Minimal, Primitive, and Irreducible Polynomials

Wayne Edward Aitken

June 2021 Edition*

This document covers the concepts of minimal and primitive polynomials. It also discusses ways to show that a polynomial is irreducible. Aside from the first section, proofs are provided with minor details left to the reader, sometimes in the form of exercises.

This document was originally written as a handout for my Math 520 course in Fall 2010. Based on the aims of the course, these notes emphasize polynomials in $\mathbb{Q}[X]$ and $\mathbb{Z}[X]$. However, much of the material can be generalized. For example, much of the material on primitive polynomials extends to $R[X]$ where R is a UFD.

1 Background

We begin by stating prerequisites and reviewing some basic materials concerning polynomial rings.

1.1 Prerequisites

I will assume that the reader has had a good one-semester introduction to abstract algebra, and so is comfortable with groups, rings, fields, integral domains, and ideals. I will assumes a basic familiarity with standard rings and fields such as $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$. The basics of polynomial rings $R[X]$ are also assumed, but most of what is needed in reviewed in Section 1.2 below.

The basics of the theory of factorization in UFDs is assumed. So ideas such as *irreducible*, *units*, *associates* are assumed. Some basics concerning Euclidean domains and PIDs are also assumed. Actually not much is needed about PIDs and UFDs in general, but only as they related to polynomial rings in a single variable, and $\mathbb{Z}$ of course. Section 1.2 mentions Noetherian rings and the Hilbert basis theorem. This is not essential for what follows, but was mentioned to put polynomial rings in context.

Basic facts about quotient rings are assumed. Understanding of prime ideals and maximal ideals are required together the following:

Theorem 1. *Let R be a commutative ring with unity and let I be an ideal of R. Then R/I is an integral domain if and only if I is a prime ideal. Similarly, R/I is a field if and only if I is a maximal ideal.*

*Version of June 8, 2021.

The last section on cyclotomic polynomials assumes knowledge of roots of unit in $\mathbb{C}$ using exponential notation. The proof of the main theorem in that section assumes that reader knows, or can prove, that $(X-1)^p \equiv X^p - 1$ modulo a prime p.

1.2 Polynomial Rings

We review some basics concerning polynomial rings. If R is a commutative ring with unity and X is a symbolic variable, then $R[X]$ is the ring of polynomials with coefficients in R and variable X. There is a formal way to construct $R[X]$ in terms of finite sequences of elements in R using suitable definitions for addition and multiplication. In practice the usual, somewhat informal, way of thinking about polynomials is reliable enough. One can add and multiply polynomials in the usual way, and these binary operations satisfy all the usual laws. In fact, $R[X]$ is a commutative ring. If R is an integral domain, then so is $R[X]$. If F is a field, then $F[X]$ is not a field, but is a rather special type of integral domain: $F[X]$ is a Euclidean domain. Since $F[X]$ is a Euclidean domain, is also a PID and a UFD.

Definition 1. Suppose S is a ring with subring R. Then we call S an *extension* of R, or we say that S is a *ring extension of* R. If S happens to be a field we call S a *field extension of* R.

Remark. The terms *subring* and *extension* are often used in a situation that goes a bit beyond the above definition. Suppose that we have an injective ring homomorphism $R \to S$ which we fix once and for all, and treat as canonical. Then the image of $R \to S$ is a subring of S which is isomorphic to R. We identify R with its image in S, and we consider R to be a subring of S. We consider S to be an extension of R.

This is what happens with the standard map $R \to R[X]$ sending any given element $c \in R$ to the corresponding constant polynomial in $R[X]$. We consider this injective homomorphism as canonical, we view R as a subring of $R[X]$, and we consider $R[X]$ as an extension of R. The subring R of $R[X]$ is called the *coefficient ring* of $R[X]$.

Degrees of nonzero polynomials are defined in the usual way. If the coefficient ring R is an integral domain then the degree of a product will be the sum of the degrees of the factors. (If R is not an integral domain, we get an inequality at least).

There is a division algorithm and a corresponding quotient-remainder theorem for $F[X]$ when F is a field. This is why $F[X]$ is a Euclidean domain. All Euclidean domains have the property that every ideal is principal, which means that $F[X]$ is a PID (Principal Ideal Domain). All PIDs have unique factorization: every nonzero element factors uniquely into a unit times a finite number of irreducible elements (perhaps zero irreducible factors, and perhaps with repetitions of irreducible factors). In other words, $F[X]$ is a UFD. The division algorithm and a form of the quotient-remainder theorem are valid more generally in $R[X]$ where R is a commutative ring (with unity) but only when we divide $g \in R[X]$ by $f \in R[X]$ where the leading coefficient of f is a unit in R. (Uniqueness in the quotient-remainder theorem holds if R is an integral domain).

One can define polynomials in several variable such as $R[X, Y]$ or $R[X_1, \ldots, X_n]$. If $R = F$ is a field, these polynomial rings in several variables are UFDs, but not PIDs in general.

Note that $R[X, Y]$ is isomorphic to $R'[Y]$ where $R' = R[X]$. In other words, the ring $R[X, Y]$ is isomorphic to $R[X][Y]$. The *Hilbert basis theorem* says that if R is Noetherian, then so is $R[X]$. Thus, by induction, $R[X_1, \ldots, X_n]$ is Noetherian as well. Since a field F is trivially Noetherian, $F[X_1, \ldots, X_n]$ is always Noetherian.

Let $f \in R[X]$ be a polynomial. Let S be an extension ring of R. If $a \in S$, then $f(a)$ denotes the element of S obtained by substituting X with a in the polynomial f. The rule

$$f \mapsto f(a)$$

defines a function

$$\sigma_a \colon R[X] \to S.$$

It turns out that this is a ring homomorphism. In other words, $(fg)(a) = f(a)g(a)$ and $(f + g)(a) = f(a) + g(a)$. Why do these laws hold? It turns out that the definitions of addition and multiplication for $R[X]$ are exactly what is needed to make these laws hold. We call σ_a a *substitution homomorphism.*

There is another homomorphism that we will need. Suppose we are given a ring homomorphism $\pi \colon R \to S$. Then there is a unique ring homomorphism

$$\tilde{\pi} \colon R[X] \to S[X]$$

such that (1) $\tilde{\pi}$ extends π, and (2) X maps to X. An important example of this is when $\pi \colon \mathbb{Z} \to \mathbb{Z}_n$ where $\mathbb{Z}_n$ is the integers modulo n with n a positive integer. In other words, $\mathbb{Z}_n$ is the quotient ring $\mathbb{Z}/\langle n \rangle$. This result in a homomorphism

$$\mathbb{Z}[X] \to \mathbb{Z}_n[X]$$

which is the reduction modulo n map at the level of polynomials. For example modulo 5 the polynomial $10X^3 + 13X^2 + 100X - 1$ maps to $\overline{3}X^2 + \overline{4} \in \mathbb{F}_5[X]$.

Another important background fact is that the polynomial ring $F[X]$ where F is a field has the property that every nonzero prime idea is maximal. This is a consequence of $F[X]$ being a PID. Also, an ideal is maximal if and only if its generator is irreducible. Also note that every nonzero ideal has a unique monic generator.[1]

2 The Ring $R[a]$

Above we considered $R[X]$ where X is a symbolic variable. Now we extend this notation to $R[a]$ where a might not be a symbolic variable, but can be any element in an extension of R.

Definition 2. Let $a \in S$ where S is an extension ring of R. The image of the substitution homomorphism $\sigma_a \colon R[X] \to S$ is written $R[a]$. In other words,

$$R[a] = \{ f(a) \mid f \in R[X] \}.$$

[1] A polynomial is *monic* if its leading coefficient is 1.

Since $R[a]$ is the image of a ring homomorphism, it is a subring of S. The ring $R[a]$ is called the *ring extension of R generated by a*. This terminology is used because any subring T of S containing R and a must contain $R[a]$ as a subring. In other words, $R[a]$ is the unique minimal subring of S containing R, as a subset, and containing the element a.

Remark. The above definition seems to depend on S, but it can be easily seen to be independent of S in the following sense: if $a \in S \subseteq S'$ where S in an extension of R and S' is an extension of S, then $R[a]$ is the same ring whether we use S or S' in the definition. Likewise, the following definition is independent of S in this sense.

Definition 3. Let $a \in S$ where S is an extension of R. The kernel of σ_a is called the *vanishing ideal of a* over R. In other words, the vanishing ideal is the set I_a where

$$I = \big\{ f \in R[X] \mid f(a) = 0 \big\}.$$

Since the kernel of any ring homomorphism is an ideal, I_a is indeed an ideal of the ring $R[X]$.

Informally the vanishing ideal of a is the collection of polynomials with root a.

Using the fundamental homomorphism theorem linking images and kernels of homomorphisms, we get the following:

Proposition 2. *Let $a \in S$ where S is an extension of R. Then*

$$R[a] \cong R[X]/I_a$$

where I_a is the vanishing ideal of a over R.

Proposition 3. *Let $a \in S$ where S is an extension of R. If S is an integral domain, then the vanishing ideal I_a of a over R is a prime ideal of $R[X]$.*

Proof. Since $R[a]$ is a subring of S, it is also an integral domain. We conclude that the ideal I_a appearing in Proposition 2 must be a prime ideal since the quotient ring is an integral domain (Theorem 1). □

Many of these ideas can be generalized to more than one variable. For example, if $a, b \in S$, where S is an extension of R, and if $f \in R[X, Y]$ then $f(a, b)$ is defined in the usual way. The map

$$f \mapsto f(a, b)$$

defines a ring homomorphism

$$R[X, Y] \to S$$

and the image of this homomorphism is written $R[a, b]$. The kernel consists of all polynomials in two variables vanishing at the poin $(a, b) \in R^2$.

3 Algebraic versus Transcendental

Now we apply the above ideas to the concept of algebraic and transcendental numbers.

Definition 4. Suppose $\alpha \in \mathbb{C}$. If there is a nonzero polynomial $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$ then α is said to be *algebraic*. If α is not algebraic then it is said to be *transcendental*.

For example, $\sqrt{2}$ is algebraic since it is a root of $X^2 - 2$. On the other hand, according to famous theorems, π and e are transcendental.[2]

Observe that $\alpha \in \mathbb{C}$ is algebraic if and only if the vanishing ideal of α in $\mathbb{Q}[X]$ is nonzero. The vanishing ideal is a prime ideal by Proposition 3, and in $\mathbb{Q}[X]$ all nonzero prime ideals are maximal. So we get the following:

Proposition 4. *An element $\alpha \in \mathbb{C}$ is algebraic if and only if the vanishing ideal of α in $\mathbb{Q}[X]$ is maximal.*

Corollary 5. *An element $\alpha \in \mathbb{C}$ is algebraic if and only if $\mathbb{Q}[\alpha]$ is a field.*

Proof. This follows from Proposition 2 together with the previous proposition. Recall that the quotient of a commutative ring by an ideal is a field if and only if the ideal is maximal (Theorem 1). □

Definition 5. Let $\alpha \in \mathbb{C}$ be algebraic. Then $\mathbb{Q}[\alpha]$ is called the *field extension of $\mathbb{Q}$ generated by α*. We also write this fields as $\mathbb{Q}(\alpha)$ to emphasize that it is a field.

Proposition 6. *An element $\alpha \in \mathbb{C}$ is transcendental if and only if $\mathbb{Q}[\alpha]$ is isomorphic to the polynomial ring $\mathbb{Q}[X]$.*

Proof. If α is transcendental then the vanishing ideal is the zero ideal. By Proposition 2 we conclude that $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[X]$ (recall that the quotient of a ring R by the zero ideal is isomorphic to R).

The other direction follows from the above corollary: if $\mathbb{Q}[\alpha]$ is isomorphic to $\mathbb{Q}[X]$ then it cannot be a field, and so α is not algebraic. □

If $\alpha \in \mathbb{C}$ is transcendental, then consider the set

$$\mathbb{Q}(\alpha) \stackrel{\text{def}}{=} \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{Q}[X] \text{ with } g \neq 0 \right\}$$

It is easy enough to check that $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{C}$, and to prove the following.

Proposition 7. *If $\alpha \in \mathbb{C}$ is transcendental then the field $\mathbb{Q}(\alpha)$ is the minimal subfield of $\mathbb{C}$ containing α.*

Definition 6. Let $\alpha \in \mathbb{C}$ be transcendental. Then $\mathbb{Q}(\alpha)$ is called the *field extension of $\mathbb{Q}$ generated by α*.

Suppose that $\alpha \in \mathbb{C}$ is algebraic. Then its vanishing ideal is generated by a nonzero polynomial $f \in \mathbb{Q}[X]$. We can normalize so that f is monic (leading coefficient 1). Such f is called the *minimal polynomial* of α. We will discuss this further in the next section in a more general setting.

[2] In 1873, the French mathematician Hermite showed that e is transcendental. A few years later, in 1882, the German mathematician Lindemann showed that π is transcendental using the techniques of Hermite.

With some thought, one sees that the set of all algebraic numbers forms a countable subfield of $\mathbb{C}$. On the other hand, since $\mathbb{R}$ is uncountable, $\mathbb{C}$ is also uncountable. Thus there are an uncountable number of transcendental numbers: there are more transcendental numbers than algebraic numbers.[3]

4 Minimal Polynomials

Much of what we discussed in the previous section generalizes from base field $\mathbb{Q}$ to a general base field F.

Definition 7. Let F be a field, and let $\alpha \in E$ where E is an extension ring of F. Let $I \subseteq F[X]$ be the vanishing ideal of α in $F[X]$. If I is not the zero ideal, then we say that α *is algebraic over* F. Otherwise, we say that α is *transcendental over* F.

Recall that $F[X]$ is a PID, so the vanishing ideal in the above definition is a principal ideal. If the vanishing ideal is not zero and if we require that the generator be *monic* then the generator is unique:

Definition 8. Let F be a field, and let $\alpha \in E$ be algebraic over F, where E is an extension ring of F. Then the *minimal polynomial* of α over F is the unique monic generator of the vanishing ideal of α over F.

We can rephrase the definition as follows:

Proposition 8. *Let F be a field, and let $\alpha \in E$ be algebraic over F, where E is an extension ring of F. The minimal polynomial of α over F is the unique monic polynomial $f \in F[X]$ with the following property: $g(\alpha) = 0$ if and only if g is a multiple of f in $F[X]$.*

We are most interested in the case where E is a field (or integral domain) extending F. In this case, the vanishing ideal must be a prime ideal (Proposition 3). Because of this, Proposition 4 and Corollary 5 generalize easily with essentially the same proofs.

Proposition 9. *Let E be a field extension of F. An element $\alpha \in E$ is algebraic over F if and only if the vanishing ideal of α in $F[X]$ is maximal.*

Corollary 10. *Let E be a field extension of F. An element $\alpha \in E$ is algebraic over F if and only if $F[\alpha]$ is a field.*

We view $F[\alpha]$ as the field extension of F generated by α:

Proposition 11. *Let $\alpha \in E$ be algebraic over F where E is a field extension of the field F. Then $F[\alpha]$ is the minimal extension of F containing α in the following sense: If $K \subseteq E$ is a field extension of F containing α then $F[\alpha] \subseteq K$.*

Definition 9. Let F be a field, and let $\alpha \in E$ where E is a field extension of F. Then $F[\alpha]$ is called the *field extension of F generated by α*. In this case, we also write $F[\alpha]$ as $F(\alpha)$ to indicate that it is a field.

[3]This is the basis of Cantor's proof of the existence of transcendental numbers in the 1870s. His proof was thought to be miraculous at the time, and suspicious to some, since it shows transcendental numbers exist without constructing any particular transcendental number.

Since the vanishing ideal is a prime ideal we must have the following:

Proposition 12. *Let F be a field, and let $\alpha \in E$ be algebraic over F, where E is an extension field of F. Then the minimal polynomial of α over F is irreducible in $F[X]$.*

We can strengthen this, providing an alternative characterization of a minimal polynomial:

Proposition 13. *Let F be a field, and let $\alpha \in E$ be algebraic over F where E is an extension field of F. Then the minimal polynomial of α over F is the unique polynomial $f \in F[X]$ that is* (1) *monic,* (2) *irreducible, and* (3) *satisfies $f(\alpha) = 0$.*

Proof. From previous results and definitions it follows that the minimal polynomial satisfies (1), (2), and (3). Conversely, suppose $f \in F[X]$ satisfies (1), (2), (3). By property (3) f is in the vanishing ideal, so is a multiple of the minimal polynomial. By (1) and (2) this means that f is the minimal polynomial. □

Using Proposition 2, and the definition of minimal polynomial, we obtain the following:

Proposition 14. *Let $\alpha \in E$ be algebraic over F where E is a field extension of the field F. Let f be the minimal polynomial of α over F. Then*

$$F[\alpha] \cong F[X]/\langle f \rangle .$$

Finally we mention the generalization of Proposition 6 (with essentially the same proof).

Proposition 15. *Let F be a field, and let $\alpha \in E$ where E is an extension field of F. Then α is transcendental over F if and only if $F[\alpha]$ is isomorphic to the polynomial ring $F[X]$.*

Exercise 1. Let F be a field with extension field E. Suppose that $f \in F[X]$ is monic of degree two or three, and has no roots in F. Show that f is the minimal polynomial of α over F for all roots α of f in E.

Exercise 2. Show that the minimal polynomial of $\sqrt{2}$ is $X^2 - 2$. (Here $F = \mathbb{Q}$).

Exercise 3. Show that $\mathbb{C}$ is $\mathbb{R}[i]$. Show that $X^2 + 1$ is the minimal polynomial of i over $\mathbb{R}$. Conclude that $\mathbb{C}$ is isomorphic to $\mathbb{R}[X]/\left\langle X^2 + 1 \right\rangle$. (Note: one could even define $\mathbb{C}$ to be the field $\mathbb{R}[X]/\left\langle X^2 + 1 \right\rangle$, and define i to be the coset of X).

5 Degrees of Field Extensions

Recall that a field extension of a field F is simply a field containing F as a subring. For example, $\mathbb{C}$ is an extension field of $\mathbb{R}$. We can also think of a field extension E of F as an F-vector space. To do so, view the addition of E as the vector space addition. Think of the product cx with $c \in F$ and $x \in E$ as the scalar multiplication. (For now, we conveniently "forget" about multiplication cx when c is in E but not in F). We easily check that E is a vector space over F by checking all the axioms of a vector space.

Proposition 16. *If E is an extension field of the field F, then E is a vector space over F (using the operations described above).*

Recall that every vector space has a cardinal assigned to it called the *dimension*. It can be defined as the cardinality of a basis.

Definition 10. Let E be a field extension of F. Then the dimension of E, thought of as a vector space over F, is called the *degree* of the field extension E over F. This degree is written $[E : F]$. If $[E : F]$ is finite, then we say that E is a *finite extension* of F.

In the case of $E = F[\alpha]$ where α is algebraic over F, the degree $[E : F]$ turns out to be the degree of the minimal polynomial of α over F. Showing this is the theme of the next two exercises.

Exercise 4. Suppose α is algebraic over F with minimal polynomial f of degree d. Show that $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ span the vector space $F[\alpha]$.

Hint: given $g(\alpha) \in E$, use quotients and remainders in $F[X]$ to write $g = qf + r$ where $q, r \in F[X]$. Now substitute α for X.

Exercise 5. Suppose α is algebraic over F with minimal polynomial f of degree d. Show that $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ are linearly independent vectors in the vector space $F[\alpha]$. Hint: from a linear combination form a polynomial.

From these exercises we get the following basic facts:

Proposition 17. *Let $E = F[\alpha]$ be an extension of F generated by α, where α is algebraic over F. Let $f \in F[X]$ be the minimal polynomial of α with degree d. Then*

$$1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$$

is a basis of the vector space E.

Proposition 18. *Let $E = F[\alpha]$ be an extension of F generated by α, where α is algebraic over F. Let $f \in F[X]$ be the minimal polynomial of α. Then*

$$\big[F[\alpha] : F\big] = \deg f.$$

Exercise 6. Show $\mathbb{Q}[i]$ has basis $1, i$ over $\mathbb{Q}$. In other words, show that

$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Exercise 7. Suppose $[E : \mathbb{F}_p] = d$ where $\mathbb{F}_p$ is the field with p elements. Show that the field E has p^d elements. Hint: write a general element of E in terms of a basis. How many possibilities are there?

6 Constructing Extension Fields

If F is a subfield of $\mathbb{C}$ and if $f \in F[X]$ has positive degree, then the equation

$$f(\alpha) = 0$$

has a solution with $\alpha \in \mathbb{C}$; this is just the fundamental theorem of algebra. In this case you can do computations involving α by working in $\mathbb{C}$. In fact, the field $F[\alpha]$ is a subfield of $\mathbb{C}$.

What if F is not a subfield of $\mathbb{C}$? Or what if you want to do computations in $F[\alpha]$ but do not want to work in the complex numbers? Perhaps you do not want to identify α with a specific complex number. This section will provide a way of constructing roots and field extensions using a generalization of modular arithmetic, namely quotient rings.

Exercise 8. Show that a finite field cannot occur as a subfield of $\mathbb{C}$. So you cannot form field extensions of a finite field simply by taking subfields of $\mathbb{C}$.

In an earlier exercise, you were asked to show that $\mathbb{C}$ is isomorphic to

$$\mathbb{R}[X]/\left\langle X^2+1\right\rangle.$$

We observed that forming this quotient ring is actually a valid way to construct $\mathbb{C}$ from the reals $\mathbb{R}$. Our strategy is to generalize this construction.

So let F be a field, and let $f \in F[X]$ be an irreducible polynomial of positive degree. Then since f is irreducible and nonzero, we know that the ideal generated by f is maximal. Thus

$$E = F[X]/\langle f\rangle$$

is a field.

Exercise 9. Let $f \in F[X]$ be a nonconstant polynomial. Show that the canonical map

$$F[X] \to F[X]/\langle f\rangle$$

restricted to F is injective.

By the above exercise, we can think of F as a subfield of E. In other words, E is an extension of F. Here we identify a constant c with it image $\overline{c}$ (the equivalence class containing c).

For a polynomial g in $F[X]$, we denote by $\overline{g}$ the image of g in $F[X]/\langle f\rangle$. In other words, $\overline{g}$ is the coset (equivalence class) containing g. Given $g, h \in F[X]$, we say that $g \equiv h$ modulo $\langle f\rangle$ if an only if $g - h \in \langle f\rangle$. Note the following are equivalent:

1. $g \equiv h$ modulo $\langle f\rangle$.
2. $g - h$ is a multiple of f.
3. The images of g, h in $E = F[X]/\langle f\rangle$ are equal: $\overline{g} = \overline{h}$.

This allows us to do computations in E using rules of modular arithmetic, applied to polynomials.

Recall that, in $\mathbb{Z}/\langle m\rangle$, we have $m \equiv 0$ modulo m by basic modular arithmetic. Something similar happens in E: since $f - 0$ is trivially a multiple of f we get that $f \equiv 0$ modulo $\langle f\rangle$. In other words, in the field $E = F[X]/\langle f\rangle$ we have the equation $\overline{f} = \overline{0}$. This means that f is in the kernel of the canonical map.

The image of X in $E = F[X]/\langle f \rangle$ plays a special role in this situation. Define the element α to be $\overline{X}$. By this definition, the canonical map

$$F[X] \to F[X]/\langle f \rangle$$

sends X to its image α.

Suppose that $g(X) \in F[X]$ is given by

$$g(X) = a_n X^n + \ldots + a_1 X + a_0.$$

Since the canonical map is a homomorphism, we have

$$\overline{g(X)} = \overline{a_n}(\overline{X})^n + \ldots + \overline{a_1}\overline{X} + \overline{a_0} = a_n\alpha^n + \ldots + a_1\alpha + a_0 = g(\alpha).$$

Here we used the identification of $\overline{a}$ with a for all $a \in F$. So $g(X)$ maps to $g(\alpha)$. This means that the canonical map is just the substitution homomorphism:

Proposition 19. *Let F be a field, and let $f \in F[X]$ be an irreducible polynomial of positive degree. Let α be the image of X under the canonical map*

$$F[X] \to F[X]/\langle f \rangle .$$

Then the canonical map is the substitution homomorphism sending X to α. In other words, any polynomial $g(X) \in F[X]$ has image $g(\alpha)$.

Because the canonical map is the substitution homomorphisn, we get the following (as in Section 2):

Corollary 20. *Let F be a field, and let $f \in F[X]$ be an irreducible polynomial of positive degree. Let α be the image of X under the canonical map. Then*

$$F[X]/\langle f \rangle = F[\alpha]$$

Remark. Note the similarity between Proposition 14 and the above corollary. One difference is that Proposition 14 describes an isomorphism, but here we have a true equality.

Proof of corollary. By the previous proposition (Proposition 19), the canonical map is the substitution homomorphism. By Definition 2 we have that $F[\alpha]$ is the image of this map. However, the canonical map

$$F[X] \to F[X]/\langle f \rangle .$$

is surjective. So $F[\alpha]$ is all of $F[X]/\langle f \rangle$. □

Proposition 21. *Let F be a field and let $f \in F[X]$ be an irreducible monic polynomial of positive degree. Let α be the image of X under the canonical map*

$$F[X] \to F[X]/\langle f \rangle = F[\alpha]$$

Then α is a root of f:

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

Proof. As observed earlier, f is in the kernel of the canonical map, and so f maps to 0. But the canonical map is the substitution homomorphism and maps $f(X)$ to $f(\alpha)$. Thus $f(\alpha) = 0$. □

Given an irreducible polynomial f of positive degree, we used a quotient ring to create an extension $F[\alpha]$ where α is a root of f. If, in addition, f is monic, we will have that f is exactly the minimal polynomial of this element α. We assert this fact, and summarize the situation as a whole, in the following:

Theorem 22. *Let E be the field $F[X]/\langle f\rangle$ where f is an irreducible monic polynomial of positive degree. Let $\alpha = \overline{X}$. In other words, α is the coset in E containing X. Then α is algebraic over F with minimal polynomial f and*

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

Proof. This is largely just a summary of previous results. To complete the proof we just need to show that f is the minimal polynomial of α. By assumption, f is irreducible and monic. By Proposition 21, $f(\alpha) = 0$. Thus f is the minimal polynomial of α by Proposition 13. □

Corollary 23. *Every irreducible monic polynomial $f \in F[X]$ of positive degree is the minimal polynomial for some α in some field extension E.*

Exercise 10. Use the polynomial $X^2 + 1 \in \mathbb{F}_3[X]$ to form a field extension of $\mathbb{F}_3$. Show that this field contains 9 elements. Make addition and multiplication tables for this field (where α is $\overline{X}$).

Exercise 11. Use the polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$ to form a field with 8 elements. Make addition and multiplication tables for this field.

Exercise 12. Construct a field with four elements. Make addition and multiplication tables for this field.

7 Primitive Polynomials

The ring $\mathbb{Z}[X]$ is not a PID. In fact, the ideal $\langle 2, X\rangle$ is not a principal ideal. However, the integral domain $\mathbb{Z}[X]$ is nonetheless a UFD, and finding irreducible factors in $\mathbb{Z}[X]$ is very closely related to finding irreducible factors in the ring $\mathbb{Q}[X]$ which is a PID. To explain and justify this connection requires *primitive polynomials*.

First we point out that being irreducible in $\mathbb{Z}[X]$ is different than being irreducible in $\mathbb{Q}[X]$. For example, $2X^2+2$ is considered to be irreducible in $\mathbb{Q}[X]$ since 2 is a unit in $\mathbb{Q}[x]$, but reducible in $\mathbb{Z}[X]$ (neither 2 nor X^2+1 is a unit in $\mathbb{Z}[X]$). On the other hand, 2 is irreducible in $\mathbb{Z}[X]$, but is not irreducible in $\mathbb{Q}[X]$ (it is just a unit). However, there is a big overlap between irreducible elements in $\mathbb{Z}[X]$ and irreducible elements in $\mathbb{Q}[X]$; for example, X^2+1 is irreducible in both. In fact, we will see that examples such as $2X^2 + 2$ that involve constants are really the only cases where they differ. Primitive polynomials in $\mathbb{Z}[X]$ are polynomials with such constants factored out.

Definition 11. A nonzero polynomial f in $\mathbb{Z}[X]$ is said to be *primitive* if there is no prime p that divides all the coefficients of f. In other words, primitive polynomials are polynomials whose coefficients have GCD equal to 1.

For example, the polynomials $X^2 + 1$ and $-12X^2 + 15X - 50$ are primitive, but $2X^2 + 2$ and $-12X^2 + 15X - 30$ are not. Monic polynomials in $\mathbb{Z}[X]$ are always primitive.

The notion of primitive polynomial and many of the following results concerning such polynomials generalize to $R[X]$ where R is a PID. However, the following definition is particular to $\mathbb{Z}$ since it involves positivity.

Definition 12. A polynomial f in $\mathbb{Z}[X]$ is said to be *positive primitive* if it is primitive and its leading coeficient is positive.

As discussed in Section 1, we can associate to any prime number p a homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ given by sending a polynomial f with coefficients in $\mathbb{Z}$ to the same polynomial except with the coefficients considered to be in $\mathbb{F}_p$. For example, the image of $3X^3 + 4X^2 + 5X + 6$ under the map $\mathbb{Z}[X] \to \mathbb{F}_3[X]$ is $X^2 + \overline{2}X$.

Exercise 13. Show that a nonzero polynomial f in $\mathbb{Z}[X]$ is primitive if and only if its image under $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ is nonzero for each prime p.

Theorem 24 (Gauss's lemma, first form)**.** *The set of primitive polynomials in $\mathbb{Z}[X]$ is closed under multiplication. The set of positive primitive polynomials is also closed under multiplication.*

Proof. Suppose f and g are primitive. Let p be a prime, and consider the canonical map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ where $h \mapsto \overline{h}$. Then $\overline{fg} = \overline{f}\,\overline{g}$ since the map is a homomorphism of rings. Since f and g are primitive $\overline{f}$ and $\overline{g}$ are nonzero. Since $\mathbb{F}_p[X]$ is an integral domain, the product is nonzero as well. So $\overline{fg}$ is nonzero. This is true for every prime p, so fg is primitive.

If f and g are positive primitive as well, then fg must have positive leading coefficient since the leading coefficient of fg is the product of the leading coefficients of f and g. So fg is positive primitive. □

Exercise 14. Show that the set of primitive polynomials in $\mathbb{Z}[X]$ is not closed under addition.

Lemma 25. *Every nonzero $f \in \mathbb{Z}[X]$ can be factored as $f = c\tilde{f}$ where $c \in \mathbb{Z}$ is nonzero and $\tilde{f}$ is a positive primitive polynomial.*

Proof. Factor out the greatest common divisor of the coefficients. Factor out -1 if necessary to force the leading coefficient to be positive. (Another argument: if there is a prime p dividing all the coefficients, factor it out. Repeat until there are no primes left dividing all the coefficients). □

Later we will see that the c and $\tilde{f}$ above are unique.

Lemma 26. *Every nonzero $f \in \mathbb{Q}[X]$ can be factored as $f = c\tilde{f}$ where $c \in \mathbb{Q}^\times$ and $\tilde{f} \in \mathbb{Z}[X]$ is a positive primitive polynomial.*

Proof. Factor out $1/b$ where b is a common denominator of the coefficients. What is left is a polynomial in $\mathbb{Z}[X]$. Factor this polynomial as $a\tilde{f}$ where $\tilde{f}$ is positive primitive (Lemma 25). Observe that $f = c\tilde{f}$ where $c = a/b$. □

To get uniqueness we need the following lemma.

Lemma 27. *Suppose f is a positive primitive polynomial. If $c \in \mathbb{Q}$ is such that cf is also positive primitive, then $c = 1$. In other words, if two positive primitive polynomials are associates in $\mathbb{Q}[X]$ then they are equal.*

Proof. Suppose f and cf are positive primitive. Since the leading coefficients are positive, $c \in \mathbb{Q}$ is positive. Write $c = a/b$ where a and b are relatively prime positive integers.

Suppose p is a prime dividing b, and write $b = pb'$ for some positive integer b'. Since f is primitive, it has at least one coefficient $u_i \in \mathbb{Z}$ not divisible by p. The ith coefficient of cf is $au_i/b'p$. Since p does not divide u_i and does not divide a, it cannot divide the product au_i. Thus the ith coefficient of cf is not an integer. In other words, cf is not even in $\mathbb{Z}[X]$, contradicting the definition of primitive polynomial. We conclude that no such p divides b. This implies that $b = 1$, so c is a positive integer.

If $c \in \mathbb{Z}$ is divisible by a prime p, then every coefficient of cf is divisible by p as well. So cf would not be primitive, a contradiction. So no such p divides c. This implies that $c = 1$. □

Proposition 28. *Every nonzero $f \in \mathbb{Q}[X]$ can be factored uniquely as $f = c\tilde{f}$ where $c \in \mathbb{Q}^\times$ and $\tilde{f} \in \mathbb{Z}[X]$ is a positive primitive polynomial.*

Proof. Existence follows from Lemma 26. Suppose $f = c\tilde{f} = d\tilde{g}$ where $c, d \in \mathbb{Q}^\times$ and $\tilde{f}$ and $\tilde{g}$ are positive primitive. Then $d^{-1}c\tilde{f} = \tilde{g}$. Thus $\tilde{f}$ and $cd^{-1}\tilde{f}$ are both positive primitive. By Lemma 27, this means $cd^{-1} = 1$, in other words $c = d$. Thus $c\tilde{f} = c\tilde{g}$, which implies $\tilde{f} = \tilde{g}$. □

Corollary 29. *Every nonzero $f \in \mathbb{Z}[X]$ can be factored uniquely as $f = c\tilde{f}$ where $c \in \mathbb{Z}$ is nonzero and $\tilde{f} \in \mathbb{Z}[X]$ is a positive primitive polynomial.*

Proof. Existence follows from Lemma 25. Uniqueness is a corollary of Proposition 28 □

Exercise 15. Suppose that $f, g \in \mathbb{Z}[X]$ and that f is a primitive polynomial. Show that f divides g in $\mathbb{Z}[X]$ if and only if f divides g in $\mathbb{Q}[X]$.

8 Factorization into Primitive Polynomials

Primitive polynomials live both in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ since $\mathbb{Z}[X]$ is a subring of $\mathbb{Q}[X]$. It turns out that for primitive polynomials there is no difference between being irreducible in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$. Before proving this, we prove a lemma.

Lemma 30. *Suppose $f \in \mathbb{Z}[X]$ is a nonconstant positive primitive polynomial. If f is reducible in $\mathbb{Q}[X]$ then we can write f as the product of two nonconstant positive primitive polynomials in $\mathbb{Z}[X]$.*

Proof. Since f is reducible, we can write $f = gh$ where $g, h \in \mathbb{Q}[X]$ are nonconstant. By Proposition 28 we can write g as $c\tilde{g}$ and h as $d\tilde{h}$ where $c, d \in \mathbb{Q}$ and $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ are positive primitive polynomials. Thus $f = cd\tilde{g}\tilde{h}$. Since $\tilde{g}\tilde{h}$ is positive primitive (Theorem 24), Lemma 27 implies that $cd = 1$. So $f = \tilde{g}\tilde{h}$. □

Theorem 31. *Let $f \in \mathbb{Z}[X]$ be a nonconstant positive primitive polynomial. Then f is irreducible in $\mathbb{Z}[X]$ if and only if f is irreducible in $\mathbb{Q}[X]$.*

Proof. Suppose f is irreducible in $\mathbb{Z}[X]$. We wish to show f is irreducible in $\mathbb{Q}[X]$. Suppose otherwise. Then by Lemma 30 we can factor f in terms of nonconstant polynomials of $\mathbb{Z}[X]$. So f is reducible in $\mathbb{Z}[X]$, a contradiction.

Now suppose f is irreducible in $\mathbb{Q}[X]$. We wish to show f is irreducible in $\mathbb{Z}[X]$. We do so by supposing $f = gh$ where $g, h \in \mathbb{Z}[X]$, and showing g or h is a unit in $\mathbb{Z}$. Since f is irreducible in $\mathbb{Q}[X]$, either g or h is a constant. Without loss of generality, suppose $g = c$ is a constant. Note that $c \in \mathbb{Z}$ since $g \in \mathbb{Z}[X]$. If a prime p divides c, then each coefficient of $f = ch$ is divisible by p, a contradiction to the assumption that f is primitive. Thus c must be ± 1 as desired. □

Corollary 32 (Gauss's lemma, second form)**.** *Let $f \in \mathbb{Z}[X]$ be a primitive polynomial. Then f is irreducible in $\mathbb{Z}[X]$ if and only if f is irreducible in $\mathbb{Q}[X]$.*

Proof. Replace f with $-f$ if necessary, and then use the above theorem. (Also note that the only constant primitive polynomials are the units ± 1, and so are not irreducible in $\mathbb{Z}[X]$ or $\mathbb{Q}[X]$.) □

Proposition 33. *Every nonconstant polynomial $f \in \mathbb{Q}[X]$ is the product of a constant $c \in \mathbb{Q}^\times$ times one or more irreducible positive primitive polynomials:*

$$f = cf_1 \cdots f_k.$$

Moreover, this product is unique up to rearrangement of factors f_i.

Proof. We know that $\mathbb{Q}[X]$ has unique factorization, so we can factor f into irreducibles in $\mathbb{Q}[X]$:

$$f = ag_1 \cdots g_k.$$

By Proposition 28, $g_i = b_i f_i$ where $b_i \in \mathbb{Q}^\times$ and f_i is a positive primitive polynomial. Since f_i is an associate of g_i and since g_i is irreducible, the polynomial f_i is irreducible in $\mathbb{Q}[X]$ (and hence in $\mathbb{Z}[X]$). Thus

$$f = (ab_1 \cdots b_k) f_1 \cdots f_k,$$

and so the existence claim is established.

To establish uniqueness, suppose

$$f = cf_1 \cdots f_k = c' f_1' \cdots f_l'$$

where $c, c' \in \mathbb{Q}^\times$ and f_i, f_i' are irreducible positive primitive polynomials (irreducible in both $\mathbb{Q}[X]$ and $\mathbb{Z}[X]$ by the above theorem). Since $\mathbb{Q}[X]$ is a UFD, we can conclude that $k = l$ and that, after rearranging terms, $f_i \sim f_i'$. By Lemma 27, the only way that positive primitive polynomials can be associates is if they are equal. So $f_i = f_i'$. After cancelling all the f_i, we conclude $c = c'$. □

Proposition 34. *Every nonconstant positive primitive polynomial $f \in \mathbb{Z}[X]$ is the product of irreducible positive primitive polynomials:*

$$f = f_1 \cdots f_k.$$

Moreover, this product is unique (up to rearrangement of terms).

Proof. By Proposition 33, in $\mathbb{Q}[X]$ we can write f uniquely as $cf_1 \cdots f_k$ where $c \in \mathbb{Q}$ and each f_i is a positive primitive polynomial. Let $g = f_1 \cdots f_k$. By Gauss's lemma (Theorem 24) g is a positive primitive polynomial. Since $f = cg$, Lemma 27 implies that $c = 1$, and so $f = f_1 \dots f_k$.

Uniqueness follows from Proposition 33. □

Theorem 35. *Every nonzero polynomial $f \in \mathbb{Z}[X]$ is the product of ± 1 times zero or more prime numbers times zero or more irreducible positive primitive polynomials:*

$$f = (\pm 1)p_1 \cdots p_k f_1 \cdots f_l.$$

Moreover, this product is unique up to rearrangement of the sequence of factors (p_i) and (f_i).

Proof. By Corollary 29, we can write f as $c\tilde{f}$ where $c \in \mathbb{Z}$ is nonzero and $\tilde{f}$ is positive primitive. We factor c in $\mathbb{Z}$ and factor $\tilde{f}$ using Proposition 34. This gives the existence of the desired factorization.

Suppose we have another such factorization:

$$f = (\pm 1)p'_1 \cdots p'_{k'} f'_1 \cdots f'_{l'}$$

Let $f' = f'_1 \cdots f'_{l'}$. By By Gauss's lemma (Theorem 24) f' is positive primitive. Let $c' = (\pm 1)p'_1 \cdots p'_{k'}$, so $f = c\tilde{f} = c'f'$. By Corollary 29, $c = c'$ and $\tilde{f} = f'$. By unique factorization in $\mathbb{Z}$ and by the uniqueness assertion of Proposition 34, the desired uniqueness claim follows. □

The above theorem implies that $\mathbb{Z}[X]$ is a UFD. To see this, observe that prime numbers and positive primitive irreducible polynomials are irreducible in $\mathbb{Z}[X]$. For uniqueness one needs also know that these are the only irreducible elements (up to unit):

Exercise 16. Show that every irreducible element of $\mathbb{Z}[X]$ is either $\pm p$ where p is a prime number, or $\pm f$ where f is an irreducible positive primitive polynomial.

Corollary 36. *The integral domain $\mathbb{Z}[X]$ is a UFD.*

When $f \in \mathbb{Z}[X]$ is monic, it is automatically primitive positive. We consider a few nice results that apply to monic polynomials.

Exercise 17. Suppose $f \in \mathbb{Z}[X]$ is monic. Show that f factors as the product of monic irreducible polynomials in $\mathbb{Z}[X]$.

Proposition 37. *Let $f \in \mathbb{Z}[X]$ be monic, and let $g \in \mathbb{Q}[X]$ be a monic polynomial that divides f in $\mathbb{Q}[X]$. Then $g \in \mathbb{Z}[X]$ and g divides f in $\mathbb{Z}[X]$.*

Proof. Start with $f = gh$ in $\mathbb{Q}[X]$. Since f and g are monic, the same is true of h. Write $g = c\tilde{g}$ and $h = d\tilde{h}$ where $c, d \in \mathbb{Q}^\times$ and where $\tilde{g}, \tilde{h}$ are positive primitive polynomials (Proposition 28). So $f = (cd)(g_0 h_0)$. By Gauss's lemma (Theorem 24), the product $g_0 h_0$ is positive primitive. So $cd = 1$ by Lemma 27.

Since g is monic, we see that c^{-1} is the leading coefficient of $\tilde{g}$. So c^{-1} is a positive integer. Similarly, d^{-1} is a positive integer. We have $cd = 1$ so $c^{-1}d^{-1} = 1$. Thus $c^{-1} = d^{-1} = 1$. The result follows. □

Exercise 18. Suppose $\alpha \in E$ where E is an extension field of $\mathbb{Q}$. Suppose α is a root of a monic polynomial in $\mathbb{Z}[X]$. Show that the minimal polynomial of α must also be in $\mathbb{Z}[X]$.

Exercise 19. Show that if a polynomial $f \in \mathbb{Z}[X]$ is monic, all its rational roots are actually integers. Hint: focus on linear factors.

Exercise 20. Recall that a *perfect square* is an integer of the form m^2 where $m \in \mathbb{Z}$. Suppose $n \in \mathbb{Z}$ is not a perfect square. Use the polynomial $X^2 - n$ to show that the square root of n is irrational, and that $X^2 - n$ is its minimal polynonial. Generalize to cube roots.

Exercise 21. Show that if a polynomial $f \in \mathbb{Z}[X]$ has a rational root a/b (written in lowest terms with $b > 0$) then b divides the leading coefficient of f, and a divides the constant term of f. Hint: when you factor f in $\mathbb{Q}[X]$ you have a linear term $X - a/b$. When you factor f into a constant times the product of positive primitive polynomials, this linear factor gets expressed as $bX - a$.

9 The Mod p irreducibility Test

The following gives a way to show that a given monic polynomial in $\mathbb{Z}[X]$ is irreducible. To make it work you choose a suitable prime p and reduce the polynomial modulo p.

Proposition 38. *Suppose $f \in \mathbb{Z}[X]$ is a nonconstant monic polynomial and p is a prime number. If f maps to an irreducible polynomial under the canonical ring homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ then f itself is irreducible (in both $\mathbb{Q}[X]$ and $\mathbb{Z}[X]$).*

Proof. We suppose f is reducible and derive a contradiction. Since f is monic, it must be positive primitive. By Lemma 30, we can factor f as gh where g and h are nonconstant positive primitive polynomials.

Note that g and h are monic since the product of the leading coefficients is 1. Thus the images $\overline{g}$ and $\overline{h}$ are nonconstant in $\mathbb{F}_p[X]$. In $\mathbb{F}_p[X]$ we have $\overline{f} = \overline{g}\overline{h}$. Thus $\overline{f}$ is a reducible polynomial, a contradiction. □

If f is primitive, but not monic, the above theorem fails as stated, but can be repaired as follows:

Proposition 39. *Suppose $f \in \mathbb{Z}[X]$ is a primitive polynomial and p is a prime number not dividing the initial coefficient of f. If f maps to an irreducible polynomial under the canonical homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ then f is irreducible.*

Exercise 22. Prove the above theorem.

Exercise 23. Show that the assumption in the above proposition (p does not divide the initial coefficient) is necessary by giving a reducible primitive polynomial whose image modulo p for some prime p is irreducible.

Exercise 24. Show that $X^2 + 3aX + (3b+1)$ is irreducible for all integers a and b by reducing modulo 3.

Exercise 25. Show that $X^4 + X + 1$ is not divisible by any quadratic polynomial in $\mathbb{F}_2[X]$. Hint: show that the constant term of any quadratic divisor must be 1. Now conclude that there are only two possible divisors, and show both fail.

Exercise 26 (Continued)**.** Show that $X^4 + X + 1$ is irreducible in $\mathbb{F}_2[X]$.

Exercise 27 (Continued)**.** Let $f = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ be a primitive polynomial where a_4, a_1, and a_0 are odd, and a_3 and a_2 are even. Show that f is irreducible in $\mathbb{Q}[X]$.

10 The Eisenstein Criterion

There is a famous theorem that proves a large number of polynomials are irreducible. (In what follows, recall that all integers divide 0).

Theorem 40. *Consider a nonconstant polynomial in* $\mathbb{Z}[X]$

$$f = a_nX^n + a_{k-1}X^{k-1} + \ldots + a_1 + a_0$$

such that there is a prime p that does not divide a_n but divides a_i for each $i < n$. Suppose also that p^2 does not divide a_0. Then f is irreducible in the ring $\mathbb{Q}[X]$.

Proof. By repeatedly factoring out any prime dividing all the a_i, and by changing sign if necessary, we can assume that f is a positive primitive polynomial. (Note that p will not be such a prime since it does not divide the leading coefficient). Suppose f is reducible. Then by Lemma 30 we can write $f = gh$ where $g, h \in \mathbb{Z}[X]$ are nonconstant primitive polynomials. Let b be the leading coefficient of g and let c be the leading coefficient of h. Note that p cannot divide b or c. Modulo p, the polynomial f is just $\overline{a_n}X^n$, so

$$\overline{a_n}\, X^n = \overline{g}\,\overline{h}.$$

By unique factorization in $\mathbb{F}_p[X]$ we conclude that $\overline{g} = \overline{b}X^k$ and $h = \overline{c}X^l$ where k and l are positive with $n = k + l$. Since $k, l > 0$, p divides the constant term of g and the constant term of h. So p^2 divides the constant term of $gh = f$, a contradiction. □

Exercise 28. Show that $X^5 + 6X^4 - 12X^2 + 6X + 6X$ is irreducible.

11 Cyclotomic Polynomials

For any $n > 2$ let ζ_n be the complex number $e^{2\pi i/n}$. Using the basic properties of the complex valued exponential function we have

$$\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n).$$

Note that

$$\left(\zeta_n\right)^n = \left(e^{2\pi i/n}\right)^n = e^{2\pi i} = 1,$$

so ζ_n is called a *nth root of unity*, and is a root of $X^n - 1$. Note also that if $k < n$ then

$$\left(\zeta_n\right)^k = \left(e^{2\pi i/n}\right)^k = e^{2\pi ki/n} \neq 1.$$

In other words, ζ_n has multiplicative order exactly equal to n. Consequently, ζ_n is called a *primitive* nth root of unity.

Exercise 29. Show that $\zeta_4 = i$ and $\zeta_6 = 1/2 + i\sqrt{3}/2$. What is ζ_8?

Definition 13. The minimal polynomial of ζ_n is called the nth cyclotomic polynomial.

Exercise 30. Show that the third cyclotomic polynomial is $X^2 + X + 1$ and the fourth cyclotomic polynomial is $X^2 + 1$. Hint, factor $X^n - 1$ where $n = 3, 4$.

Cyclotomic polynomials have several nice properties, and their study was developed by Gauss. There is a famous theorem that the degree of the nth cyclotomic polynomial is equal to $\varphi(n)$ where φ is the Euler phi function. We won't prove this here except for the case where n is a prime. The above exercise gives two examples of cyclotomic polynomials that are quadratic polynomials. There is one other since $\varphi(6) = 2$.

Exercise 31. Show that $X^2 - X + 1$ divides $X^3 + 1$. Show that $X^2 - X + 1$ is the sixth cyclotomic polynomial.

TO HERE

Theorem 41. *Let p be a prime. Then*

$$f = X^{p-1} + X^{p-2} + \ldots + X + 1$$

is irreducible in $\mathbb{Q}[X]$.

Proof. Observe that f is positive primitive. Suppose that f is reducible. So by Lemma 30, $f = gh$ where g and h are nonconstant positive primitive polynomials. In fact, g and h are monic since the product of their leading coefficients is 1. Note that $(X - 1)f = X^p - 1$. Thus

$$(X - 1)gh = X^p - 1.$$

Now in $\mathbb{F}_p[X]$ we have that $(X - \overline{1})^p = X^p - \overline{1}$. This follows from the binomial theorem: the binomial coeffients, except the first and last, are divisible by p. So in $\mathbb{F}_p[X]$ we have

$$(X - \overline{1})\,\overline{g}\,\overline{h} = X^p - \overline{1} = (X - \overline{1})^p.$$

By unique factorization in $\mathbb{F}_p[X]$ (and the fact that g, h are monic) we have

$$\overline{g} = (X - \overline{1})^k, \ \ \overline{h} = (X - \overline{1})^l$$

where $k + l = p - 1$ and k, l are positive. This implies that $\overline{1}$ is a root of g and a root of h. In particular, $g(1)$ and $h(1)$ are congruent to zero modulo p. In other words p divides $g(1)$ and $h(1)$. Since $f = gh$, we have p^2 divides $f(1)$.

However,

$$f(1) = 1^{p-1} + 1^{p-2} + \ldots \ 1^1 + 1 = p$$

so p^2 does not divide $f(1)$, a contradiction. □

Corollary 42. *If p is a prime, then $X^{p-1}+X^{p-2}+\ldots+X+1$ is the pth cyclotomic polynomial.*

Exercise 32. Justify the above corollary.

Definition 14. The field $\mathbb{Q}[\zeta_n]$ is called the *nth cyclotomic extension.*

Exercise 33. Justify the following.

Corollary 43. *Let $E = \mathbb{Q}[\zeta_p]$ where p is a prime. Then $[E : \mathbb{Q}] = p - 1$. Furthermore, $1, \zeta^p, \ldots, \zeta^{p-2}$ is a basis for E over $\mathbb{Q}$.*

Exercise 34. Show that the third cyclotomic field and the sixth cyclotomic field are equal.

Exercise 35. Show that if n is odd, the nth cyclotomic field and the $2n$th cyclotomic field are equal.