Field and Galois Theory

by Ivan Aidun

These are notes interspersed with exercises. The purpose of these notes is to be more fleshed out than Evan Dummit's old notes, but shorter and more focused than a textbook treatment. Halfway between Dummit and Dummit and Foote, so to speak. I hope these are helpful to you!

Overview

Galois theory was created to understand the roots of polynomials in one variable. The key insight of Galois theory is that we can understand polynomials by understanding the possible symmetries of their roots. A motto to keep in mind about the Fundamental Theorem of Galois Theory (or any equivalence you meet for the rest of your life): what the equivalence gives you is flexibility. You can use that flexibility when solving problems, by seeing which equivalent formulation is best suited to information you have available. (Different parts of a problem might be better suited to different sides of the equivalence, so you may end up passing back and forth more than once!)

I think the most important things to know in these notes are: the examples given in Example 1, and the basic properties of cyclotomic extensions and finite fields given immediately before; the basic relations between the minimal polynomial of an element, the degree of that element, and the degree of a field extension; the composite and intersection of two fields; the definition of a separable extension, and examples of inseparable extensions; the Fundamental Theorem, and the Galois groups of all the examples in Example 1.

Important examples to keep in mind:

The following examples of field extensions are in fact all Galois extensions, so whenever you read a fact about field extensions or about Galois theory you should start by testing what that fact says about these extensions.

Example 1.

- Starting with any field K, if $\mu \in K$ is not a square, then $K(\sqrt{\mu})$ is an extension of degree 2. In particular, this lets you think of lots of degree 2 extensions of $\mathbb{Q}$. **Exercise 1.** If n, m are different squarefree integers, show that $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{m})$ are different extensions of $\mathbb{Q}$.
- For every n, the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree $\varphi(n)$. (See **Cyclotomic extensions** below.)
- For any p, and any d, there is an extension of $\mathbb{F}_p$ of degree d. In fact, a non-transparent fact is that any two extensions of $\mathbb{F}_p$ of degree d are actually the same! So, we call this unique extension $\mathbb{F}_{p^d}$ *the* finite field with p^d elements. (Sometimes also called the "Galois field with p^d elements", and sometimes denoted $GF(p, d)$.) (See **Extensions of finite fields** below.)
- Combining some of the above examples, given an field K and an element $\mu \in K$ which is not a perfect nth power, then we can form the extension $K(\sqrt[n]{\mu}, \zeta_n)$, which is the field containing all

the roots of the polynomial $x^n - \mu$ (see **Splitting fields and normal extensions** below). For example, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Quick Recap on Polynomials

(This first exercise is also in the ring theory notes.) Recall that there is a notion of "division with remainder" for polynomials: if $f(x)$ and $g(x)$ are polynomials over a field, then there are unique polynomials $q(x)$ and $r(x)$ so that $f(x) = g(x)q(x) + r(x)$ and either $\deg(r) < \deg(g)$ or $r(x) = 0$.

Exercise 2. Let K be a field, prove that $K[x]$ is a principal ideal domain.

Exercise 3.

(a) Let K be a field, $f \in K[x]$, and suppose there is $a \in K$ so that $f(a) = 0$. Prove that $(x-a) \mid f$.

(b) Conclude that a polynomial over a field cannot have more roots than its degree.

(c) Verify that the polynomial $x^2 - 1$ has 4 roots in $\mathbb{Z}/8\mathbb{Z}$.

Since we're going to be making statements about irreducible polynomials over various fields, you might reasonably wonder how to show that a given polynomial is irreducible. In general, it is pretty hard to tell directly. Here's a quick and dirty list of facts that can be helpful:

(1) Quadratic polynomials are easy to check (except in characteristic 2) because you can use the quadratic formula. In particular, a quadratic polynomial is itreducible if and only if its discriminant $b^2 - 4ac$ is not a square (again, things are more complicated in characteristic 2).

(2) (Gauss' Lemma) A polynomial in $\mathbb{Q}[x]$ with coprime integer coefficients is irreducible if and only if it is irreducible in $\mathbb{Z}[x]$. Since we can always multiply through to clear denominators, this means that understanding irreducibility of polynomials over $\mathbb{Q}$ is the same as understanding irreducibility of polynomials over $\mathbb{Z}$. This is useful because...

(3) A polynomial in $\mathbb{Z}[x]$ with coprime coefficients is irreducible if it is irreducible over $\mathbb{Z}/m\mathbb{Z}$ for some integer m. This is usually most useful when the degree is 3 and m is a small prime number because, as mentioned below, in that case $\mathbb{Z}/p\mathbb{Z}$ is a field, so you can check irreducibility by just checking if any of the p elements of $\mathbb{Z}/p\mathbb{Z}$ are roots. (I want to state the fact for any m, even tho on the qual you usually only use it for a prime number, because I think it's neat.)

(4) (Eisenstein's criterion) There's one more test which can only be used for polynomials in $\mathbb{Z}[x]$: suppose you write your polynomial $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, and suppose there is a prime number p such that:

- the leading coefficient a_n is not divisible by p,
- every other coefficient *is* divisible by p, and
- the constant term a_0 is not divisible by p^2.

Then f is irreducible. (In fact, this can be modified to work for any PID, and indeed any integral domain. Eisenstein discovered it while working over the ring $\mathbb{Z}[i]$.)

(5) (Rational root theorem) Writing f as above, the rational root theorem says any rational root of f must be of the form $\pm d/e$, where $d \mid a_0$ and $e \mid a_n$. Again, for degree 2 or 3 polynomials this lets you compute if f is irreducible by ruling out all the possible rational roots.

- In particular, the rational root theorem implies that any rational root of a monic polynomial is in fact an integer root.

(6) (Galois theory) Finally, tho not least, Galois theory gives us another tool for showing that a polynomial is irreducible. If we can, by hook or by crook, find the splitting field K of a given polynomial and compute the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$, we can check if the original polynomial is irreducible or not by checking whether or not G acts transitively on its roots. While this may sound far-fetched, in practice this is the most powerful item on this list.

Exercise 4. Some practice showing polynomials are irreducible using these techniques.

(a) Consider the polynomial $f(x) = x^2 - 2x - 4$. Show that $f(x)$ is irreducible over $\mathbb{Q}$ by reducing mod p for some prime p, and checking that it has no roots mod p. (If you have a number-theoretic instinct, you might wonder how to choose a good p in advance...)

(b) Consider the polynomial $x^3 + 2x^2 + 3x + 4$.

(i) Use rational root theorem to check that this polynomial has no linear factors over $\mathbb{Q}$, and is therefore irreducible.

(ii) The next two parts outline another possible argument. Reduce this polynomial mod 4. Prove that any root of this polynomial must be divisible by 4.

(iii) Reduce this polynomial mod 8, and check that $x = 4$ is not a root. Therefore, this polynomial is irreducible mod 8.

(c) Consider the polynomial $g(x) = x^4 - tx^2 - t$ over the field of rational functions $\mathbb{Q}(t)$. Show that this polynomial is irreducible by showing it is Eisenstein in the ring $\mathbb{Q}[t]$.

Fields

Definitions and basic examples

Example 2. You already are friends with the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Here are some other examples that come up:

- If K is any field, I can form the field $K(x)$, the field of all rational functions in the variable x. This is the field of fractions of the ring of polynomials $K[x]$. I could equally well form $K(x, y)$, which is the field of rational functions in the variables x, y. These fields are good to keep in mind because a lot of counterexamples come from them.

- For any prime number p, the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field. Often, when people are thinking about $\mathbb{Z}/p\mathbb{Z}$ as a field (rather than as one of the quotients $\mathbb{Z}/m\mathbb{Z}$ that just by chance happens to be a field), they will denote it as $\mathbb{F}_p$. If you have never done it before, **Exercise 5.** prove that $\mathbb{Z}/p\mathbb{Z}$ is a field (i.e. prove that you can "divide" by any nonzero element).

- A generalization of the previous example: if R is a ring, and m is a maximal ideal of R, then R/m is a field. If you have never done it before, **Exercise 6.** prove this (again, the sticking point is showing you can divide).
  - A special case of this, which is most important to us, is the case when $R = K[x]$, and $m = (f)$ for an irreducible polynomial f. If you have never done it before, **Exercise 7.** prove that this is indeed a maximal ideal.

Comment. Notationally, writing square brackets $K[x]$ means "K adjoin x (as a ring)", while writing the parentheses $K(x)$ means "K adjoin x (as a field)". That is to say, $K[x]$ has all the elements of K, the element x, and anything that is has to have by adding, subtracting, and multiplying, while $K(x)$ also has everything it must have through division as well. This notation makes sense even if x is not an indeterminate variable, but an actual number. So, for example, one can write things like $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[1/2]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\pi)$. If you have never done it before, **Exercise 8.** figure out what a general element of each of the preceding rings/fields looks like. Figure out why $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$. Figure out what I mean when I write $\mathbb{C}(x + x^{-1})$.

A **field extension** of a field K is a field L such that $L \supset K$. (Sometimes it's better to say an extension is a field L and an injective homomorphism $f\colon K \to L$.) Often, we will write a field extension by just writing L/K, read aloud as "L over K". Unfortunately, this looks a lot like the notation for a quotient group, but that is *not* what this notation means. Rather, we imagine that the extension field lies physically "above" the base field, which we depict:

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

A field extension is **algebraic** if it can be obtained by adjoining roots of polynomials to the base field. (Possibly infinitely many!)

Example 3.

- $\mathbb{C}$ is an algebraic field extension of $\mathbb{R}$. $\mathbb{R}$ is a non-algebraic field extension of both $\mathbb{Q}(\pi)$ and $\mathbb{Q}(\sqrt{2})$. $\mathbb{Q}(\pi)$ and $\mathbb{Q}(\sqrt{2})$ are both field extensions of $\mathbb{Q}$, but $\mathbb{Q}(\sqrt{2})$ is algebraic over $\mathbb{Q}$ while $\mathbb{Q}(\pi)$ is not.
- Given any field K, and any irreducible polynomial f, we can use our favorite construction to get an algebraic field extension of K that contains a root of f: $K[x]/(f)$. In the field $K[x]/(f)$, the equivalence class of x is a root of f, because we have modded out by f exactly with the goal of making $f(x) = 0$ in the quotient.
  - $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$
  - $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$.
  - Over $\mathbb{F}_3$, the polynomial $x^2 + 1$ is irreducible. So, I can form a field $\mathbb{F}_3[x]/(x^2 + 1)$, which it seems reasonable to call $\mathbb{F}_3(i)$. **Exercise 9.** List all the elements of this field.

- Over $\mathbb{F}_5$, the polynomial $x^2 - 2$ is irreducible. So, I can form a field $\mathbb{F}_5[x]/(x^2-2)$, which it seems reasonable to call $\mathbb{F}_5(\sqrt{2})$. **Exercise 10.** How many elements does it have?

Given a field extension L/K, observe that L is a K-vector space. This modest observation is central to everything else.

Given a field extension L/K, we define the **degree** of the extension, written $[L : K]$, to be the dimension of L as a K-vector space. An extension is called "finite" if $[L : K]$ is finite, otherwise an extension is called "infinite". **Exercise 11.** find a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $\mathbb{Q}(\pi)$ as extensions of $\mathbb{Q}$. Do the numbers you find line up with your intuition?

Proposition (multiplicativity of degrees)**.** Suppose L is an extension of K, and M is an extension of L. Then $[M : K] = [M : L][L : K]$. In diagram form:

$$\begin{tikzcd}
M \arrow[d, dash, "d_2"'] \arrow[dd, dash, bend left, "d_1 d_2"] \\
L \arrow[d, dash, "d_1"'] \\
K
\end{tikzcd}$$

Here are several facts about some really fundamental examples.

Cyclotomic extensions:

The complex numbers $\zeta_n^k = e^{2k\pi i/n}$ for $0 \le k < n$ are the n distinct roots of the polynomial $x^n - 1$. They are called "nth roots of unity" because they satisfy $x^n = 1$. If k and n share a common factor, then $\zeta_n^k = \zeta_d^\ell$, where $\ell = k/\gcd(n,k)$ and $d = n/\gcd(n,k)$, so the nth roots of unity include all the dth roots of unity for every d dividing n. The numbers ζ_n^k where k is coprime to n are the nth roots of unity that are not dth roots of unity for any smaller d, they are called the "primitive nth roots of unity". There are $\varphi(n)$ of them, where $\varphi(n)$ is Euler's φ function, which counts the number of positive integers up to n which are coprime to n.

If you are not already familiar with the function $\varphi(n)$, here are a few of its properties (which you may prove if you desire):

- $\varphi(p) = p - 1$ and $\varphi(p^k) = p^{k-1}(p-1)$ for any prime number p.
- $\varphi(n)$ is equal to the number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$, the group of units mod n.
- $\varphi(ab) = \varphi(a)\varphi(b)$ for any coprime integers a, b. (This follows from the previous bullet along with the Chinese Remainder Theorem.)

We define the **cyclotomic polynomial** $\Phi_n(x)$ as follows:

- $\Phi_1(x) = x - 1$,
- for $n > 1$, $\displaystyle\prod_{d|n} \Phi_d(x) = x^n - 1$,

where the notation means the product is taken over all positive integers d which divide n. The polynomial $\Phi_n(x)$ is monic, has coefficients in $\mathbb{Z}$, is irreducible over $\mathbb{Z}$, and its roots in $\mathbb{C}$ are exactly the primitive nth roots of unity. (The term "cyclotomic" means "circle cutting", and Gauss chose it because the nth roots of unity evenly divide the unit circle in the complex plane.)

Exercise 12. Compute $\Phi_n(x)$ for $n = 2, \ldots, 20$. Yes, I'm serious.

Exercise 13. Prove that $\Phi_p(x+1)$ is p-Eisenstein.

We can see that $\Phi_n(x)$ splits in the field $\mathbb{Q}(\zeta_n)$, since indeed $x^n - 1$ splits and Φ_n is a divisor. Later, we will see that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension with Galois group of order $\varphi(n)$, which implies that Φ_n is irreducible over $\mathbb{Q}$ for general n. As far as I know, this is the best way to prove that Φ_n is irreducible. In Exercise 13, you proved that $\Phi_p(x)$ is irreducible by showing it is Eisenstein, and one can check the irreducibility of Φ_n directly (as Gauss did, and as Dummit and Foote do more briefly), but doing so is much more difficult than computing the Galois group of its splitting field.

Extensions of finite fields

Exercise 14. (Frobenius) Suppose K is a field of characteristic p. Show that the map $x \mapsto x^p$ is an injective field homomorphism $K \to K$. This map is known as the **Frobenius map**.

Exercise 15. Consider the finite field $\mathbb{F}_p$, and the polynomial $x^{p^n} - x$. As we will see later, this polynomial is separable, and so has distinct roots in its splitting field.

(a) Use 14 to show that the p^n roots of this polynomial form a field.

(b) Show that an extension of $\mathbb{F}_p$ has p^n elements if and only if it is a degree n extension.

(c) Let $L/\mathbb{F}_p$ be any extension of $\mathbb{F}_p$ of degree n. Show that every $\alpha \in L$ satisfies $\alpha^{p^n} = \alpha$, and hence that up to isomorphism there is a unique extension of $\mathbb{F}_p$ of degree n. This unique extension is denoted $\mathbb{F}_{p^n}$, or often people will write $\mathbb{F}_q$ and it is understood that $q = p^n$ for some p, n.

Exercise 16. (January 2023 Problem 4) Consider the finite field $\mathbb{F}_p$ where p is a prime number.

(a) How many monic irreducible polynomials of degree 5 are there over $\mathbb{F}_p$? (Your answer should be a function of p.)

(b) Let $P(x), Q(x) \in \mathbb{F}_p[x]$ be irreducible polynomials. Give a necessary and sufficient condition for there to exist a third polynomial $R(x) \in \mathbb{F}_p[x]$ such that $Q(x)$ divides $P(R(x))$. (The polynomial $R(x)$ need not be irreducible.)

As a note, the multiplicative group of $\mathbb{F}_{p^n}$ is in fact *cyclic*, so there exists some element α which has exact order $p^n - 1$.

Minimal polynomial and degree of an element

Several of our examples indicate that individual *elements* of field extensions also have a notion of "degree" attached to them: if α is a root of an irreducible polynomial f of degree d, then α ought to be called "algebraic of degree d". We might be a little cautious, though, because it's not exactly clear how the degree of an individual element will relate to the degree of the field, because if I make a field extension like $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, I not only get $\sqrt{2}$ and $\sqrt{3}$, but also $\sqrt{2}+\sqrt{3}$, $5/(\sqrt{6}-\sqrt{2})$, and a bunch of other stuff. One might guess that these elements are in fact algebraic numbers, and that their degrees are less than or equal to the degree of the given field extension, but it seems far from straightforward to prove that.

Here's where the linear algebra will help us! Suppose that $\alpha \in L$, then there is a map from $L \to L$ given by $x \mapsto \alpha x$, the "multiply by α" map. This map is *not* a ring homomorphism, but it is K-linear. If, moreover, $[L : K]$ is finite, then I can choose a finite K-basis for L and write the multiplication by α map as a matrix M_α. That matrix will have a minimal polynomial, which is actually independent of the particular basis chosen, and that minimal polynomial will have α as a root. (Note that since the matrix M_α has entries in K, its minimal polynomial will have coefficients in K. In particular, the minimal polynomial of α probably won't be just $x-\alpha$ unless $\alpha \in K$.)

Proposition. Let L/K be a finite extension, let $\alpha \in L$, and let $f(x)$ be the minimal polynomial of the matrix M_α. Then:

(1) $f(x)$ is irreducible over K, and

(2) $f(\alpha) = 0$.

The polynomial $f(x)$ is called the "minimal polynomial of α". (Another way to phrase this is: every element of a finite-degree field extension is algebraic.)

If α is algebraic of degree d over K, then $[K(\alpha) : K] = d$.

Exercise 17. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is degree 4 over $\mathbb{Q}$, and we can take a $\mathbb{Q}$-basis to be $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

(a) In this basis, write down the matrix associated to multiplication by $\sqrt{2}+\sqrt{3}$.

(b) Use that matrix to find the minimal polynomial of $\sqrt{2}+\sqrt{3}$.

Algebraic closure

A field K is **algebraically closed** if every polynomial with coefficients in K has a root in K. The **algebraic closure** of a field K, denoted $\overline{K}$, is an extension of K with the following two properties:

(1) $\overline{K}$ is algebraically closed, and

(2) no subfield of $\overline{K}$ containing K is algebraically closed.

Proposition. Every field is contained in an algebraically closed field. By Zorn's Lemma, this in particular implies every field has an algebraic closure.

Composite and intersection of two fields

Fix an algebraic closure $\overline{K}/K$, and let L_1, L_2 be extensions of K contained in $\overline{K}$. Then we can form other fields out of the extensions L_1, L_2:

- The intersection $L_1 \cap L_2$ is a field extension of K.
- The composite (or compositum) L_1L_2 is defined to be the smallest extension of K that contains both L_1 and L_2 as subextensions. More concretely, for every pair of elements $\ell_1 \in L_1, \ell_2 \in L_2$, the product $\ell_1\ell_2$ must lie in L_1L_2 (hence the notation). But, then you also have to throw in all the finite sums of those products, and all the inverses of those sums, to make sure what you end up with is still a field.

Example 4.

- Let $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{3})$. Then $K_1 \cap K_2 = \mathbb{Q}$, $K_1K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- Let $K_1 = \mathbb{Q}(\zeta_8)$, $K_2 = \mathbb{Q}(\sqrt{\sqrt{2}+1})$.

  Exercise 18. Prove that $K_1 \cap K_2 = \mathbb{Q}(\sqrt{2})$, $K_1K_2 = \mathbb{Q}(\zeta_{16})$. (It might be helpful to know that $\zeta_8 = \sqrt{i} = (1+i)/\sqrt{2}$.)

Separable polynomials and extensions

A polynomial $f \in K[x]$ is called **separable** if it has distinct roots in its splitting field, and an extension is called separable if it can be obtained by adjoining roots of separable polynomials. A trivial example of an inseparable polynomial is something like $(x-2)^2$ over $\mathbb{Q}$. In characteristic 0, every irreducible polynomial turns out to be separable, but this need not be the case in characteristic p. For example, in the field $\mathbb{F}_p(t)$, the polynomial $x^p - t$ is irreducible (by Eisenstein), but as soon as we adjoin a root, it will split as $(x - \sqrt[p]{t})^p$.

There is a criterion for determining if a polynomial is separable.

Exercise 19. Let $f \in K[x]$ be a polynomial, and let f' be its **formal derivative**. That is, f' is obtained from f by just applying the power rule to each of the terms in f. Prove that f is separable over K if and only if $\gcd(f, f') = 1$.

In particular, this shows that $x^{p^n} - x$ is a separable polynomial over $\mathbb{F}_p$, as mentioned previously.

A field where every finite extension is separable is called a **perfect field**, and we've already seen that all finite fields and fields of characteristic 0 are perfect. On the other hand, the above example shows that $\mathbb{F}_p(t)$ is not a perfect field, and inseparable extensions can arise when taking an irreducible polynomials of degree a power of p. (In fact, every inseparable irreducible polynomial is of the form $f(x^{p^k})$ for some irreducible polynomial f.)

Exercise 20. (August 2022 Problem 4) Let p be a prime number, $\mathbb{F}_p$ the finite field with p elements, and $K = \mathbb{F}_p(t)$ the field of rational functions in one variable t over $\mathbb{F}_p$. (So that K is the fraction field of the polynomial ring $\mathbb{F}_p[t]$).

(a) Show that the splitting field of the polynomial $x^p - t \in K[x]$ over K is inseparable.

(b) Show that the splitting field of $x^p - t - 1 \in K[x]$ over K is the same as the splitting field of $x^p - t$.

(c) Show that K has a single degree p inseparable extension.

The primitive element theorem

Several of our examples have been of the form $K(\alpha)$ for some algebraic number α. However, we've also had examples like $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, where we adjoin two different algebraic numbers. A field where we've only adjoined one thing (called a **simple extension**) is sometimes easier to think about, so a reasonable question is: can every field extension be written as $K(\alpha)$ for some α? In this case, the element α is called a **primitive element** for the extension. Above, we computed that $\sqrt{2} + \sqrt{3}$ is a degree 4 element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so it must be a primitive element for that extension.

The following proposition gives a partial answer to when we can find a primitive element, and the answer is basically "in most of the cases where it matters".

Proposition (Primitive element theorem)**.** Let L/K be a finite extension of characteristic 0. Then there is an algebraic $\alpha \in L$ so that $L = K(\alpha)$. In particular, every finite extension of $\mathbb{Q}$ can be written as $\mathbb{Q}(\alpha)$ for some algebraic number.

There is a more precise, but also more abstract, form of the primitive element theorem, which allows us to obtain exact conditions under which a field extension is simple.

Proposition (Primitive element theorem, again)**.** If L/K is a separable extension (possibly of characteristic p), then we can find $\alpha \in L$ so that $L = K(\alpha)$. In maximum generality: there exists a primitive element $\alpha \in L$ if and only if there are only finitely many intermediate fields between L and K.

Exercise 21. Find an example of a field extension that does not have a primitive element.

Galois Theory

Splitting fields and normal extensions

We've talked about forming field extensions by adding on a root of a polynomial. However, you may have noticed, this does not always make the polynomial factor completely into linear terms! For example, in $\mathbb{Q}(\sqrt[3]{2})$, the polynomial $x^3 - 2$ factors into a linear term and an irreducible quadratic. (How do I know?) In order to use Galois theory to understand a polynomial, we need to have all of its roots living in the field.

We define the **splitting field** of a polynomial f (not necessarily irreducible) to be the smallest extension of K that contains all the roots of f. We might get the splitting field after adjoining only one root of f, or we might need to adjoin each root, one after the other.

Exercise 22. Suppose f is irreducible of degree n, and that L/K is the splitting field of f. Prove that $n \leq [L : K] \leq n!$. What do you think the most likely value of $[L : K]$ is for a "random" polynomial f? (This latter question is somewhat ill-defined, interpret it in a way that seems reasonable to you.)

A related notion is the notion of a normal extension. A **normal extension** is an extension L/K such that every polynomial which has *any one* root in L, actually has *all* of its roots in L. This is stronger than saying that L is the splitting field of some f: this is saying that L contains the splitting field for every f that has even a single root contained in L. That seems like it's infinitely more powerful than just being the splitting field of a single f.

... Well, it seems that way, but actually, the two things are exactly equivalent.

Proposition. A finite extension L/K is normal if and only if L is the splitting field of some polynomial over K.

Automorphism group of an extension

Okay, and we said we are going to study polynomials using group theory, so at some point we better introduce some groups. Given an extension L/K, we define the **automorphism group of the extension** $\mathrm{Aut}(L/K)$ to be the group of all self-isomorphisms $\sigma\colon L \to L$ that fix K pointwise; that is, such that for every $x \in K$, $\sigma(x) = x$.

Importantly, such an automorphism is moreover a K-linear map! That means once we choose a basis for L as a K-vector space, we can uniquely specify such an automorphism by just specifying what it does to each basis vector. Often, we choose to have $1 \in L$ be one of our basis vectors, so then an automorphism fixing K is the same thing as an automorphism that sends $1 \mapsto 1$.

We must keep in mind, not every linear map defines an automorphism, it must also respect the multiplication of the field L. In particular, **Exercise 23.** for every $\sigma \in \mathrm{Aut}(L/K)$, if $\alpha \in L$ is a root of an irreducible polynomial f, then $\sigma(\alpha)$ must also be a root of f.

Example 5.

Consider the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. We can write a basis for this as $\{1, \sqrt{2}\}$, as promised in the preceding paragraphs. Then any automorphism of this extension must fix 1, and must send $\sqrt{2}$ to $\pm\sqrt{2}$, so there are exactly 2 such automorphisms. Thus, the automorphism group is a group of order 2.

Consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. We can write a basis for this as $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. However, to specify an automorphism, it's enough to specify what happens to $\sqrt[3]{2}$, because then the action on $\sqrt[3]{4}$ will be determined by multiplication. By the above, any automorphism must send $\sqrt[3]{2}$ to another root of $x^3 - 2$, but there is only one such root inside the field, so the only possible automorphism is the identity automorphism.

Consider the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$. Think about it long enough to decide that it has automorphism group S_3 (or D_3 if you are a fan of dihedral groups).

It is always the case that $|\mathrm{Aut}(L/K)| \leq [L:K]$. Equality is achieved if and only if L is the splitting field of a separable polynomial. (!!!) In such a case, we call $\mathrm{Aut}(L/K)$ the Galois group, and write it as $\mathrm{Gal}(L/K)$.

The Fundamental Theorem of Galois Theory

Now, we come to the big theorem. It basically says: all the data contained in a field is reflected in its Galois group.

Proposition (Fundamental Theorem of Galois Theory)**.** Suppose L/K is a Galois extension with Galois group G. There is a correspondence between the subgroups H of G and the intermediate fields $L \supset F \supset K$, given by taking the subfield of L fixed by H, denoted L^H. This correspondence has the following properties:

(a) It is a bijection, so every intermediate field F is the fixed field of some H. We would prove this by proving first that ...

(b) L is always Galois over any intermediate field F, and $\mathrm{Gal}(L/F)$ is a subgroup of G.

(c) The bijection is order-reversing: if $L \supset F_1 \supset F_2 \supset K$, the correspondence sends this to the chain $\{1\} \subset H_1 \subset H_2 \subset G$.

(d) The degree $[L:F]$ is equal to the size of the corresponding H.

(e) An intermediate field is Galois over K if and only if the corresponding subgroup H is normal in G. This is why they are called "normal extensions", they correspond to normal subgroups. In this case, $\mathrm{Gal}(F/K) = G/H$.

(f) If F_1, F_2 are intermediate extensions corresponding to the subgroups H_1, H_2, then the composite F_1F_2 corresponds to $H_1 \cap H_2$, and the intersection $F_1 \cap F_2$ corresponds to the subgroup generated by H_1 and H_2.

Exercise 24.

(a) Let $K = \mathbb{Q}(\zeta_n)$. What is $[K:\mathbb{Q}]$?

(b) Show that K is a Galois extension of $\mathbb{Q}$ by explicitly finding $[K:\mathbb{Q}]$-many automorphisms.

Exercise 25. Consider $\mathbb{F}_{p^n}/\mathbb{F}_p$. Let F be the Frobenius map. Prove that the powers of Frobenius give n distinct automorphisms of $\mathbb{F}_{p^n}$ fixing $\mathbb{F}_p$, and therefore that the Galois group is cyclic of order n.

Exercise 26.

(a) Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$, and find its Galois group.

(b) Show that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is Galois over $\mathbb{Q}$, and find its Galois group.

Exercise 27. (August 2016 Problem 5, modified) Consider the field $K = \mathbb{Q}(\zeta_7)$. According to your computation above, $\mathrm{Gal}(K/\mathbb{Q})$ is abelian and has even order, so has a normal subgroup of index 2. By the Fundamental Theorem of Galois Theory, this subgroup corresponds to a field $\mathbb{Q}(x) \subset K$ such that $[\mathbb{Q}(x) : \mathbb{Q}] = 2$, where x is some element of K. Compute an element x in terms of ζ_7 which generates this quadratic subfield.

Exercise 28. (Stolen from another school's algebra qual) Let $f \in \mathbb{Q}[x]$ be a degree 5 irreducible polynomial, let $K/\mathbb{Q}$ be its splitting field, and let $\alpha, \beta, \gamma, \delta, \epsilon \in K$ be the roots of f. Suppose that $\mathrm{Gal}(K/\mathbb{Q}) = S_5$, the symmetric group on 5 elements.

(a) Find the Galois group of $K/\mathbb{Q}(\alpha, \beta)$.

(b) Find the Galois group of $K/\mathbb{Q}(\alpha + \beta, \alpha\beta)$.

(c) The field $\mathbb{Q}(\alpha, \beta)$ contains the field $\mathbb{Q}(\alpha + \beta, \alpha\beta)$. Find the degree $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha + \beta, \alpha\beta)]$.

Exercise 29. (August 2017 Problem 4) Suppose that $K \subseteq \mathbb{C}$ is a Galois extension of $\mathbb{Q}$, $[K : \mathbb{Q}] = 4$, and $\sqrt{-m} \in K$ for some positive integer m. Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.