12.1 Field extensions

Before beginning our introduction to algebraic geometry we recall some standard facts about field extensions. Most of these should be familiar to you and can be found in any standard introductory algebra text, such as [1, 2]. We will occasionally need to results in slightly greater generality than you may have seen before, and here we may reference [3, 4].[1]

We start in the general setting of an arbitrary field extension L/k with no restrictions on k or L. The fields k and L necessarily have the same prime field (the subfield of k generated by the multiplicative identity), and therefore the same characteristic. The *degree* of the extension L/k, denoted $[L\colon k]$, is the dimension of L as a k-vector space, a not necessarily finite cardinal number. If have a tower of fields $k \subseteq L \subseteq M$, then

$$[M : k] = [M : L][L : k],$$

where the RHS is a product of cardinals.[2] When $[L : k]$ is finite we say that L/k is a *finite extension*.

An element $\alpha \in L$ is said to be *algebraic* over k if it is the root of a polynomial in $k[x]$, and otherwise it is *transendental* over k. The extension L/k is algebraic if every element of L is algebraic over k, and otherwise it is transcendental. If M/L and L/k are both algebraic extensions, so is M/k. A necessary and sufficient condition for L/k to be algebraic is that L be equal to the union of all finite extensions of k contained in L; in particular, every finite extension is algebraic.

The subset of L consisting of the elements that are algebraic over k forms a field called the *algebraic closure* of k in L. A field k is *algebraically closed* if every every non-constant polynomial in $k[x]$ has a root in k; equivalently, k has no non-trivial algebraic extensions. For every field k there exists an extension $\bar{k}/k$ with $\bar{k}$ algebraically closed; such a $\bar{k}$ is called an *algebraic closure* of k, and all such $\bar{k}$ are isomorphic (but this isomorphism is not unique in general). Any algebraic extension L/k can be embedded into any algebraic closure of k, since every algebraic closure of L is also an algebraic closure of k.

Remark 12.1. When working with algebraic extensions of k it is convenient to view them all as subfields of a some fixed algebraic closure $\bar{k}$ (there is in general no canonical choice). The key point is that we can always (not necessarily uniquely) embed any algebraic extension of L/k in our chosen $\bar{k}$, and if we have another extension M/L, our embedding of L into $\bar{k}$ can always be extended to an embedding of M into $\bar{k}$.

A set $S \subseteq L$ is said to be *algebraically independent* (over k) if for every finite subset $\{s_1, \dots, s_n\}$ of S and every nonzero polynomial $f \in k[x_1, \dots, x_n]$ we have

$$f(s_1, \dots, s_n) \neq 0.$$

[1] With the exception of [1], which you should be familiar to you from 18.701/18.702, these references are all available online through the MIT library system (just click the title links in the references section at the end of these notes). I encourage you to consult them for further details on anything that is unfamiliar to you. One note of caution: when jumping into the middle of a textbook (or, especially, the results of a web search), be wary of assumptions that may have been stated much earlier (e.g. at the beginning of a chapter).

[2] Recall that a cardinal number is an equivalence class of equipotent sets (sets that can be put in bijection). The product of $n_1 = \#S_1$ and $n_2 = \#S_2$ is $n_1 n_2 = \#(S_1 \times S_2)$ and the sum is the cardinality of the disjoint union: $n_1 + n_2 = \#(S_1 \sqcup S_2)$. But we shall be primarily interested in finite cardinals (natural numbers).

Note that this means the empty set is algebraically independent (just as the empty set is linearly independent in any vector space). An algebraically independent set $S \subseteq L$ for which $L/k(S)$ is algebraic is called a *transcendence basis* for the extension L/k.

Theorem 12.2. *Every transcendence basis for L/k has the same cardinality.*

Proof. We will only prove this in the case that L/k has a finite transcendence basis (which includes all extensions of interest to us); see [3, Theorem 7.9] for the general case. Let $S = \{s_1, \dots, s_m\}$ be a smallest transcendence basis and let $T = \{t_1, \dots, t_n\}$ be any other transcendence basis, with $n \geq m$. The set $\{t_1, s_1, \dots, s_m\}$ must then algebraically dependent, since $t_1 \in L$ is algebraic over $k(S)$, and since t_1 is transcendental over k, some s_i, say s_1, must be algebraic over $k(t_1, s_2, \dots, s_m)$. It follows that L is algebraic over $k(t_1, s_2, \dots, s_m)$, and the set $T_1 = \{t_1, s_2, \dots, s_m\}$ must be algebraically independent, otherwise it would contain a transcendence basis for L/k smaller than S. So T_1 is a transcendence basis for L/k of cardinality m that contains t_1.

Continuing in this fashion, for $i = 2, \dots, m$ we can iteratively construct transcendence bases T_i of cardinality m that contain $\{t_1, \dots, t_i\}$, until $T_m \subseteq T$ is a transcendence basis of cardinality m; but then we must have $T_m = T$, so $n = m$. □

Definition 12.3. The *transcendence degree* of a field extension L/K is the cardinality of any (hence every) transcendence basis for L/k.

Unlike extension degrees, which multiply in towers, transcendence degrees add in towers: for any fields $k \subseteq L \subseteq M$, the transcendence degree of M/k is the sum (as cardinals) of the transcendence degrees of M/L and L/k.

We say that the extension L/k is *purely transcendental* if $L = k(S)$ for some transcendence basis S for L/k. All purely transcendental extensions of k with the same transcendence degree are isomorphic. Every field extension L/k can be viewed as an algebraic extension of a purely transcendental extension: if S is a transcendence basis of L/k then $L/k(S)$ is an algebraic extension of the purely transcendental extension $k(S)/k$.

Remark 12.4. It is not the case that every field extension is a purely transcendental extension of an algebraic extension. Indeed, there are already plenty of counterexamples with transcendence degree 1, as we shall soon see.

The field extension L/k is said to be *simple* if $L = k(x)$ for some $x \in L$. A purely transcendental extension of transcendence degree 1 is obviously simple, but, less trivially, so is any finite separable extension (see below for the definition of separable); this is known as the primitive element theorem.

Remark 12.5. The notation $k(x)$ can be slightly confusing. If $x \in L$ is transcendental over k then $k(x)$ is isomorphic to the field of rational functions over k, in which case we may as well regard x as a variable. But if $x \in L$ is algebraic over k, then every rational expression $r(x)$ with nonzero denominator can be simplified to a polynomial in x of degree less than $n = [k(x) : k]$ by reducing modulo the minimal polynomial f of x (note that we can invert nonzero denominators modulo f); indeed, this follows from the fact that $\{1, x, \dots, x^{n-1}\}$ is a basis for the n-dimensional k-vector space $k(x)$.

12.1.1 Algebraic extensions

We now assume that L/k is algebraic and fix $\bar{k}$ so that $L \in \bar{k}$. The extension L/k is *normal* if it satisfies either of the equivalent conditions:

- every irreducible polynomial in $k[x]$ with a root in L splits completely in L;
- $\sigma(L) = L$ for all $\sigma \in \mathrm{Aut}(\overline{k}/k)$ (every automorphism of $\overline{k}$ that fixes k also fixes L).[3]

Even if L/k is not normal, there is always an algebraic extension M/L for which M/k is normal. The minimal such extension is called the *normal closure* of L/k; it exists because intersections of normal extensions are normal. It is not true in general that if L/k and M/L are normal extensions then so is M/k, but if $k \subseteq L \subseteq M$ is a tower of fields with M/k normal, then M/L is normal (but L/k need not be).

A polynomial $f \in k[x]$ is *separable* if any of the following equivalent conditions hold:

- the factors of f in $\bar{k}[x]$ are all distinct;
- f and f' have no common root in $\bar{k}$;
- $\gcd(f, f') = 1$ in $k[x]$.

An element $\alpha \in L$ is separable over k if any of the following equivalent conditions hold:

- α is a root of a separable polynomial $f \in k[x]$;
- the minimal polynomial of α is separable;
- $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p > 0$ and the minimal polynomial of α is not of the form $g(x^p)$ for some $g \in k[x]$.

The elements of L that are separable over k form a field called the *separable closure* of k in L. The separable closure of k in its algebraic closure $\bar{k}$ is denoted k^{sep} and is simply called the separable closure of k. If $k \subseteq L \subseteq M$ then M/k is separable if and only if both M/L and L/k are separable.

A field k is said to be *perfect* if any of the following equivalent conditions hold:

- $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p > 0$ and $k = \{x^p : x \in k\}$ (k is fixed by Frobenius);
- every finite extension of k is separable over k;
- every algebraic extension of k is separable over k.

Note that finite fields and all fields of characteristic 0 are perfect.

Example 12.6. The rational function field $k = \mathbb{F}_p(t)$ is not perfect. If we consider the finite extension $L = k(t^{1/p})$ obtained by adjoining a pth root of t to k, the minimal polynomial of $t^{1/p}$ is $x^p - t$, which is irreducible over k but not separable (its derivative is 0).

An algebraic extension L/k is *Galois* if it is both normal and separable, and in this case we call $\mathrm{Gal}(L/k) = \mathrm{Aut}(L/k)$ the *Galois group* of L/k. The extension k^{sep}/k is always normal: if an irreducible polynomial $f \in k[x]$ has a root α in k^{sep}, then (up to scalars) f is the minimal polynomial of α over k, hence separable over k, so all its roots lie in k^{sep}. Thus k^{sep}/k is a Galois extension and its Galois group

$$G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$$

[3] Some authors write $\mathrm{Gal}(L/k)$ for $\mathrm{Aut}(L/k)$, others only use $\mathrm{Gal}(L/k)$ when L/k is known to be Galois; we will use the later convention.

is the *absolute Galois group* of k (we could also define G_k as $\mathrm{Aut}(\bar{k}/k)$, the restriction map from $\mathrm{Aut}(\bar{k}/k)$ to $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ is always an isomorphism).

The *splitting field* of a polynomial $f \in k[x]$ is the extension of k obtained by adjoining all the roots of f (which lie in $\bar{k}$). Every splitting field is normal, and every finite normal extension of k is the splitting field of some polynomial over k; when k is a perfect field we can go further and say that L/k is a finite Galois extension if and only if it is the splitting field of some polynomial over k.

For finite Galois extensions M/k we always have $\#\mathrm{Gal}(M/k) = [M : k]$, and the fundamental theorem of Galois theory gives an inclusion-reversing bijection between subgroups $H \subseteq \mathrm{Gal}(M/k)$ and intermediate fields $k \subseteq L \subseteq M$ in which $L = M^H$ and $H = \mathrm{Gal}(M/L)$ (note that M/L is necessarily Galois). Beware that none of the statements in this paragraph necessarily applies to infinite Galois extensions, some modifications are required (this will be explored further on the next problem set).

12.2 Affine space

Let k be a perfect field and fix an algbebraic closure $\bar{k}$.

Definition 12.7. n-dimensional *affine space* over k is the set

$$\mathbb{A}^n_k = \{(x_1, \dots, x_n) \in \bar{k}^n\},$$

equivalently $\mathbb{A}^n_k$ is the vector space $\bar{k}^n$ regarded as a set. When k is clear from context we may just write $\mathbb{A}^n$. If $k \subseteq L \subseteq \bar{k}$, the set of *$L$-rational points* (or just L-points) in $\mathbb{A}^n$ is

$$\mathbb{A}^n(L) = \{(x_1, \dots, x_n) \in L^n\} = \mathbb{A}^n(\bar{k})^{G_L},$$

where $A^n(\bar{k})^{G_L}$ denotes the set of points in $\mathbb{A}^n(\bar{k})$ fixed by $G_L = \mathrm{Gal}(L^{\mathrm{sep}}/L) = \mathrm{Gal}(\bar{k}/L)$. In particular, $\mathbb{A}^n(k) = \mathbb{A}^n(\bar{k})^{G_k}$.

Definition 12.8. If S is a set of polynomials in $A = \bar{k}[x_1, \dots, x_n]$, the set of points

$$Z_S = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in S\},$$

is called an (affine) *algebraic set*. If $k \subseteq L \subseteq \bar{k}$, the set of L-rational points in Z_S is

$$Z_S(L) = Z_S \cap \mathbb{A}^n(L).$$

When S is a singleton $\{f\}$ we may write Z_f in place of $Z_{\{f\}}$.

Note that if I is the A-ideal generated by S, then $Z_I = Z_S$, since $f(P) = g(P) = 0$ implies $(f + g)(P) = 0$ and $f(P) = 0$ implies $(fg)(P) = 0$. Thus we can always replace S by the ideal (S) that it generates, or by any set of generators for (S).

Example 12.9. We have $Z_\emptyset = Z_{(0)} = \mathbb{A}^n$ and $Z_{\{1\}} = Z_{(1)} = \emptyset$.

For any $S, T \subseteq A$ we have

$$S \subseteq T \quad \Longrightarrow \quad Z_T \subseteq Z_S,$$

but the converse need not hold, even if S and T are ideals: consider $T = (x_1)$ and $S = (x_1^2)$.

We now recall the notion of a Noetherian ring and the Hilbert basis theorem.

Definition 12.10. A commutative ring R is *noetherian* if every R-ideal is finitely generated.[4] Equivalently, every infinite ascending chain of R-ideals

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

eventually stabilizes, that is, $I_{n+1} = I_n$ for all sufficiently large n.

Theorem 12.11 (Hilbert basis theorem)**.** *If R is a noetherian ring, then so is $R[x]$.*

Proof. See [1, Theorem 14.6.7] or [2, Theorem 8.32]. □

Note that we can apply the Hilbert basis theorem repeatedly: if R is noetherian then so is $R[x_1]$, and so is $(R[x_1])[x_2] = R[x_1, x_2]$, ..., and so is $R[x_1, \ldots, x_n]$. Like every field, $\bar{k}$ is a noetherian ring (it has just two ideals, so it certainly satisfies the ascending chain condition). Thus $A = \bar{k}[x_1, \ldots, x_n]$ is noetherian, so every A-ideal is finitely generated. It follows that every algebraic set can be written in the form Z_S with S finite.

Definition 12.12. For an algebraic set $Z \subseteq \mathbb{A}^n$, the *ideal of Z* is the set

$$I(Z) = \{f \in A : f(P) = 0 \text{ for all } P \in Z\},$$

where A is the polynomial ring $\bar{k}[x_1, \ldots, x_n]$.

The set $I(Z)$ is clearly an A-ideal (it is closed under addition and under multiplication by elements of A), and we note that

$$Y \subseteq Z \quad \Longrightarrow \quad I(Z) \subseteq I(Y)$$

and

$$I(Y \cup Z) = I(Y) \cap I(Z)$$

(both statements are immediate from the definition).

We have $Z = Z_{I(Z)}$ for every algebraic set Z, but it is not true that $I = I(Z_I)$ for every ideal I. As a counterexample, consider $I = (f^2)$ for some polynomial $f \in A$. In this case

$$I(Z_{(f^2)}) = (f) \neq (f^2).$$

In order to avoid this situation, we want to restrict our attention to *radical* ideals.

Definition 12.13. Let R be a commutative ring. For any R-ideal I we define

$$\sqrt{I} = \{x \in R : x^r \in I \text{ for some integer } r > 0\},$$

and say that I is a *radical ideal* if $I = \sqrt{I}$.

Lemma 12.14. *For any ideal I in a commutative ring R, the set $\sqrt{I}$ is an ideal.*

Proof. Let $x \in \sqrt{I}$ with $x^r \in I$. For any $y \in R$ we have $y^r x^r = (xy)^r \in I$, so $xy \in \sqrt{I}$. If $y \in \sqrt{I}$ with $y^s \in I$, then every term in the sum

$$(x+y)^{r+s} = \sum_i \binom{r+s}{i} x^i y^{r+s-i}$$

is a multiple of either $x^r \in I$ or $y^s \in I$, hence lies in I, so $(x+y)^{r+s} \in I$ and $(x+y) \in \sqrt{I}$. □

[4] The term "noetherian" refers to the mathematician Emmy Noether. The word noetherian is used so commonly in algebraic geometry (and elsewhere) that it is typically no longer capitalized (like abelian).

Theorem 12.15 (Hilbert's *Nullstellensatz*)**.** *For every ideal $I \subseteq \bar{k}[x_1, \ldots, x_n]$ we have*

$$I(Z_I) = \sqrt{I}.$$

Proof. See [3, Theorem 7.1]. □

Nullstellensatz literally means "zero locus theorem." The theorem above is the strong of the *Nullstellensatz*; it implies the weak *Nullstellensatz*:

Theorem 12.16 (weak *Nullstellensatz*)**.** *For any proper ideal $I \subseteq \bar{k}[x_1, \ldots, x_n]$ the variety Z_I is nonempty.*

Proof. Suppose I is an ideal for which Z_I is the empty set. Then $I(Z_I) = (1)$, and by the strong *Nullstellensatz*, $\sqrt{I} = (1)$. But then $1^r = 1 \in I$, so I is not proper. □

Note the importance of working over $\bar{k}$. It is easy to find proper ideals I for which $Z_I(k) = \emptyset$ when k is not algebraically closed; consider $Z_{(x^2+y^2+1)}(\mathbb{Q})$ in $\mathbb{A}^2$. A useful corollary of the weak *Nullstellensatz* is the following.

Corollary 12.17. *The maximal ideals of the ring $\bar{k}[x_1, \ldots, x_n]$ are all of the form*

$$m_P = (x_1 - P_1, \ldots, x_n - P_n)$$

for some point $P = (P_1, \ldots, P_n)$ in $\mathbb{A}^n(\bar{k})$.

Proof. The evaluation map that sends $f \in \bar{k}[x_1, \ldots, x_n]$ to $f(P) \in \bar{k}$ is a surjective ring homomorphism with kernel m_P. Thus $\bar{k}[x_1, \ldots, x_n]/m_P \simeq \bar{k}$ is a field, hence m_P is a maximal ideal. If m is any maximal ideal in $\bar{k}[x_1, \ldots, x_n]$, then it is a proper ideal, and by the weak *Nullstellensatz* the algebraic set Z_m is nonempty and contains a point $P \in \mathbb{A}^n$. So $m_P \subseteq I(Z_m)$, but also $m \subseteq I(Z_m)$. The ideal $I(Z_m)$ is a proper ideal (since Z_m is nonempty) and the ideals m and m_P are both maximal, so $m = I(Z_m) = m_P$. □

We also have the following corollary of the strong *Nullstellensatz*.

Corollary 12.18. *There is a one-to-one inclusion-reversing correspondence between radical ideals $I \subseteq \bar{k}[x_1, \ldots, x_n]$ and algebraic sets $Z \subseteq \mathbb{A}^n(\bar{k})$ in which $I = I(Z)$ and $Z = Z_I$.*

Remark 12.19. It is hard to overstate the importance of Corollary 12.18; it is the basic fact that underlies nearly all of algebraic geometry. It tells us that the study of algebraic sets (geometric objects) is the same thing as the study of radical ideals (algebraic objects). It also suggests ways in which we might generalize our notion of an algebraic set: there is no reason to restrict ourselves to radical ideals in the ring $\bar{k}[x_1, \ldots, x_n]$, there are many other rings we might consider. This approach eventually leads to the much more general notion of a *scheme*, but for our first foray into algebraic geometry we will stick to algebraic sets (in particular, varieties, which we will define momentarily).

Definition 12.20. A algebraic set is *irreducible* if it is nonempty and not the union of two smaller algebraic sets.

Theorem 12.21. *An algebraic set is irreducible if and only if its ideal is prime.*

Proof. ($\Rightarrow$) Let Y be an irreducible algebraic set and suppose $fg \in I(Y)$ for some $f, g \in A$. We will show that either $f \in I(Y)$ or $g \in I(Y)$ (and therefore $I(Y)$ is prime).

$$\begin{aligned} Y &\subseteq Z_{fg} = Z_f \cup Z_g \\ &= (Y \cap Z_f) \cup (Y \cap Z_g), \end{aligned}$$

and since Y is irreducible we must have either $Y = (Y \cap Z_f) = Z_f$ or $Y = (Y \cap Z_g) = Z_g$), hence either $f \in I(Y)$ or $g \in I(Y)$. Therefore $I(Y)$ is a prime ideal.

($\Leftarrow$) Now suppose $I(Y)$ is prime and that $Y = Y_1 \cup Y_2$. We will show that either $Y = Y_1$ or $Y = Y_2$. This will show that Y is irreducible, since Y must be nonempty ($I(Y) \neq A$ because $I(Y)$ is prime). We have

$$I(Y) = I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2) \supseteq I(Y_1)I(Y_2),$$

and therefore $I(Y)$ divides/contains either $I(Y_1)$ or $I(Y_2)$, since $I(Y)$ is a prime ideal, but it is also contained in both $I(Y_1)$ and $I(Y_2)$, so either $I(Y) = I(Y_1)$ or $I(Y) = I(Y_2)$. Thus either $Y = Y_1$ or $Y = Y_2$, since algebraic sets with the same ideal must be equal. □

References

[1] M. Artin, *Algebra*, 2nd edition, Pearson Education, 2011.

[2] A. Knapp, *Basic Algebra*, Springer, 2006.

[3] A. Knapp, *Advanced Algebra*, Springer, 2007.

[4] J.S. Milne, *Fields and Galois Theory*, 2012.

18.782 Introduction to Arithmetic Geometry
Fall 2013