Factorization in Polynomial Rings

David Corwin

May 16, 2019

1 Background

You are expected to follow Paulin's notes until the bottom of p.64. This includes the definition of associated elements, the definition of an irreducible element, the definition of a UFD, the definition of HCF (aka gcd) and LCM, and the fact that HCF and LCM always exist in a UFD.

The idea is that this will contain everything you need to know after p.64, though I will occasionally refer to proofs in Paulin's notes (but then it is not required to know the proofs).

2 Remainder Theorem for Polynomials

Recall that for a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ where $a_n \neq 0_R$ is said to have degree n. Note that degree is defined only when $f(x)$ is not the zero polynomial. Recall that *if R is an integral domain*, then

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Note that a polynomial $f(x)$ has degree zero if and only if it is nonzero and constant.

We then have the remainder theorem for polynomials:

Theorem 2.1. *Let F be a field, and let $f(x), g(x) \in F[x]$, with $g(x) \neq 0$ (i.e., it is not the zero polynomial). Then there exist $q(x), r(x) \in F[x]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

where either $r(x) = 0$, *or* $\deg r(x) < \deg g(x)$.

Remark 2.2. Notice that this looks very similar to the Remainder Theorem for integers (p.8 of Paulin's notes), with the absolute value in place of the degree function. The notion of *Euclidean Domain* described in Paulin's notes is a generalization of both of these examples, and the absolute value (in the case of $\mathbb{Z}$) and the degree (in the case of $F[x]$) are examples of *Euclidean functions*.

You don't technically need to know the term "Euclidean domain," but you should understand the similarity between the Remainder Theorem for $\mathbb{Z}$ and that for $F[x]$. And that similarity is precisely what the notion of "Euclidean domain" is about.

The proof of Theorem 2.1 is described in the Theorem at the bottom of p.65 of Paulin's notes (phrased as the statement that $F[x]$ is a Euclidean domain). Notice that it crucially uses the fact that F is a field, because you might have to divide by a coefficient. Therefore, the theorem is false for $\mathbb{Z}[x]$ in place of $F[x]$, as can be seen by taking $f(x) = x$ and $g(x) = 2$.

The Remainder Theorem is useful because it allows one to show that $F[x]$ is a PID, which also implies that it is a UFD. We now talk about PID's.

3 PID

Definition 3.1. An integral domain R is a *principal ideal domain (PID)* if every ideal of R is of the form $aR = (a)$ for some element $a \in R$.

Here are a few non-examples:

Example 3.2. The ring $R = F[x, y]$ is not a PID. One may check that the ideal (x, y) is not principal.

Example 3.3. The ring $R = \mathbb{Z}[x, y]$ is not a PID. One may check that the ideal $(2, x)$ is not principal.

Example 3.4. The ring $R = \mathbb{Z}[\sqrt{-5}]$ is not a PID. This is a bit harder, and it follows from 6(b) on HW 11.

Here are some examples:

Example 3.5. The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathbb{Z}\left[\frac{\sqrt{-163}+1}{2}\right]$ are PID's. The first four can be proven using methods similar to those used for $F[x]$ below; the last one is harder to prove (and is not something we will cover).

3.1 RT implies PID

We now explain how the remainder theorem can be used to show that $F[x]$ is a PID.

Proposition 3.6. *The ring $R = F[x]$ is a PID.*

Proof. Let I be an ideal in R. If $I = \{0\}$ or $I = R$, then I is principal (as it is (0) or (1), respectively).

If not, then I has at least some nonzero element, call it $f(x)$. Then $f(x)$ has a degree, which is a non-negative integer. If $f(x)$ has the smallest possible degree among nonzero elements of I, then we fix $f(x)$; if not, we replace $f(x)$ with an element of I with smallest possible degree (there is always a smallest possible degree, because the degree is ≥ 0). Let this element be $g(x)$.

We want to show that $I = g(x)R$. For this, let $h(x)$ be a general element of I. We want to show that $h(x)$ is a multiple of $g(x)$. For this, apply the remainder theorem to find $h(x) = q(x)g(x) + r(x)$, where $r(x)$ is zero or has smaller degree than $g(x)$. Note that because $g(x), h(x) \in I$, we have $r(x) = h(x) - q(x)g(x) \in I$. Therefore, $r(x)$ cannot have smaller degree than $g(x)$ (by the definition of $g(x)$), so $r(x) = 0$. That means that $h(x) = g(x)q(x)$, so $g(x)$ divides $h(x)$, as desired. □

Remark 3.7. The proof of Proposition 3.6 implies that if I is an ideal and f is an element of I of minimal degree, then f generates I. This is explained in more detail in Proposition 4.6 below.

3.2 Consequences of Being a PID

One important fact about PID's is that they are UFD's. We will not give the entire proof of this fact. The proof has two important steps:

1. Showing that factorization into irreducibles exist
2. Showing that that factorization is unique

1. can be proven using the stuff about ascending chains of ideals in 4.10 of Paulin, but we won't worry about that. For 2., an important step is showing that all irreducible elements are prime (this fact is both true in a UFD and is a step in proving that a given ring is a UFD).

Example 3.8. To see why "irreducible implies prime" is related to uniqueness of factorization, consider the ring $\mathbb{Z}[\sqrt{-5}]$, which is neither a PID nor a UFD. Then the fact that $(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$ are two different factorizations into irreducibles of the same element (6) is related to the fact that 2 is not prime. Indeed, 2 is irreducible, divides $(1+\sqrt{-5})(1-\sqrt{-5})$, but does not divide either factor. So 2 is *irreducible but not prime.*

Let's now prove that every irreducible element of a UFD is prime. Remember that a nonzero element is prime if and only if the ideal it generates is prime (by definition), and recall that maximal ideals are always prime. Therefore, it suffices to prove that every irreducible element generates an ideal that is maximal:

Proposition 3.9. *Let R be a PID, and suppose $a \in R$ is irreducible. Then aR is maximal.*

Proof. First, note that aR is not R, or else a would be a unit, and by definition irreducible elements are not units.

Now suppose that J is an ideal with $aR \subseteq J \subseteq R$. As R is a PID, we have $J = bR$ for some $b \in R$. Since $a \in aR \subseteq J$, we know that $b \mid a$. As a is irreducible, this means that either b is a unit, or b is associated to a. Int he former case, we have $J = R$, and in the latter case, we have $J = aR$. As J was arbitrary, this means that aR is maximal. □

As mentioned before, maximal implies prime (for ideals). And in any UFD, every irreducible element is prime. HOWEVER, in UFD's that are NOT PID's, there can be nonzero non-maximal primes. For example:

Example 3.10. In $R = \mathbb{Z}[x]$, let $I = xR$. Then x is in fact prime, but $R/I \cong \mathbb{Z}$, which is an integral domain but not a field. Therefore, I is maximal but not prime. This essentially happens because R is a UFD but not a PID.

In fact, note that the ONLY non-maximal prime ideal in a PID is the zero ideal. Therefore, if R is a PID, then every prime ideal is either aR for $a \in R$ irreducible or $\{0\}$. This latter fact can be used to prove, for example, that $\mathbb{Q}[\sqrt{2}]$ is not just a ring but also a field; for it is the quotient of $\mathbb{Q}[x]$ by the ideal generated by the irreducible polynomial $x^2 - 2$, and this ideal must be maximal.

Here's another fact that holds in PID's but not in general UFD's: Recall from p.64 of Paulin's notes that HCF's always exist in a UFD. In a PID, we can say a little bit more about HCF's:

Proposition 3.11. *Let R be a PID, $x, y \in R$, and d an HCF of x and y. Then there exist $a, b \in R$ such that $ax + by = d$.*

Proof. Let I be the ideal generated by x and y. Then I is the set of all elements of R of the form $ax + by$ for $a, b \in R$. Thus we have to show that $d \in I$.

Because R is a PID, we know that I is principal, say $I = zR$ for some $z \in R$. Then since $x, y \in I$, we know $z \mid x$ and $z \mid y$. By definition of HCF, we find that $z \mid d$. But then $d \in I = zR$, so we are done. □

4 Factorization of Polynomials

We collect some facts about factorization of polynomials that will be useful in our discussion of field extensions in Section 5. These facts are mostly just summaries of what was discussed in the previous two sections.

First, here's a description of all the ideals in $F[x]$:

Fact 4.1.

1. Every ideal in $F[x]$ is of the form $(f(x))$ for $f(x) \in F[x]$.
2. Two such ideals $(f(x))$ and $(g(x))$ are the same ideal if and only if $g(x)$ is a nonzero constant multiple of $f(x)$.
3. The only non-maximal prime ideal is (0).
4. The maximal ideals are precisely those of the form $(p(x))$ for an irreducible polynomial $p(x)$.
5. If I is a nonzero ideal, then it has a unique monic generator (recall that monic means the leading coefficient is 1).

Recall that whether a given polynomial is irreducible depends on F. For example, $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$.

Now let's talk about how to recognize whether a given element generates an ideal. First, a definition:

Definition 4.2. If I is an ideal in $R = F[x]$, then $f(x)$ has *minimal degree* in I if for any $g(x) \in I \setminus \{0\}$, we have $\deg f(x) \leq \deg g(x)$.

Example 4.3. In $\mathbb{C}[x]$, the ideal generated by $x^3 - x + 1$ has no elements of degrees 0, 1, or 2. All of its elements are either 0 (which does not have a degree) or have degree at least 3.

Example 4.4. More generally, if $f(x)$ is a polynomial of degree n in $F[x]$, then $(f(x))$ has no elements of degree less than n.

Example 4.5. An ideal $I \subseteq F[x]$ has elements of degree zero if and only if it is the whole ring.

We then have the following facts, which essentially follow from the proof of 2.1 and from the facts mentioned above:

Fact 4.6.
1. If I is an ideal of $F[x]$, and if $f(x) \in I$ has minimal degree, then $f(x)$ generates I.
2. Any two elements of I of minimal degree are constant multiples of each other.
3. If I is a nonzero ideal, then I has an element of minimal degree.
4. If I is generated by $0 \neq f(x) \in F[x]$, then $f(x)$ has minimal degree in I.

Finally, we note the following important fact:

Proposition 4.7. *If I is an ideal not equal to R, $p(x) \in I$ is an irreducible element of $F[x]$, then $p(x)$ generates I. In particular, $p(x)$ has minimal degree in I, and any other irreducible $q(x) \in I$ is a nonzero constant multiple of $p(x)$.*

Proof. The ideal $(p(x))$ is then contained in I. Since $(p(x))$ is maximal, and I is not all of R, we must have $I = (p(x))$. □

4.1 Linear Factors of Polynomials

Finally, here's an important consequence of the Remainder Theorem. This gives a relationship between factorization of polynomials and roots of polynomials.

Lemma 4.8. *If F is a field, $\alpha \in F$, and $f(x) \in F[x]$, then $(x-\alpha) \mid f(x)$ if and only if $f(\alpha) = 0$.*

Proof. If $(x-\alpha) \mid f(x)$, then $f(x) = (x-\alpha)g(x)$ for some $g(x) \in F[x]$. Therefore, $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0$.

Conversely, suppose $f(\alpha) = 0$. By the Remainder Theorem, we can write

$$f(x) = q(x)(x - \alpha) + r(x),$$

where $r(x)$ is either zero or has degree 0. Therefore, $r(x)$ is constant. But $r(\alpha) = f(\alpha) - q(\alpha)(\alpha - \alpha) = 0$, so $r(x)$ is just 0. Therefore, $f(x) = q(x)(x - \alpha)$, so $(x - \alpha) \mid f(x)$. □

One can repeatedly apply Lemma 4.8 to show that a polynomial of degree n can have at most n roots.

5 Ring and Field Extensions

Recall that if R is a subring of a ring S, and $\alpha \in S$, then there is an evaluation homomorphism

$$\mathrm{ev}_\alpha \colon R[x] \to S,$$

sending $f(X) \in R[x]$ to $f(\alpha) \in S$. The image is a subring of S denoted $R[\alpha]$, and $R[\alpha]$ is the smallest subring of S containing R and α.

If R and S are both fields, then we let $R(\alpha)$ denote the smallest sub*field* of S containing R and α. Note that we always have $R[\alpha] \subseteq R(\alpha)$, and these are equal if and only if $R[\alpha]$ is already a field. We want to understand when this does and doesn't happen.

We now set $F = R$ and $E = S$. The pair of E and F, often denoted E/F, is called a *field extension*. Note that this is NOT any kind of quotient - the use of "/" is just historically a piece of notation used for field extensions.

Given a field extension E/F and $\alpha \in E$, we set

$$I_\alpha \coloneqq \ker \mathrm{ev}_\alpha.$$

Note that I_α is an ideal in $F[x]$, so we can apply everything we know from Section 4 to it.

By the first isomorphism theorem for rings, we have $F[\alpha] \cong F[x]/I_\alpha$. Note that E is a field and therefore an integral domain, so it has no zero-divisors. But that means that $F[\alpha]$, being a subring of E, also has no zero-divisors. Therefore, $F[\alpha]$ is an integral domain (ID), so I_α is a prime ideal in $F[x]$.

By Fact 4.1, we either have $I_\alpha = (p(x))$ for $p(x)$ an irreducible element of $F[x]$, or $I_\alpha = \{0\}$. We distinguish these two cases with a pair of definitions:

Definition 5.1. If E/F is a field extension and $\alpha \in E$, then α is *algebraic over* F if I_α has a nonzero element. Equivalently, α is the root of a nonzero polynomial with coefficients in F.

Definition 5.2. If E/F is a field extension and $\alpha \in E$, then α is *transcendental over* F if $I_\alpha = \{0\}$. Equivalently, α is not the root of any nonzero polynomial with coefficients in F.

By Fact 4.1, we find that $F[\alpha]$ is a field (and hence $F[\alpha] = F(\alpha)$) if and only if α is algebraic over F.

Example 5.3. Any element of F itself is trivially algebraic over F.

Example 5.4. The numbers $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, and more generally, $\sqrt[n]{a}$ for $a \in \mathbb{Q}$ and $n \in \mathbb{N}$ are algebraic over $\mathbb{Q}$.

Example 5.5. The complex number i is algebraic over $\mathbb{Q}$ (and over $\mathbb{R}$).

Example 5.6. The numbers $e = 2.71828...$ and $\pi = 3.14159...$ are transcendental over $\mathbb{Q}$. See `https://en.wikipedia.org/wiki/Lindemann%E2%80%93Weierstrass_theorem` for some of the history of this. It was a conjecture of Lambert in 1768, but only proven (in the case of π) in 1882 by Lindemann.

Example 5.7. The number π is algebraic over $\mathbb{R}$, even though it is transcendental over $\mathbb{Q}$. In fact, it is also algebraic over a field like $\mathbb{Q}(\pi^2)$.

The last two examples show that whether an element is transcendental or algebraic depends on the field F. Clasically, people only considered the following definition:

Definition 5.8. A complex number α is said to be *an algebraic number* if it is algebraic over $\mathbb{Q}$. It is said to be *a transcendental number* if it is transcendental over $\mathbb{Q}$.

For some time, people didn't know if there even were transcendental numbers. The first number proven to be transcendental was

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}},$$

which was done by Liouville. You can find out about more numbers that are known to be transcendental at `https://en.wikipedia.org/wiki/Transcendental_number#Numbers_proven_to_be_transcendental`.

Remark 5.9. This material is non-examinable: The subset of $\mathbb{C}$ consisting of all algebraic numbers is denoted $\overline{\mathbb{Q}}$. It turns out that this subset is in fact a subfield,

and it is known as the *algebraic closure of* $\mathbb{Q}$. It is *algebraically closed* in the sense that every polynomial with coefficients in it has a root (and in fact splits into linear factors). You can read more at `https://en.wikipedia.org/wiki/Algebraic_number#The_field_of_algebraic_numbers` and the links contained therein.

5.1 Minimal Polynomials

Let E/F be a field extension, and suppose that $\alpha \in E$ is algebraic. Then the ideal $I_\alpha \subseteq F[x]$ has a unique monic generator by Fact 4.1. This generator is called the *minimal polynomial* of α *over* F.

How can we tell if a given polynomial is the minimal polynomial of a given $\alpha \in R$? Well if $p(x) \in F[x]$ is irreducible such that $p(\alpha) = 0$, then Fact 4.7 implies that $p(x)$ generates I_α. Therefore, the unique monic multiple of $p(x)$ is the minimal polynomial of α.

Note that $\alpha \in F$ if and only if its minimal polynomial is $x-\alpha$ (or equivalently, as long as its minimal polynomial is linear).

Example 5.10. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

Example 5.11. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}[\sqrt{2}]$ is just $x - \sqrt{2}$.

Example 5.12. The minimal polynomial of i over $\mathbb{Q}$, or even over $\mathbb{R}$, is $x^2 + 1$.

Example 5.13. The minimal polynomial of the Golden Ratio $\dfrac{\sqrt{5}+1}{2}$ over $\mathbb{Q}$ is $x^2 - x - 1$.

In order to find the minimal polynomial of α, it suffices to find a polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$ and then show that $f(x)$ is irreducible. This latter step can be tricky.

Example 5.14. The minimal polynomial of $\alpha = e^{2\pi i/7} = \cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$ is $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Note that

$$f(x) = \frac{x^7 - 1}{x - 1},$$

so it is clear that $f(\alpha) = 0$. To show that $f(x)$ is irreducible in $\mathbb{Q}[x]$, one needs to use the Eisenstein Criterion from p.74 of Paulin's notes. However, we will not cover the Eisenstein Criterion in this semester.

We can, however, prove irreducibility in the following cases:

Proposition 5.15. *If $f(x) \in F[x]$ is quadratic or cubic (i.e., degree 2 or 3), then $f(x)$ is irreducible iff $f(x)$ has no root in F.*

Proof. If $f(x)$ were reducible, then because degrees add when you multiply polynomials, it would have to have a (non-constant) linear factor. But any nonconstant linear polynomial over F is of the form $ax + b$ for $a, b \in F$, with $a \neq 0$. Since F is a field, this linear polynomial has a solution $-\dfrac{b}{a} \in F$. Therefore, if $f(x)$ is reducible, then $f(x)$ has a root in F.

Conversely, if $f(x)$ has a root in F, then by Lemma 4.8, it is divisible by a linear polynomial, so it is reducible (since it is quadratic or cubic and therefore not linear). □

Example 5.16. This allows one to prove that $x^2 - 2$ is indeed the minimal polynomial of $\sqrt{2}$ or that $x^2 + 1$ is indeed the minimal polynomial of i (once you prove that neither 2 nor -1 has a square root in $\mathbb{Q}$).

Example 5.17. For a cubic example, note that 2 has no cube root in $\mathbb{Q}$, so $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, hence $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.

Example 5.18. Note that $x^3 - 2$ is reducible in $\mathbb{R}[x]$, so it is not the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{R}$. In fact, over $\mathbb{R}[x]$, we have the factorization $x^3 - 2 = (x^2 + \sqrt[3]{2}x + \sqrt[3]{4})(x - \sqrt[3]{2})$, yet the polynomial $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ is irreducible over $\mathbb{R}$ (i.e., in $\mathbb{R}[x]$) because it has no real roots.

Note that there are reducible quartic polynomials with no root in F. For an easy example, take $(x^2 - 2)^2$ for $F = \mathbb{Q}$.

6 Material Beyond Our Course

6.1 Toward Galois Theory

6.1.1 Degree of a Field Extension

Definition 6.1. Let E/F be a field extension. Then a *basis* of E over F is a subset $\{x_1, \cdots, x_n\} \subseteq F$ such that every $x \in E$ can be uniquely expressed as a linear combination

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$$

for $\lambda_i \in F$.

Definition 6.2. We say that an extension E/F is *finite* if it has a finite basis. The *degree* of a finite extension E/F, denoted $[E : F]$, is the size of the basis. (Note: it is a theorem that this size does not depend on which basis one chooses.)

Given an extension, how can one determine its degree? It should be clear that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ has degree 2 over $\mathbb{Q}$. We also know that $[E : F] = 1$ if and only if $E = F$. The following fact is helpful:

Fact 6.3. If $\alpha \in E$ is algebraic over F, then $F[\alpha]/F$ is a finite extension whose degree is the degree of the minimal polynomial of α over F.

More concretely, if that degree is n, then one can choose $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ as a basis.

For a more complicated field extension like $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, there are a couple of approaches. One could try to show that in this case, $E = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ and that this representation is unique. Or, one could show that $E = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ as in one of the homework problems, and then show that $\sqrt{2} + \sqrt{3}$ has minimal polynomial $x^4 - 10x^2 + 1$ over $\mathbb{Q}$.

An even better way is to use the following proposition:

Fact 6.4. If $E/K/F$ is a sequence of (finite) field extensions, then $[E : F] = [E : K][K : F]$.

The proof proceeds by taking a basis $x_1, \cdots, x_n$ of E over K and a basis $y_1, \cdots, y_m$ of K over F and then showing that the set of mn products $\{x_i y_j\}$ is a basis for E over F.

The notion of degree of a field extension is the key to showing that one cannot construct, for example, a septagon, using ruler and compass. The idea is this: whenever one does a ruler and compass construction, the coordinates of the points one can construct can be found by addition, multiplication, subtraction, division, and square roots (because of the distance formula in Cartesian geometry, and because ruler and compass construction is all about drawing circles!). This means that they all lie in a field extension of $\mathbb{Q}$ given by taking square roots; by applying Fact 6.4 over and over, one sees that such an extension must have degree a power of 2.

Note that any divisor of a power of 2 is also a power of 2. Thus any *subfield* of such a field extension would also have degree a power of 2 by Fact 6.4. However,

the number $\cos\frac{2\pi}{7}$ has minimal polynomial $x^3 + \frac{x^2}{2} - \frac{x}{2} - \frac{1}{8}$, which has degree 3. Therefore, $\mathbb{Q}[\cos\frac{2\pi}{7}]$ has degree 3 over $\mathbb{Q}$, so it cannot be contained in a field extension of $\mathbb{Q}$ whose degree is a power of 2.

6.1.2 Galois Theory

Given a polynomial $f(x) \in F[x]$, one can define the *splitting field* E_f of $f(x)$ over F. It is a field obtained by "adjoining" (inside some larger field, such as $\mathbb{C}$) all the roots of $f(x)$ to F. In other words, it is the smallest field E in which $f(x)$ *splits* into linear factors in $E[x]$.

One then defines the *Galois group* $\mathrm{Gal}(E_f/F)$ of $f(x)$ over F to be the group of automorphisms of the field E_f that act as the identity on F.

Note that if $\sigma \in \mathrm{Gal}(E_f/F)$, $\alpha \in E_f$, and $g(x) \in F[x]$, then $\sigma(g(\alpha)) = g(\sigma(\alpha))$ (this is an exercise in the definition of a ring homomorphism and of a polynomial!). In particular, if α is a root of $f(x)$, then $\sigma(\alpha)$ is also a root of $f(x)$. In particular, the elements of $\mathrm{Gal}(E_f/F)$ *permute* the roots of $f(x)$. If we let Z denote the set of roots of $f(x)$, then $\mathrm{Gal}(E_f/F)$ is a subgroup of $\Sigma(Z)$. For example, if $f(x)$ is a quintic polynomial with distinct roots, then $\mathrm{Gal}(E_f/F)$ is a subgroup of Sym_5.

A basic result of Galois says that $\mathrm{Gal}(E_f/F)$ acts transitively on the set of roots. The philosophy behind this is that any two roots "look the same algebraically, from the viewpoint of F."

Here are some examples:

Example 6.5. If $n \in \mathbb{Z}$ is not a square, then $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ has Galois group of order 2. The non-identity element corresponds to the automorphism $a + b\sqrt{n} \mapsto a - b\sqrt{n}$.

Example 6.6. We can do the previous example over $\mathbb{R}$ instead of $\mathbb{Q}$ if n is negative, to get the extension $\mathbb{C}/\mathbb{R}$. The Galois group is once again size 2, and the non-trivial automorphism (i.e. non-identity element of the group) is complex conjugation.

Example 6.7. The field $\mathbb{Q}[\sqrt[3]{2}]$ is not a splitting field, because $\sqrt[3]{2}$ is not the *only* root of the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. In fact, we have to all add the roots $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, where $\omega = \frac{-1 + i\sqrt{3}}{2}$ is a primitive third root of unity. The field $\mathbb{Q}[\sqrt[3]{2}, \omega]$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. In this case, there are

three roots, and the Galois group is the full symmetric group Sym_3. This is an example of a *non-abelian* Galois group.

To learn more about Galois theory, pick up any text on abstract algebra, search "Galois theory notes" on Google, or see my notes at `https://math.berkeley.edu/~dcorwin/files/galoisthy.pdf`.

One set of notes I particularly like are those of Miles Reid at `https://homepages.warwick.ac.uk/~masda/MA3D5/Galois.pdf`. He has a really nice introductory section that explains the cubic and quartic formulas in light of the philosophy of Galois theory, so it really helps motivate Galois theory. Or see my account of the same topic at `https://math.berkeley.edu/~dcorwin/files/symmetry_cubic.pdf`.

6.2 Algebraic Geometry

Algebraic geometry is a very important field of mathematics that has influenced many other fields, ranging from number theory to mathematical physics, and even to computer engineering.

Algebraic geometry is, on its surface, the study of solutions to polynomial equations in multiple variables. More specifically, it is the study of the relationship between solution sets of polynomials in multiple variables (geometry) and the ring theory of certain rings (algebra).

How does one associate a ring to a system of polynomial equations? Let's say $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)$ is collection of m polynomials in n variables with coefficients in a field F. We define the solution set or *variety* defined by $f_1, \cdots, f_m$ to be the set

$$V(f_1, \cdots, f_m) = \{(x_1, \cdots, x_n) \in F^n \mid f_i(x_1, \cdots, x_n) = 0 \, \forall \, i = 1, \cdots, m\}.$$

Then one associates the ring

$$A = A(V(f_1, \cdots, f_m)) \coloneqq F[x_1, \cdots, x_n]/(f_1, \cdots, f_m).$$

The idea is that the polynomials $f_1, \cdots, f_m$ are zero as functions on $V(f_1, \cdots, f_m)$, so we should mod out by them.

The ring $A(V(f_1, \cdots, f_m))$ is known as the *affine coordinate ring* of the variety. Algebraic geometers in the first half of the 20th century made the

important observation that geometric properties of $V(f_1, \cdots, f_m)$ are equivalent to certain algebraic properties of the ring A. Here are three examples of this phenomenon:

If F is algebraically closed, then Hilbert's Nullstellensatz says that there's a natural bijection between the points of $V(f_1, \cdots, f_m)$ and the maximal ideals of the ring A.

If the variety is smooth (this means that the Jacobian of partial derivatives of the map from F^n to F^m defined by the polynomials f_i has full rank at every point of $V(f_1, \cdots, f_m)$, so that one may apply the implicit function theorem), then A is a UFD.

Finally, the ring A is an integral domain if and only if the variety is *irreducible*, which roughly means that it cannot be broken down as a union of smaller varieties. For example, the variety defined by the single equation $x_1 x_2 = 0$ is reducible, because it is the union of the variety defined by $x_1 = 0$ and the variety defined by $x_2 = 0$. Indeed, notice that $F[x_1, x_2]/(x_1 x_2)$ is not an integral domain.

The book `https://www.amazon.com/Invitation-Algebraic-Geometry-Universitext/dp/0387989803` is a wonderful introduction to algebraic geometry. You can probably even start reading this book just with the background you learned in this class!