POLYNOMIAL RINGS

TIM SMITS

Polynomial rings serve as class of familiar rings with interesting properties. In particular, polynomial rings over a field will have many analogous properties to the integers. Understanding why this happens will be key to abstracting their important properties.

1. Basic definitions

Definition 1.1. Let R be a ring. The polynomial ring $R[T]$ in the indeterminate T with coefficients in R is the set of all formal sums $a_nT^n + \ldots + a_1T + a_0$ with $n \geq 0$ and $a_i \in R$. If $a_n \neq 0$, then the polynomial is said to have degree n. A polynomial is called **monic** if $a_n = 1$. We'll usually write a polynomial in $R[T]$ as either $f(T)$, or dropping the indeterminate, just f if it's clear from the context.

Addition of polynomials is defined "component wise", by the rule

$$\sum_{i=0}^{n} a_iT^i + \sum_{i=0}^{n} b_iT^i = \sum_{i=0}^{n}(a_i + b_i)T^i$$

and multiplication is defined by

$$\left(\sum_{i=0}^{n} a_iT^i\right)\left(\sum_{i=0}^{m} b_iT^i\right) = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_ib_{k-i}\right)T^i$$

Note that we interpret $a_k = 0$ for $k > n$ and $b_k = 0$ for $k > m$. The operations above make $R[T]$ into a ring, and $R[T]$ inherits many of the properties of the ring R. For example, we have the following:

Proposition 1. *Let R be an integral domain. Then $R[T]$ is an integral domain.*

Proof. We prove the product of non-zero polynomials is non-zero, which is equivalent to showing that $R[T]$ is an integral domain. Suppose that $f, g \neq 0 \in R[T]$. We can write $f(T) = a_nT^n + \ldots a_0$ and $b(T) = b_mT^m + \ldots + b_0$ for some a_i, b_i where $a_n \neq 0$ and $b_m \neq 0$. Then $fg = a_nb_mT^{n+m} +$ lower degree terms. Since R is an integral domain and $a_n, b_m \neq 0$, this says $a_nb_m \neq 0$ so that $fg \neq 0$. □

Corollary 1.2. *Let R be an integral domain, and let $f, g \in R[T]$ be non-zero polynomials. Then* $\deg(fg) = \deg(f) + \deg(g)$.

Proof. This follows immediately from the above proof. □

Note that the above really does require that R is an integral domain. For example, in $(\mathbb{Z}/4\mathbb{Z})[T]$, we have $(2T) \cdot (2T + 1) = 2T$. The terms on the left hand side both have degree 1, which is the *same* as the term on the right hand side. Therefore, in order for the degree of a polynomial to have any value to us, most of our theory of polynomial rings will require that R be an integral domain. In fact, we'll generally assume that R is a field – the reason

for doing so will become more clear in the next section. Before doing so however, it will be useful to know what the units of a polynomial ring are.

Theorem 1.3. *Let R be a commutative ring. A polynomial $f(T) = a_nT^n + \ldots + a_0$ in $R[T]$ is a unit if and only if $a_0 \in R^\times$ and a_i are nilpotent for $1 \leq i \leq n$.*

Proof. First, we prove that if a_0 is a unit and a_i are nilpotent for $1 \leq i \leq n$, that f is a unit. Since a_i are nilpotent, clearly a_iT^i are nilpotent. Since a sum of nilpotent elements are nilpontent, we see that $a_1T+\ldots+a_nT^n$ is nilpotent, so $a_0+\ldots+a_nT^n = a_0+(a_1T+\ldots+a_nT^n)$ is a unit plus a nilpotent, and therefore is a unit.

Conversely, suppose that $f = a_0+\ldots+a_nT^n$ is a unit in $R[T]$, and let $g = b_0+\ldots+b_mT^m$ be it's inverse, so $fg = 1$ in $R[T]$. By the way polynomial multiplication works, we can write $fg = \sum_{k=0}^{n+m} d_kT^k$ where $d_k = \sum_{i=0}^{k} a_kb_{k-i}$. Since $fg = 1$, in particular, by comparing coefficients of both sides this says that $d_0 = a_0b_0 = 1$ and $d_k = 0$ for $k \geq 1$. Note that $a_0b_0 = 1$ says a_0 (and b_0) are units.

We now analyze the other coefficients. We have $d_{m+n} = a_nb_m = 0$. We also have $d_{m+n-1} = a_{m-1}b_m + a_nb_{m-1} = 0$. Multiplying this by a_n, and using that $d_{m+n} = 0$, we find that $a_n^2b_{m-1} = 0$. By multiplying each step by the correct power of a_n, and using the previous equations, we get the following chain of reasoning:

$$\begin{aligned} a_nb_m &= 0 \\ a_{n-1}b_m + a_nb_{m-1} = 0 &\implies a_n^2b_{m-1} = 0 \\ a_{n-2}b_m + a_{n-1}b_{m-1} + a_nb_{m-2} = 0 &\implies a_n^3b_{m-2} = 0 \\ &\vdots \\ \ldots + a_{n-2}b_2 + a_{n-1}b_1 + a_nb_0 = 0 &\implies a_n^{m+1}b_0 = 0 \end{aligned}$$

Since b_0 is a unit, this says that $a_n^{m+1} = 0$, so that a_n is nilpotent, and a_nT^n is nilpotent. We then have $f - a_nT^n$ is a unit plus a nilpotent, which says that $f - a_nT^n = a_0 + a_1T + \ldots + a_{n-1}T^{n-1}$ is a unit with strictly smaller degree. If we inductively apply this argument, we then find that $a_1, \ldots, a_n$ are all nilpotent.

□

Corollary 1.4. *Let R be an integral domain. Then $f \in R[T]$ is a unit if and only if $f(T) = a$ for some $a \in R^\times$.*

Example 1.5. In $(\mathbb{Z}/4\mathbb{Z})[T]$, the polynomial $f(T) = 1 + 2T$ is a unit, because $2^2 = 0$ says 2 is nilpotent. The inverse can be computed by analyzing the formal power series of $\frac{1}{1+2T}$. From basic calculus, we have $\frac{1}{1+2T} = \sum_{k=0}^{\infty}(-1)^k2^kT^k = 1-2T+4T^2-\ldots = 1-2T$ because all the higher powers of 2 die off in the sum. Indeed, one can check that $(1+2T)(1-2T) = 1$, so this is in fact the inverse.

2. Analogies between $F[T]$ and $\mathbb{Z}$

In this section, we assume that F is a field and restrict our attention to the polynomial ring $F[T]$. The reason for doing so is that this ring bears a striking resemblance to the

integers in many ways. The key to this lies in the fact that polynomial rings over a field have a division algorithm. This is not generally true in $R[T]$ if R is just an integral domain.

Example 2.1. In $\mathbb{Z}[T]$, there is no way to make sense of division of $2T^2+1$ by $3T+2$. If you try to use the long division algorithm you're familiar with from high school, you'll quickly see the obstruction is that there is no solution to the equation $3x = 2$ in $\mathbb{Z}$, i.e. 3 is not a unit.

Of course, over a *field*, all non-zero elements have a multiplicative inverse, and this is no longer something we have to worry about.

Theorem 2.2 (Division algorithm)**.** *Let $f(T), g(T) \in F[T]$ with $g(T) \neq 0$. Then there exist unique polynomials $q(T), r(T) \in F[T]$ with $f(T) = g(T)q(T) + r(T)$ with $r(T) = 0$ or $0 \leq \deg(r) < \deg(g)$.*

Proof. The proof will be analogous to the proof of the division algorithm in the integers. The idea will be to use the well ordering principle on the *degree* of the remainder term, but some care will be needed since the inequalities with the integers we get in the proof in $\mathbb{Z}$ don't carry over as nicely. First, note the theorem is obvious if $g(T) = c$ is a non-zero constant: $f(T) = (c)(\frac{1}{c}f(T)) + 0$. Now suppose that $\deg(g) > 0$ and let $A = \{f(T) - g(T)q(T) : q(T) \in F[T]\}$ and $S = \{\deg(p(T)) \geq 0 : p(T) \in A\}$. Notice that $S \neq \emptyset$, because $f(T) \in A$. By the well-ordering principle, S contains a least element d, so there is a polynomial $r(T) \in A$ with $\deg(r) = d$. This means we can write $r(T) = f(T) - g(T)q(T)$ for some $q(T) \in F[T]$, so that $f(T) = g(T)q(T) + r(T)$. Suppose that $r(T) \neq 0$, then we'll show that $0 \leq \deg(r) < \deg(g)$. Suppose otherwise, that $\deg(r) \geq \deg(g)$. Let's let $\deg(g) = k$. Then we may write $r(T) = r_dT^d + \text{lower degree terms}$, and $g(T) = g_kT^k + \text{lower degree terms}$. We then see that $g(T)(r_d/g_kT^{d-k}) = r_dT^d + \text{lower degree terms}$, so $r(T) - g(T)(r_d/g_kT^{d-k}) = (f(T) - g(T)q(T)) - g(T)(r_d/g_kT^{d-k}) = f(T) - g(T)(q(T) + r_d/g_kT^{d-k})$ is a polynomial in A of strictly smaller degree than d. This contradicts the definition of d. Therefore, if $r(T) \neq 0$, we must have $0 \leq \deg(r) < \deg(g)$. This proves the existence of such $q(T)$ and $r(T)$. It remains to prove uniqueness.

Suppose that we may write $f(T) = g(T)q_1(T) + r_1(T)$ and $f(T) = g(T)q_2(T) + r_2(T)$ for some q_1, q_2, r_1, r_2 satisfying the conditions of the theorem. This says that $g(T)(q_1(T) - q_2(T)) = r_2(T) - r_1(T)$. If we assume that both $q_1(T) - q_2(T)$ and $r_1(T) - r_2(T)$ are both non-zero, then taking degrees, this says $\deg(g(T)) + \deg(q_1(T) - q_2(T)) = \deg(r_2(T) - r_1(T))$. From the degree bounds on r_1, r_2, the right hand side must be at most $\deg(g)$ (if it's non-zero), which gives a contradiction. Therefore, either $q_1(T) - q_2(T) = 0$ or $r_1(T) - r_2(T) = 0$. In either case, once one of these is true it's immediately clear that the other is true as well. This gives $r_1(T) = r_2(T)$ and $q_1(T) = q_2(T)$ as desired. □

Example 2.3. In $\mathbb{Q}[T]$, we have $2T^2 + 1 = (3T + 2)(\frac{2}{3}T - \frac{4}{9}) + \frac{17}{9}$.

Where in the proof of the division algorithm did we actually use that F was a field? It was used exactly twice. First, we had to divide by the leading coefficient of $g(T)$. Second, we used that a field is an integral domain, in order to use the fact that the degree of a product is the sum of their degrees. This means that in an arbitrary integral domain R, we still have a division algorithm in $R[T]$ as long as we divide by a polynomial where the leading coefficient is a *unit*. We'll state this as a theorem for emphasis:

Theorem 2.4. *Let R be an integral domain. Let $f(T) \in R[T]$ and $g(T) \neq 0$ in $R[T]$ such that the leading coefficient of $g(T)$ is a unit. Then there exist unique polynomials $p(T), q(T) \in R[T]$ such that $f(T) = g(T)q(T) + r(T)$ with $r(T) = 0$ or $0 \leq \deg(r) < \deg(g)$.*

Example 2.5. In $(\mathbb{Z}/4\mathbb{Z})[T]$, we have $2T^2 + 1 = (3T + 2)(2T) + 1$.

Once we've obtained a division algorithm, it makes sense to talk about division in $F[T]$.

Definition 2.6. Let $f(T), g(T) \in F[T]$. We say that $f(T)$ **divides** $g(T)$ and write $f(T) \mid g(T)$ if there is a non-zero polynomial $h(T) \in F[T]$ such that $g(T) = f(T)h(T)$.

Example 2.7. In $\mathbb{Q}[T]$, we see that $T + 1 \mid T^2 - 1$, since $T^2 - 1 = (T + 1)(T - 1)$. For any $c \neq 0 \in \mathbb{Q}$, we have $c \mid T^2 - 1$ since $T^2 - 1 = \frac{1}{c}(T^2 - 1) \cdot c$.

Definition 2.8. A non-constant polynomial $\pi(T) \in F[T]$ is called **irreducible**[1] if it has no divisors $d(T)$ with $1 \leq \deg(d(T)) < \deg(\pi(T))$. A polynomial that is not irreducible is called **reducible**.

Example 2.9. The polynomial $T^2 + 1$ is irreducible in $\mathbb{R}[T]$. However, this polynomial *is* reducible in $\mathbb{C}[T]$: we may write $T^2 + 1 = (T - i)(T + i)$. This means that reducibility is an algebraic property of the field where you view the coefficients as living in.

Our definitions of divisors and irreducible polynomials should feel very familiar to how we defined divisors and primes in the integers. In fact, several quantities in $\mathbb{Z}$ and $F[T]$ are analogous to each other:

$\mathbb{Z}$	$F[T]$
± 1	non-zero constants
$\lvert n \rvert$	$\deg(f)$
positive	monic
prime	irreducible

In the integers, ± 1 play the role of the units, and we've seen the units in $F[T]$ are the non-zero constant polynomials. We have a notion of "size" in the integers, namely the absolute value of an integer, which lets us "compare" integers. Similarly, the right way of "comparing" polynomials is by their degree. Any non-zero integer can be turned into a positive integer by multiplying by a unit (namely, -1 if it's negative). Any non-zero polynomial can be turned into a monic polynomial by multiplying by the inverse of the leading coefficient. Prime integers have no non-trivial divisors, and irreducible polynomials have no non-trivial divisors.

In the integers, we had the following chain of reasoning:

$$\text{Division algorithm} \implies \text{Bezout's lemma} \implies \text{Euclid's lemma} \implies \text{Unique factorization.}$$

This told us that any positive integer could be factored uniquely into a product of primes. Since we have just determined that $F[T]$ has a division algorithm, we will have an analogous chain of reasoning:

$$\text{Division algorithm} \implies \text{Bezout's lemma} \implies \text{Euclid's lemma} \implies \text{Unique factorization.}$$

[1]The definition of irreducibility in $R[T]$ for an arbitrary integral domain R is slightly more subtle: $f(T) \in R[T]$ with $f(T) \neq 0$ or a unit is called **irreducible** if $f(T) = g(T)h(T)$ means that $g(T)$ or $h(T)$ is a unit in $R[T]$.

This will tell us that any monic polynomial can be factored uniquely into a product of monic irreducible polynomials. All that we need to do is to make sure that all the relevant terms in the statements in $\mathbb{Z}$ are replaced with their analogues in $F[T]$, and the proofs will be essentially identical. Before doing so, we'll list some analogous properties of divisibility that polynomials have that are similar to the integers.

Proposition 2. *Let $f, g, h \in F[T]$.*

1. *If $f \mid g$ and $g \mid h$ then $f \mid h$.*
2. *If $f \mid g$ and $f \mid h$ then $f \mid pg + qh$ for any $p, q \in F[T]$.*
3. *If $f \mid g$ then $\deg(f) \leq \deg(g)$.*

Before giving a statment of Bezout's lemma, we have to give a definition of the greatest common divisor of two polynomials.

Definition 2.10. Let $f, g \in F[T]$. The **greatest common divisor** of f and g is the monic polynomial $d(T)$ of largest degree such that:

1. $d \mid f$ and $d \mid g$.
2. If $h \mid f$ and $h \mid g$ for some $h(T) \in F[T]$, then $\deg(h) \leq \deg(g)$.

We of course write $\gcd(f, g)$ or (f, g) to denote the greatest common divisor, and if $(f, g) = 1$ we say that f and g are **relatively prime**.

As before, the greatest common divisor is well-defined because of property 3 above, and the monic condition forces it to be unique. If $f = 0$, then for any $g \in F[T]$ we have $(0, g) = \tilde{g}$, where $\tilde{g}$ is the monic rescaling of $g(T)$, and again we have that $(0, 0)$ is undefined.

Example 2.11. In $(\mathbb{Z}/3\mathbb{Z})[T]$ we have that $\gcd(T^3 + T^2 + 2T + 2, T^2 + T) = T + 1$ which can easily be found by factoring.

Theorem 2.12 (Bezout's lemma)**.** *Let $f, g \in F[T]$. There exist polynomials $p, q \in F[T]$ such that $f(T)p(T) + g(T)q(T) = d(T)$, where $d = \gcd(f, g)$.*

Proof. In the integers, we looked at the set of all positive linear combinations of two integers and used the well ordering principle. In $F[T]$, we'll look at the set of all monic non-constant linear combinations of f and g and then use the well ordering principle.

The theorem is obvious if one of f, g are zero, so assume that both $f, g \neq 0$. Let $A = \{f(T)p(T)+g(T)q(T) \text{ monic} : p, q \in F[T]\}$ and let $S = \{\deg(h(T)) : h(T) \in A\}$. Notice that $S \neq \emptyset$, because the monic rescalings of both f and g are elements of A. By the well ordering principle, there is a minimal element of S, say k, which corresponds to a monic polynomial $d_0 \in A$ with $\deg(d(T)) = k$. Since $d_0(T) \in A$, we can write $d_0(T) = f(T)p(T) + g(T)q(T)$ for some $p(T), q(T) \in F[T]$. We will show that $d_0(T) = d(T)$.

Since $d(T) \mid f(T)$ and $d(T) \mid g(T)$ by definition, we have $d(T) \mid f(T)p(T) + g(T)q(T)$ so $d(T) \mid d_0(T)$. This means that $\deg(d(T)) \leq \deg(d_0(T))$. Next, we show that $d_0(T)$ divides every element of A. Let $s(T) \in A$, and write $s(T) = f(T)p_0(T) + g(T)q_0(T)$ for some $p_0, q_0 \in F[T]$. By the division algorithm, we may write $s(T) = d_0(T)b(T) + r(T)$ for unique $b(T), r(T) \in F[T]$ with $r(T) = 0$ or $0 \leq \deg(r) < \deg(d_0)$. Suppose that $r(T) \neq 0$. Then $0 \leq \deg(r) < \deg(d_0)$. We have $r(T) = s(T) - d_0(T)b(T) = f(T)p_0(T) + g(T)q_0(T) - (f(T)p(T)+g(T)q(T))b(T) = f(T)(p_0(T)-p(T)b(T))+g(T)(q_0(T)-q(T)b(T))$. By rescaling $r(T)$ to be monic, we see that $r(T)$ is an element of A with strictly smaller degree than d_0,

a contradiction to the definition of d_0. Therefore, $r(T) = 0$ so $d_0(T) \mid s(T)$. Since the monic rescalings of f and g are in A, we see that $d_0(T)$ must divide both f and g. By definition of the greatest common divisor, this says that $\deg(d_0(T)) \leq \deg(d(T))$, so that $\deg(d_0(T)) = \deg(d(T))$. Since $d(T) \mid d_0(T)$, and $d_0(T)$,$d(T)$ are both *monic* polynomials of the same degree, this forces $d(T) = d_0(T)$ as desired. □

Corollary 2.13. *Let $f, g, h \in F[T]$ with $f \mid gh$ and $(f, h) = 1$. Then $f \mid g$.*

Proof. By Bezout, there are polynomials $p, q \in F[T]$ such that $fp + hq = 1$. Multiplying by g says that $fpg + hqg = g$. Since $f \mid fpg$ and $f \mid hqg$, this says $f \mid g$. □

Proposition 3 (Euclid's lemma)**.** *Let $\pi \in F[T]$. Then π is irreducible if and only if for any polynomials $f, g \in F[T]$, $\pi \mid fg \implies \pi \mid f$ or $\pi \mid g$.*

Proof. First, suppose that π is irreducible in $F[T]$, and suppose that $\pi \mid fg$. Assume that $\pi \nmid f$. Then because π has no non-trivial divisors, this says that $(\pi, f) = 1$. By the previous result, this means that $\pi \mid g$. Conversely, suppose that $\pi \in F[T]$ is a polynomial with the property that $\pi \mid fg \implies \pi \mid f$ or $\pi \mid g$. Let $d \in F[T]$ be a monic divisor of π. Then we may write $\pi(T) = d(T)h(T)$ for some $h(T) \in F[T]$. We then have that $\pi \mid dh$, so $\pi \mid d$ or $\pi \mid h$ by assumption. This means that $\deg(\pi) \leq \deg(d)$ or $\deg(\pi) \leq \deg(h)$. However, since $0 \leq \deg(d), \deg(h) \leq \deg(\pi)$ and $\deg(\pi) = \deg(d) + \deg(h)$, the only way this is possible is if $\deg(d) = 0$ and $\deg(h) = \deg(\pi)$ or $\deg(d) = \deg(\pi)$ and $\deg(h) = 0$, i.e. π is irreducible. □

Theorem 2.14 (Unique factorization)**.** *Let $f(T) \in F[T]$ be a monic, non-constant polynomial. Then there exist unique monic irreducible polynomials $\pi_1(T), \ldots, \pi_k(T) \in F[T]$ and unique positive integers $e_1, \ldots, e_k$ such that $f(T) = \pi_1(T)^{e_1} \cdots \pi_k(T)^{e_k}$. That is, every non-constant monic polynomial has a unique factorization into a product of monic irreducible polynomials.*

Proof. The proof has two parts: we first show that every monic polynomial can be written as a product of *some* monic irreducible polynomials, and then we show that such a choice of irreducibles is *unique*. Both parts will use strong induction on the degree of f.

Existence:
If $\deg(f) = 1$, then f is irreducible by definition, so any monic degree 1 polynomial is a product of monic irreducibles. Now, suppose that we know for any monic polynomial $p(T)$ of degree $\leq k$ that $p(T)$ can be written as a product of monic irreducible polynomials. Let $f(T)$ be a monic polynomial of degree $k + 1$. If $f(T)$ is irreducible, we're done. Otherwise, it has a non-trivial divisor, so we may write $f(T) = g(T)h(T)$ for some $g(T), h(T) \in F[T]$ with $1 \leq \deg(g), \deg(h) < \deg(f)$. Now $g(T)$ and $h(T)$ might *not* be monic, but we can easily fix this: if $g(T)$ has leading coefficent a and $h(T)$ has leading coefficient b, then since $f(T)$ is monic, this forces $ab = 1$. Then $f(T) = ab(\frac{1}{a}g(T))(\frac{1}{b}h(T)) = (\frac{1}{a}g(T))(\frac{1}{b}h(T))$ and now $\frac{1}{a}g(T)$ and $\frac{1}{b}h(T)$ *are* monic. Therefore without loss of generality, we may assume that $g(T), h(T)$ are monic. By induction hypothesis, both $g(T)$ and $h(T)$ may be written as the product of monic irreducible polynomials, and therefore so can $f(T)$. By induction, any non-constant monic polynomial can be written as a product of monic irreducible polynomials.

Uniqueness:
If $\deg(f) = 1$, we noted that f is irreducible, so if f is monic and has degree 1, it's a product of monic irreducibles in a unique way. Now suppose we know for k that any monic polynomial

of degree $\leq k$ has a factorization using a unique set of monic irreducibles. Let $f(T)$ be a monic polynomial of degree $k+1$. If $f(T)$ is irreducible, we're done. Otherwise, suppose we can write $f(T) = \pi_1(T)\cdots\pi_m(T) = q_1(T)\cdots q_\ell(T)$ as a product of monic irreducibles π_i, q_j in two ways. Then $\pi_1(T) \mid q_1(T)\cdots q_\ell(T)$, so by inductively applying Euclid's lemma, we see that $\pi_1(T) \mid q_j(T)$ for some j. Since π_i and q_j are all *monic*, this says that $\pi_1(T) = q_j(T)$ for some j. By re-ordering the factors as necessary, we may assume that $\pi_1(T) = q_1(T)$. Canceling $\pi_1(T)$ from both sides, this says that $a(T) = \pi_2(T)\cdots\pi_m(T) = q_2(T)\cdots q_\ell(T)$. However, $\deg(a(T)) < k+1$, so by our induction hypothesis, this says that $a(T)$ has a unique factorization. This forces $m = \ell$ and $\pi_i = q_i$ (again, up to reordering) for $1 \leq i \leq m$. Since $f(T) = \pi_1(T)a(T)$ and we deduced that $\pi_1(T) = q_1(T)$, this says that $f(T)$ actually had a unique factorization as well. By induction, this says that any monic polynomial has a unique factorization into monic irreducible polynomials. Collecting terms of the same irreducible polynomial together gives the form as stated in the theorem, and the uniqueness of the exponents is immediate. □

We stated unique factorization for monic polynomials so that we actually get uniqueness of irreducibles in the factorization. If you don't require this condition, then an irreducible factorization is only unique up to unit multiple of the factors. Of course, everything still works out if you drop this condition.

3. Computations in $F[T]$

Since $F[T]$ has a division algorithm, we also get a Euclidean algorithm:

Theorem 3.1 (Euclidean Algorithm)**.** *Let $f, g \in F[T]$ be non-zero polynomials. Repeatedly carry out the division algorithm as follows:*

$$\begin{aligned} f(T) &= g(T)q_1(T) + r_1(T) \quad r_1(T) = 0 \text{ or } 0 \leq \deg(r_1) < \deg(q_1) \\ g(T) &= r_1(T)q_2(T) + r_2(T) \quad r_2(T) = 0 \text{ or } 0 \leq \deg(r_2) < \deg(r_1) \\ r_1(T) &= r_2(T)q_3(T) + r_3(T) \quad r_3(T) = 0 \text{ or } 0 \leq \deg(r_3) < \deg(r_2) \\ &\vdots \end{aligned}$$

There is some integer n such that $r_n(T) = 0$. The last non-zero remainder is the greatest common divisor of f and g (after rescaling to be monic).

Like before, having a Euclidean algorithm then allows us to find an explicit $F[T]$-linear combination in Bezout's lemma. The computations are all pretty much identical to their integer counterparts: they just become slightly more annoying to deal with, because polynomial division is harder to do mentally. Since everything works over an arbitrary field F, it's a little more flexible, and one just needs to take care of how to interpret the division that's happening in F.

Example 3.2. In $(\mathbb{Z}/2\mathbb{Z})[T]$, let $f(T) = T^3 + T^2 + 1$ and $g(T) = T^2 + T + 1$. We have:

$$\begin{aligned} T^3 + T^2 + 1 &= (T^2 + T + 1)(T) + (T + 1) \\ T^2 + T + 1 &= (T + 1)T + 1 \\ T + 1 &= 1 \cdot (T + 1) + 0 \end{aligned}$$

Which says that $(T^3 + T^2 + 1, T^2 + T + 1) = 1$. To find which $F[T]$-linear combination of $f(T)$ and $g(T)$ give us 1 we perform back substitution:

$$\begin{aligned} 1 &= (T^2 + T + 1) + T(T + 1) \\ 1 &= (T^2 + T + 1) + T((T^3 + T^2 + 1) + T(T^2 + T + 1)) \\ &= (T^2 + T + 1)(T^2 + 1) + (T^3 + T^2 + 1)(T) \end{aligned}$$

This says that with $p(T) = T^2 + 1$ and $q(T) = T$ we have $f(T)p(T) + g(T)q(T) = 1$.

4. Irreducibility tests

Since (monic) irreducble polynomials are the building blocks of $F[T]$, it's rather important to know *when* a polynomial $\pi(T) \in F[T]$ is irreducible. In the integers, there's an easy to check if an integer n is prime: any composite integer n has a factor m with $1 < m \leq \sqrt{n}$. This is true because if $n = ab$ is composite and both $a, b > \sqrt{n}$, then $ab > n$. One can then check if n is divisible by any integer in this range. This doesn't generalize at all to $F[T]$, because there are usually *infinitely many* irreducible polynomials of a given degree. Fortunately, polynomial rings have extra structure that the integers do not: a polynomial $f(T) \in F[T]$ can be thought of as a function $f : F \to F$! Most irreducibility tests will rely on this extra structure.

Definition 4.1. A **root** of a polynomial $f(T) \in F[T]$ is an element $r \in F$ such that $f(r) = 0$, where $f : F \to F$ is viewed as a function.

Our first goal is to determine when is an element of F a root of $f(T)$.

Theorem 4.2 (Factor theorem)**.** *Let $f(T) \in F[T]$, and let $a \in F$. Then a is a root of $f(T)$ if and only if $T - a$ is a factor of $f(T)$ in $F[T]$.*

Proof. By the division algorithm, we may write $f(T) = (T - a)q(T) + r(T)$ with $r(T) = 0$ or $\deg(r) = 0$. We then see that a is a root of $f(T)$ if and only if $f(a) = r(a) = 0$, i.e. $r = 0$. □

The factor theorem gives us the following key result:

Theorem 4.3. *Let $f(T) \in F[T]$ be a non-zero polynomial of degree n. Then $f(T)$ has at most n roots in F.*

Proof. We induct on the degree of f. If $\deg(f) = 0$ and $f \neq 0$, then f has no roots, which is consistent with the theorem. Now suppose that any polynomial of degree k has at most k roots in F. Let $f(T)$ be a polynomial of degree $k + 1$. If $f(T)$ has no roots in F, we're done. Otherwise, $f(T)$ has a root in F, say a, so by the factor theorem, we may write $f(T) = (T - a)g(T)$ for some $g(T) \in F[T]$. Since $\deg(g) = k$, this means that $g(T)$ has at most k roots in F. Let's say that g has r roots, $c_1, \ldots, c_r$. Then the factor theorem says that $T - c_i \mid g$, for all i, and since $T - c_i$ are all relatively prime, we have $(T - c_1) \ldots (T - c_r) \mid g$. Therefore, we may write $g(T) = (T - c_1) \ldots (T - c_r)h(T)$ for some $h(T)$, where $h(T)$ has no

roots in F. This says that $f(T) = (T-a)(T-c_1)\dots(T-c_r)h(T)$. Any root of $f(T)$ distinct from $a, c_1, \dots, c_r$ would then necessarily have to be a root of $h(T)$, which means that these are *all* the roots of $f(T)$. This says $f(T)$ has a total of $r+1 \leq k+1$ roots in F, which is what we wanted. By induction, we're done. □

It's worth pointing out that nowhere in the above proof we needed that F was a *field*. The same proof would still go through if we replaced $F[T]$ with $R[T]$ where R is an integral domain. However, this is definitely required:

Example 4.4. In $(\mathbb{Z}/8\mathbb{Z})[T]$, the polynomial $T^2 - 1$ has roots $[1], [3], [5], [7]$.

The above theorem gives us our first useful irreducibility test.

Theorem 4.5. *Let $f(T) \in F[T]$ be a polynomial of degree 2 or 3. Then $f(T)$ is irreducible if and only if $f(T)$ has no roots in $F[T]$.*

Proof. We'll show that $f(T)$ is reducible if and only if $f(T)$ has a root in $F[T]$. The backwards direction is immediate by the factor theorem. Now suppose that $f(T)$ is reducible. By definition, we can write $f(T) = g(T)h(T)$ for some $g, h \in F[T]$ with $1 \leq \deg(g), \deg(h) < \deg(f)$. Since $\deg(g)+\deg(h) = \deg(f)$, we see that $\deg(g)+\deg(h) = 2$ or $\deg(g)+\deg(h) = 3$. The bounds mean that either g or h has degree 1. Without loss of generality, we'll assume that $g(T) = aT + b$ is a degree 1 divisor of $f(T)$, so $f(T) = (aT+b)q(T)$ for some $q(T)$. Plugging in $-\frac{b}{a}$ says $f(-\frac{b}{a}) = 0$, so that f has a root in F. □

Note that in this proof, we *did* use that F was a field! We needed to be able to divide by an *arbitrary* element $a \in F$. Being an integral domain is not enough:

Example 4.6. The polynomial $f(T) = 3(T^2+1)$ *is* reducible in $\mathbb{Z}[T]$, but $f(T)$ has no roots in $\mathbb{Z}$.

Example 4.7. The polynomial $T^3 + T + 1 \in (\mathbb{Z}/5\mathbb{Z})[T]$ is irreducible, because manually plugging in the different equivalence classes shows it has no roots.

Our next few irreducibility tests will be for polynomials with *rational* coefficients. We'll later be able to generalize a few of these to an arbitrary polynomial ring $R[T]$ for an integral domain R, but we need the language of ideals to do so.

Theorem 4.8 (Rational root test)**.** *Let $f(T) = a_nT^n + \dots + a_0 \in \mathbb{Z}[T]$. If $\frac{r}{s} \in \mathbb{Q}$ (in lowest terms) is a root of $f(T)$, then $r \mid a_0$ and $s \mid a_n$.*

Proof. Suppose that $f(\frac{r}{s}) = 0$. This says that $a_n\left(\frac{r}{s}\right)^n + \dots + a_0 = 0$. Multiplying through by s^n, we have $a_nr^n + a_{n-1}r^{n-1}s + \dots + a_0s^n = 0$. Every term after the first in the sum is divisible by s, so this means $s \mid a_nr^n$. Since $(r, s) = 1$, this means $s \mid a_n$. Similarly, every term except the last contains an r, so this means $r \mid a_0s^n$. Since $(r, s) = 1$, we have $r \mid a_0$. □

Example 4.9. Let $f(T) = T^3+4T^2+T-1 \in \mathbb{Q}[T]$. Then the only possible rational roots of $f(T)$ are ± 1. It's clear neither of these are roots, which then tells us that $f(T)$ is irreducible since $f(T)$ is a degree 3 polynomial in $\mathbb{Q}[T]$ with no roots.

Example 4.10. The rational root test can be used to give a slick proof that $\sqrt{2}$ is not rational. If it were, it would be a root of the polynomial $T^2 - 2 \in \mathbb{Q}[T]$. The rational root theorem says the only possible rational roots are $\pm 1, \pm 2$, and it's clear none of these are roots. This says $f(T)$ has no rational roots, which gives a contradiction.

Since the rational numbers are built from ratios of integers, it might not be surprising to hear that there is a connection between irreducibility in $\mathbb{Z}[T]$ and irreducibility in $\mathbb{Q}[T]$. To describe this, we make the following definition:

Definition 4.11. A polynomial $f(T) = a_nT^n + \ldots + a_0 \in \mathbb{Z}[T]$ is called **primitive** if $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Example 4.12. The polynomial $f(T) = 3T^2+2T+5 \in \mathbb{Z}[T]$ is primitive because $\gcd(3, 2, 5) = 1$. Any monic polynomial is automatically primitive.

The key to our next few results will be the following basic fact:

Lemma 4.13. *Let p be a prime. Then the map $\varphi : \mathbb{Z}[T] \to (\mathbb{Z}/p\mathbb{Z})[T]$ defined by $\varphi(a_0 + \ldots + a_nT^n) = [a_0] + \ldots + [a_n]T^n$ is a ring homomorphism.*

Proof. Exercise. □

The map above is usually referred to as "reduction mod p". The polynomial $\varphi(f)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$ will usually be denoted as $\bar{f}(T)$.

Theorem 4.14 (Gauss's lemma)**.** *Let $f(T)$ be a non-constant primitive polynomial. Then $f(T) \in \mathbb{Z}[T]$ is irreducible if and only if $f(T) \in \mathbb{Q}[T]$ is irreducible.*

Proof. We'll prove that $f(T)$ is reducible in $\mathbb{Z}[T]$ if and only if $f(T)$ is reducible in $\mathbb{Q}[T]$. Clearly if $f(T) = g(T)h(T)$ is a non-trivial factorization into polynomials in $\mathbb{Z}[T]$, it's also a factorization into polynomials in $\mathbb{Q}[T]$. The subtly however, is that $f(T)$ being reducible in $\mathbb{Z}[T]$ means $f(T)$ can be written as the product of two non-units in $\mathbb{Z}[T]$, and because the units of $\mathbb{Z}[T]$ and $\mathbb{Q}[T]$ are not the same, a non-trivial factorization in $\mathbb{Z}[T]$ might not remain non-trivial in $\mathbb{Q}[T]$. We're clearly fine if both $\deg(g), \deg(h) > 0$, so we only have to worry about what happens if one of the factors is a constant. The point is that if $f(T) = g(T)h(T)$ in $\mathbb{Z}[T]$ and say, $\deg(g) = 0$, then this would mean we could write $f(T) = ch(T)$ for some constant c. By multiplying each coefficient of $h(T)$ by c, we'd find that $f(T)$ is *not* primitive, unless $c = \pm 1$. This means the only possible degree 0 factors of $f(T)$ are ± 1, which means there are no non-trivial factorizations of $f(T)$ in $\mathbb{Z}[T]$ with a degree 0 factor. Therefore a non-trivial factorization of $f(T)$ in $\mathbb{Z}[T]$ remains non-trivial in $\mathbb{Q}[T]$.

Conversely, suppose that $f(T) = g(T)h(T)$ is a factorization in $\mathbb{Q}[T]$. Let c, d be integers such that $cg(T)$ and $dh(T)$ are polynomials with integer coefficients. These can be chosen by taking c, d to be the least common multiple of the denominators that appear in the coefficients of $g(T)$ and $h(T)$ respectively. Then $cdf(T) = (cg(T))(dh(T))$ is a factorization of $cdf(T)$ in $\mathbb{Z}[T]$. Let p be a prime dividing cd. Since $cdf(T) = (cg(T))(dh(T))$, applying the reduction mod p map φ to both sides says that $\varphi(cg(T))\varphi(dh(T)) = 0$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $(\mathbb{Z}/p\mathbb{Z})[T]$ is an integral domain, so either $\varphi(cg(T)) = 0$ or $\varphi(dh(T)) = 0$ in $(\mathbb{Z}/pZ)[T]$. The only way this is possible is if all coefficients of the reduced polynomial are $[0]$ in $\mathbb{Z}/p\mathbb{Z}$, i.e. all coefficients of either $cg(T)$ or $dh(T)$ are divisible by p.

What we've just show is that if $p \mid cd$, then p must divide all the coefficients of either $cg(T)$ or $dh(T)$. Therefore, we can safely cancel p from both sides of the equality $cdf(T) = (cg(T))(dh(T))$. Running the same argument as above, we may keep canceling prime factors of cd from both sides until eventually, we are left with $\pm f(T)$ on the left hand side, and a product of integer polynomials on the right hand side. □

Example 4.15. We'll show that $f(T) = T^4 - 10T^2 + 1$ is irreducible in $\mathbb{Q}[T]$. By the rational root theorem, the only possible roots of $f(T)$ are ± 1, and it's clear neither of these work. Therefore if $f(T)$ is reducible, it must factor as a product of two quadratics, and by dividing through by the leading coefficients if necessary, we may assume said quadratics are monic. Since $f(T)$ is primitive, we may write $T^4 - 10T^2 + 1 = (T^2 + aT + b)(T^2 + cT + d)$ for some $a, b, c, d \in \mathbb{Z}$. Expanding says $T^4 - 10T^2 + 1 = T^4 + (a+c)T^3 + (ac+b+d)T^2 + (ad+bc)T + bd$. Comparing coefficients says $a = -c$, $b + d = c^2 - 10$, $c(b - d) = 0$, and $bd = 1$. The last equation means $b = d = 1$ or $b = d = -1$, so the second equation means $c^2 = 12$ or $c^2 = 8$, both of which are not possible to solve in the integers. This means no such factorization is possible, and therefore $f(T)$ is irreducible.

An easy application of Gauss's lemma is the following irreducibility criterion:

Theorem 4.16 (Eisenstein's criterion)**.** *Let $f(T) = a_n T^n + \ldots + a_0 \in \mathbb{Z}[T]$. Suppose there is a prime p such that:*

(i) $p \mid a_i$ *for* $0 \leq i < n$.
(ii) $p \nmid a_n$
(iii) $p^2 \nmid a_0$

Then $f(T)$ is irreducible in $\mathbb{Q}[T]$.

Proof. Let $c = \gcd(a_0, \ldots, a_n)$. We may write $f(T) = c\tilde{f}(T)$, where $\tilde{f}(T) = \frac{1}{c} f(T) \in \mathbb{Z}[T]$ is primitive. Note that the conditions in the theorem mean that $(p, c) = 1$, and therefore this means that $\tilde{f}$ is now a primitive polynomial that satisfies the same hypothesis as $f(T)$. Therefore, we'll assume that $f(T)$ is primitive. Suppose that $f(T) = g(T)h(T)$ is reducible in $\mathbb{Q}[T]$, where $g(T) = g_0 + \ldots + g_m T^m$ and $h(T) = h_0 + \ldots + h_\ell T^\ell$. Then by Gauss's lemma, we may assume that $g(T), h(T) \in \mathbb{Z}[T]$. Reducing mod p, this says that $\bar{g}(T)\bar{h}(T) = [a_n]T^n$ in $(\mathbb{Z}/p\mathbb{Z})[T]$, where $\bar{g}(T)$ and $\bar{h}(T)$ denote the images of g and h inside $(\mathbb{Z}/p\mathbb{Z})[T]$ under the reduction map. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $(\mathbb{Z}/p\mathbb{Z})[T]$ has unique factorization. Therefore, we must have $\bar{g}(T) = [g_m]T^m$ and $\bar{h}(T) = [h_\ell]T^\ell$. In particular, this means both $[g_0]$ and $[h_0]$ equal $[0]$ in $\mathbb{Z}/p\mathbb{Z}$, so p divides both g_0 and h_0. However, the constant term of $f(T)$ is the product $g_0 h_0$, and since p divides both factors this would mean $p^2 \mid a_0$, a contradiction. Therefore, $f(T)$ is irreducible in $\mathbb{Q}[T]$.

□

Eisenstein's criterion is useful for producing examples of irreducible polynomials. However in practice, it's not that useful: the "typical" $f(T) \in \mathbb{Z}[T]$ will not satisfy Eisenstein's criterion for *any* prime p!.

Example 4.17. For any $n \geq 2$, Eisenstein's criterion says that $T^n - 2$ is Eisenstein at the prime 2, and therefore is irreducible in $\mathbb{Q}[T]$. That is to say, $\sqrt[n]{2}$ is irrational for all $n \geq 2$.

Example 4.18. Let $f(T) = T^4 - 4T^3 + 6T^2 - 2T + 1$. We can't directly apply Eisenstein's criterion, but we can do the following: set $g(T) = f(T + c)$ for any $c \in \mathbb{Q}$. Saying $f(T) = a(T)b(T)$ for some $a, b \in \mathbb{Q}[T]$ is the same as saying that $g(T) = a(T+c)b(T+c)$. Conversely, if $g(T) = a(T)b(T)$ for some $a, b \in \mathbb{Q}$ then $f(T) = a(T - c)b(T - c)$ is a factorization of $f(T)$. Therefore, $f(T)$ and $g(T)$ are either both irreducible, or both reducible. We notice that $f(T + 1) = T^4 + 2T + 2$ which is Eisenstein at 2, so $f(T)$ is irreducible in $\mathbb{Q}[T]$.

Theorem 4.19. *Let $f(T) \in \mathbb{Z}[T]$. Suppose there is a prime p with $\deg(\bar{f}) = \deg(f)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. If $\bar{f}(T)$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[T]$, then $f(T)$ is irreducible in $\mathbb{Q}[T]$.*

Proof. We prove the contrapositive, that if $f(T)$ is reducible in $\mathbb{Q}[T]$, that $\bar{f}(T)$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[T]$. First, assume that $f(T)$ is primitive and suppose that $f(T) = g(T)h(T)$ in $\mathbb{Q}[T]$. Then by Gauss's lemma, we may assume that $g(T), h(T) \in \mathbb{Z}[T]$, and since $f(T)$ is reducible, this means that $\deg(g), \deg(h) \geq 1$. Reducing mod p says that $\bar{f}(T) = \bar{h}(T)\bar{g}(T)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. Since $\deg(\bar{f}) = \deg(f)$, this means that $\deg(\bar{g}) = \deg(g)$ and $\deg(\bar{h}) = \deg(h)$ because $(\mathbb{Z}/p\mathbb{Z})[T]$ is an integral domain, i.e. $\bar{f}(T)$ has a non-trivial factorization in $(\mathbb{Z}/p\mathbb{Z})[T]$.
If f is not primitive, then instead look at the primitive polynomial $\tilde{f}(T) = \frac{1}{c}f(T) \in \mathbb{Z}[T]$, where c is the greatest common divisor of the coefficients of f. Running the same argument says that if $\tilde{f}$ is reducible in $\mathbb{Q}[T]$, then $\tilde{f}$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[T]$. The degree condition forces $(c, p) = 1$, so $[c] \neq [0]$ in $\mathbb{Z}/p\mathbb{Z}$. The point is then if $\tilde{f}(T) = a(T)b(T)$ is a non-trivial factorization of $\tilde{f}$, we have $f(T) = c\tilde{f}(T) = ca(T)b(T)$ is a non-trivial factorization of $f(T)$ in $\mathbb{Q}[T]$ and then reducing mod p gives a non-trivial factorization of $\bar{f}(T)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$. □

Example 4.20. The polynomial $f(T) = T^3 - 4T^2 + 3T + 1$ is irreducible in $\mathbb{Q}[T]$ because $\bar{f}(T) = T^3 + T + 1 \in (\mathbb{Z}/2\mathbb{Z})[T]$ is irreducible (it has no root in $\mathbb{Z}/2\mathbb{Z}$).

5. Repeated roots of polynomials

Given a polynomial $f(T) \in \mathbb{C}[T]$, the factor theorem says that a root of $f(T)$ corresponds to a linear factor of $f(T)$. How can we check for divisibility of a polynomial by a *repeated* linear factor?

Definition 5.1. A number $c \in \mathbb{C}$ is called a **repeated root** of $f(T) \in \mathbb{C}[T]$ if $(T-c)^k \mid f(T)$ for some $k \geq 2$. The **multiplicity** of c is the largest number k such that $(T-c)^k \mid f(T)$ and $(T-c)^{k+1} \nmid f(T)$.

Example 5.2. The polynomial $f(T) = T^2 - 2T + 1 = (T-1)^2$ has a repeated root at 1 of multiplicity 2.

It turns out, there is a surprisingly easy criterion in terms of the *derivative* of the polynomial $f(T)$. The derivative of a polynomial makes sense in the more general context of fields, even where calculus does not.

Definition 5.3. For a field F, the **derivative** $f'(T) \in F[T]$ of the polynomial $f(T) = a_nT^n + \ldots + a_1T + a_0$ is defined by $f'(T) = na_nT^{n-1} + \ldots + a_1$.

The derivative still has the familiar properties you would want it to from calculus, which can just be verified by an easy computation.

Proposition 4. *Let $f(T), g(T) \in F[T]$. Then the following hold:*
(a) *(Linearity) $(af + bg)'(T) = af'(T) + bg'(T)$ for any $a, b \in F$.*
(b) *(Product rule) $(fg)'(T) = f'(T)g(T) + f(T)g'(T)$.*
(c) *(Chain rule) $(f \circ g)'(T) = f'(g(T))g'(T)$.*

Proof. Exercise. □

We will state our result for polynomials with *rational* coefficients, which relies on the fundamental theorem of algebra:

Theorem 5.4. *If $f(T) \in \mathbb{C}[T]$ is non-constant, then $f(T) = (T-r_1)^{e_1} \ldots (T-r_k)^{e_k}$ for some $r_1, \ldots, r_k \in \mathbb{C}$ and some e_i with $e_1 + \ldots + e_k = \deg(f)$. That is to say, every non-constant polynomial in $\mathbb{C}[T]$ splits completely into linear factors.*

Corollary 5.5. *Let $f(T) \in \mathbb{Q}[T]$ and $c \in \mathbb{C}$. Then c is a root of $f(T)$ of multiplicity k if and only if $f(c) = f'(c) = \ldots = f^{(k-1)}(c) = 0$ and $f^{(k)}(c) \neq 0$.*

Proof. Assume the derivative conditions hold. By the fundamental theorem of algebra, we may choose e maximal such that we may write $f(T) = (T-c)^e h(T)$ for some $h(T) \in \mathbb{C}[T]$ with $(T-c) \nmid h(T)$. Setting $g(T) = (T-c)^e$, we have $f^{(k)}(T) = \sum_{i=0}^{k} \binom{k}{i} g^{(i)}(T) h^{(k-i)}(T)$ by repeatedly applying the product rule. In particular, we have $(T-c)^{e-k} \mid f^{(k)}(T)$, so because $f^{(k)}(c) \neq 0$, this means that $e \leq k$. If $e < k$, then examining $f^{(e)}(T)$ says $f^{(e)}(T) = \sum_{i=0}^{e} \binom{e}{i} g^{(i)}(T) h^{(e-i)}(T)$. Plugging in c says $0 = f^{(e)}(c) = e! h(c)$, so $h(c) = 0$, i.e. $(T-c) \mid h(T)$, a contradiction. Therefore, $e = k$. It's clear from the above derivative computation that if c is a root of multiplicity k that $f(c) = f'(c) = \ldots = f^{(k-1)}(c) = 0$ and $f^{(k)}(c) \neq 0$, so we're done. □

Given a root of a polynomial, the above easily lets us determine it's multiplicity. However, finding roots of a polynomial is a very hard problem. In most applications, one only cares about if a polynomial has *some* repeated root or not. Once this is determined, if one cares about the multiplicity of the root, other methods can be used to locate it. The following criterion allows us to check for a repeated root without having to know anything about what the roots are!

Theorem 5.6. *Let $f(T) \in \mathbb{Q}[T]$. Then $f(T)$ has no repeated root (in $\mathbb{C}$) if and only if $(f(T), f'(T)) = 1$ in $\mathbb{Q}[T]$.*

Proof. The proof relies on the following fact: two polynomials being coprime does not depend over what field ($\mathbb{Q}$ or $\mathbb{C}$) we view them as living in!. What we'll first show is that $(f, f') = 1$ in $\mathbb{Q}[T]$ if and only if $(f, f') = 1$ in $\mathbb{C}[T]$. Suppose that $(f, f') = 1$ in $\mathbb{Q}[T]$. Then there are polynomial $p, q \in \mathbb{Q}[T]$ such that $fp + f'q = 1$. Since $\mathbb{Q}[T] \subset \mathbb{C}[T]$, we've found a $\mathbb{C}[T]$-linear combination of polynomials that give 1, so $(f, f') = 1$ in $\mathbb{C}[T]$. Conversely, suppose that $(f, f') = 1$ in $\mathbb{C}[T]$. If $d(T) \in \mathbb{Q}[T]$ is a divisor of both $f(T)$ and $f'(T)$, then $d(T) \in \mathbb{C}[T]$ is still a common divisor, and therefore must divide 1, so that $(f, f') = 1$ in $\mathbb{Q}[T]$.

Now that we have this, the proof is fairly straightforward. We'll prove that $f(T)$ has a repeated root if and only if $(f, f') \neq 1$ in $\mathbb{Q}[T]$. Suppose that $f(T)$ has a repeated root in $\mathbb{C}$, so $(T-a)^k \mid f(T)$ in $\mathbb{C}[T]$ for some $a \in \mathbb{C}$ and $k \geq 2$. We can write $f(T) = (T-a)^k g(T)$ for some $g(T) \in \mathbb{C}[T]$. Taking a derivative, $f'(T) = k(T-a)^{k-1} g(T) + (T-a)^k g'(T)$ says that $(T-a)^{k-1} \mid f$ and $(T-a)^{k-1} \mid f'$, so $(T-a)^{k-1} \mid (f, f')$ in $\mathbb{C}[T]$, so that $(f, f') \neq 1$ in $\mathbb{Q}[T]$. Conversely, suppose that $(f, f') = d(T) \neq 1$ in $\mathbb{Q}[T]$. Let $\pi(T)$ be any irreducible factor of $d(T)$. Then we can write $f(T) = \pi(T) g(T)$ and $f'(T) = \pi(T) h(T)$ for some $g(T), h(T) \in \mathbb{Q}[T]$. Taking a derivative, this says $f'(T) = \pi'(T) g(T) + \pi(T) g'(T)$, so $\pi'(T) g(T) + \pi(T) g'(T) = \pi(T) h(T)$. This means that $\pi(T) \mid \pi'(T) g(T)$. Since $\pi(T)$ is *irreducible*, for degree reasons we must have $(\pi(T), \pi'(T)) = 1$. This means that $\pi(T) \mid g(T)$, so $\pi(T)^2 \mid f(T)$. Now, by the fundamental theorem of algebra, $\pi(T)$ has a root $c \in \mathbb{C}$, so $T - c \mid \pi(T)$ in $\mathbb{C}[T]$. This means that $(T-c)^2 \mid f(T)$ in $\mathbb{C}[T]$, so $f(T)$ has c as a repeated root in $\mathbb{C}$. □

Example 5.7. The polynomial $f(T) = T^3 - 4T^2 + 5T - 2$ has derivative $f'(T) = 3T^2 - 8T + 5$. Note that $f(1) = f'(1) = 0$, so $(T-1)^2 \mid f(T)$. One then easily finds $f(T) = (T-1)^2(T-2)$.

Example 5.8. If $f(T) \in \mathbb{Q}[T]$ is irreducible, we must have $(f, f') = 1$ because f' has smaller degree, and $f'(T) \neq 0$ (constant polynomials cannot be irreducible – this is important!).

This means that any irreducible polynomial in $\mathbb{Q}[T]$ has *distinct* roots in $\mathbb{C}[T]$. For example, $f(T) = T^7 - 48T + 24$ is Eisenstein at 3, so it is irreducible in $\mathbb{Q}[T]$, and therefore splits into a product of distinct linear factors in $\mathbb{C}[T]$.