Shahriari August 2018

# Galois Theory Guide & Assignments

Based on

Shahriari Shahriari, *Algebra in Action. A course in Groups, Rings, and Fields*, AMS, 2017.

What follows is a detailed self-study guide for Galois Theory using *Algebra in Action*. Instructors teaching a traditional class in Galois Theory can modify the assignments and use the outlines to plan their lectures. This course assumes a knowledge of groups and rings as presented in the first two parts of *Algebra in Action*. A detailed syllabus for such a course is available on the publisher's webpage for the text (`https://www.ams.org/bookpages/amstext-27`). While it is assumed that the student has familiarity with groups and rings, the relevant ring theory is reviewed (rather rapidly) at the beginning of this course. In fact, a quarter of the course is devoted to (re)learning the relevant ring theory. Among the assigned problems, the ones in italics have a complete solution in Appendix C of the text. To facilitate self-study many of these have been assigned. To modify this guide for use in a traditional class, the instructor may choose to replace some (or all) of these problems. Each assignment asks you to read one or two sections of the book and to do six problems. An outline describes the main point of the reading. The problems are meant to be challenging, and so do not be discouraged if you can't do them right away. Often you will have to read the assigned reading several times and work out examples before any success with the problems.

**Assignment 1.** Read Chapter 21. Review Chapter 15 (Sections 2-3). Do Problems *15.2.7*, 15.2.12, 15.2.16, 15.2.21, 15.2.24, 21.3.1

**Outline**.
Chapter 21 is an introductory chapter and gives an overview of what is to come. Section 21.1 gives an overview of the kind of problems that field theory will allow us to address. Section 21.2 gives an example to show how finding the roots of a polynomial may be related to groups. Section 21.3 gives two problems in order for you to begin reviewing Ring Theory. The first two sections are not meant to be fully understood at this point. They will give you an overview and things to think about. The third section is important because we will be using ring theory extensively. Some of the ring theory needed—mainly stuff from Chapter 19—we haven't done yet and we will do in detail in future assignments. However, do go through the outline solutions to Problems 21.10 and 21.12 and try to expand on them and to make sure that you understand the logic and put in as much of the the details as you can.

From Chapter 15, review the definitions (and examples) of Rings, Zero Divisors, Integral Domains, and Fields. Remind yourself of examples of rings on page 320 (especially polynomial rings), and of cancellation laws in integral domains (Propositions 15.23).

**Assignment 2.** Review Chapter 16 (Sections 1-3), Chapter 17 (Section 1), and Section 18.1 Do Problems 16.1.5, 16.1.8, *16.2.4*, *16.2.7*, 17.1.7, 18.1.25

**Outline**.
Review Subrings, ring homomorphisms, kernels, ideals, principal ideals, maximal ideals, quotient rings, homomorphism theorems, and characteristic of rings. Pay attention to Example 16.5, Lemma 16.6, Def 16.7, Lemma 16.23, Proposition 16.32. Don't worry about Zorn's Lemma on page 334. Be comfortable with cosets, and Theorems 16.43 and 16.45. Pay attention to Definition 16.54 and Corollary 16.55. You should know Theorem 17.1, that every integral domain can be embedded in a field (its field of fractions). Read examples 17.5 and 17.6 as well as Remark 17.7. Review all the definitions needed for Theorem 18.12.

**Assignment 3.** Review Chapter 18 (Sections 1–4) Do Problems *18.1.15*, 18.1.19, 18.1.30, 18.3.7, 18.4.8, 21.3.4

**Outline**.
You should know Section 18.1 really well. Pay attention to all the definitions, examples, and the theorems. You should also know what noetherian, UFD, PID, and ED mean but the details of the proofs are less important. Do pay attention to the examples in the book as well as Theorems 18.40, and 18.50 and their proofs. If you remember anything from Ring Theory, it should be the statement of Corollary 18.51. Also, take a look at Figure 18.2.

**Assignment 4.** Read Sections 19.1 and 19.2 Do Problems 19.1.3, 19.1.4, 19.1.5, 19.2.2, 19.2.4, *19.2.9*

**Outline**.
Polynomials play an important role in Galois Theory and in Chapter 19 we explore rings of polynomials. We especially want to know how to decide if a polynomial is irreducible. For this assignment go over sections 19.1 and 19.2. The first section is almost all definitions. Go through these carefully. Make sure that you understand the definition of $R[\alpha]$. This notation (as in $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Q}[\sqrt[3]{5}]$, or $\mathbb{R}[i]$) will be used repeatedly. To define $R[\alpha]$ we need a ring $R$ and an element $\alpha$. But where does $\alpha$ come from? So that we can add, subtract, and multiply $\alpha$ with elements of $R$, the element $\alpha$ as well as the ring $R$ have to be part of a bigger ring $S$. We want this bigger ring $S$ to have the same identity as $R$ and such a ring (a ring that contains $R$ and has the same identity as $R$) is called a *unitary overring of* $R$ (sounds fancier than it actually is). The second section proves one thing. If $F$ is a field then $F[x]$ is an ED. This is an important result that we use all the time. It is important that $F$ be a field since otherwise the division algorithm doesn't always work. But not all is lost. The section tells you when you can divide $f$ by $g$ and get an appropriate quotient and remainder even if $F$ is just an integral domain. One of the homework problems asks about greatest common divisors. Read as much of section 18.5 as necessary (no particular reason to dwell over the proofs of that section). Here are some things you need to know about greatest common divisors. In a general commutative ring, greatest common divisors may or may not exist. If a gcd exists, it doesn't have to be unique. In an integral domain, the associates of a gcd are also a gcd. In a UFD, every pair of non-zero elements has a gcd (Theorem 18.62). In a PID, the gcd of a pair of non-zero elements can be written as a linear combination of the two elements (Theorem 18.63). Finally, in an ED, you can find the gcd of a pair of non-zero elements using the Euclidean algorithm (Theorem 18.69).

**Assignment 5.** Read Section 19.3 Do Problems 19.2.10, *19.3.3*, (19.3.6, 19.3.7), *19.3.13*, *19.3.15*, 19.3.19

**Outline**.

In this section, we discuss the relation between roots of a polynomial and factoring. This is something that you know from Algebra in high school but here the setting is not just the real numbers but any integral domain. We also discuss the units and irreducible elements of $R[x]$. We then start with a field $F$, and consider $F[x]$, the ring of polynomials in $x$ with coefficients from $F$. We find an irreducible polynomial in $F[x]$, mod out by the ideal generated by that polynomial, and get a field. This new field will contain a copy of the old field $F$ but is big enough that our irreducible polynomial now has a root in this new field. You want to understand basically everything in this section.

**Assignment 6.** Read Section 19.4 Do Problems *19.2.11*, 19.3.9, 19.3.18, 19.3.24, *19.4.5*, 19.4.14

**Outline**.

Section 19.4 is somewhat long (the next section is short by contrast). It has several aims. For most of the section $R$ is a UFD and $F$ is its field of fractions. An example of this is $\mathbb{Z}$ and $\mathbb{Q}$, and, for many (but not all) applications you can limit yourself to this special case. Given a polynomial in $p(x) \in R[x]$, we can think of $p(x)$ as a polynomial in $F[x]$. This is advantageous since $F[x]$ is an ED. The question is whether information about $p(x) \in F[x]$ translates to information about $p(x) \in R[x]$. In this section, two results in this direction stand out. Corollary 19.35 says that if $f(x) \in \mathbb{Z}[x]$ is monic and if it has a rational root then it must have an integer root. Corollary 19.53 says that if $f \in \mathbb{Z}[x]$ is not a constant and if you can factor it in $\mathbb{Q}[x]$, then you can already factor it in $\mathbb{Z}[x]$. To get these results for a general UFD and its field of fractions (as opposed to $\mathbb{Z}$ and $\mathbb{Q}$) a bit of technical language (e.g., content and primitive polynomials) has to be introduced. It looks harder than it really is. Make sure that you work through the examples and especially the remarks. The "Rational Roots Theorem" at the beginning of the section is very useful, but the key result in the section is Gauss's Lemma (Theorem 19.51). Make sure that you understand what it says exactly. Before starting this section, do read the outline for Assignment 4 above where it explains what you need to know about greatest common divisors.

**Assignment 7.** Read Section 19.5 Do Problems 19.4.15, *19.4.17*, 19.5.1, *19.5.3*, 19.5.4, 21.3.2

**Outline**.

You thought you were done with factoring polynomials in high school algebra. We have seen that knowing when a polynomial is irreducible is important in constructing fields and also in figuring out if ideals are maximal or not. In future chapters, we shall see a remarkable symmetry between the different roots of an irreducible polynomial, and this will be crucial in Galois Theory. For now, we have to learn more tools for deciding whether a polynomial is irreducible or not. This is not an easy task and we can't always do it successfully. This section gives us two crucial tools for recognizing irreducible polynomials. In Theorem 19.58 we let $n \in \mathbb{Z}$ be a positive integer, and $p(x)$ a polynomial in $\mathbb{Z}[x]$ of degree $d$. We assume that $n$ does not divide the coefficient of $x^d$, and we reduce every coefficient of the polynomial mod $n$. If the resulting polynomial is irreducible in $\mathbb{Z}/n\mathbb{Z}[x]$, then the original polynomial is irreducible in $\mathbb{Z}[x]$. The crux of the section is Corollary 19.64. On the face of it, it gives some weird conditions on a polynomial, and if all of these conditions are satisfied, then the given polynomial is irreducible in $\mathbb{Z}[x]$. This criterion is called the Schönemann-Eisenstein criterion (actually it is just called Eisenstein's criterion almost universally) and, you will be surprised how much we use it in the sequel.

**Assignment 8.** Read Section 22.1 Do Problems 19.4.7, 19.5.5, 19.5.10, 22.1.4, 22.1.7, 22.1.11
**Outline**.
The idea of a *field extension* is crucial in what is to follow. This is a straightforward idea. If $F \subseteq E$ and both $F$ and $E$ are fields, then $E$ is a field extension of $F$. A field extension is just a bigger field that contains our original field. $\mathbb{R}$ is a field extension of $\mathbb{Q}$ and $\mathbb{C}$ is a field extension of $\mathbb{R}$. Section 22.1 is mostly definitions, remarks, and examples but these are important. Read this section carefully. It tells you the difference between $F[x]$ and $F(x)$—the latter is a field while the former is just a ring—and defines the concepts of simple and algebraic extension. If $F \subseteq E$ is a field extension, and if $\alpha \in E$, then $\alpha$ is algebraic over $F$ if $\alpha$ is the root of a polynomial in $F[x]$. We prove (Theorem 22.16) that if $\alpha$ is algebraic over $F$, then there is something called its *minimal polynomial*, a unique monic irreducible polynomial in $F[x]$ that has $\alpha$ as a root.

**Assignment 9.** Review Linear Algebra and Read Section 22.2 Do Problems 22.1.2, *22.1.9*, *22.1.13*, *22.1.17*, 22.1.18, 22.2.3
**Outline**.
Section 22.2 is a quick and short review of linear algebra. (I am stalling on the readings a bit to give us a chance to do more problems from Section 22.1.) You may not have seen linear algebra over general fields (this means that the scalars are not real numbers but possibly are elements of some other field) but all you know in linear algebra continues to work in this more general context. You need to know what a vector space is and what we mean by a basis for this vector space. What is a vector space? You first have to have a field of scalars (in elementary linear algebra this is usually $\mathbb{R}$, the field of real numbers, but the scalars don't have to be the real numbers, they could be the elements of any field). A vector space is then a set of elements together with two operations: addition and multiplication with scalars. These operations have to follow certain very reasonable rules. The elements of a vector space are called a vectors. So in a vector space, you have to be able to add two vectors and get a vector and you have to be able to multiply a vector by a scalar and get another vector. The rules for these operations are spelled out in Section 22.2. If $V$ is the set of the vectors and $F$ is the field of scalars, then we say *$V$ is a vector space over $F$*. Why do we care about vector spaces? One important byproduct of having a vector space is that vector spaces have bases. A basis is a set of linearly independent vectors that span the vector space. Why am I talking about vector spaces in the middle of a course on fields? The next section will make this abundantly clear.

**Assignment 10.** Read Section 22.3 Do Problems 22.3.2, *22.3.3*, 22.3.9, *22.3.15*, 22.3.17, 22.3.21
**Outline**.
A very crucial observation is that if $R$ is a commutative ring with identity and if $F$ is a field contained in $R$, then $R$ is a *vector space* over $F$. In other words, we can use the elements of $F$ as scalars and turn $R$ into a vector space. This is not hard to see (after all, we know that we can add elements of $R$ to each other and we can multiply an element of $F$ with an element of $R$—in fact, we can multiply any two elements of $R$—and they follow the silly rules of a vector space. But this ends up being an incredibly useful observation as this section shows. In this section we prove lots of things using this

fact (often are in the special case of when $F \subseteq K$ are both fields and we use the fact that $K$ is a vector space over $F$). Among other things, we prove that the number of elements of any finite field must be a power of a prime (i.e., no fields with 6 or 10 elements). We also prove a number of very useful equivalent conditions for $\alpha \in E$ to be algebraic over $F$ (Theorem 22.35). We also introduce partial lattice diagrams of fields (Yay!) and discuss the field of algebraic numbers. When $F \subseteq E$ are two fields, we say that $E$ is a field extension of $F$. In this section, the key is that $E$ is also a vector space over $F$. The *degree* of this field extension is the dimension of the vector space $E$ (over $F$) and denoted by $|E\colon F|$. These are the numbers that will appear as edge lengths in lattice diagrams. This section is giving us some powerful tools. Be careful and don't forget about hints and short answers!

**Assignment 11.** Read Chapter 23 Do Problems 22.3.18, 22.3.29, *22.3.31*, 22.3.36, 23.1.2, 23.2.7
**Outline**.
While we continue to work on problems from section 22.3, we are taking a fun little detour in Chapter 23. In this short chapter, we answer the ancient geometry problems. Can you double a cube? Can you trisect an angle? Can you square a circle? The answer, of course, depends on the tools that you are wiling to use, but, in the tradition of geometry developed in Greece and Alexandria, we want to use only a compass and a straightedge. In this chapter, we do a bit of geometry and then turn all of these construction problems to a question about field extensions. Just what we learned in section 22.3 that a field extension can also be viewed as a vector space will be sufficient to answer these questions that had vexed humanity for about 2000 years! If you skip this chapter, you will not lose much in terms of learning Galois theory but this is a fun application of the abstract theory of fields.

**Assignment 12.** Read Section 24.1 Do Problems *22.3.37*, 22.3.38, 23.1.3, 24.1.7, 24.1.11, 24.1.13
**Outline**.
In Chapter 19, we studies roots of polynomials as well as irreducible polynomials. In Chapter 22, we studied field extensions. We will now start bringing these two together. First we show that if you have any polynomial with coefficients in a field $F$, then you can find an extension of that field so that your polynomial will have a root in it. (We have seen this in practice often, but here we will prove that it can always be done). If your polynomial is monic and irreducible, then you can do better. You can find a simple extension $F(\alpha)$ of $F$ such that not only $\alpha$ is root of $f$ but $f$ is the minimal polynomial of $\alpha$. After this, we embark on a journey to convince you that different roots of an irreducible polynomial are indistinguishable. To discuss this properly—but this turns out to be really important way of looking at things—we turn to $F$-isomorphisms. Theorem 24.6 is important and shows that we can always translate any statement about one root of an irreducible polynomial to a statement about any other root. But the key new concept in this section is $F$-isomorphisms and methods for constructing them. Theorem 24.6, Proposition 24.13, and Theorem 24.14 all do this. They each have slightly different purposes but we will be using Theorem 24.14 (which is a generalization of 24.6) often.

**Assignment 13.** Read Section 24.2 Do Problems *23.2.9*, *24.1.15*, 24.1.16, *24.2.3*, 24.2.4, *24.2.7*
**Outline**.
In Section 24.1, starting with a field and a polynomial over that field, we constructed a field extension (a bigger field containing a copy of the original field) in such a way that the polynomial now had a

root in the new field. In this section we take that idea further. Rather than getting just one root, we want to construct a field in which our polynomial has *all* of its roots. The smallest such field is called the *splitting field* of the polynomial. In this section we prove that splitting fields always exist (Theorem 24.18) and that they are unique (Corollary 24.22). Examples 24.19 and 24.23 should be studied carefully since identifying splitting fields is not necessarily that easy. If $F \subseteq E$ are fields, then sometimes $E$ is a splitting field of some polynomial in $F[x]$ and sometimes it is not. The fields $E$ that are splitting fields of polynomials end up being very special. This will be explored in future sections, but Theorem 24.24 of this section is a start. It shows that if $E$ is a splitting field over $F$, and if $\phi\colon F \to F$ is an isomorphism, then $\phi$ can be extended to an $F$-automorphism of $E$. (Actually the theorem says something even stronger.) At this first reading, you should skip the material on Algebraic Closure pp. 503–507.

**Assignment 14.** Read Section 24.3 Do Problems 24.1.17, *24.1.19*, 24.2.10, 24.3.2, 24.3.5, 24.3.7
**Outline**.
In this section we begin applying group theory and group actions to the study of field extensions. If $F \subseteq E$ is a field extension, then the Galois group of this extension, denoted $\mathrm{Gal}(E/F)$ is the group of $F$-automorphisms of $E$. In other words, the elements of this group are functions from $E$ to $E$ that are field isomorphisms and that fix every element of $F$. The operation of this group is function composition. $\mathrm{Gal}(E/F)$ will be central in our understanding of fields. This group acts on the set of roots of any polynomial in $F[x]$, and we will coming back to this action time and again. Hence, this is a good time to review group actions. (When a group acts on a set, we have orbits, and stabilizers. The orbits partition the set and the stabilizers are subgroups of the group. The size of an orbit is the same as the index of the stabilizer, and if the set is size $n$, then we automatically get a homomorphism from our group into $S_n$. The kernel of this homomorphism is the kernel of the action and is a normal subgroup of the group. The group mod the kernel is isomorphic to a subgroup of $S_n$.) In this section some examples of finding Galois groups is given and a few important theorems are proved. Theorem 24.37: If $E$ is the splitting field of some polynomial over $F$ (continuing the point from last assignment that splitting fields are special) and if $f \in F[x]$ is irreducible, then the action of $\mathrm{Gal}(E/F)$ on the roots of $f$ is transitive (has exactly one orbit). Theorem 24.43: If $|E\colon F| < \infty$ then $\mathrm{Gal}(E/F)$ is a finite group. How do we find elements of $\mathrm{Gal}(E/F)$? We often start with the identity map $F \to F$ and then extend it up to $E$—sometimes in steps—using the Theorems on extending $F$-isomorphisms in Section 24.1 and 24.2 (Theorem 24.6, Proposition 24.13, Theorems 24.14 and 24.24). A picture is emerging of three interrelated worlds: Polynomials, Field Extensions, and Galois groups. In this section, we are starting to explore the connection between Field extensions and Galois groups. On the other hand, if you just start with a polynomial $f \in F[x]$, then you move to the world of field extensions by letting $E$ to be the splitting field of $f$ over $E$, and then to the world of groups by finding $\mathrm{Gal}(E/F)$. This group is then called $\mathrm{Gal}(f)$. This will all become clear in Chapter 25.

**Assignment 15.** Read Section 25.1 Do Problems 24.2.9, 24.2.11, 24.3.6, 24.3.8, 25.1.1, 25.1.2
**Outline**.
This is a short section but introduces an important concept. Let $F \subseteq E$ be fields. We are interested in studying the *intermediate* fields between $F$ and $E$. We also have a group, the Galois group of $E$ over $F$, denoted by $\mathrm{Gal}(E/F)$. This group has subgroups and we know from group theory that the subgroups of a group carry much information. In this section, we define two maps. One from

the set of subgroups of Gal$(E/F)$ to intermediate fields between $F$ and $E$, the other from the set of intermediate fields to subgroups of Gal$(E/F)$. These two maps are *not*, in general, inverses of each other, but for "good" extensions they are inverses of each other. After defining them, we will be exploring and using these two maps all the time.

**Assignment 16.** Read Section 25.2 Do Problems 24.3.9, 24.3.10, 25.1.4, 25.2.1, 25.2.3, *25.2.7*
**Outline**.
In this section, we introduce three types of field extensions: Galois extensions, normal extensions, and separable extensions. Let $F \subset E$ be a field extension. This is a *Galois extension* if $\text{Fix}(\text{Gal}(E/F)) = F$. Eventually, we will prove (as part of the Fundamental Theorem of Galois Theory) that this implies that the the two maps defined in the previous section—between intermediate fields between $F$ and $E$ and the subgroups of Gal$(E/F)$—are inverses of each other. The extension $F \subseteq E$ is a normal extension if any irreducible polynomial of $F[x]$ that has a root in $E$ also splits in $E$ (if one root is in $E$ then all roots are in $E$). Finally, $F \subseteq E$ is a separable extension if, for all $\alpha \in E$, the $\min_F(\alpha)$ does not have a repeated root in its splitting field. We very much like Galois extensions since these end up giving a 1-1 correspondence between intermediate fields of the extension and subgroups of the Galois group. Normal and separable extensions are important since we prove in this section that an extension is Galois if and only if it is normal and separable. We also see at least one use for Galois extensions. Theorem 25.9 gives a way for constructing minimal polynomials using Galois groups.

**Assignment 17.** Read Section 25.3 Do Problems 25.2.8, 25.2.10, *25.2.11*, 25.3.3, 25.3.6, *25.3.7*
**Outline**.
If $E$ is a normal extension of $F$ then *every* irreducible in $F[x]$ that has a root in $E$ splits in $E$. On the other hand, if we say that $E$ is a splitting field over $F$ then we mean that there exists *one* polynomial in $F[x]$ for which $E$ is a splitting field. In this section we focus on nomal extensions and we show that, for finite degree extensions, an extension is normal if and only if it is a splitting field. In other words, if $E$ is the splitting field of just one polynomial over $F$, then *every* irreducible polynomial with a root in $E$, splits in $E$! This is a counter-intuitive and important result. What do we do if $E$ is *not* a normal extension of $F$? We show that, if $|E\colon F| < \infty$, then there is a smallest field containing $E$ that is a normal extension of $F$. This field is called the *normal closure* of $E$ over $F$.

**Assignment 18.** Read Section 25.4 Do Problems *25.3.11*, 25.3.15, 25.4.1, 25.4.3, 25.4.4, 25.4.5
**Outline**.
This section is about separable extensions. Recall that $F \subseteq E$ is a separable extension if every $\alpha \in E$ has *distinct* roots in some splitting field. So separable extensions are about making sure that irreducible polynomials don't have repeated roots. Now the fact is that most extensions are actually separable and is not that trivial to find inseparable extensions. In this section, we give an example of an inseparable extension, then come up with some tools (actually the derivative) to decide if a polynomial is separable or not. We then show if $\text{char}(F) = 0$ (for example if $F = \mathbb{Q}$) then all polynomials are separable (this means that if we wanted to limit ourself to extensions of $\mathbb{Q}$, then we wouldn't have to worry about separability). We also show that if $F$ is a finite field, then all polynomials over $F$ are separable. So what is left? The only extensions $F \subset E$ that could be inseparable are those with $F$ an infinite field of characteristic $p$. In the discussion about finite fields, we introduce the very important Frobenius map.

**Assignment 19.** Read Section 25.5 Do Problems 25.2.9, 25.4.9, 25.4.12, 25.5.1, *25.5.3*, 25.5.4
**Outline**.
Starting with this section, the gloves are off. We will proving consequential results in succession and quickly. You may have to read many of the results multiple times to really understand the arguments. The main purpose of this section is to prove the primitive element theorem, Theorem 25.45. This theorem says that if $F \subseteq E$ is a finite degree separable field extension, then $E = F[\alpha]$ for some $\alpha \in E$. This is remarkable and not at all obvious. For example, we know (from Section 25.4) that all extensions of $\mathbb{Q}$ are separable, and so this theorem says that a field like $\mathbb{Q}(\sqrt[4]{7}, i\sqrt{3}, \sqrt[3]{47})$ is generated by one element and we can write is as $\mathbb{Q}[\alpha]$ for a judicious choice of $\alpha$. This theorem proves very powerful and will be used often. To prove it we do two different cases based on if $F$ is finite or infinite. In the case of a finite field, we prove something that turns out to be a stronger statement. We show (Theorem 25.41) that if $G$ is a finite subgroup of $F^\times$ (where $F$ is a finite field), then $G$ is a cyclic group. At the end of the section, we already show the power of the primitive element Theorem by showing two facts about the size of the Galois group of an extension. Let $F \subseteq E$ be a finite degree extension. We show that $|\mathrm{Gal}(E/F)| \leq |E \colon F|$ with equality if and only if $E$ is a Galois extension of $F$. I want to reemphasize this last result. $F \subseteq E$ is a Galois extension if and only if $|\mathrm{Gal}(E/F)| = |E \colon F|$. So in the case of Galois extensions, we know the size of the Galois group before we start finding the group!

**Assignment 20.** Read Section 26.1 Do Problems *25.4.13*, 25.5.9, 25.5.11, 26.1.1, 26.1.3, 26.1.6
**Outline**.
Let $F \subseteq E$ be a Galois extension. We already know two important things. (1) $E = F(\alpha)$ for some element $\alpha \in E$, and (2) $|\mathrm{Gal}(E/F)| = |E \colon F|$. We now want to work toward the Fundamental Theorem of Galois Theory that says that there is a one to one correspondence (i.e., a bijective map) between the intermediate fields that contain $F$ and are contained in $E$ and the subgroups of $\mathrm{Gal}(E/F)$. This correspondence is order reversing which is why to make a drawing of it, we always draw the group upside down. The map that sends a subgroup of $\mathrm{Gal}(E/F)$ to an intermediate field is $\mathrm{Fix}(\cdot)$. In other words, if you have a subgroup of $\mathrm{Gal}(E/F)$ then find its fixed field and you get an intermediate field. The inverse map is $\mathrm{Gal}(E/\cdot)$. In other words, if $F \subseteq K \subseteq E$, then you map $K$ to $\mathrm{Gal}(E/K)$. The fundamental theorem says that these two maps are inverses of each other (and so both are bijections) and, moreover, in this correspondence normal subgroups of the Galois group correspond to the normal extensions of $F$. In this section, we just prove that the map $\mathrm{Fix}(\cdot)$ is $1-1$. In fact, to show this, we don't even need $E$ to be a Galois extension of $F$. It is enough that $|E \colon F| < \infty$.

**Assignment 21.** Read Section 26.2 Do Problems 25.5.12, 25.5.13, 25.6.21, 26.2.2, 26.2.4, *26.2.7*
**Outline**.
In this section, we complete the proof of the Fundamental Theorem of Galois Theory. At the beginning of the section, we focus on normal subgroups of $\mathrm{Gal}(E/F)$. We know that normal subgroups are special in group theory, and so if $N \lhd \mathrm{Gal}(E/F)$ and $K = \mathrm{Fix}(N)$, then what can we say about $K$? We prove in Proposition 26.7 that $K$ is a normal extension of $F$. So normal subgroups correspond to normal extensions! We then bring everything together in Theorem 26.9 and state the bijection

between subgroups of Gal$(E/F)$ and intermediate fields between $F$ and $E$ as long as $E$ is a Galois extension of $F$. At the end of the section, there is a proof of the Fundamental Theorem of Algebra using Galois theory. This is optional but a very fun proof that shows some of the power of Galois Theory.

**Assignment 22.** Read Section 26.3 Do Problems 25.5.14, 26.2.11, 26.2.15, *26.3.1*, 26.3.2, 26.3.4
**Outline**.
This section gives three examples of Galois groups and the Galois correspondence. There are no new theorems and a chance to consolidate your understanding of what Galois groups are, how we construct them, and how we use them to understand field extensions.

**Assignment 23.** Read Section 27.1 Do Problems 26.2.18, 26.3.5, 27.1.1, 27.1.3, 27.1.5,27.1.6
**Outline**.
We already know a number of facts about finite fields. Every finite field is of characteristic $p$, a prime, and so has a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$, the multiplicative group of a finite field is cyclic, and the only finite fields are of order $p^n$, where $p$ is a prime. Here we show that indeed there exists a field of order $p^n$ for every prime $p$ and integer $n$ and that such a field is unique up to isomorphism. We also explicitly find the Galois group of a finite field extension and use it to find all the intermediate fields.

**Assignment 24.** Read Section 27.2 Do Problems 27.1.8, *27.1.9*, 27.1.17, *27.2.5*, 27.2.7, 27.2.10
**Outline**.
In this section, we begin our march toward studying solvability and non-solvability of certain polynomial equations by concentrating on the polynomial $x^n - 1$. This polynomial is not irreducible and so we find its irreducible factors which are important polynomials called the *cyclotomic polynomials*. The most substantial theorem in this section is a theorem of Gauss that shows that these cyclotomic polynomials are irreducible. The roots of $x^n - 1$ are called the $n$th roots of unity. For example, 1, $-1$, $i$, and $-i$ are the 4th roots of unity. But $-1$ is already a second root of unity and 1 is also a first root of unity. The elements $i$ and $-i$ though are not $n$th roots of unity for any $n$ smaller than 4. We call $i$ and $-i$ *primitive* fourth roots of unity. It turns out that the cyclotomic polynomials are the minimal polynomials of these primitive roots of unity. If $\xi$ is a primitive unity, we will find Gal$(\mathbb{Q}(\xi)/\mathbb{Q})$ and prove that it is an abelian group. In fact, it is a group familiar from group theory. If $\xi$ is a primitive $n$ root of unity, this group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

**Assignment 25.** Read 27.3 Do Problems *27.1.19*, 27.2.12, *27.2.15*, 27.2.19, 27.3.2, 27.3.9
**Outline**.
When solving algebraic equations, at some point you may have to take $n$th roots. This is the same as solving the equation $x^n - a$. We have already studied the equation $x^n - 1$ in the previous section. In this section, we take a look at the equation $x^n - a$. If $a$ is an element of the field $F$, and $E$ is the splitting field of $x^n - a$ over $F$, as long as char$(F)$ is not a factor of $n$, we prove that $E$ is Galois over $F$ and we find a fair amount of information about Gal$(E/F)$. In fact, Gal$(E/F)$ will have a cyclic normal subgroup with an abelian quotient group. To prove this theorem, we first consider the case, when the base field already contains a primitive $n$th root of unity.

**Assignment 26.** Read 14.1 Do Problems 14.1.2, 14.1.3, 14.1.6, *27.1.21*, 27.2.20, 28.4.11

**Outline**.

To tackle solvability by radicals, we need to review solvable groups. Section 14.1 provides a good introduction to solvable groups. There is much to say here and we don't need all of it. We need to know the definition of solvable groups (Def 14.1), Theorem 14.18, and Theorem 14.20. There are many equivalent ways of defining what a solvable group is, and Theorem 14.16 gives some of these. Theorem 14.18 says that subgroups and quotient groups of solvable groups are solvable and if $N \lhd G$ with $N$ and $G/N$ both solvable then $G$ is also solvable. Finally Theorem 14.20 proves that the alternating groups $A_n$ for $n \geq 5$ are simple (and hence not solvable). The section also defines commutator subgroups and characteristic subgroups. These are very useful concepts in group theory and are used to prove the Theorems in this section but we will not be using them directly. As long as you understand the definition of solvable groups, understand Theorem 14.18, and know that the alternating groups are not solvable, then you are ready to move on.

**Assignment 27.** Read 28.1 Do Problems 25.6.1, 27.2.21, 28.1.6, 28.1.8, *28.1.9*, 28.4.12

**Outline**.

Given a polynomial equation, we define in this section what we mean by "solvability by radicals". In other words, we translate the question of solvability of a polynomial to a certain concept about field extensions. We need to know what a repeated radical extension is and prove that if a finite degree extension is a repeated radical extension, then so is its normal closure.

**Assignment 28.** Read 28.2 Do Problems 25.6.2, 27.2.22, 28.1.10, 28.2.1, 28.2.7, 28.4.13

**Outline**.

In this section we prove that a solvable polynomial has a solvable Galois group. In fact, we prove something that ends up being more general. We prove that if $L$ is a repeated radical extension of $F$, and if $F \subseteq E \subseteq L$, then $\mathrm{Gal}(E/F)$ is a solvable group. As a result, we can then exhibit very specific polynomials—e.g., $x^5 - 10x + 5$—whose roots cannot be expressed using the four arithmetical operations and any combination of radicals.

**Assignment 29.** Read 28.3 Do Problems 25.6.3, *27.2.23*, 27.4.1, 28.3.4, 28.3.5, 28.4.14

**Outline**.

This final section is optional. Here we prove the other direction of Galois's Theorem. Let $f \in F[x]$, and $E$ is the splitting field of $f$ over $E$. As long as $\mathrm{char}(F)$ does not divide $|E\colon F|$, if $\mathrm{Gal}(E/F)$ is a solvable group, then $f$ is solvable by radicals. This direction is harder to prove and requires that a number of tools that were developed earlier be strengthened. This completes our study of Galois Theory.