Theorem 1. Let $F$ be a field and $f(x) \in F[x]$ a nonconstant polynomial. Then $f(x)$ is a product of (one or more) irreducible polynomials.

Proof. Suppose not. Then some nonconstant polynomial is not the product of irreducible polynomials. Choose one such polynomial, say $f(x)$, of smallest possible degree. That is, every nonconstant polynomial of degree smaller than $\deg f(x)$ is the product of irreducibles. Now, $f(x)$ is not irreducible (else it is the product of one irreducible), which means $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x)$ and $h(x)$ in $F[x]$. Since $\deg f = \deg g + \deg h$ and $\deg g \geq 1$ and $\deg h \geq 1$, we must have $\deg g < \deg f$ and $\deg h < \deg f$. Hence, $g$ and $h$ are the product of irreducibles, and hence $f$ is also, a contradiction. □

For the uniqueness of this factorization, we need to be a little careful with constant multipliers. For example,

$$x^2 - 1 = (x - 1)(x + 1) = (2x - 2)(\frac{1}{2}x + \frac{1}{2})$$

are two different factorizations of $x^2 - 1$ into irreducibles. But, the number of irreducible factors in each factorization is the same, and further, the factors in each factorization only differ by constant multiples. For nonzero polynomials $f(x), g(x) \in F[x]$, we write $f \sim g$ if $f = cg$ for some $c \in F$.

Exercise: Prove that $\sim$ defined above is an equivalence relation on the set of nonzero polynomials in $F[x]$.

We’ll also need the following result, which shows that irreducible polynomials have the same property as primes do in the integers:

Lemma 2. Let $F$ be a field and $f(x), g(x), h(x) \in F[x]$ with $f$ irreducible. Suppose $f \mid gh$. Then $f \mid g$ and $f \mid h$.

Proof. Consider $d = \gcd(f, g)$. If $d = 1$ then $f \mid h$ by one of the Exercises on Worksheet #17. Otherwise, suppose $d \neq 1$. Write $f = dq$ for some $q \in F[x]$. Since $d \neq 1$, $d$ cannot be a constant (since it must be monic). As $f$ is irreducible, we must have $q$ is a constant. Hence, $f \mid d$. And since $d \mid g$, we get $f \mid g$. □

Theorem 3. Let $F$ be a field and $f(x) \in F[x]$ a nonconstant polynomial. Consider two factorizations of $f(x)$ into irreducible polynomials:

$$f(x) = p_1(x) \cdots p_k(x)$$
$$= q_1(x) \cdots q_\ell(x),$$

where the $p_i$’s and the $q_j$’s are all irreducible. Then $k = \ell$ and, after reordering, $p_i \sim q_i$ for $i = 1, \ldots, k$.

Proof. The proof is almost identical to the proof of the Fundamental Theorem of Arithmetic. □

Corollary 4. Let $F$ be a field and $f(x)$ a nonzero polynomial with $n = \deg f$. Then $f(x)$ has at most $n$ roots in $F$. 


Proof. Let \( c_1, \ldots, c_m \) be the roots of \( f(x) \) in \( F \). By the Root Theorem, this means \( x - c_i \) is a factor of \( f(x) \). Since \( x - c_i \not\sim x - c_j \) (for \( i \neq j \)), each of these factors must appear in an factorization of \( f(x) \) into irreducibles. Hence, the polynomial \((x - c_1) \cdots (x - c_m)\) divides \( f(x) \). Since the degree of \((x - c_1) \cdots (x - c_m)\) is \( m \) and \( \deg f = n \), we must have \( m \leq n \). Hence, \( f(x) \) has at most \( n \) roots.

Corollary 5. Let \( F \) be a field and \( f(x), g(x) \in F[x] \). Suppose \( F \) has infinitely many elements and that \( f(a) = g(a) \) for every \( a \in F \) (i.e., \( f \) and \( g \) are equal as functions on \( F \)). Then \( f(x) = g(x) \) as polynomials (i.e., \( f \) and \( g \) have the exact same coefficients).

Proof. Let \( h = f - g \in F[x] \). By assumption, \( h(a) = 0 \) for every \( a \in F \); i.e., \( h \) has infinitely many roots. If \( h(x) \neq 0 \), this would contradict the previous Corollary. Hence, \( h = 0 \) and so \( f(x) = g(x) \).

Now we move on to some results about specific fields. We begin with \( \mathbb{C} \), the field of complex numbers. The first theorem is called The Fundamental Theorem of Algebra. It was first proved by Gauss around 1800.

Theorem 6. Let \( f(x) \in \mathbb{C}[x] \). Then \( f(x) \) is irreducible if and only if \( \deg f = 1 \). Consequently, every nonconstant polynomial in \( \mathbb{C}[x] \) can be factored into linear (degree one) polynomials.

Theorem 7. Let \( f(x) \in \mathbb{R}[x] \). Then \( f(x) \) is irreducible if and only if \( \deg f = 1 \) or \( f = ax^2+bx+c \) where \( b^2 - 4ac < 0 \). Consequently, every nonconstant polynomial in \( \mathbb{R}[x] \) is a product of linear and quadratic (degree two) polynomials.

Checking whether polynomials in \( \mathbb{Q}[x] \) are irreducible in general is difficult. For degree two and three polynomials, one can check for roots using the Rational Root Theorem. Here is one useful result:

Theorem 8. (Eisenstein’s Criterion) Let \( f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x] \). Suppose there exists a prime \( p \) such that

1. \( p \) does not divide \( a_n \);
2. \( p \) divides \( a_i \) for \( 0 \leq i \leq n - 1 \);
3. \( p^2 \) does not divide \( a_0 \).

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

Homework/Exercises:

1. Factor \( x^4 - 4 \) into irreducibles in \( \mathbb{Q}[x] \).
2. Factor \( x^4 - 4 \) into irreducibles in \( \mathbb{R}[x] \).
3. Factor \( x^4 - 4 \) into irreducibles in \( \mathbb{C}[x] \).
4. Factor \( x^6 - 1 \) into irreducibles in \( \mathbb{Z}_7[x] \).
5. Prove \( x^4 + x + 1 \) is irreducible in \( \mathbb{Z}_2[x] \).
6. Prove \( f(x) = 2x^6 - 6x^3 + 18x^2 - 12 \) is irreducible in \( \mathbb{Q}[x] \).