.) These are the ideas you will address early in our Analysis 1 (MATH 4217/5217) class.

Note. We now establish some "basic facts" about algebraic field extensions.

Theorem V.1.11. If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.

Theorem V.1.12. If F is an extension field of K and X is a subset of 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.

Theorem V.1.13. 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.

Theorem V.1.14. 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 (which is, of course, algebraic over K).

Note. Theorem V.1.14 justifies the claim that the algebraic real numbers, $\mathbb{A}$, are a field:

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

Of course, the same can be said for the algebraic complex numbers.

Revised: 12/30/2023