A quick introduction to Galois theory

A mathematical essay by Wayne Aitken*

Summer 2019†

In the Summer of 2003 I wrote a series of sixteen one-page worksheets on Galois theory for my graduates students. The purpose of these worksheets was for the students to learn principles of Galois theory by proving the theorems themselves (with generous hints). Many years later, in 2019, I reviewed these worksheets, and found them to constitute a nice introductory course to Galois theory that was both quick and rigorous. These worksheets inspired me to write this essay as a short introduction to Galois theory, using the worksheets as a guide.

Officially this essay was written as a summary and companion to these 16 worksheets. In particular, I have updated the worksheets and will make them available alongside this essay. However, this essay can be read independently of the worksheets as an overview of some topics in Galois theory, especially if the reader is willing to skip some of the details of the proofs. If the reader wants to work through the proofs of the results carefully then I would advise that they work through the worksheets, using this essay for additional perspective and as a source of hints and ideas for working on the worksheets.[1]

This essay plus the worksheets provides a short self-contained introduction to Galois theory. This introduction includes some interesting and important topics including the following:

- A full proof of the fundamental theorem of Galois theory
- Cyclotomic extensions including the irreducibility of the cyclotomic polynomials
- A proof of quadratic reciprocity, using cyclotomic extensions
- Ruler and compass constructions, including a classification of which regular polygons are constructible

†Version of September 12, 2019 (with minor corrections).

[1]The worksheets were written and used long before this essay was written, and so obviously can be used independently of this essay. However this essay provides commentary that goes beyond what could be included in the worksheet given the aim and terse format of the worksheet series. Also, the worksheets were part of a graduate student seminar and so benefited from face to face explanations from the author. My hope is that this essay will help provide context and additional guidance to readers working through the worksheets, especially for readers without the benefit of face to face interactions with an instructor or mentor.

- The Galois theory of finite fields
- A Galois theoretic proof of the fundamental theorem of algebra

The main gap in the above list of topics concerns the solvability of polynomials in terms of radicals. This may be surprising since questions of solvability played such an important role in the history of Galois theory and modern algebra generally.[2] The approach here is definitely a selective approach, but I regard this limitation of scope as a feature, not a bug. This approach allows the reader to build up the basics of Galois theory quickly, and see several significant applications of Galois theory in quick order. For this reason, I think this approach is potentially valuable to the reader, in spite of the existence of many good books that cover Galois theory more thoroughly. The reader who masters the worksheets will have good idea about how Galois theory works and will be in an excellent position to study further topics in Galois theory from other sources that take a more traditional or comprehensive approach.

Some background

This essay and the accompanying worksheets should be useful for self-study for anyone who wants to learn, or brush up on, the areas of Galois theory covered here. It does require some background, however. For self-study we assume that the reader has a good level of proficiency with the basics of linear algebra, and about a year worth of abstract algebra at an undergraduate level. Of course, the reader working through the worksheets will need stronger skills and background than the reader who is just reading the summaries in this essay. Another possibility is that the reader work through this material with the help of an instructor or mentor, in which case the needed background can be covered or reviewed as needed.

Below we discuss some of the specific assumptions for the worksheets.

Linear algebra background

Galois theory requires a bit of linear algebra. Here are some specifics:

- The definition of *vector space*, *linear map*, and *isomorphism* between vector spaces. These should be for an arbitrary field F of scalars.
- The idea of linearly independent and dependent vectors, and the idea of a spanning set of vectors.
- The definition of *basis* as a set of independent vectors that span. The existence theorem for a basis. (For infinitely generated vector space, this requires Zorn's lemma. But our focus here will be on finite dimensional spaces; do not worry too much about spaces with infinite bases).

[2] This essay aims for an efficient approach to Galois theory, as opposed to a historical approach. A more historical approach has a lot of value, and I may at some point write a follow-up essay with a more historical outlook. This would, of course, focus more on the solvability of polynomials.

- The fact that all bases have the same cardinality. The definition of *dimension* in terms of the cardinality of the basis. Invariance of dimension and other properties under isomorphism.
- The fact that if there are more vectors than the dimension, then the vectors are dependent.
- The fact that if there are n linearly independent vectors where n is the dimension, then these vectors form a basis.
- Representing linear maps between finite dimension spaces by matrices.

Field theory and polynomial background

We assume the reader is familiar with the notion of a field extension of E over F. For example, the reader should know that an extension E can be regarded as a vector space with scalar field F. The reader should know what it means for $\alpha \in E$ to be algebraic or transcendental over F. If α is algebraic, then the reader should know about the existence and some basic properties of its minimal polynomial $f \in F[X]$. We assume familiarity with the ring $F[\alpha]$ (in an extension E) generated by F and $\alpha \in E$ as well as the field $F(\alpha)$ generated by F and α. (The ring and field turn out to equal if α is algebraic over F). Much of this background is covered in my essay *Minimal, Primitive, and Irreducible Polynomials* (2010, updated 2019) together with the background assumed in that essay. For example, the reader should know that if α is algebraic in an extension E of F then $F[\alpha]$ is isomorphic to $F[X]/\langle f \rangle$ where f is the minimal polynomial of α. Here the isomorphism maps α to the coset containing X.

A few basic properties of finite fields are assumed. For example, we assume that the multiplicative group $F^\times$ of a finite field F is cyclic. This is a special case of the following:

Fact. *If F is a field then any finite subgroup of $F^\times$ is cyclic.*

The reader should know what *characteristic* is, and that the characteristic of a finite field is a prime. If a field F has characteristic $p > 0$, the reader should know (and be able to prove) that $(x + y)^p = x^p + y^p$ for all $x, y \in F$.

The theory of formal derivatives is assumed for polynomial rings in general. But the rules for differentiation follow the rules of differential calculus closely, and so should not present too much of a hurdle. Of course, the basics of groups, quotient groups, rings, ideals, and quotient rings are assumed.

We take for granted that $\mathbb{C}$ is algebraically closed, but actually a Galois-theoretic proof is given in the last worksheet.

We make use of the following:

Fact. *The numbers π and e are transcendental over $\mathbb{Q}$.*

Fact. *Given a field F there is a field E containing F that is algebraically closed.*

There may be other background assumptions that are special for a particular worksheet. We will comment on this below. For example, Worksheet 8 assumes familiarity with the field of fractions of an integral domain in a few of its examples.

Outline

We will essentially follow updated versions of the original sixteen worksheets which are labelled GT 1 to GT 16. The first half of these worksheets set up basic Galois theory, and the last half give applications.

- The first seven worksheets constitute an efficient introduction to Galois theory, culminating in the fundamental theorem of Galois theory.
- Worksheet 8 helps round out a basic understanding of Galois theory. However, it is not required for the worksheets that follow.
- Worksheets 9 and 10 concern cyclotomic extensions and the irreducibility of cyclotomic polynomials in $\mathbb{Q}[X]$.
- Worksheets 11 and 12 lead to a proof of Gauss's quadratic reciprocity after identifying the quadratic subfield of the qth cyclotomic extension for odd primes q (using Gauss sums).
- Worksheets 13 and 14 concern ruler and compass constructions. Worksheet 13 does not require much background really, just Worksheet 1. Worksheet 14 requires familiarity with the complex numbers, and more familiarity with the prior worksheets (but does not require Worksheets 8, 11, and 12).
- Worksheet 15 concerns the Galois theory of finite fields. Much of this is accessible after the first seven worksheets. The last problem builds on Worksheet 9 as well.
- Worksheet 16 concerns the fundamental theorem of algebra. It uses the first seven worksheets, some of Worksheet 10 (concerning quadratic extensions), and a few basic facts from finite group theory (one of the Sylow theorems for example) and analysis (the intermediate value theorem).

Worksheet 1: Algebraic extensions

We fix a field F which we call the *base field*. This is $\mathbb{Q}$ in many cases, but allowing more general base fields is important.

Definition 1. Suppose that E is an extension field of the base field F. Then E is called an *algebraic extension* of F every $\alpha \in E$ is algebraic over F. In other words, E is algebraic if and only if for every $\alpha \in E$ there is a nonzero polynomial in $F[X]$ with root α.

Definition 2. Suppose that E is an extension field of the base field F. Then E can be regarded as a vector space over F. The extension E is called a *finite extension* of F if the dimension $[E : F]$ is finite. The dimension $[E : F]$ is also called the *degree* of the field extension E over F.

The main results concerning algebraic and finite extensions are as follows:

Proposition 1. *If E is a finite extension of F, then E is an algebraic extension of F. In fact, if $[E : F] = n$, then the minimal polynomial of each $\alpha \in E$ has degree at most n.*

Proposition 2. *Suppose E is finite extension of F, and L is finite extension of E. Suppose $e_1, \ldots, e_n$ is a basis for E as an F-vector space, and that $\ell_1, \ldots, \ell_m$ is a basis for L as an E-vector space. Then the mn elements of the form $e_i \ell_j$ yield a basis for L as a F-vector space.*

As a corollary we get the important degree formula for a tower of extensions:

Corollary 3. *Suppose E is a degree n extension of F, and L is a degree m extension of E. Then*

$$[L : F] = [L : E][E : F].$$

Note also that $[E : F] = 1$ if and only if $E = F$.

If $\alpha \in E$ is algebraic over F with minimal polynomial of degree d then $F[\alpha]$ is a field that has degree d over F. Recall that if $\alpha_1, \alpha_2, \ldots \alpha_n \in E$ where E is an extension field of the base field F, then $F[\alpha_1, \alpha_2, \ldots \alpha_n]$ denotes the smallest subring of E containing each α_i and every element of F. Using the above corollary we get the following:

Proposition 4. *Suppose $\alpha_1, \alpha_2, \ldots \alpha_n \in E$ are algebraic over F where E is a field extension of the base field F. Then $F[\alpha_1, \alpha_2, \ldots \alpha_n]$ is a field, and is a finite extension of F.*

This allows us to conclude that the sum and product of algebraic elements is algebraic. In fact, we have the following:

Proposition 5. *Suppose E is a field extension of the base field F. Then the subset of all $\alpha \in E$ that are algebraic over F forms a subfield of E.*

Above we saw that a tower of finite extensions produces a finite extension. The following asserts an analogous result: a tower of algebraic extensions is algebraic.

Proposition 6. *If L is an algebraic extension of E, and if E is an algebraic extension of F, then L is an algebraic extension of F.*

Next we consider algebraically closed fields and algebraic closures. Recall that a field E is algebraically closed if every nonconstant polynomial has a root in E, which implies that every nonconstant polynomial in $E[X]$ factors into linear polynomials in $E[X]$, and that a polynomial is irreducible if and only if it is linear. The field of complex numbers $\mathbb{C}$ is the standard example of an algebraically closed field (the fundamental theorem of algebra).

Definition 3. Let F be a field. We say that E is an *algebraic closure of F* if (i) E is algebraic over F, and (ii) there is no field extension E' of E with $E' \neq E$ that is algebraic over F.

Proposition 7. *Let E be a field extension of the base field F. Then E is an algebraic closure of F if and only if (i) E is algebraic over F, and (ii) E is algebraically closed.*

Proposition 8. *Suppose E is an algebraically closed field, and that F is a subfield. Then there is a unique subfield $\overline{F}$ of E that is an algebraic closure of F.*

Corollary 9. *There is a unique algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$.*

If we assume the existence of an algebraically closed extension of F, then the above proposition gives the existence of an algebraic closure; similarly, the existence of an algebraic closure of F gives the existence of an algebraically closed extension of F. It turns out that the algebraic closure of F is unique up to isomorphism, but we will not really need this fact here (and even existence is not absolutely critical). We mention it because of its importance:

Fact. *Every field F has an algebraic closure. Any two algebraic closures of F are isomorphic with an isomorphism fixing F.*

Worksheet 2: Splitting fields, Galois extensions, extension of homomorphisms

There are several equivalent ways to define the concept of a Galois extension. In this essay we will officially define a finite Galois extension as a kind of splitting field. So we start with splitting fields.

Definition 4. Let E be a field. If $f \in E[X]$ is a nonconstant polynomial that factors into linear factors in $E[X]$, then we say that f *splits* in E.

If f splits in E and if the linear factor of f are distinct (not associates) then we say that f *has distinct roots in E* or that f *separates in E*. Otherwise we say that f has *multiple roots*.

Definition 5. Let E be a field extension of a field F. Let $f \in F[X]$ be a nonconstant polynomial. Then E is a *splitting field of f over F* if (i) f splits in E, and (ii) $E = F[\alpha_1, \ldots, \alpha_n]$ where α_i are the roots of f in E.

If we have an algebraic closure L of F, then we can produce the splitting field of $f \in F[X]$ by taking the field generated by F and the roots of f in L. In general we can form a splitting field as a subfield of any field L in which f splits:

Proposition 10. *Suppose $f \in F[x]$ is a nonconstant polynomial where F is a field. Then there exists a splitting field for f over F. In fact, given an extension L in which f splits, there is a unique splitting field E of f contained in L. Any splitting field of f over F is a finite extension of F.*

In particular, splitting fields are unique in a given algebraic closure of F. In the abstract however, the splitting field of $f \in F[X]$ is not unique as a set. This is not too much of a problem since later we will see that two splitting fields of f over F are isomorphic with an isomorphism fixing F.

One way to prove the existence claim of Proposition 10 is to start with an algebraically closed field L containing F and form the splitting field as a subfield of L. There is a way to construct splitting fields which does not require the existence of an algebraic closure. The main idea is to use $F_1 = F[X]/\langle f_1 \rangle$ where f_1 is a nonlinear irreducible polynomial of f in $F[X]$. Recall that F_1 is a field, and that

we can identify F with a subfield of F_1. The polynomial f_1 has a root in F_1 (namely the coset of X), and so is no longer irreducible in $F_1[X]$, but has a linear factor.[3] This basic idea can be iterated to construct a splitting field for a given nonconstant $f \in F[X]$. Start by choosing a nonlinear irreducible factor f_1 of f (if this does not exist, we are done: f splits in F). Form F_1 as above. Then in $F_1[X]$ the polynomial f will have at least one more linear factor than it did in $F[X]$. Now choose a nonlinear irreducible factor f_2 of f in $F_1[X]$. If this does not exist, we are done: f splits in F_1. Otherwise, form the extension $F_2 = F_1[X]/\langle f_2 \rangle$ of F_1. By continuing in this way, we eventually construct a splitting field for f.

Next we use splitting fields as the basis for defining Galois extensions and Galois groups.

Definition 6. Let E be a finite extension of a field F. We say that E is a *Galois extension* of F if there is a nonconstant $f \in F[X]$ with no multiple roots in E such that E is the splitting field of f over F.

For such an extension E, the *Galois group* of E over F is the group of automorphisms of E that fix the base field F.

Remark. Here, an *automorphism* of a ring R is a ring isomorphism from R to R. In Galois theory we are concerned with automorphisms of a field E to itself.

Lemma 11. *The Galois group of E over F as defined above is indeed a group under composition.*

Example 1. If $\sqrt{d}$ is not in $\mathbb{Q}$ then the quadratic extension $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}[\sqrt{d}\,]$ is Galois over $\mathbb{Q}$. (Here we can regard the extension as a subfield of $\mathbb{C}$).

Example 2. The extension $\mathbb{Q}\left(2^{1/4}, i\right) \subseteq \mathbb{C}$ is Galois over $\mathbb{Q}$. (It turns out that $\mathbb{Q}\left(2^{1/4}\right)$ is not Galois over $\mathbb{Q}$).

Example 3. If $\zeta_6 \in \mathbb{C}$ is a primitive sixth root of unity, then $\mathbb{Q}\left[\zeta_6\right]$ is Galois over $\mathbb{Q}$.

The following can be verified using the fact that $X^q - X$ factors into distinct linear factors in a field with q elements.

Example 4. If E is a finite field of characteristic p, then E is Galois over $\mathbb{F}_p$.

Suppose $\alpha \in E$. If $\sigma(\alpha) = \alpha$ where σ is an automorphism of E, we say that σ *fixes* α.

Definition 7. Let E be a finite Galois extension of F with Galois group G. If H is a subgroup of G, then the *fixed field of H*, written E^H, is defined to be the set of elements of E fixed by every $\sigma \in H$:

$$E^H \stackrel{\text{def}}{=} \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

Lemma 12. *The fixed field E^H as defined above is indeed a field; it is an intermediate field between F and E.*

[3] See my essay, *Minimal, Primitive, and Irreducible Polynomials* (2010, updated 2019).

Next we discuss extending homomorphisms $R_1 \to R_2$ to homomorphisms of polynomial rings $R_1[X] \to R_2[X]$. This is based on the following universal property of polynomials (which we take as a given, and fundamental, property of polynomial rings):

Fact (Universal property for polynomial rings)**.** *Let R and A be commutative rings with unity. Let $\psi : R \to A$ be a ring homomorphism, and let $a \in A$. Then there is a unique ring homomorphism $R[X] \to A$ such that $X \mapsto a$ and such that its restriction to R is ψ.*

If ψ is an inclusion map, the universal property yields the familiar substitution map $R[X] \to A$ sending f to $f(a)$.

We will be interested in applying the universal property in the following situation: we start with a homomorphism $\phi : R_1 \to R_2$. We compose with the canonical map $R_2 \to R_2[X]$ to get a homomorphism $\psi : R_1 \to R_2[X]$. Using the universal property, we get a unique homomorphism $R_1[X] \to R_2[X]$ that extends ψ and sends X to X. Observe that this also extends ϕ, and is the unique homomorphism that does so and, at the same time, sends X to X.

Definition 8. Let $\phi : R_1 \to R_2$ be a homomorphism between commutative rings with unity. Let $\phi_X : R_1[X] \to R_2[X]$ be the unique extension that sends X to X.

The map ϕ_X can be described very concretely as follows:

$$a_n X^n + \ldots + a_1 X + a_0 \quad \mapsto \quad \phi(a_n)X^n + \ldots + \phi(a_1)X + \phi(a_0).$$

Using this concrete description we can prove the following:

Lemma 13. *Let ϕ and ϕ_X be as above. If ϕ is injective, then ϕ_X is a degree-preserving injection. If ϕ is an isomorphism, then ϕ_X is an isomorphism.*

Observe that if $\phi\colon F_1 \to F_2$ is an isomorphism between fields, then the factorization of a nonzero polynomial $f \in F_1[X]$ in $F_1[X]$ is reflected by the factorization of $\phi_X f$ in $F_2[X]$.

We can use ϕ_X to show that ϕ maps roots to roots:

Proposition 14. *Let $\phi : R_1 \to R_2$ be a homomorphism between commutative rings with unity. If $f \in R_1[X]$ and $\alpha \in R_1$, then $\phi\big(f(\alpha)\big) = (\phi_X f)(\phi\,\alpha)$. In particular, if α is a root of f, then $\phi(\alpha)$ is a root of $\phi_X f$.*

Remark. This can be proved using the concrete description of ϕ_X above. Or one can use the universal property of polynomials to produce a suitable commutative diagram.

In the next worksheet we will need Lemma 16 which is in turn based on the following:

Lemma 15. *Let $\phi : R_1 \to R_2$ be a homomorphism between commutative rings with unity, and let $f \in R_1[X]$ be a polynomial. Then there is a homomorphism*

$$R_1[X]/\langle f\rangle \to R_2[X]/\langle \phi_X f\rangle$$

That sends the coset $\overline{a}$ to $\overline{\phi a}$ for all $a \in R_1$, and sends the coset $\overline{X}$ to the coset $\overline{X}$.

If ϕ is an isomorphism, then the resulting homomorphism on quotients is also an isomorphism.

In the above, we are most interested in the case where $\phi\colon F_1 \to F_2$ is an isomorphism between fields and where $f \in F_1[X]$ is an irreducible nonconstant polynomial. Then $\phi_X f$ will also be irreducible. In this case $L_1 = F[X]/\langle f \rangle$ can be thought of as a finite extensions of F_1, and $L_2 = F_2[X]/\langle \phi_X f \rangle$ can be thought of as a finite extension of F_2. The lemma yields an isomorphism $L_1 \to L_2$ extending ϕ which sends $\overline{X}$ to $\overline{X}$.

In addition, suppose α is an algebraic element in an extension field of F_1 with minimal polynomial f. Then the reader of the worksheets is expected to be familiar with the result that $F_1[\alpha]$ is isomorphic to L_1 above where α maps to $\overline{X}$.[4] A similar statement holds for a given root β of $\phi_X f$. Putting this together gives a lemma, used in the next worksheet:

Lemma 16. *Suppose $\phi : F_1 \to F_2$ is an isomorphism between fields, and suppose $f \in F_1[X]$ is nonconstant and irreducible. Let E_1 be an extension of F_1 containing a root α of f, and let E_2 be an extension of F_2 containing a root β of $\phi_X f$. Then there is a unique isomorphism $F_1[\alpha] \to F_2[\beta]$ that extends ϕ and sends α to β.*

Worksheet 3: Galois theory basics

We begin by proving a fairly technical extension lemma.

Lemma 17. *Let $f \in F[X]$ be a nonconstant polynomial where F is a field. Let E and E' be splitting fields of f over F. Let L be a subfield of E that contains F. Then every homomorphism $\phi : L \to E'$ fixing F can be extended to a homomorphism $E \to E'$. If f does not have multiple roots in E', then there are exactly $[E : L]$ such extensions. (In general, whether or not f has multiple roots, $[E : L]$ is an upper bound.)*

The basic idea of the proof is to first consider extensions of the domain from L to $L[\alpha]$ where α is a root of f. This can be done using Lemma 16. By induction we continue the rest of the way from $L_1 = L[\alpha]$ to E.

We leverage this lemma to prove a useful theorem about splitting fields:

Proposition 18. *Let $f \in F[X]$ be a nonconstant polynomial where F is a field. Let E and E' be splitting fields of f over F. Then there is an isomorphism $E \to E'$ fixing F. The number of such isomorphisms is bounded by $[E : F]$. Furthermore, we have $[E : F] = [E' : F]$, and f has distinct roots in E if and only if it has distinct roots in E'. In the case of distinct roots, the number of such isomorphisms is exactly $[E : F]$.*

The special case where $E = E'$, and where E is a Galois extension of F, yields the following, our first major theorem in Galois theory:

Theorem 19. *If E is a finite Galois extension of the field F, then the Galois group of E over F has exactly $[E : F]$ elements.*

The following theorem is easy to prove, but it is important:

[4] See my essay, *Minimal, Primitive, and Irreducible Polynomials* (2010, updated 2019).

Theorem 20. *Suppose that E is a finite Galois extension of F. If L is an intermediate field between F and E then E is Galois over L and* $\mathrm{Gal}(E/L)$ *is a subgroup of* $\mathrm{Gal}(E/F)$.

Another important observation is that $\mathrm{Gal}(E/E^G) = \mathrm{Gal}(E/F)$ if E is a finite Galois extension of F. So by Theorem 19 we have $[E : E^G] = [E : F]$. This is the key to the next major theorem in Galois theory:

Theorem 21. *Suppose E is a finite Galois extension of F, and that G is the Galois group of E over F. Then $E^G = F$.*

The following is another consequence of Lemma 17:

Proposition 22. *Suppose E is a splitting field over F, and L is an intermediate field between F and E. Then any automorphism of L fixing F can be extended to an automorphism of E.*

So if, in the above proposition, E and L are Galois over F, then every element of $\mathrm{Gal}(L/F)$ can be extended to an element of $\mathrm{Gal}(E/F)$.

Worksheet 4: Conjugates and minimal polynomials

Next we consider the idea of a *conjugate*:

Definition 9. Let E be a finite Galois extension of F with Galois group G. Let $\alpha \in E$. Then any element of the form $\sigma\alpha$ with $\sigma \in G$ is called a *G-conjugate* of α (or simply a *conjugate* of α if G is clear from context).

Let E be a finite Galois extension of a field F with Galois group G, and let $\alpha \in E$. Then α is a conjugate of itself. Observe that $\alpha \in F$ if and only if the only conjugate of α is α. This fact is just a restatement of Theorem 21. More generally, there is a natural association between conjugates of α and cosets. To make this precise, let $H = \{\sigma \in G \mid \sigma\alpha = \alpha\}$. Then H is a subgroup, and we associate to each conjugate $\sigma\alpha$ the left coset σH. So the number of conjugates is equal to the index $[G : H]$. (This association is a special case of what happens with an orbit under a general group action). Since the number of conjugates is equal to $[G : H]$, we conclude that the number of conjugates divides $|G| = [E : F]$.

If $\alpha \in E$ has minimal polynomial $f \in F[X]$ over F, where E is a finite Galois extension of F, then we observe that every conjugate of α is a root of f. In particular, if $\alpha' \in E$ is a conjugate then $X - \alpha'$ is a root of f. We can prove that these are the only roots, and we can derive the following important formula:

Theorem 23. *Let E be a finite Galois extension of F with Galois group G. Let $\alpha_1, \ldots, \alpha_m$ be the distinct G-conjugates of $\alpha \in E$. Then the minimal polynomial f of α in $F[X]$ is*

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i).$$

Corollary 24. *Let E be a finite Galois extension of F. If $f \in F[X]$ is irreducible, and if at least one root of f is in E, then f splits in E and f has distinct roots in E.*

Next we consider how elements of a Galois group correspond to permutations of roots of a polynomial. Let G be the Galois group of a Galois extension E over F, and let $f \in F[X]$ be a nonconstant polynomial that splits in E. As mentioned above, $\sigma \in G$ must map roots of f to roots. In other words, σ restricts to a bijection $\sigma' \colon R \to R$ where R is the set of roots of f. This type of restriction satisfies the law $(\sigma \circ \tau)' = \sigma' \circ \tau'$. In other words $\sigma \mapsto \sigma'$ is a homomorphism $G \to \mathcal{S}_R$ where $\mathcal{S}_R$ is the group of bijections of R under composition. Because of this, we say that G *acts on the set of roots* R. If E is the splitting field of f over F, then this homomorphism is a injection, and G is isomorphic to a subgroup of $\mathcal{S}_R$. If we choose a polynomial f that is irreducible, then elements of R are conjugate to any particular $\alpha \in R$ (Theorem 23). Thus, if f is irreducible, the image of G in $\mathcal{S}_R$ is transitive (in other words, for any $\alpha, \alpha' \in R$ there is an element of $\mathcal{S}_R$ in the image that maps α to α').

Let f and R be as above. When we number the roots in R we get a homomorphism $G \to \mathcal{S}_m$ where $\mathcal{S}_m$ is the permutation group of $\{1, \ldots, m\}$. To see this formally, fix a bijection $\rho \colon \{1, \ldots, m\} \to R$. Then $\sigma \in G$ is sent to the permutation $\tilde{\sigma} \in \mathcal{S}_m$ defined by the rule

$$\tilde{\sigma}(i) = \rho^{-1}(\sigma(\rho(i))) = (\rho^{-1} \circ \sigma' \circ \rho)(i)$$

In other words

$$\tilde{\sigma} = \rho^{-1} \circ \sigma' \circ \rho.$$

So

$$\tilde{\sigma} \circ \tilde{\tau} = \rho^{-1} \circ \sigma' \circ \rho \circ \rho^{-1} \circ \tau' \circ \rho = \rho^{-1} \circ \sigma' \circ \tau' \circ \rho = \rho^{-1} \circ (\sigma \circ \tau)' \circ \rho = \widetilde{\sigma \circ \tau}.$$

So we have confirmed that $\sigma \mapsto \tilde{\sigma}$ is a homomorphism $G \to \mathcal{S}_m$. In special cases we get the following:

- If E is the splitting field of f over F, then $G \to \mathcal{S}_m$ is injective. So we can represent G as a subgroup of $\mathcal{S}_m$.
- If f is irreducible, then the image of $G \to \mathcal{S}_m$ is a transitive subgroup of $\mathcal{S}_m$.

So if $f \in F[X]$ is an irreducible polynomial of degree $n \geq 1$ with distinct roots (in any splitting field), then the extension E generated by the roots of f is by definition a Galois extension. The Galois group of E over F is sometimes called the *Galois group of* f. By the above we can identify elements of G with permutations of the roots of f. When we fix a numbering of the roots, we can identify G with a transitive subgroup of $\mathcal{S}_n$.

For example, if f is linear then the Galois group is represented as $\mathcal{S}_1$, the trivial group. If f is an irreducible quadratic polynomial, then the Galois group is represented as a transitive subgroup of $\mathcal{S}_2$, which must be all of $\mathcal{S}_2$ (a group of order 2). If f is an irreducible cubic polynomial then the Galois group is represented as a transitive subgroup of $\mathcal{S}_3$, so it is isomorphic to all of $\mathcal{S}_3$, or to the alternating group $\mathcal{A}_3$ (of even permutations). If f is an irreducible fourth degree polynomial then the Galois group is represented as a transitive subgroup of $\mathcal{S}_4$. (It turns out that this means that the Galois group is isomorphic to either $\mathcal{S}_4, \mathcal{A}_4$, the dihedral group with eight elements, the cyclic group with four elements, or the Klein four

group. Note: on this list, only the Klein four group occurs as a proper subgroup of $\mathcal{A}_4$.)

Remark. The above construction actually extends to group actions in general. A *group action* of a group G on a set R can be defined as a homomorphism $G \to \mathcal{S}_R$. Given such a group action, for each $\sigma \in G$ write σ' be the image of σ under this $G \to \mathcal{S}_R$. For $\sigma \in G$ and $r \in R$, we often write $\sigma'(r)$ as σr.

Now suppose R is finite with m elements and fix a bijection $\rho\colon \{1, \ldots, m\} \to R$. Then we can define a homomorphism $G \to \mathcal{S}_m$ by the rule $\sigma \mapsto \tilde{\sigma}$ where

$$\tilde{\sigma} = \rho^{-1} \circ \sigma' \circ \rho.$$

This can be shown to be a homomorphism using the earlier argument. Also $\sigma \mapsto \sigma'$ is injective if and only if $\sigma \mapsto \tilde{\sigma}$ is injective. Similarly, $\sigma \mapsto \sigma'$ has transitive image if and only if $\sigma \mapsto \tilde{\sigma}$ has transitive image.

Example 5. Let $E = \mathbb{Q}\left(2^{1/4}, i\right)$ and $F = \mathbb{Q}$. As an exercise, the reader is asked to find an irreducible polynomial f in $\mathbb{Q}[X]$ such that E is the splitting field of f over $\mathbb{Q}$. So E is Galois over F. By looking at the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(2^{1/4}) \subseteq E,$$

one can show that the degree $[E : \mathbb{Q}]$ is 8, and that the Galois group G has 8 elements. One can describe all 8 elements of G by how they map the generators $2^{1/4}$ and i. By looking how G acts on the roots of $X^4 - 2$, one sees that G is isomorphic to the symmetries of a square. In other words, G is isomorphic to the dihedral group with 8 elements.

Worksheet 5: The primitive element theorem

The next main result is the primitive element theorem. Our proof relies on the fact that if E is a finite Galois extension of F then there are only a finite number of intermediate fields. We establish this fact first.

If L is such an intermediate field between E and F where E is a finite Galois extension of F with Galois group $G = \mathrm{Gal}(E/F)$, then E is Galois over L (Theorem 20). Here we use the notation

$$G_L \stackrel{\text{def}}{=} \{\sigma \in G \mid \sigma\beta = \beta \text{ for all } \beta \in L\}.$$

Observe that G_L is a subgroup of G, and that $G_L = \mathrm{Gal}(E/L)$. In particular, the association $L \mapsto G_L$ maps intermediate subfields to subgroups of G. By Theorem 21 this association is injective:

Proposition 25. *Suppose L and L' are distinct intermediate fields between F and E, where E is a finite galois extension of F with Galois group G. Then*

$$G_L \neq G_{L'}.$$

Corollary 26. *Suppose E is a finite galois extension of F. Then there are only a finite number of intermediate fields between F and E.*

Corollary 27. *Suppose L is an extension of F contained in a finite Galois extension of F. Then there are only a finite number of intermediate fields between F and L.*

Recall that if L is an extension of F, then we can regard L as a vector space over F. Also intermediate subfields between F and L correspond to of subspaces of L. Here is a fairly easy (and intuitive) lemma from linear algebra:

Lemma 28. *Let $W_1, \ldots, W_n$ be proper subspaces of a vector space V. Suppose that the scalar field F of V is infinite (or at least has more than n elements), then there is a vector $\alpha \in V$ not in the union $W_1 \cup \cdots \cup W_n$.*

In our situation, this means that if F is infinite then there is an $\alpha \in L$ outside of the finite number of intermediate fields properly contained in L. This leads directly to a proof of the following in the case when F is infinite:

Theorem 29 (Primitive Element Theorem)**.** *Let L be an extension of F that is contained in a finite Galois extension of F. Then there is an $\alpha \in L$ such that*

$$L = F[\alpha].$$

To prove this in the case that F, and hence L, are finite, then just take a generator α of the cyclic group $L^\times$.

Remark. Gallian attributes the Primitive Element Theorem to Steinitz (1910). I have not looked up Steinitz's original proof, but I have observed that the proof outlined here is different than that given in most contemporary accounts.

Worksheet 6: Separable extensions

We assume familiarity with the derivative rules for polynomials with coefficients in a general field. These rules generalize the usual rules of calculus for polynomials functions with real coefficients. These rules give straightforward proofs of the following:

Proposition 30. *Let F be a field. Suppose a nonzero $f \in F[X]$ splits in an extension E. Then f has a multiple root in E if and only if $\gcd(f, f')$ is of positive degree.*

Corollary 31. *Let F be a field. Suppose $f \in F[X]$ is irreducible and splits in an extension E. Then f has multiple roots in E if and only if $f' = 0$.*

Next we introduce a few definitions:

Definition 10. Let F be a field. Suppose $f \in F[X]$ is nonzero. If f splits with distinct roots in an extension E then we say that f is *separable*. So if f is irreducible, then f is separable if and only if $f' \neq 0$.

Definition 11. A field F is called *perfect* if $f' \neq 0$ for all irreducible $f \in F[X]$.

Clearly any field of characteristic zero is perfect. In general we prove the following:

Theorem 32. *Every field of characteristic zero is perfect. If F has characteristic $p > 0$, then F is perfect if and only if $F^p = F$ where F^p is the set of pth powers in F. Every finite field F of characteristic p has the property that $F^p = F$, so all finite fields are perfect.*

Next we consider separable extensions:

Definition 12. An algebraic extension L of a field F is called *separable* over F if the minimal polynomial in $F[X]$ of every element of L is separable.

Based on our earlier formula for minimal polynomials, we have the following:

Lemma 33. *Suppose E is a finite Galois extension of F. Then any intermediate field L with $F \subseteq L \subseteq E$ is separable over F.*

Observe that a nonconstant $f \in F[X]$ is separable if and only if it factors into distinct (nonassociate) separable irreducible polynomials. This observation helps justify the following:

Lemma 34. *Let F be a field, and let $L = F[\alpha_1, \ldots, \alpha_n]$ where the minimal polynomial of each α_i in $F[X]$ is separable. Then L is contained in a finite Galois extension of F, and so L is separable.*

Putting these lemmas together (together with the primitive element theorem) yields the following:

Proposition 35. *Let L be a finite extension of F. The following are equivalent.*

1. *L is separable over F.*
2. *L is contained in a finite Galois extension of F.*
3. *$L = F[\alpha]$ where the minimal polynomial of α in $F[X]$ is separable.*

Of course the following is obvious from our definitions:

Proposition 36. *Every algebraic extension of a perfect field is separable.*

Worksheet 7: The fundamental theorem of Galois theory

We are almost ready for the fundamental theorem. There is one last piece to the puzzle: we need to establish that every subgroup of a Galois group is itself a Galois group of an intermediate field. Observe that if H is a subgroup of $G = \mathrm{Gal}(E/F)$ where E is a finite Galois extension of F, then $H \subseteq \mathrm{Gal}(E/E^H)$; we need to show this inclusion is an equality.

The primitive element theorem helps here. Let $\alpha \in E$ be such that $E = F[\alpha]$. Consider the following polynomial

$$g \stackrel{\text{def}}{=} \prod_{\sigma \in H} \big(X - \sigma(\alpha)\big).$$

Observe that $g \in E^H[X]$. Comparing with the minimal polynomial formula, established earlier, we see that g divides the minimal polynomial of α over E^H, hence g

is the minimal polynomial of α over E^H. The degree of g is both $|H|$ and $[E : E^H]$. This is enough to show that H is the full galois group $\mathrm{Gal}(E/E^H)$. So we have the following:

Proposition 37. *Let E be a finite Galois extension of F with Galois group G. Then every subgroup of G is itself a Galois group. More specifically, if H is a subgroup of G, then $H = \mathrm{Gal}\big(E/E^H\big)$. In other words, $G_{E^H} = H$.*

Here we are using the notation of G_L for $\mathrm{Gal}(E/L)$, where L is an intermediate field between F and E. The above proposition complements the following corollary of Theorem 21:

Corollary 38. *Let E be a finite Galois extension of F with Galois group G. If L is an intermediate field between F and E then Then $E^{G_L} = L$.*

Let $G = \mathrm{Gal}(E/F)$ where F is a finite Galois extension of F. We now consider two maps. The first is $H \mapsto E^H$ which maps subgroups of G to intermediate fields E^H between F and E. The second is $L \mapsto G_L$ which maps intermediate fields between F and E to subgroups of G. The above proposition and corollary show these are inverses. Both maps are clearly inclusion reversing. So we get the following:

Theorem 39 (Galois Correspondence)**.** *Let E be a finite Galois extension of F with Galois group G. There is an inclusion reversing bijection between (i) the set of subgroups of G and (ii) the set of intermediate fields L between F and E. The bijection from (i) to (ii) sends a subgroup H to E^H. The inverse bijection from (ii) to (i), which is also inclusion reversing, sends an intermediate field L to G_L.*

Next we consider this correspondence when H is a normal subgroup of the Galois group $G = \mathrm{Gal}(E/F)$ where E is a finite Galois extension of F. The first observation is that if $\beta \in E^H$ where H is a normal subgroup, then all the G-conjugates of β are in E^H. From this we argue that E^H is Galois over F. Conversely, H is a subgroup of G such that E^H is Galois over F, we can show that we get a restriction homomorphism $G \to \mathrm{Gal}\big(E^H/F\big)$ that is surjective with kernel H. So H is normal and G/H is isomorphic to $\mathrm{Gal}\big(E^H/F\big)$. This gives us the last part of the fundamental theorem of Galois theory:

Theorem 40 (Galois Correspondence, Part 2)**.** *Under the bijections of the previous theorem, normal subgroups of G correspond to Galois extensions of F (contained in E). If H is a normal subgroup of G and E^H is Galois over F, then*

$$\mathrm{Gal}\Big(E^H/F\Big) \cong G/H.$$

Worksheet 8: Automorphisms groups of fields

We spend one last worksheet on the basic theory. Here we consider a field E and a finite subgroup G of $\mathrm{Aut}(E)$ where $\mathrm{Aut}(E)$ is the group of automorphisms of E. (As we will see, $\mathrm{Aut}(E)$ itself can contain elements of infinite order, and so can be an infinite group).

Given such a finite subgroup G of $\mathrm{Aut}(E)$, we let $F = E^G$ be the fixed field. Unlike before where we started with F and constructed E as an extension, here we start with E and then define F as a subfield. So I call the current approach the "top-down" approach. Using the techniques and results of the previous worksheets we can prove the following:

Theorem 41. *Let E be a field. Let G be a finite subgroup of the automorphism group of E. Then E is a finite Galois extension of $F = E^G$ with Galois group G.*

Next we apply this theorem to finite extensions E of F that are not necessarily Galois. Let $\mathrm{Aut}(E/F)$ be the group of automorphisms of E that fix the subfield F. We start by arguing that $G = \mathrm{Aut}(E/F)$ is a finite subgroup of $\mathrm{Aut}(E)$, so we can apply the above theorem. Then E^G is an intermediate field between F and E. By the above theorem $[E : E^G] = |G|$. This gives us the following:

Lemma 42. *Let E be a finite extension of F. Then the size of $\mathrm{Aut}(E/F)$ divides the degree $[E : F]$, and is equal to $[E : F]$ if and only if $E^G = F$.*

We now consider the common viewpoint that a Galois extension is one where the number of automorphisms are as large as possible.

Definition 13. Let E be a finite extension of F. If the number of automorphisms of E fixing F is $[E : F]$ then we say that E is *numerically Galois* over F.

The above results gives us what we need to prove the following:

Proposition 43. *Suppose that E is a finite extension of F. Then E is numerically Galois over F if and only if E is Galois over F.*

The worksheet ends with a few examples. These assume familiarity with the field of fractions of an integral domain. Here $K(X)$ denotes the field of fractions of $K[X]$ (where K is a field). The following is used in the examples:

Fact. *Suppose R is an integral domain, and that F is a field. Then any injective ring homomorphism $R \to F$ extends uniquely to a homomorphism from the field of fractions of R to F.*

Example 6. Consider the evaluation homomorphism $K[X] \to K[X]$ which sends X to $X - 1$, and where K is a field. This extends to an automorphism σ of $K(X)$. If the field K is infinite, then σ has infinite order in $\mathrm{Aut}(K(X))$.

Example 7. Let K be a field containing an element $\zeta \neq 1$ such that $\zeta^3 = 1$. Consider the evaluation homomorphism $K[X] \to K[X]$ which sends X to ζX. This extends to an automorphism of $K(X)$ of order 3. Let G be the subgroup of $\mathrm{Aut}(K(X))$ generated by this automorphism. Observe that $X^3 \in K(X)^G$ and that X satisfies a cubic equation with coefficients in $K(X^3)$. We conclude that

$$K(X)^G = K(X^3).$$

Example 8. 9. Consider the evaluation homomorphism $K[X] \to K(X)$ which sends X to $1/X$ where K is a field. This extends to an automorphism of $K(X)$ of order 2. Let G be the subgroup of $\mathrm{Aut}(K(X))$ generated by this automorphism. Observe that $X + X^{-1} \in K(X)^G$ and that X satisfies a quadratic equation with coefficients in $K(X + X^{-1})$. We conclude that $K(X)^G = K\big(X + X^{-1}\big)$.

Worksheet 9: Cyclotomic extensions and polynomials

This and the next worksheet are devoted to nth cyclotomic extensions and the associated cyclotomic polynomials. We will typically assume that the characteristic of the base field does not divide n. (This assumption, for example, holds in characteristic zero).

Definition 14. Roots of $X^n - 1$ in a field E are called *nth roots of unity.* If an nth root of unity has multiplicative order exactly n then it is called a *primitive nth root of unity.*

Definition 15. The *nth cyclotomic extension of a field F* is the splitting field of $X^n - 1$ over F. Let μ_n be the multiplicative group of n roots of unity in the nth cyclotomic extension of F.

Technically μ_n depends on the choice of the splitting field of $X^n - 1$. If we work in a given algebraic closure of F then μ_n and the nth cyclotomic extension are unique; in general, they are unique up to isomorphism.

We assume the reader is comfortable with finite cyclic groups, and the following fact:

Fact. *If F is a field, then any finite subgroup of $F^\times$ is cyclic. If C is a cyclic group of order n then there are $\phi(n)$ elements which generate C where $\phi(n)$ is the Euler phi function. In fact, if $g \in C$ is a generator, then g^k (in multiplicative notation) is a generator if and only if k is relatively prime to n.*

For the remainder of this section (and Worksheet 9) assume that F is a field (the base field). Let n be a positive integer not divisible by the characteristic of F. (For example, this holds in characteristic zero). Under these assumptions $X^n - 1$ and its derivate nX^{n-1} are relatively prime, so $X^n - 1$ is separable. This means that the nth cyclotomic extension is a Galois extension of F, and μ_n is a cyclic group of order n. There are $\phi(n)$ primitive nth roots of unity.

Let E be the nth cyclotomic extension, and let ζ_n be a primitive nth root of unity. Observe that $E = F[\zeta_n]$. Let G be the Galois group of E over F. Any $\sigma \in G$ is characterized by the image $\sigma\zeta_n$, and we can show that $\sigma\zeta_n$ must also be a primitive nth root of unity. Thus $\sigma\zeta_n = \zeta_n^{m(\sigma)}$ where $m(\sigma)$ is an integer relatively prime to n, and is uniquely determined modulo n. In other words, we can think of $m(\sigma)$ as an element of $(\mathbb{Z}/n\mathbb{Z})^\times$. We are able to prove the following:

Proposition 44. *Let $\sigma \mapsto m(\sigma)$ be the map $G \to (\mathbb{Z}/n\mathbb{Z})^\times$ described above. This map is a an injective homomorphism. Furthermore, $\sigma\alpha = \alpha^{m(\sigma)}$ for all $\alpha \in \mu_n$. In particular, this homomorphism is independent of choice of primitive nth root of unity ζ_n. Therefore, G can be naturally identified with a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, and the order $|G| = [E : F]$ divides $\phi(n)$.*

In particular, the Galois group G must be abelian.

Now we consider the important class of cyclotomic polynomials. Let μ_n' be the set of primitive nth roots of unity. Then we define the nth cyclotomic polynomial to be

$$\Phi_F(n) \stackrel{\text{def}}{=} \prod_{\alpha \in \mu_n'} (X - \alpha).$$

The coefficients are invariant under G, so it a polynomial in $F[x]$ of degree $\phi(n)$. Observe that the the minimal polynomial of ζ_n divides $\Phi_F(n)$. When we write $\Phi(n)$, we mean $\Phi_{\mathbb{Q}}(n)$. We call $\Phi(n)$ the *nth cyclotomic polynomial*, and $\Phi_F(n)$ the *nth cyclotomic polynomial relative to* F. (Note: these polynomials do not depend on the choice of splitting field of $X^n - 1$ since such splitting fields are isomorphic with an isomorphism fixing F).

For each positive divisor d of n we can choose the dth cyclotomic field to be a subfield of the given nth cyclotomic field E. Observe that we can factor $X^n - 1$ in $F[X]$ as follows:

$$X^n - 1 = \prod_{d|n} \Phi_F(d).$$

We can use this as a recursive formula for calculating cyclotomic polynomials. Clearly $\Phi(1) = X - 1$. So $\Phi(2) = X + 1$, and $\Phi(3) = X^2 + X + 1$, and $\Phi(4) = X^2 + 1$, and $\Phi(5) = X^4 + X^3 + X^2 + X + 1$, and $\Phi(6) = X^2 - X + 1$, and

$$\Phi(7) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

and $\Phi(8) = X^4 + 1$, and $\Phi(9) = X^6 + X^3 + 1$, and $\Phi(10) = X^4 - X^3 + X^2 - X + 1$. For any prime p

$$\Phi(p) = X^{p-1} + X^{p-2} + \ldots + X + 1.$$

There are other interesting formulas and relationships for cyclotomic polynomials, but we will skip these and focus mainly on showing that each $\Phi(n)$ is irreducible in $\mathbb{Q}[X]$.

If F contains $\mathbb{Q}$ (so has characteristic zero), then the above recursion formula can be used to prove that $\Phi_F(n) = \Phi(n)$ (this can also be proved using the formula by working with subfields of a fixed splitting field of $X^n - 1$ over F).

Since $\Phi(n)$ is monic and divides $X^n - 1$, which is a monic polynomial in $\mathbb{Z}[X]$, we conclude that $\Phi(n) \in \mathbb{Z}[X]$. If F contains $\mathbb{F}_p$ (so has characteristic p), then the above recursion formula can be used to prove that $\Phi_F(n)$ is obtained by reducing the coefficients of $\Phi(n)$ modulo p, and so $\Phi_F(n) = \Phi_{\mathbb{F}_p}(n) \in \mathbb{F}_p[X]$.

The above fact, and the following proposition requires some knowledge of the polynomial ring $\mathbb{Z}[X]$.[5] In particular

- If a monic polynomial $g \in \mathbb{Q}[X]$ divides $X^n - 1$, or divides any monic polynomial in $\mathbb{Z}[X]$, then $g \in \mathbb{Z}[X]$.
- The ring $\mathbb{Z}[X]$ is a UFD. Every nonzero element of $\mathbb{Z}[X]$ factors as ± 1 times the product of primes in $\mathbb{Z}$ times the product of irreducible primitive polynomials. (This factorization is unique up to order and sign).
- If f and g in $\mathbb{Z}[X]$ are both primitive polynomials (such as monic polynomials), and if they are associates in $\mathbb{Q}[X]$, then $f = \pm g$.

Since our goal is to show that each $\Phi(n)$ is irreducible in $\mathbb{Q}[X]$, we consider the monic minimal polynomial $f \in \mathbb{Q}[X]$ of ζ_n in the case where $F = \mathbb{Q}$. So f divides $\Phi(n)$. Our goal is to show that $f = \Phi(n)$. Since f is monic and divides the

[5] This is covered in my essay, *Minimal, Primitive, and Irreducible Polynomials* (2010, updated 2019).

polynomial $X^n - 1$ we know that $f \in \mathbb{Z}[X]$, and f is in fact an irreducible primitive polynomial.

If $g \in \mathbb{Z}[X]$ has the property that $g(\zeta_n) = 0$, then f divides g in $\mathbb{Q}[X]$. When we factor g in $\mathbb{Z}[X]$, then f must be an associate in $\mathbb{Q}[X]$ to one of the irreducible principle factors of g. Thus f is (up to sign) a factor of g by the fact quoted above. From this we conclude that the kernel of the evaluation map $\mathbb{Z}[X] \to \mathbb{Z}[\zeta_n]$ sending g to $g(\zeta_n)$ is the ideal $\langle f \rangle$. Thus we get the following.

Proposition 45. *There is an isomorphism*

$$\mathbb{Z}[X]/\langle f \rangle \cong \mathbb{Z}[\zeta_n].$$

fixing $\mathbb{Z}$ and sending the coset $\overline{X}$ to ζ^n.

Worksheet 10: Irreducibility of cyclotomic polynomials

Next we show that the nth cyclotomic polynomial $\Phi(n)$ is irreducible in $\mathbb{Q}[X]$, and use this fact to describe the Galois theory of the nth cyclotomic extension.

Let E be the nth cyclotomic extension of $\mathbb{Q}$, and let μ_n be the nth roots of unity. Let ζ_n be a fixed generator of the cyclic group μ_n, and let $f \in \mathbb{Q}[X]$ be the (monic) minimal polynomial of ζ_n.

We start by fixing a prime p not dividing n in order to define a pth reduction map on the ring $\mathbb{Z}[\zeta_n]$. Let $\overline{E}$ be the nth cyclotomic extension of $\mathbb{F}_p$. Let $\overline{\mu}_n$ be the nth roots of unity in $\overline{E}$.

Let $\pi : \mathbb{Z} \to \mathbb{F}_p$ be the reduction homomorphism. Recall that π extends to a homomorphism $\pi_X : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ which takes a polynomial and reduces its coefficents modulo p. Of course f divides $\Phi(n)$ in $\mathbb{Q}[X]$. Properties of primitive polynomials allows us to write $\Phi(n) = fg$ where $g \in \mathbb{Z}[X]$. Thus $\Phi_{\mathbb{F}_p}(n) = \overline{f}\overline{g}$ where $\overline{f} = \pi_X f$ and $\overline{g} = \pi_X g$. Let $\overline{\zeta}_n$ be a choice of root of $\overline{f}$ in $\overline{E}$. Observe that $\overline{\zeta}_n$ is a primitive nth root of unity in $\overline{E}$.

If we compose $\pi_X : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ with the evaluation map $\mathbb{F}_p[X] \to \mathbb{F}_p\big[\,\overline{\zeta}_n\big]$ sending X to $\overline{\zeta}_n$, we get a homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p\big[\,\overline{\zeta}_n\big]$ which sends X to $\overline{\zeta_n}$ and sends any $a \in \mathbb{Z}$ to its image in $\mathbb{F}_p$. Since f is in the kernel of this map, We get a map $\mathbb{Z}[X]/\langle f \rangle \to \mathbb{F}_p\big[\,\overline{\zeta}_n\big]$. Composing with the map of Proposition 45, we get a homomorphism $\mathbb{Z}[\zeta_n] \to \mathbb{F}_p\big[\,\overline{\zeta}_n\big]$ with $\zeta_n \mapsto \overline{\zeta}_n$. Call this map the *$p$ reduction map*. If $\alpha \in \mathbb{Z}[\zeta_n]$ then we write $\overline{\alpha}$ for its image in $\mathbb{F}_p\big[\,\overline{\zeta}_n\big]$.

The pth reduction map induces an isomorphism $\mu_n \to \overline{\mu}_n$. Furthermore it induces a bijection between roots of f and roots of $\overline{f}$. Using the Frobenius automorphism $x \mapsto x^p$, we know that if α is a root of a polynomial in $\mathbb{F}_p[X]$, then so is α^p. Using the pth reduction map, we have a similar property for f:

Lemma 46. *Let n, E and f be as above. For all primes p not dividing n, if $\alpha \in E$ is a root of f then so is α^p.*

By using the above with possibly different primes p we get the following:

Corollary 47. *Let n, ζ_n and f be as above. For all k relatively prime to n, the kth power ζ_n^k is a root of f.*

Corollary 48. *Let n and f be as above. Then $f = \Phi(n)$.*

This yields a major theorem and corollary:

Theorem 49. *The nth cyclotomic polynomial $\Phi(n)$ is irreducible in $\mathbb{Q}[X]$.*

Corollary 50. *The nth cyclotomic extension E of $\mathbb{Q}$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Hence $[E : \mathbb{Q}] = \phi(n)$.*

Because of Galois theory, we can describe all the intermediate fields between $\mathbb{Q}$ and the nth cyclotomic extension. For example, if $n = q$ is a prime, we know that the Galois group $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic of order $q-1$, so we get the following particularly simple situation:

Corollary 51. *Suppose E is the qth cyclotomic extension of $\mathbb{Q}$ where q is a prime. If L is a field intermediate between $\mathbb{Q}$ and E, then $[L : \mathbb{Q}]$ divides $q - 1$. For every divisor d of $q-1$ there is a unique intermediate extension L_d with $[L_d : \mathbb{Q}] = d$. The field L_d is Galois over $\mathbb{Q}$ with Galois group cyclic of order d. For such divisors d, d', the field L_d is contained in $L_{d'}$ if and only if $d|d'$.*

In particular, the qth cyclotomic extension of $\mathbb{Q}$ contains a unique quadratic extension. But what is this extension? The next worksheet addresses this question. To prepare for this investigation, we now establish a few basic tools for quadratic extensions.

So let E be a quadratic (degree 2) extension of a field F. Assume that the characteristic of F is not 2. The extension E must then be Galois over F with Galois group of size two. If $\beta \in E$ then write $\overline{\beta}$ for $\sigma\beta$ where σ is the nonidentity element of the Galois group.

If $\beta \in E$ but not in F, then $E = F[\beta]$. To get a square-root type generator, consider $\delta = \beta - \overline{\beta}$. Then $\overline{\delta} = -\delta$. Here $\delta \neq 0$ must be another generator with minimal polynomial $(X - \delta)(X + \delta) = X^2 - \delta^2$. So $d = \delta^2 \in F$, and $E = F[\delta]$. We write δ as $\sqrt{d}$ (although, really d has two square roots in E, which differ by a sign), and we write E as $F[\sqrt{d}]$. Observe that

$$\overline{a + b\sqrt{d}} = a - b\sqrt{d}$$

for any $a, b \in F$.

In the above, we can replace d with dx^2 for any nonzero $x \in F$ (and replace β and δ by βx and δx). In particular, if $F = \mathbb{Q}$ we can replace d with a unique square-free integer $d \neq 1$. If $d > 0$ then E is called a *real quadratic field* and we take the positive square root as the standard generator; if $d < 0$ then E is called an *imaginary quadratic field*.

Worksheet 11: Quadratic generator (Gauss sum formula)

Suppose you have a finite Galois extension E of F with Galois group G, and suppose you are interested in a particular quadratic extension of F contained in E. This corresponds to a subgroup H of G of index 2, and E^H will be the quadratic extension of F. We want to use the ideas mentioned at the end of the previous worksheet to

find an element $d \in F$ whose square root generates E^H over F. As above, we will assume that the characteristic of F is not 2.

Above we started with an element β in the quadratic extension (here E^H). Here we take the point of view that we do not start with elements of E^H, but only with certain elements of E. We need to find a suitable element of E^H from elements of E. There is an averaging trick to get elements of E^H. If $\alpha \in E$ then consider the average of its H-conjugates

$$\frac{1}{|H|} \sum_{\sigma \in H} \sigma\alpha.$$

This is necessarily fixed by H, so is in E^H. Since dividing by $|H|$ does not change the field of an element, and since dividing by an integer might creates problems in finite characteristic, we just consider

$$\beta = \sum_{\sigma \in H} \sigma\alpha.$$

Giving us an element $\beta \in E^H$. (Note: this "trace" idea works for any subgroup of H, not just index 2 subgroups).

Let α, β be as above. Since E^H is quadratic, we have a conjugate $\overline{\beta} \in E^H$. If $\tau \in G$ is not in H, then its restriction to E^H will not be the identity. So the conjugate of β in E^H is $\tau\beta$. Thus

$$\overline{\beta} = \tau \left(\sum_{\gamma \in H} \gamma\alpha \right) = \sum_{\gamma \in H} \tau\gamma\alpha = \sum_{\sigma \in \tau H} \sigma\alpha = \sum_{\sigma \notin H} \sigma\alpha.$$

Recall we formed $\delta = \beta - \overline{\beta}$, which satisfies $\overline{\delta} = -\delta$. In this case we get

$$\delta = \beta - \overline{\beta} = \sum_{\sigma \in H} \sigma\alpha - \sum_{\sigma \notin H} \sigma\alpha = \sum_{\sigma \in G} \chi(\sigma)\sigma\alpha$$

where $\chi : G \to \{\pm 1\}$ is as defined as follows:

Definition 16. The *quadratic character* $\chi : G \to \{\pm 1\}$ associated to H is the map defined by the rule $\chi(\sigma) = 1$ if $\sigma \in H$ and $\chi(\sigma) = -1$ if $\sigma \notin H$.

This quadratic character χ is actually a surjective group homomorphism from G to the group $\{\pm 1\} \subseteq F^\times$.

Recall that the desired $d \in F$ is δ^2. More precisely, if $\beta \notin F$, or equivalently if $\delta \neq 0$, then $d = \delta^2 \in F$ and $E^H = F[\delta]$. From the formula for δ we get the following formula for d:

$$d = \sum_{\sigma, \tau \in G} \chi(\sigma\tau)(\sigma\alpha)(\tau\alpha).$$

If $d \neq 0$ then we have $E^H = F[\sqrt{d}\,]$.

We are particularly interested in the unique quadratic extension of $\mathbb{Q}$ contained in the qth cyclotomic extension (call it E) of $\mathbb{Q}$ where q is an odd prime numbers. It turns out that identifying this will lead to a proof of the famous quadratic

reciprocity theorem. We will use the formula above to find a d whose square root generates the this quadratic extension.

To do this, let $\alpha = \zeta$ be a primitive qth root of unity in E. We identify the Galois group G of E over $\mathbb{Q}$ with the cyclic group $(\mathbb{Z}/q\mathbb{Z})^\times$. Note that the unique subgroup H of index 2 is the subgroup of squares in $(\mathbb{Z}/q\mathbb{Z})^\times$. Such squares are often called "quadratic residues" (think of "residue" as an old fashion term for remainder, here upon division by q, and think of "quadratic" as meaning square). Half the elements of G are quadratic residues in H, and the other half (in the other coset of H) are not quadratic residues.

Recall that the element of G corresponding to $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ takes ζ to ζ^k. Thus the above formula for d becomes

$$d = \sum_{\sigma,\tau\in G} \chi(\sigma\tau)(\sigma\zeta)(\tau\zeta) = \sum_{k,l\in(\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right)\zeta^k\zeta^l = \sum_{k,l\in(\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right)\zeta^{k+l}.$$

Here we use the Legendre symbol

$$\left(\frac{a}{q}\right) = \begin{cases} +1 & \text{if } a \text{ is a nonzero square modulo } q \\ -1 & \text{if } a \text{ is not a square modulo } q \\ 0 & \text{if } q \text{ divides } a \end{cases}$$

It is just the quadratic character of G associated to the H in our current situation. So have the following:

Lemma 52. *Let E be the qth cyclotomic extension of $\mathbb{Q}$ where q is an odd prime. Let ζ be a primitive qth root of unity. Let*

$$d \stackrel{\text{def}}{=} \sum_{k,l\in(\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{kl}{q}\right)\zeta^{k+l}.$$

Then d is in $\mathbb{Q}$. Furthermore, if $d \neq 0$ then $\mathbb{Q}[\sqrt{d}]$ is the unique quadratic extension of $\mathbb{Q}$ contained in E.

We will calculate the d in the next worksheet, and find out that d is not zero.

Remark. In this field δ is given by the formula

$$\delta = \sum_{\sigma\in G} \chi(\sigma)\sigma\alpha = \sum_{k\in(\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{k}{q}\right)\zeta^k.$$

Note that δ is in the ring $\mathbb{Z}[\zeta]$. The rightmost summation is called a *Gauss sum*, and the formula for d in the above lemma is a formula for the square of this Gauss sum. Gauss sums are used in proofs of quadratic reciprocity, including the proof below since our proof is based on the computation of d.

Worksheet 12: Quadratic reciprocity

The next big goal is to prove quadratic reciprocity. As a preliminary step, we calculate the d whose formula was given in Lemma 52. The worksheet guides the

reader through one way to do the calculation, and the results is

$$d = \left(\frac{-1}{q}\right) q.$$

This yields the following theorem:

Theorem 53. *Let E be the qth cyclotomic extension of $\mathbb{Q}$ where q is an odd prime. Define $*q = \left(\frac{-1}{q}\right) q$. Then $\mathbb{Q}\big[\sqrt{*q}\big]$ is the unique quadratic extension of $\mathbb{Q}$ contained in E. Furthermore, $\sqrt{*q}$ is in the ring $\mathbb{Z}[\zeta]$ where ζ is a primitive qth root of unity.*

Our proof of the quadratic reciprocity law is based on the pth reduction map from Worksheet 10. Specifically we will investigate whether or not $\sqrt{*q}$ lands in $\mathbb{F}_p$ under this map $\mathbb{Z}[\zeta] \to \mathbb{F}_p\big[\,\overline{\zeta}\,\big]$, or in an extension of $\mathbb{F}_p$. Here, as before, E is the qth cyclotomic extension where q is an odd prime and $p \neq q$ is any other odd prime. Here ζ be a primitive qth root of unity. If $\alpha \in \mathbb{Z}[\zeta]$, let $\overline{\alpha} \in \mathbb{F}_p[\overline{\zeta}]$ be the image under the pth reduction map (where $\overline{\zeta}$ is a qth root of unity in characteristic p as in Worksheet 10).

To determine if a given $\alpha \in \mathbb{Z}[\zeta]$ maps to an element of $\mathbb{F}_p$, we just see if the image $\overline{\alpha}$ is fixed by the Frobenius automorphism $x \mapsto x^p$. We identify the Galois group G of E over $\mathbb{Q}$ with $(\mathbb{Z}/q\mathbb{Z})^\times$, and there is an element $\sigma_p \in G$ which maps α to α^p if α is a qth root of unity. Of course $\sigma_p(\alpha) = \alpha^p$ does not hold for all $\alpha \in E$. However, we can show that if $\alpha \in \mathbb{Z}[\zeta]$ then $\overline{\sigma_p \alpha} = \overline{\alpha}^p$. So σ_p does induce the Frobenius automorphism.

There are two cases to consider. First consider the case where p is a square modulo q. This means that σ_p is in the subgroup H of index two in G. In particular $\sqrt{*q}$ is fixed by σ_p. This means that image $\overline{\sqrt{*q}}$ in $\mathbb{F}_p[\overline{\zeta}\,]$ is fixed by the Frobenius automorphism, hence is in $\mathbb{F}_p$ itself. Thus $*q$ is a square modulo p.

The second case is where p is not a square modulo q. This means that σ_p is not in the subgroup H of index two in G. In particular $\sqrt{*q}$ is sent to $-\sqrt{*q}$ under σ_p. This means that image $\overline{\sqrt{*q}}$ in $\mathbb{F}_p[\overline{\zeta}\,]$ is not fixed by the Frobenius automorphism, hence cannot be in $\mathbb{F}_p$ itself. Observe that $*q$ cannot be a square modulo p since the roots of $X^p - \overline{*q}$ are outside $\mathbb{F}_p$.

We can combine the two cases into the following equation of Legendre symbols.

$$\left(\frac{p}{q}\right) = \left(\frac{*q}{p}\right).$$

Finally, we note that -1 is a square modulo q if and only if $q \equiv 1$ modulo 4, because $(\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $q-1$. A similar statement holds for -1 modulo p. From this we can derive Gauss's famous law:

Theorem 54 (Quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

Worksheet 13: Ruler and compass constructions (part 1)

In this and the next worksheet we apply Galois theory to ruler and compass constructions. This handout specifically concerns the impossibility of squaring the circle and duplicating the cube. It takes the following fact as given:

Fact. *The number π is transcendental.*

We lay the groundwork with a few definitions:

Definition 17. Let F be a subfield of $\mathbb{R}$. A point (a, b) of $\mathbb{R}^2$ is called *F-rational* if $a, b \in F$. A line of $\mathbb{R}^2$ is said to be *generated* by two distinct points (a, b) and (c, d) if it contains the two points. A circle of $\mathbb{R}^2$ is said to be *generated* by $(a, b), (c, d)$ and (e, f) if has center (a, b) and radius equal to the distance from (c, d) to (e, f). (Here we assume that (c, d) and (e, f) are distinct).

Definition 18. Let S be a set of points of $\mathbb{R}^2$. Let $RC^1(S)$ be the set consisting of S together with any point (a, b) which is the point of intersection of (distinct) curves C_1 and C_2 where C_i is either a line generated by two points of S or a circle generated by three points of S.

Let $RC^2(S)$ be $RC^1(RC^1(S))$, let $RC^{n+1} = RC^1(RC^n(S))$. Let $RC(S)$ be the union of the sets $RC^n(S)$.

Definition 19. A point is said to be *constructible* if it is in $RC(S)$ where S is the set $\{(0, 0), (1, 0)\}$. A line generated by constructible points is said to be a *constructible line*. A circle generated by constructible points is said to be a *constructible circle*. Let $\mathbb{E}$ be the set of all $a \in \mathbb{R}$ that occur as a coordinate of a constructible point.

We begin by looking at the algebraic equations for lines and circles generated by F-rational points where F is a subfield of $\mathbb{R}$. We look at the points of intersection of two such curves, and conclude that the coordinates of the intersection points are in F or in a quadratic extension of F. This leads to the following:

Proposition 55. *If (a, b) is constructible, then then there is a sequence F_i of subfields of $\mathbb{R}$ such that*

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_{n-1} \subsetneq F_n,$$

such that each $[F_{i+1} : F_i] = 2$, and such that $a, b \in F_n$.

Corollary 56. *If $a \in \mathbb{E}$ then a is algebraic and $[\mathbb{Q}[a] : \mathbb{Q}]$ is a power of two.*

Corollary 57. *The number $2^{1/3}$ is not in $\mathbb{E}$. No transcendental number is in $\mathbb{E}$.*

The problem of duplicating the unit cube is to find two constructible points P and Q such that PQ has length a, where a is the length of the side of a cube with volume 2. If we could do so, we could construct the point $(2^{1/3}, 0)$, and $2^{1/3}$ would have to be in E. Thus

Corollary 58. *The problem of duplicating the cube, as described here, has no solution.*

The problem of squaring the unit circle, say, is to find two constructible points P and Q such that PQ has length a, where a is the length of the side of a square with area equal to that of the unit circle. If we could do so, we could construct the point $(\pi^{1/2}, 0)$. But $\pi^{1/2}$ is transcendental (if it were algebraic, then its square π would be algebraic).

Corollary 59. *The problem of squaring the circle, as described here, has no solution.*

Worksheet 14: Ruler and compass constructions (part 2)

Our next goal is to describe the field $\mathbb{E} \subseteq \mathbb{R}$ of constructible coordinates. We will then regard the set of constructible points as a subfield of $\mathbb{C}$, and describe this field. This worksheet builds on our knowledge of cyclotomic fields, and assumes some familiarity with the Euler ϕ-function.

Recall that $\mathbb{E}$ is defined to be the set of real numbers that occur as a coordinate of a constructible point. In other words, if (a, b) is constructible, then $a, b \in \mathbb{E}$. With some basic constructions we can extend this to a biconditional: (a, b) is constructible if and only if both a and b are in $\mathbb{E}$. By definition of constructible, we have $0, 1 \in \mathbb{E}$. We can then prove various closure laws giving us the following:

Proposition 60. *The set $\mathbb{E}$ is a subfield field of $\mathbb{R}$.*

Actually $\mathbb{E}$ is a subfield of the algebraic closure $\overline{\mathbb{Q}}$ since every element of $\mathbb{E}$ is algebraic. The closure under addition and additive inverse are straightforward. To see closure under multiplication and division, suppose $a, b \in \mathbb{E}$ with $a \neq 0$. Then construct the point $(1, a)$, and let ℓ be the line through $(0, 0)$ and $(1, a)$. Now intersect this line with the lines defined by $x = b$ and $y = 1$. This allows us to construct (b, ab) and $(1/a, 1)$. Thus $ab \in \mathbb{E}$ and $1/a \in \mathbb{E}$.

Suppose $a > 0$ is in $\mathbb{E}$. Then the circle with center $(0, 0)$ and radius $r = (a+1)/2$ is constructible. By intersecting this with the constructible line $x = (a - 1)/2$, we see that $a^{1/2}$ is in $\mathbb{E}$. Thus we have the following:

Proposition 61. *The field $\mathbb{E}$ is closed under square roots of nonnegative elements.*

This allows us to strengthen Proposition 55:

Proposition 62. *Let $a \in \mathbb{R}$. Then $a \in \mathbb{E}$ if and only if there is a sequence F_i of subfields of $\mathbb{R}$ such that*

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_{n-1} \subsetneq F_n,$$

such that each $[F_{i+1} : F_i] = 2$, and such that $a \in F_n$.

Now we will identify a point (a, b) with $a + bi \in \mathbb{C}$. We say $\alpha = a + bi$ is *constructible* if and only if (a, b) is constructible.

Proposition 63. *The point (a, b) is constructible if and only if $a + bi \in \mathbb{E}[i]$.*

Using angle bisection, we can show that if $\alpha \in \mathbb{C}$ is constructible then so its square root. We can then prove the complex analogue of Proposition 62:

Theorem 64. *Suppose $\alpha = a + bi \in \mathbb{C}$ where $a, b \in \mathbb{R}$. Then (a, b) is constructible if and only if there is a sequence of subfields of $\mathbb{C}$*

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_{n-1} \subsetneq F_n,$$

such that each $[F_{i+1} : F_i] = 2$, and such that $\alpha \in F_n$.

Corollary 65. *If $\alpha \in \mathbb{E}[i]$ then α is algebraic and the degree $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ is a power of two.*

Which primitive nth roots of unity are constructible? If ζ_n is a primitive nth root of unity is constructible, then $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$. Thus a necessary condition is that $\phi(n)$ be a power of two by the above corollary. On the other hand, if $\phi(n)$ is a power of two, then the Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group of order equal to a power of two. In such a group it is easy to prove there is an element of order 2, and so a normal subgroup of order 2. We look at the quotient of the group by this normal subgroup, and fix a normal subgroup of order 2 in the quotient. We iterate this process. This process gives us a sequence of subgroups

$$\{1\} = H_0 \subsetneq H_1 \subsetneq \cdots \subsetneq H_k = (\mathbb{Z}/n\mathbb{Z})^\times$$

where each $[H_{i-1} : H_i] = 2$. By the Galois correspondence, we get a sequence of fields

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_{k-1} \subsetneq F_k = \mathbb{Q}[\zeta_n].$$

Thus ζ_n is constructible, and must be in $\mathbb{E}[i]$.

Theorem 66. *A primitive nth root of unity in $\mathbb{C}$ is in $\mathbb{E}[i]$ if and only if $\phi(n)$ is a power of two.*

Clearly if a primitive nth root of unity is in $\mathbb{E}[i]$. then we can construct a regular n-gon. Conversely, if you can construct the vertices of a regular n-gon, you can construct the center. This would give you elements of $\mathbb{E}[i]$ whose ratio is a primitive nth root of unity. Thus we have the following:

Theorem 67. *A regular n-gon is constructible if and only if $\phi(n)$ is a power of two.*

These results are due to Gauss. At a young age he showed that the 17-gon was constructible (where $\phi(17) = 16 = 2^4$). The fact that the triangle and pentagon are constructible was known to the ancient Greeks.

Of course, when we say that a polygon is constructible, we mean that the vertices are constructible. Similarly, when we say that an angle is constructible, we mean that the vertex and at least one point on each side is constructible. Since $\zeta_6 \in \mathbb{E}[i]$, we can construct a 60-degree angle.

However, we cannot construct a 20-degree angle. For if we could, we could use the constructible points on that angle to show that ζ_{18} is in $\mathbb{E}[i]$. But $\phi(18) = 6$, which is not a power of two.

Theorem 68. *One can construct a 60-degree angle. However, 20-degree angles are not constructible. Thus there are constructible angles that cannot be trisected with ruler and compass.*

Finally, we point out that one can describe all n such that $\phi(n)$ is a power of two in terms of Fermat primes. Fermat primes are primes of the form $2^n + 1$. We leave the details to the reader (this requires some basic properties of $\phi(n)$).

Worksheet 15: The Galois theory of finite fields

Now we consider the Galois theory of finite fields. We take the following as given:

Fact. *Every finite field has characteristic p for some prime p, and has a subfield canonically isomorphic to $\mathbb{F}_p$. So we regard every finite field of characteristic p as a finite extension of $\mathbb{F}_p$.*

If F is a field with q elements, then every element of $F^\times$ is a root of $X^{q-1} - 1$ (by Lagrange's theorem). In other words, every element of F is a root of $X^q - X$, and the polynomials $X^{q-1} - 1$ and $X^q - X$ are seen to split in $F[X]$ with distinct linear factors. In particular, they are separable.

Let F be a field with q elements, and let E be a finite extension of degree n. Then E is seen to be a field with q^n elements, and so E must be the splitting field of $X^{q^n} - X$ over F. In particular, E is Galois over F with a Galois group of size n. Our goal will be to describe this Galois group.

Before discussing the Galois group, consider the special case $F = \mathbb{F}_p$. We see that every finite field E of characteristic p is Galois over $\mathbb{F}_p$ and has p^n elements for some n.

Over finite fields we have explicit automorphisms which are useful for describing Galois groups:

Definition 20. Suppose that F is a field of characteristic p. Let q be a power of p. Then the qth power *Frobenius map* $\mathrm{Fr}_q \colon F \to F$ is the function $x \mapsto x^q$.

We can prove that Fr_q is actually an automorphism of F, and that $(\mathrm{Fr}_q)^k = \mathrm{Fr}_{q^k}$ in the automorphism group of F. We can even prove the following:

Theorem 69. *Let F be a finite field with q elements, and let E be a finite extension of degree n. Then Fr_q is an element of $\mathrm{Gal}(E/F)$. Further, $\mathrm{Gal}(E/F)$ is cyclic of order n with generator Fr_q.*

Corollary 70. *Let F be a finite field with q elements, and let E be a degree n extension. For all positive divisors k of n, there is a unique field L_k intermediate between F and E such that E has size q^k.*

This gives us a good description of the Galois theory of finite extensions of finite fields, when we are given a finite F and a finite extension E. In the above discussion we started with a field F of size q and an extension E of degree n, and showed E is the splitting field of $X^{q^n} - 1$ over F. Reasoning the other way, we can start with the splitting field E_n of $X^{q^n} - 1$ over a field F of size q, and then show that E_n is a degree n extension. From this we can prove the following:

Theorem 71. *Let F be a finite field. For each $n \geq 1$ there is an extension of F of degree n. This extension is the splitting field of $X^{q^n} - X$ over F, and is unique up to isomorphism (and the isomorphisms can be required to fix F).*

Corollary 72. *Let p^n be a power of a prime. There is a field with p^n elements, and any two such fields are isomorphic.*

Often we work within a fixed algebraic closure of $\mathbb{F}_p$ where we have the following:

Theorem 73. *Let E be an algebraic closure of $\mathbb{F}_p$. For each power p^n, there is a unique subfield of E of order p^n. These yield all the finite subfields of E. If L_1 and L_2 are finite subfields of E then $L_1 \subseteq L_2$ if and only if $|L_2|$ is a power of $|L_1|$.*

Finally we mention that finite fields are special cases of cyclotomic extensions. In particular, E is a field with p^n elements if and only if it is the $p^n - 1$ cyclotomic extension of $\mathbb{F}_p$. Let E have size p^n. Then the cyclotomic polynomial $\Phi_{\mathbb{F}_p}(p^n - 1)$ splits, and each root has multiplicative order $p^n - 1$ in $E^\times$. Note that $\Phi_{\mathbb{F}_p}(p^n - 1)$ is a polynomial of degree $\phi(p^n - 1)$ which factors into irreducible factors of degree n. Also $E = \mathbb{F}_p[\alpha]$ where α is any root of any of the irreducible factors.

Worksheet 16: The fundamental theorem of algebra

We now consider a short Galois-theoretic proof of the fundamental theorem of algebra. This relies on four facts: two from analysis, and two from finite group theory.

Fact 1. Every polynomial $f \in \mathbb{R}[X]$ of odd degree has a real root. If $a > 0$ then $x^2 = a$ has solutions in $\mathbb{R}$.

Fact 2. If $a \in \mathbb{C}$ then $x^2 = a$ has a solution in $\mathbb{C}$.

Fact 3. Let G be a finite group, p a prime, and p^n the largest power of p dividing $|G|$. Then G has a subgroup of order p^n (called a *p-Sylow subgroup*).

Fact 4. Let G be a finite group of order 2^n with $n \geq 1$. Then G has a subgroup of index 2.

Fact 1 is a basic application of the the intermediate value theorem. Fact 2 can be proved from fact 1 using the geometric description of multiplication in $\mathbb{C}$. Or one can simply verify Lemma 77 and Corollary 78 in the case of $R = \mathbb{R}$.

Fact 3 is one of the Sylow theorems which is one of the basic theorems for finite groups, and we take it as given. Fact 4 is also a standard fact from Group theory, and the worksheet outlines an easy proof.

We begin with a lemma on extensions of $\mathbb{R}$.

Lemma 74. *If E is a finite Galois extension of $\mathbb{R}$, then the Galois group G has size equal to a power of 2.*

The idea here is to look at a 2-sylow subgroup H of G, and look at $[E^H : \mathbb{R}]$. This is an odd extension, and we can use Fact 1 to argue that $[E^H : \mathbb{R}] = 1$.

Next we consider a lemma on extensions of $\mathbb{C}$.

Lemma 75. *If F is a finite extension of $\mathbb{C}$, then $F = \mathbb{C}$.*

The idea here is to fix a Galois extension E of $\mathbb{R}$ containing F. This group must have size a power of 2 by the previous lemma. Also E is Galois over $\mathbb{C}$ of degree equal to a power of two. If $[E:\mathbb{C}] > 1$ then use Fact 4 to form a quadratic extension of $\mathbb{C}$, contradicting Fact 2.

From these lemmas we get the following:

Theorem 76 (Fundamental theorem of algebra)**.** *The field $\mathbb{C}$ is algebraically closed. The field $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. All irreducible polynomials in $\mathbb{R}[x]$ are either linear, or quadratic with distinct conjugate roots in $\mathbb{C}$.*

We can generalize the above argument a bit where we replace $\mathbb{R}$ with any real closed field. We assume the reader is familiar with ordered fields. The definition of a real closed field is a follows:

Definition 21. Let R be an ordered field. We say that R is a *real closed field* if (i) every odd degree polynomial $f \in R[X]$ has a root in R. and (ii) every positive element has a square root in R.

Let R be a real closed field. Since R is an ordered field, it has characteristic zero, and X^2+1 is irreducible. Let C be the splitting field of X^2+1 over R, and let i be a root of X^2+1 in C, so $C = R[i]$. If $a, b \in R$, then define the norm of $\alpha = a + bi \in C$ to be $\alpha\overline{\alpha} = a^2 + b^2$. The norm must be multiplicative, and the norm of any α is nonnegative. We need the following lemma and corollary.

Lemma 77. *Suppose R is a real closed field. Suppose $u = a + bi$ has norm 1 and $b \geq 0$. Then $-1 \leq a \leq 1$., and*

$$\sqrt{\frac{1+a}{2}} + i\sqrt{\frac{1-a}{2}}$$

yields a square root of u. (Where the square roots are taken as nonnegative roots in R).

Corollary 78. *Suppose R is a real closed field, and $C = R[i]$. Every element of C has a square root in C.*

With this corollary, we can prove a fundamental theorem of algebra for R and C analogous to that for $\mathbb{R}$ and $\mathbb{C}$ above.

Additional Topics

There is quite a bit more to Galois theory than we have presented here. Here are some topics that the reader may wish to follow-up on (and for which I may have essays in the future).

- The history of Galois theory
- The Galois theory of cubic and quartic equations including solvability of cubic and quartic equations in terms of radicals
- Symmetric Polynomials, discriminants, norms and traces

- Solvability and non-solvability in general
- Kummer theory
- Infinite Galois extensions