Notes on graduate algebra

Robert Harron

Department of Mathematics, Keller Hall, University of Hawaiʻi at Mānoa, Honolulu, HI 96822, USA
E-mail address: rharron@math.hawaii.edu

Abstract. Graduate algebra

Contents

CHAPTER 1

Fields and Galois theory

1. Field extensions

(Note: these notes loosely follow Lang's *Algebra*)

We will follow the typical course and study field extensions. This subject grows out of the study of roots of polynomials. The setup is to fix a field F called the *base field* and to study fields K containing F. Rather than referring to F as a subfield of K, we speak of K as an *extension* of F, denoted K/F.

Example 1.1. For instance, $\mathbf{C}$ is an extension of $\mathbf{R}$. If $d \neq 0, 1$ is a squarefree integer, then $\mathbf{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbf{Q}\}$ is an extension of $\mathbf{Q}$. Also, $\mathbf{R}$ and $\mathbf{C}$ are extensions of $\mathbf{Q}$.

There's a big difference between extensions like $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ or $\mathbf{C}/\mathbf{R}$ and those like $\mathbf{R}/\mathbf{Q}$ or $\mathbf{C}/\mathbf{Q}$.

Definition 1.2. Let K/F be an extension.

- An element $\alpha \in K$ is called *algebraic* over F if it is a root of a polynomial over F, i.e. if there's a non-zero $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise, α is said to be *transcendental* over F.
- The extension K/F is called *algebraic* if every element of K is algebraic over F. Otherwise, the extension is called *transcendental.*

Let's also introduce two bits of notation to differentiate between these two situations. Given a commutative ring A, a subring R, and $\alpha \in A$, let $R[\alpha]$ denote the smallest subring of A containing both R and α (note that an arbitrary intersection of subrings of a ring is itself a subring). Given a field extension K/F and an element $\alpha \in K$, let $F(\alpha)$ denote the smallest subfield of K containing F and α (again, note that an arbitrary intersection of subfields is a subfield). More generally, if $F \leq K$ and $S \subset K$, then $F(S)$ is the smallest subfield of K containing F and S (similarly, for $R \leq A$ and $R[S]$).

Proposition 1.3. *Let K/F be a field extension and $\alpha \in K$. Then,*

(i) *α is transcendental if and only if $F[\alpha] \cong F[x]$ (the polynomial ring over F);*

(ii) *α is algebraic if and only if $F[\alpha] = F(\alpha)$, i.e. $F[\alpha]$ is a field; in which case, $F(\alpha) \cong F[x]/(f_\alpha(x))$, where $f_\alpha(x) \in F[x]$ is a monic irreducible polynomial.*

The polynomial $f_\alpha(x)$ is called the *minimal polynomial* of α (over F).

Proof. In either case, consider the unique map $\varphi_\alpha : F[x] \to K$ which is the identity on F and sends x to α (the existence and uniqueness come from the universal property of polynomial rings). As φ_α is a ring homomorphism, it sends a polynomial $f(x)$ to $f(\alpha)$. The image of φ_α contains F and α and it's fairly easy to convince one's self that it is the smallest such subring of K. Thus, $F[\alpha] \cong F[x]/\ker(\varphi_\alpha)$. Now, α is algebraic if and only if φ_α has a non-trivial kernel. If this is the case, the kernel is generated by a polynomial $f_\alpha(x)$ of positive degree that we may simply choose to be monic (since the non-zero constants are all units). If $f_\alpha(x) = f(x)g(x)$ is a proper factorization of $f_\alpha(x)$, then, by the Chinese Remainder Theorem, $F[x]/(f_\alpha(x)) \cong F[x]/(f(x)) \times F[x]/(g(x))$, where the right-hand side is s product of non-zero rings. But such a product is never a field. Thus, $f_\alpha(x)$ must be irreducible. Since it is irreducible, and $F[x]$ is a PID, the ideal $(f_\alpha(x))$ is maximal, so $F[\alpha] \cong F[x]/(f_\alpha(x))$ is a field. □

Note that if α is transcendental over F, then $F(\alpha)$ is simply the fraction field of $F[\alpha] \cong F[x]$; as such it is isomorphic to the *rational function field* $F(x)$. Note that every transcendental extension K/F can be broken down into two extensions $K/k/F$, where $k \cong F(\{x_i : i \in I\})$ (i.e. a rational function field in some number of variables)—a so-called a *purely transcendental extension*—and where K/k is algebraic. We'll now focus on algebraic extensions.

Part of the power of studying roots of polynomials by studying field extensions comes from the following fundamental result due to Kronecker. Note first that any homomorphism from a field F to another field K is necessarily injective and so we typically identify F with its image inside K and thus consider any field K a given field F maps to as an extension K/F.

Theorem 1.4. *Let F be a field and let $f(x) \in F[x]$ be a non-constant polynomial. Then, there is an extension of F in which $f(x)$ has a root.*

Proof. Let $g(x)$ be an irreducible factor of $f(x)$ and let $K := F[x]/g(x)$. This is a field as $g(x)$ is irreducible. There is a natural map $F \to F[x]$. Composing this with the quotient map $F[x] \to K$ allows us to view K as an extension of F. Let $\alpha := x + (g(x))$ be the congruence class of x. Then, $g(\alpha) = g(x) + (g(x)) = 0$, so that the class of x is itself a root of $g(x)$, and hence of $f(x)$, in K. □

The field K in the above proof is said to be obtained from F by *adjoining* a root of $f(x)$. Often, one might say: let $f(x)$ be a (non-constant) polynomial over F, let α be a root of $f(x)$ (which we know exists in *some* extension of F), and let $K := F(\alpha)$. Note that if $f(x)$ is irreducible, then for any root α of $f(x)$, the fields $F(\alpha)$ are all isomorphic (to $F[x]/(f(x))$).

Example 1.5. Let $K = \mathbf{Q}(\sqrt[3]{2})$ be the field obtained by adjoining the real cube root of 2 to $\mathbf{Q}$. On the other hand, let $K' = \mathbf{Q}(\omega\sqrt[3]{2})$, where $\omega = e^{2\pi i/3}$ is a primitive cube root of unity. Then, K and K' are distinct fields inside of $\mathbf{C}$, but they are isomorphic as abstract fields because $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ are both roots of the irreducible polynomial $x^3 - 2 \in \mathbf{Q}[x]$. On the other hand, if K is the field obtained by adjoining a root of $f(x) = x^3 - x^2 - 2x + 1$ to $\mathbf{Q}$, then K, viewed as a subfield of $\mathbf{C}$ say, contains all three roots of $f(x)$, the abstract isomorphisms between the fields obtained by adjoining each of the roots of $f(x)$ then become *automorphisms* of K. The extension $K/\mathbf{Q}$ is an example of a *Galois* extension: it has three automorphisms, which is the same as the degree of $f(x)$ (whereas $\mathbf{Q}(\sqrt[3]{2})$ only has the identity automorphism).

One can study the structure of the roots of a polynomial $f(x) \in F[x]$ by studying field extensions of F obtained by adjoining roots of $f(x)$. The culmination of this is Galois theory.

A basic invariant of a field extension is its *degree.* If K/F is a field extension, then K is an F-algebra and so, in particular, an F-vector space.

Definition 1.6. The *degree* of K/F is defined to be the dimension of K as an F-vector space and is denoted $[K : F]$. The extension is called *finite* if the degree is finite, and infinite otherwise.

Proposition 1.7. *Let F be a field, let $f(x) \in F[x]$ be irreducible and non-constant, and let α be a root of $f(x)$. Then, $[F(\alpha) : F] = \deg f(x)$.*

Proof. Recall that we may identify $F(\alpha)$ with $F[x]/(f(x))$, and thus identify α with $\overline{x} := x + (f(x))$. Let $d := \deg f(x)$. We claim that $\{1, x, x^2, \ldots, x^{d-1}\}$ is a basis of $F[x]/(f(x))$ as an F-vector space. □

Example 1.8. The extensions $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ and $\mathbf{C}/\mathbf{R}$ have degree two. The extensions $\mathbf{R}/\mathbf{Q}$ and $\mathbf{C}/\mathbf{Q}$ are infinite; for instance, they both contain the extension $\mathbf{Q}(\pi)/\mathbf{Q}$ and $\mathbf{Q}(\pi)$ contains $\mathbf{Q}[\pi] \cong \mathbf{Q}[x]$, which is an infinite-dimensional $\mathbf{Q}$-vector space). More generally, any transcendental extension is infinite.

Proposition 1.9. *Every finite extension is algebraic.*

Proof. Let K/F have degree $d < \infty$ and let $\alpha \in K$. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ has $> d$ elements and so must be linearly dependent. Thus, there are elements $a_0, a_1, \ldots, a_d \in F$ such that

$$a_0 \cdot 1 + a_1\alpha + a_2\alpha^2 + \cdots + a_d\alpha^d = 0.$$

Thus, α is a root of $a_0 + a_1 x + \cdots + a_d x^d \in F[x]$. □

There are however infinite algebraic extensions. For instance, we'll see that the set of complex numbers that are algebraic over $\mathbf{Q}$ form a field, and that this field has infinite degree (but is algebraic by definition).

DEFINITION 1.10. An extension K/F is called *finitely generated* if there is a finite subset $S \subseteq K$ such that $K = F(S)$.

EXAMPLE 1.11. The field $\mathbf{Q}(i, \sqrt{2})$ is a finitely generated algebraic extension of $\mathbf{Q}$. The field of rational functions $\mathbf{Q}(x_1, \cdots, x_n)$ in finitely many variables is a finitely generated transcendental extension of $\mathbf{Q}$.

PROPOSITION 1.12. *A finite extension is finitely generated.*

PROOF. A finite extension K/F has a finite basis. This finite basis is *a fortiori* a finite generation set. □

We often denote a field extension K/F by the diagram

$$\begin{tikzcd} K \arrow[d, dash] \\ F \end{tikzcd}$$

thinking of K as being 'over' F. A diagram of the form

$$\begin{tikzcd} K_n \arrow[d, dash] \\ \vdots \arrow[d, dash] \\ K_1 \arrow[d, dash] \\ K_0 \end{tikzcd}$$

will then denote what is called a *tower of fields*, also denote $K_n / \cdots / K_1 / K_0$, where K_i is an extension of K_{i-1}. The degree of an extension is multiplicative in towers.

PROPOSITION 1.13. *If*

$$\begin{tikzcd} K_n \arrow[d, dash] \\ \vdots \arrow[d, dash] \\ K_1 \arrow[d, dash] \\ K_0 \end{tikzcd}$$

is a tower of fields, then

$$[K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}].$$

Proof. By induction, we only need to consider the case $n = 2$, i.e. suppose $K/k/F$ is a tower of fields, we'll show that $[K : F] = [K : k] \cdot [k : F]$. Let $\{\alpha_i : i \in I\}$ be a basis for k/F and let $\{\beta_j : j \in J\}$ be a basis for K/k. We claim that $\{\alpha_i\beta_j : i \in I, j \in J\}$ is a basis for K/F. First, let's show this is a spanning set. Let $z \in K$, then there are elements $a_j \in k$ (almost all 0) such that

$$z = \sum_{j\in J} a_j\beta_j.$$

Each (non-zero) a_j in turn can be written as

$$a_j = \sum_{i\in I} b_{ij}\alpha_i,$$

with only finitely many $b_{ij} \in F$ non-zero. Combing these, we obtain

$$z = \sum_{i\in I}\sum_{j\in J} b_{ij}\alpha_i\beta_j.$$

Now, let's show linear independence. Suppose

$$\sum_{i\in I}\sum_{j\in J} c_{ij}\alpha_i\beta_j = 0$$

with $c_{ij} \in F$, almost all 0. As $\{\beta_j : j \in J\}$ is linear independent, it must be that for all $j \in J$

$$\sum_{i\in I} c_{ij}\alpha_i = 0.$$

The linear independence of $\{\alpha_i : i \in I\}$ then forces all c_{ij} to be zero. □

One way to obtain a tower of fields is to begin with an extension K/F, take two elements $\alpha, \beta \in K$, and form the tower

$$\begin{tikzcd}
F(\alpha)(\beta) \arrow[d, dash] \\
F(\alpha) \arrow[d, dash] \\
F.
\end{tikzcd}$$

Note that $F(\alpha)(\beta) = F(\alpha, \beta) = F(\beta)(\alpha)$.

Proposition 1.14. *A field extension K/F is finite if and only if it is both algebraic and finitely generated.*

Proof. The left-to-right implication follows from previous results. Suppose $K = F(\alpha_1, \dots, \alpha_n)$ is algebraic and consider the tower

$$\begin{tikzcd}
F(\alpha_1,\dots,\alpha_n) = F(\alpha_1,\dots,\alpha_{n-1})(\alpha_n) \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
F(\alpha_1,\alpha_2) = F(\alpha_1)(\alpha_2) \arrow[d, dash] \\
F(\alpha_1) \arrow[d, dash] \\
F
\end{tikzcd}$$

Since each step in the tower is generated by one algebraic element, each successive extension is finite (of degree that of the minimal polynomial of α_i). The degree of K/F is then the product of these finite degrees and hence is finite. □

Proposition 1.15. *If $K = F(\{\alpha_i : i \in I\})$, then K/F is algebraic if and only if each α_i is algebraic over F.*

Proof. The left-to-right implication holds by definition. Conversely, suppose $\beta \in K$. An element of $F(\{\alpha_i : i \in I\})$ can, by definition, be written as

$$\beta = \frac{f(\alpha_{i_1}, \dots, \alpha_{i_n})}{g(\alpha_{i_1}, \dots, \alpha_{i_n})},$$

where $f, g \in F[x]$. But then $\beta \in F(\alpha_{i_1}, \dots, \alpha_{i_n})$, which is finite, so β is algebraic. □

We think of $F(\alpha, \beta)$ as being formed out of $F(\alpha)$ and $F(\beta)$. This leads to the following definition.

Definition 1.16. Suppose K and L are two extensions of F *contained in a given larger extension* E (we cannot do this without this condition), the *compositum of K and L*, denoted KL, is the smallest extension F inside E containing both K and L. We similarly define the compositum of any family $\{K_i : i \in I\}$ of subfields of a given extension E/F.

The diagram for a compositum is

$$\begin{tikzcd}
& KL \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

where K and L are tacitly assumed to be contained in a common larger extension.

Definition 1.17. Following Lang, we call a collection $\mathcal{C}$ of field extensions *distinguished* if the following two conditions hold:

(i) Let

$$\begin{tikzcd} K \arrow[d, dash] \\ k \arrow[d, dash] \\ F \end{tikzcd}$$

be a tower of fields. Then, $K/F \in \mathcal{C}$ if and only if K/k and k/F are both in $\mathcal{C}$.

(ii) If $L/F \in \mathcal{C}$ and K is any extension of F, then $KL/K \in \mathcal{C}$:

$$\begin{tikzcd} & KL \arrow[dd, dash] \\ K \arrow[ur, dash, "\mathcal{C}"] \arrow[dd, dash] & \\ & L \\ F \arrow[ur, dash, "\mathcal{C}"'] & \end{tikzcd}$$

In (ii), we think of the extension L/F being *lifted* to KL/K. Note that if $\mathcal{C}$ is a distinguished class of extensions and K/F and L/F are in $\mathcal{C}$, then KL/F is also in $\mathcal{C}$.

The notion of distinguished class will occur a few times and it's good to know when certain types of extensions are distinguished, which is why I think it's worth following Lang and naming the concept.

PROPOSITION 1.18. *The class of algebraic extensions is distinguished. So is the class of finite extensions.*

PROOF. For finite extensions, the multiplicativity of degrees in towers proves condition (i). Now, suppose L/F is finite and let K/F be arbitrary. By above, L/F is finitely generated by algebraic elements $\alpha_1, \ldots, \alpha_n$, i.e. $L = F(\alpha_1, \ldots, \alpha_n)$. Then, KL/K is also finitely generated by those elements, i.e. $KL = K(\alpha_1, \ldots, \alpha_n)$. Thus, KL/K is also finite.

Now, consider algebraic extensions. For (i), if $K/k/F$ is a tower of extensions and K/F is algebraic, then automatically so are K/k and k/F. Conversely, let $\alpha \in K$. As K/k is algebraic, there are $a_0, \ldots, a_d \in k$, not all 0, such that $a_0 + a_1\alpha + \cdots + a_d\alpha^d = 0$. Let $k' := F(a_0, a_1, \ldots, a_n)$. Then, α is algebraic over k', but also k' is finite over F (as it is finitely generated by algebraic elements). Then,

$$\begin{tikzcd} k'(\alpha) \arrow[d, dash] \\ k' = F(a_0, \ldots, a_d) \arrow[d, dash] \\ F \end{tikzcd}$$

is a tower of finite extensions and hence $k'(\alpha)/F$ is finite and so algebraic. Thus, α is algebraic over F. For (ii), suppose L/F is algebraic, let K/F be any extension with K and L both contained in a bigger extension E. Since L/F is algebraic, $L = F(\{\alpha_i : i \in I\})$ for some elements α_i. Then, $KL = K(\{\alpha_i : i \in I\})$. Since the α_i are algebraic over F, they are *a fortiori* algebraic over K. Thus, KL/K is algebraic. □

We now set out to understand more about field extensions and the maps between them. Amongst other things, this will allow us to see the structure of roots of polynomials appearing in these maps.

First, recall from above that every homomorphism between two fields is an embedding (i.e. injective). With a fixed base field F and two extensions K_1/F and K_2/F, we'll be interested in F-algebra embeddings, i.e. homomorphisms that are the identity on F. A bit more generally, we'll be interested in a situation where we have two isomorphic base fields $\sigma : F \xrightarrow{\sim} F^\sigma$ (here we use the notation F^σ instead of $\sigma(F)$, and for $a \in F$, we'll also use a^σ for $\sigma(a) \in \sigma(F)$; we call a^σ the *conjugate* of a under σ) and, for extensions K_1/F and K_2/F^σ, embeddings $\tau : K_1 \to K_2$ such that $\tau|_F = \sigma$. This extra level of generality is useful as some basic constructions, such as that in Kronecker's result above, involve constructing a field up to isomorphism.

Definition 1.19. Let $\sigma : F \to L$ be an embedding of fields and let K be an extension of F. We say an embedding $\tau : K \to L$ *extends* σ if $\tau|_F = \sigma$. We will also say that τ is an embedding *over* σ. Note that F is isomorphic to its image F^σ in L. When σ is the identity map on F, we'll simply say τ is an embedding *over* F (or an F*-embedding*).

The source of the connection between field embeddings and roots of polynomials is the following simple lemma.

Lemma 1.20 ("Embeddings bring roots of a polynomial to roots of that polynomial"). *Let $\sigma : F \to L$ be an embedding of fields and let $f(x) = a_n x^n + \cdots + a_0 \in F[x]$. Define $f^\sigma(x) = a_n^\sigma x^n + \cdots + a_0^\sigma \in F^\sigma[x]$. If K/F is an extension and $\tau : K \to L$ extends σ, then for every root α of $f(x)$ in K, we have that $\tau(\alpha)$ is a root of $f^\sigma(x)$. In particular, when σ is the identity, $\tau(\alpha)$ is again a root of $f(x)$.*

Proof. By definition,

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

so that

$$0 = \tau(0) = \tau(f(\alpha)) = \sum_{i=0}^{n} \tau(a_i)\tau(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i)\tau(\alpha)^i = f^\sigma(\tau(\alpha)).$$

□

A useful corollary.

Corollary 1.21. *If K/F is algebraic and $\tau : K \to K$ is an F-embedding, then τ is an automorphism of K.*

Proof. Note that the case where K/F is finite is immediate since τ is an injective linear transformation from a finite-dimensional F-vector space to one of the same dimension and the rank+nullity theorem ensures that injective implies surjective. The previous lemma basically allows us to reduce to the finite-dimensional case. Let $\alpha \in K$ be arbitrary. We want to show that α is in the image of τ so that τ is surjective. Since K/F is algebraic, there is a non-zero polynomial $f(x) \in F$ such that $f(\alpha) = 0$. Let K' be the subfield of K obtained by adjoining all the roots of $f(x)$ in K to F. Then, K' is algebraic and finitely-generated, hence K'/F is finite. By the previous lemma, $\tau|_{K'}$ maps K' into itself and we conclude that $\tau|_{K'}$ is an automorphism of K' by the finite case. Since $\alpha \in K'$, it is in the image of $\tau|_{K'}$ and hence of τ itself. □

2. Algebraically closed fields and algebraic closure

Wouldn't it be great if there were fields that contained all the roots of all polynomials over itself? Wouldn't it be great if you could embed any field into an unique such field (with some additional property)? Yes and yes. And life is great!

Definition 2.1. A field Ω is called *algebraically closed* if every non-constant polynomial in $\Omega[x]$ has a root in Ω (and so every polynomial in $\Omega[x]$ has all its roots in Ω by induction).

Note that the only algebraic extension of an algebraically closed field is itself; hence the name.

Example 2.2. Possibly the only example you know is the complex numbers: the Fundamental Theorem of Algebra, first proved by Gauss, is simply the statement that $\mathbf{C}$ is algebraically closed. The standard proof is via complex analysis, but several others, including algebraic ones, exist. We'll see that the set of complex numbers that are algebraic over $\mathbf{Q}$ forms an algebraically closed field called the *field of algebraic numbers.*

Definition 2.3. Let F be a field. An *algebraic closure* of F is an algebraically closed field that is an algebraic extension of F.

The reason this is called a 'closure' is that it is a minimal algebraically closed field containing F. Indeed, from property (i) of algebraic extensions being a distinguished class, an algebraic extension of an algebraic extension is algebraic, and since algebraically closed fields can't have non-trivial extensions, once you hit an algebraically closed field, any nontrivial extension of it is no longer algebraic over F. Of course, this also means an algebraic closure is a maximal algebraic extension.

Our goal now is to show that every field has an algebraic closure and that any two algebraic closures are isomorphic over the base field. That algebraic closures are maximal algebraic extensions suggests that perhaps we should break the problem into two parts: first, show every field has some algebraically closed extension field, then show that the union of all algebraic extensions of the base field within this big algebraically closed field is itself algebraically closed.

We present Emil Artin's proof of the first part. (Let's note at this point that above we only proved that for any $f(x) \in F[x]$, F can be *embedded* into a field K that contains a root of $f(x)$; in fact, Lang's Proposition V.2.3 is a silly little thing that allows you to actually have F be a subset of K, so that K is veritably an extension of F. So, any time we construct an embedding of F into a field K so that some polynomial over F has a root in K, we can shimmy things so that K is actually an extension of F.)

Theorem 2.4. *Every field F has an extension Ω that is algebraically closed.*

Proof. (E. Artin) This is just a bit absurd. For every non-constant $f \in F[x]$, let x_f be an indeterminate and consider the polynomial ring $R_1 := F[\{x_f : f \in F[x], f \text{ non-constant}\}]$. Let $I_1 \trianglelefteq R_1$ be the ideal generated by $f(x_f)$ as f varies over all non-constant elements of $F[x]$. We'll show that I_1 is not the unit ideal and hence is contained in some maximal ideal $\mathfrak{m}_1 \trianglelefteq R_1$. Then $F_1 := R_1/\mathfrak{m}_1$ is a field that contains (an isomorphic copy of) F and a root of every non-constant polynomial over F. Iterating this construction with F_1 gives a field F_2 that is an extension of F_1 that contains a root of every non-constant polynomial over F_1. We then obtain a tower of extensions

$$\begin{tikzcd}
\vdots \arrow[d, dash] \\
F_2 \arrow[d, dash] \\
F_1 \arrow[d, dash] \\
F
\end{tikzcd}$$

such that F_n contains a root of every polynomial in F_{n-1}. It is straightforward to check that the union $\Omega := \bigcup_{n \geq 1} F_n$ is itself a field. Furthermore, we claim that Ω is algebraically closed. Indeed, a polynomial $g(x) \in \Omega[x]$ has finitely many non-zero coefficients and is thus contained in $F_n[x]$ for some n. It then has a root in F_{n+1} and hence in Ω.

If you're keeping score, you'll remember that we still have to show I_1 is a proper ideal. If $(f(x_f) : f \in F[x], \deg(f) \geq 1)$ is the unit ideal, then there are polynomials $g_1, \ldots, g_n \in R_1$ such that

$$1 = g_1 f_1(x_{f_1}) + g_1 f_2(x_{f_2}) + \cdots + g_n f_n(x_{f_n})$$

for some non-constant $f_i \in F[x]$. Since the g_i are polynomials, they only contain finitely many terms and so are polynomials in $x_{f_1}, \ldots, x_{f_n}$ and finitely many other x_f. Let F' be an extension of F in which each f_i has a root and call that root α_i. Plugging in α_i for x_{f_i} and zero for the other x_f into the above identity yields $1 = 0$ in F'. Contradiction! □

Corollary 2.5. *Every field has an algebraic closure.*

Proof. Let F be a field and let Ω be an algebraically closed extension of F. Let $\overline{F}$ be the union of all algebraic extensions of F in Ω. We claim that this is an algebraic closure of F. First off, it is a field basically because algebraic extensions are a distinguished class. Indeed, given two algebraic extensions of F in Ω, their compositum in Ω is algebraic over F, so when you, for instance, take two elements in $\overline{F}$ and try to add them, each of them is in some algebraic extension and their addition can take place in the compositum of the two extensions. (Said another way, when you take the direct limit of a bunch of algebraic extensions in a given extension, you get another algebraic extension). Secondly, $\overline{F}$ is algebraic over F. Indeed, any α in $\overline{F}$ is contained in some algebraic extension of F by definition of $\overline{F}$ as the union of all algebraic extensions of F in Ω. Finally, $\overline{F}$ is algebraically closed. Indeed, let $g(x) \in \overline{F}[x]$. Since Ω is algebraically closed, $g(x)$ has a root α in Ω. This α is algebraic over $\overline{F}$ and so by property (i) of algebraic extensions being distinguished, α is algebraic over F and hence is a root of $g(x)$ in $\overline{F}$. □

We will obtain the uniqueness as a corollary of some very important facts about extending embeddings.

Theorem 2.6. *Let $\sigma : F \to \Omega$ be an embedding of a field into an algebraically closed field, let $\alpha \in \Omega$ be algebraic over F, and let $K = F(\alpha)$. Let $f_\alpha(x) \in F[x]$ be the minimal polynomial of α over F. The number of extensions of σ to K is equal to the number of distinct roots of $f_\alpha(x)$ (in any algebraically closed field containing F), and hence is $\leq [K : F]$.*

Proof. We know from above that if $\tau : K \to \Omega$ extends σ, then $\tau(\alpha)$ must be a root of $f_\alpha^\sigma(x)$ showing that the number of τ is at most the number of distinct roots of $f_\alpha(x)$. On the other hand, given a root β of f^σ in Ω, there is a unique homomorphism $F[x] \to \Omega$ that agrees with σ on F and sends x to β (this is the freeness property of the polynomial algebra composed with the isomorphism $F[x] \cong F^\sigma[x]$). Since $K = F(\alpha) \cong F[x]/(f_\alpha(x)) \cong F^\sigma[x](f_\alpha^\sigma(x))$ and $f_\alpha^\sigma(\beta) = 0$ (i.e. the kernel of the map $F[x] \to \Omega$ is contained in $(f_\alpha(x))$), the universal property of quotients yields a unique homomorphism $K \to \Omega$ agreeing with σ on F and sending α to β. □

Example 2.7. In case you're wondering about the word *distinct* in the above proposition, consider the field $F = \mathbf{F}_p(T)$, where $\mathbf{F}_p$ is the finite field $\mathbf{Z}/p\mathbf{Z}$ for some prime p and T is a polynomial variable. The polynomial $f(x) = x^p - T$ is irreducible over F (F is the fraction field of $\mathbf{F}_p[T]$, which is a UFD, and T is a prime element, so $f(x)$ is irreducible by the Eisenstein criterion). Let $T^{1/p}$ denote a root of this polynomial in some extension of F. In that extension, $f(x) = (x - T^{1/p})^p$. Hence, $T^{1/p}$ is the *unique* root of $f(x)$ in any algebraically closed field containing F, despite the fact that f has degree $p > 1$. This kind of reprehensible behaviour only occurs in fields of characteristic p and goes by the dirty name 'inseparability'. We'll get to that soon enough.

The following theorem ramps up the existence statement in the previous theorem (and uses it in the proof).

Theorem 2.8. *Let $\sigma : F \to \Omega$ be an embedding of a field into an algebraically closed field. Then σ can be extended to any algebraic extension K of F. If K is algebraically closed and Ω is algebraic over F^σ, then any such extension is an isomorphism.*

Proof. Make Zorn's Lemma-nade! Let X be the set of all pairs (k, τ) where $F \leq k \leq K$ and $\tau : k \to \Omega$ extends σ. Define a partial order on X by $(k, \tau) \leq (k', \tau')$ if $k \leq k'$ and $\tau'|_k = \tau$. Since (F, σ) is in X, X is nonempty. Given a chain $(k_1, \tau_1) \leq (k_2, \tau_2) \leq \ldots$ of elements of X, let $k := \bigcup_{n \geq 1} k_n$ and let $\tau = \bigcup_{n \geq 1} \tau_n$. It is clear that (k, τ) is in X and is an upper bound for the chain. By Zorn's

Lemma, there is a maximal element $(\widetilde{k}, \widetilde{\tau})$ in X. We claim that $\widetilde{k} = K$. If not, let $\alpha \in K \setminus \widetilde{k}$. The previous theorem allows us to extend $\widetilde{\tau}$ to $\widetilde{k}(\alpha)$ contradicting the maximality of $(\widetilde{k}, \widetilde{\tau})$. Thus, σ can be extended to K.

If K is algebraically closed, Ω is algebraic over F^σ, and $\tau : K \to \Omega$ is an extension of σ, then K^τ is algebraically closed. Since Ω is algebraic over F^σ and $K^\tau \leq \Omega$, Ω is algebraic over K^τ. Hence, $\Omega = K^\tau$, as the latter is algebraically closed. □

Corollary 2.9. *Any two algebraic closures of a field are isomorphic (over that field).*

We therefore often refer to an algebraic closure of F as *the* algebraic closure of F, and denote it $\overline{F}$. Others use F^a or F^{ac}. Others still, will be careful to use *an* algebraic closure. If I recall correctly, there's a paper of Deligne where you can find the gem "Let $\mathbf{C}$ be an algebraic closure of $\mathbf{R}$..." or something to that effect.

Remark 2.10. *Note that if K/F is algebraic, then $\overline{K} = \overline{F}$.*

Remark 2.11. *If F is an infinite field, then $\#\overline{F} = \#F$: indeed, every element of $\overline{F}$ is a root of some unique irreducible polynomial over F and each such polynomial corresponds to at most its degree many elements of $\overline{F}$. As a polynomial is a finite expression and each is counted with a finite multiplicity (the number of distinct roots in $\overline{F}$), the cardinality of this multiset is the same as that of F. Hence, the same holds for $\overline{F}$.*

On the other hand, an algebraically closed field cannot be finite (see right below this). The same argument as above however shows that the algebraic closure of a finite field is countable.

Proposition 2.12. *Finite fields cannot be algebraically closed.*

Proof. Let F be a finite field and consider the polynomial function from F to itself sending a to $a^2 - a$. Since 0 and 1 are both sent to 0, this function is not injective. Since F is finite, it is thus not surjective either. If $\alpha \in F$ is an element not in its image, then the polynomial $x^2 - x - \alpha$ has no root in F. □

3. Splitting fields and normal extensions

A key concept in the study of field extensions is that of splitting fields.

Definition 3.1. Let F be a field and let $f(x) \in F[x]$ be a non-constant polynomial. A *splitting field of $f(x)$* is an algebraic extension K/F such that $f(x)$ splits into linear factors over K and K is generated over F by the roots of $f(x)$.

Example 3.2. The extension $\mathbf{Q}(\sqrt{D})/\mathbf{Q}$ is the splitting field of $x^2 - D$. The extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is *not* the splitting field of $x^3 - 2$, rather $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ is, where $\omega = e^{2\pi i/3}$.

Theorem 3.3. *Let K be a splitting field of $f(x) \in F[x]$. If L is another splitting field of $f(x)$, then there is an F-isomorphism $L \cong K$. Indeed, if $F \leq K \leq \overline{F}$, then any F-embedding of L into $\overline{F}$ is an F-isomorphism $L \cong K$.*

Proof. By definition,

$$f(x) = c \prod_{i=1}^{d} (x - \alpha_i)$$

in $K[x]$. Similarly, in $L[x]$,

$$f(x) = c \prod_{i=1}^{d} (x - \beta_i)$$

Let $\overline{K}$ be an algebraic closure of K, so that $\overline{K} = \overline{F}$. Given any F-embedding $\tau : L \to \overline{F}$,

$$f(x) = f^\tau(x) = c \prod_{i=1}^{d} (x - \beta_i^\tau).$$

But $f(x)$ has a unique factorization in $\overline{F}[x] \supseteq K[x]$, so $\{\beta_1^\tau, \ldots, \beta_n^\tau\}$ is a permutation of $\{\alpha_1, \ldots, \alpha_n\}$. As $K = F(\alpha_1, \ldots, \alpha_n)$ and $L = F(\beta_1, \ldots, \beta_n)$, we thus see that $L^\tau \subseteq K$. But also $K = F(\beta_1^\tau, \ldots, \beta_n^\tau)$, so $L^\tau = K$. Furthermore, we know there is an extension $\tau : L \to \overline{F}$ of the identity embedding $F \to \overline{F}$ since L/F is algebraic. □

More generally, given a family $\{f_i \in F[x] : i \in I\}$ of polynomials, we can define its splitting field to be an extension K of F such that every f_i factors into linear factors in over K and K is generated by the roots of the f_i.

Corollary 3.4. *Splitting fields exist and are unique up to F-isomorphism.*

Proof. For a single polynomial, its splitting field can simply be taken to be the subfield of $\overline{F}$ generated by its roots in $\overline{F}$. For a family of polynomials, you can do the same thing, or simply say you're taking the compositum of the splitting fields of each polynomial. This shows the existence of splitting fields. We proved the uniqueness above for a single polynomial. Now, let K and L be two splitting fields of the family $\{f_i : i \in I\}$ and let $\tau : L \to \overline{K} = \overline{F}$ be an F-embedding (which we know exists). For each $i \in I$, K and L each contain a unique splitting field K_i (and L_i, resp.) of f_i. By above, $L_i^\tau = K_i$. Thus, $L^\tau \leq K$. Since K is the compositum of the K_i, in fact, $L^\tau = K$. □

The following characterization of splitting fields is what makes them so important.

Theorem/Definition 3.5. *Let F be a field and let K/F be an extension contained in $\overline{F}$. The following are equivalent:*

(i) *K is the splitting field of a family of polynomials over F;*
(ii) *every irreducible polynomial over F that has a root in K splits into linear factors in K;*
(iii) *every F-embedding $K \to \overline{F}$ is an F-automorphism of K.*

Any extension K/F satisfying one (and hence all) of these conditions is called normal.

Proof. (i)⇒(iii): Suppose $\tau : K \to \overline{F}$ is an F-embedding. We want to show that $K^\tau = K$. From an earlier result, it suffices to show $K^\tau \subseteq K$. But since K is a splitting field, it is generated by roots of some f_i. Any root of f_i must be sent to another by τ, and so its image must still lie in K.

(iii)⇒(i): We claim that K is the splitting field of $\{f_\alpha(x) : \alpha \in K\}$ (where $f_\alpha(x)$ denotes the minimal polynomial of α over F). Let $\beta \in \overline{F}$ be a root of f_α. We wish to show that $\beta \in K$. Define $\sigma : F(\alpha) \to F(\beta)$ by the identity of F and by sending α to β. As K is algebraic over $F(\alpha)$, there is a $\tau : K \to \overline{F}$ extending σ. This τ is an automorphism of K by assumption. Thus, $\tau(\alpha) = \sigma(\alpha) = \beta \in K$.

(iii)⇒(ii): The preceding argument shows this.

(ii)⇒(iii): Let $\tau : K \to \overline{F}$ be an F-embedding. For any $\alpha \in K$, τ maps α to some other root of $f_\alpha(x)$ and by assumption this root is in K. Thus, $K^\tau \subseteq K$. But, again, an F-embedding of a field into itself is an automorphism. □

Remark 3.6. *The third equivalent condition is a useful theoretical characterization of normal extension, as we'll see in proofs below.*

Example 3.7.

(i) Any quadratic extension is normal.
(ii) The extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is not normal. Indeed, the roots $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ of $x^3 - 2$ are not in $\mathbf{Q}(\sqrt[3]{2})$.
(iii) For any $n \geq 3$, $\mathbf{Q}(\sqrt[n]{2})/\mathbf{Q}$ is not normal. Indeed, the root $\zeta_n\sqrt[n]{2}$ of $x^n - 2$ is not in $\mathbf{Q}(\sqrt[n]{2})$, where $\zeta_n = e^{2\pi i/n}$.
(iv) For any n, $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is normal, as the other roots of $f_{\zeta_n}(x)$ are merely ζ_n^j, where $(j, n) = 1$.

Proposition 3.8. *Normal extensions do not form a distinguished class. However, condition (ii) holds (i.e. a lift of a normal extension is normal). Furthermore, part of (i) holds: if $K/k/F$ is a tower of fields and K/F is normal, then K/k is normal. Also, the compositum, and also the intersection, of fields gives normal extensions.*

Proof. To show that condition (i) of the definition of distinguished classes fails simply consider the tower

$$\begin{tikzcd}
\mathbf{Q}(\sqrt[4]{2}) \arrow[d, dash] \\
\mathbf{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbf{Q}
\end{tikzcd}$$

of successive degree two extensions. Each successive extension is normal, but the big extension is not. By considering the tower

$$\begin{tikzcd}
\mathbf{Q}(\sqrt[3]{2}, \omega) \arrow[d, dash] \\
\mathbf{Q}(\sqrt[3]{2}) \arrow[d, dash] \\
\mathbf{Q}
\end{tikzcd}$$

you can also get a situation where the big extension is normal, and the top extension is normal, but the bottom one is not.

For the partial result regarding condition (i), suppose $K/k/F$ is a tower of fields and that K/F is normal. Let $\tau : K \to \overline{k}$ be a k-embedding. It is *a fortiori* an F-embedding and hence an automorphism of K.

To prove condition (ii), suppose we have the diagram

$$\begin{tikzcd}
& KL \arrow[dl, dash] \arrow[dd, dash] \\
K \arrow[dd, dash] & \\
& L \arrow[dl, dash, "\text{normal}"] \\
F &
\end{tikzcd}$$

of field extensions where L/F is normal. Let τ be an K-embedding of KL into $\overline{K}$. By definition, $K^\tau = K$, and by hypothesis, $L^\tau = L$ (since $\tau|_L$ is an F-embedding). Thus, $(KL)^\tau = K^\tau L^\tau = KL$.

Now, suppose K and L are normal over F, then for any F-embedding τ of KL into $\overline{F}$, we have

$$(KL)^\tau = K^\tau L^\tau = KL,$$

so KL is normal over F. For intersections, the proof is the same since $\tau(K \cap L) = \tau(K) \cap \tau(L)$. This works for arbitrary families of fields. □

Since the intersection of normal extensions (contained in some bigger field) is a normal extension, we can define the normal closure of a field. The idea being that a non-normal field is *missing* some elements.

Definition 3.9. Let K/F be an algebraic extension. The *normal closure of* K is

$$K^{\mathrm{nc}} := \bigcap_{\substack{L/F \text{ normal} \\ K \leq L \leq \overline{K}}} L,$$

i.e. it's the minimal normal extension of F containing K.

Here is a more explicit description of the normal closure.

Proposition 3.10. *For an algebraic extension K/F, let $\{\tau_i : i \in I\}$ be the set of F-embeddings of K into $\overline{K}$. Then, K^{nc} is the compositum of the K^{τ_i}.*

Proof. Given $\alpha \in K$, any normal L/F containing K must contain α^{τ_i} for all $i \in I$. Thus, K^{nc} contains K^{τ_i} for all $i \in I$ and so it contains their compositum. Furthermore, if τ is some F-embedding of this compositum into $\overline{K}$, then composing τ with the τ_i simply permutes them, so τ is an automorphism of the compositum. The latter is thus normal and hence the smallest normal extension of F containing K. □

Note that this shows that the normal closure of a finite extension is itself finite (being a finite compositum of finite extensions).

Example 3.11. Let $K = \mathbf{Q}(\sqrt[3]{2})$. We've seen that $K/\mathbf{Q}$ is not normal. There are three embeddings of K into $\mathbf{C}$ (and hence into $\overline{\mathbf{Q}}$) sending $\sqrt[3]{2}$ to $\sqrt[3]{2}, \omega\sqrt[3]{2}$, or $\omega^2\sqrt[3]{2}$. Thus, $K^{\mathrm{nc}} = \mathbf{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. The latter is simply $\mathbf{Q}(\sqrt[3]{2}, \omega)$: indeed, $\omega \in K^{\mathrm{nc}}$ (since $\omega = \omega\sqrt[3]{2}/\sqrt[3]{2}$) so $\mathbf{Q}(\sqrt[3]{2}, \omega) \leq K$; conversely, $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ are clearly all in $\mathbf{Q}(\sqrt[3]{2}, \omega)$. Similarly, $\mathbf{Q}(\sqrt[4]{2})^{\mathrm{nc}} = \mathbf{Q}(\sqrt[4]{2}, i)$.

4. Separable polynomials and separable extensions

Recall that above we saw that, for a finite extension $F(\alpha)/F$, the number of F-embeddings of $F(\alpha)$ into $\overline{F}$ is bounded above by the number of distinct roots of $f_\alpha(x)$. To say that $F(\alpha)$ is normal is to say that the number of such F-embeddings is *equal* to the number of distinct roots of the minimal polynomial $f_\alpha(x)$, i.e. that this number is as big as possible. We now go on to making the number really as big as possible by identifying extensions where all the roots of minimal polynomials are distinct.

Let K/F be an algebraic extension and fix an embedding $\sigma : F \to \Omega$ into an algebraically closed field. Let $\Sigma_{K,\sigma}$ be the set of extensions of σ to K. It can be verified that $\#\Sigma_{K,\sigma}$ is independent of σ and Ω.

Definition 4.1. For an algebraic extension K/F, its *separable degree* is $[K : F]_s := \#\Sigma_{K,\sigma}$.

Proposition 4.2. *The separable degree is multiplicative in towers: $[K : F]_s = [K : k]_s[k : F]_s$. If K/F is finite, $[K : F]_s \leq [K : F]$.*

Proof. The first statement basically follows from independence of σ. For the second statement, view K/F is a tower $F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \ldots, \alpha_n) = K$. From an earlier result, the inequality holds at each step of the tower. It then holds over the whole tower by multiplicativity. □

Remark 4.3. *In fact, for K/F finite, $[K : F]_s \mid [K : F]$. The quotient is called the inseparable degree $[K : F]_i$.*

Definition 4.4. A polynomial $f(x) \in F[x]$ is called *separable* if it has no multiple roots (in $\overline{F}$). Let K/F be an extension and let $\alpha \in K$ be algebraic over F. We say α is *separable over* F if its minimal polynomial $f_\alpha(x)$ is separable.

Note that if $\alpha \in K$ is separable over F, then it is separable over any field k between K and F since its minimal polynomial over k divides that over F.

Theorem/Definition 4.5. *Let K/F be a finite extension. The following are equivalent:*

(i) *every element of K is separable over F;*
(ii) $[K : F]_s = [K : F]$.

If K/F satisfies either (and hence both) of these conditions, we say K/F is separable. More generally, an infinite algebraic extension K/F is called separable if every element of K is separable over F, equivalently, if every finite subextension k/F is separable.

Proof. □

Theorem 4.6. *Separable extensions form a distinguished class.*

Proof. □

Definition 4.7. An algebraic extension K/F is called *Galois* if it is both normal and separable. The group of F-automorphisms of K is called the *Galois group of K/F* and denoted $\mathrm{Gal}(K/F)$.

From what we've seen, this implies that there are as many F-automorphisms of K as possible; in particular, for a finite extension of degree n, there are exactly n of them.

Bibliography