Goal: To generalize three well known constructions:

**Fractions:** \( \mathbb{Z} \longrightarrow \mathbb{Q} \) (the field of fractions for a ring)

**Polynomial:** \( \mathbb{R} \longrightarrow \mathbb{R}[x] \) (the polynomial ring of a field/ring)

**Extension:** \( \mathbb{R} \longrightarrow \mathbb{C} \) (an algebraic extension field)

\( \mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1 \rangle \)
What is a Polynomial?

**Question:** What is a Polynomial?

- A polynomial is a function - polynomial function
- A polynomial is an abstract construction - polynomial form
- A polynomial is an element of the ring $R[x]$

**Examples:**

- $\mathbb{Z}_2[x]$
  - Note: $0 = 0^2 = 0^3 = \ldots$ and $1 = 1^2 = 1^3 = \ldots$
  - So as functions $x = x^2 = x^3 = \ldots$

- $\mathbb{Z}_p[x]$
  - So as functions $x = x^p = x^{2p-1} = x^{3p-2} = \ldots$
  - There are only $p^p$ possible functions $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$
Polynomials: History

- Euclid - geometric interpretation - homogeneous only
- Diophantus - non-homogeneous polynomials
History of Root Finding

- Quadratic [antiquity]
- Cubic
- Quartic
- Quintic
**Def:** The *complex numbers* is the quotient field $\mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1 \rangle$

**Def:** A field $\mathbb{F}$ is *algebraically closed* if every polynomial in $\mathbb{F}[x]$ has a root in $\mathbb{F}$.

**Thm:** (Fundamental Theorem of Algebra) Any polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

**Lemma:** If every non-constant real polynomial has a root (possibly complex), then any non-constant complex polynomial has a root.

**pf:** If $p(x) \in \mathbb{C}[x]$, construct $q(x) = p(x)p(\overline{x}) \in \mathbb{R}[x]$

If $q(x_0) = 0$, then either $p(x_0) = 0$ or $p(\overline{x_0}) = 0 \spadesuit$

**Lemma:** Every non-constant real polynomial has a root (possibly complex).

**pf:**
Def: The degree
Def: The leading coefficient
Def: A monic
Ring/Algebra of Polynomials

**Prop:** If $R$ is a ring, then $R[x]$ is a ring.

**Def:** An *integral domain* is a commutative ring with no zero-divisors other than zero itself.

**Examples:**
- Any field is an integral domain
- $\mathbb{Z}$ is an integral domain
- $M_2(\mathbb{R})$ is not an integral domain

**Prop:** If $R$ is an integral domain, then $R[x]$ is an integral domain
**Def:** A *unique factorization domain*, UFD, is an integral domain with unique factorization:

- Commutative ring
- No zero-divisors (equiv: cancellation law)
- Non-zero, non-units have factorizations into irreducibles, unique up to reordering and units

**Thm:** (Gauss’s Lemma) If $R$ is a unique factorization domain, then $R[x]$ is a unique factorization domain.

**Thm:** If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a ring with unique factorization.

**Lemma:** If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a Euclidean Domain.
**Thm:** If $F$ is a field, then $F[x]$ is a ring with unique factorization.

**Thm:** If $F$ is a field, then $F[x]$ is a Euclidean Domain.

**Lemma:** (Division Algorithm) Given $a(x), b(x) \in R[x]$, where $b(x) \neq 0$, there are unique $q(x), r(x) \in R[x]$ with $\deg(r(x)) < \deg(q(x))$, such that

**Lemma:** A polynomial form, $p(x)$, over integral domain $R$ is divisible by $(x - a)$ iff $r(a) = 0$

**pf:** (Proving $\iff$, other direction is trivial)

\[ p(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n = \sum_{i=0}^{n} c_i x^i \quad (c_n \neq 0) \]

So

\[ p(x) - p(a) = \sum_{i=0}^{n} c_i(x^i - a^i) = \sum_{i=0}^{n} c_i(x - a)(x^{i-1} + x^{i-2}a + \ldots + a^{i-1}) \]

So $p(x) - p(a) = (x - a)s(x)$ for some polynomial $s(x)$.
Thm: If $F$ is a field, then $F[x]$ is a ring with unique factorization.

Thm: If $F$ is a field, then $F[x]$ is a Euclidean Domain.

Corr: If $R$ is an infinite integral domain, then $p(x)$ and $q(x)$ define the same function iff $p(x) = q(x)$

pf: (Proving $\implies$ - other direction is trivial)

Assume $\forall a \in R, p(a) = q(a)$

Let $r(x) = p(x) - q(x)$ and show that $r(x) = 0$

Degree of $r(x)$ is bounded by degrees of $p(x)$ and $q(x)$, call it $n$

So $r(x)$ has at most $n$ zeros

But $r(a) = 0$ for all (infinite number) $a \in R$ ≠

Thus $r(x) = 0$ ♠
Lagrange Interpolation

Algorithm: (Lagrange Interpolation) Given values \( \{f(x_i), i = 0, \ldots, n\} \), construct a (minimal degree) polynomial with these values.

\[
p(x) = \sum_{i=0}^{n} f(x_i) \frac{\prod_{j \neq i} (x-x_j)}{\prod_{j \neq i} (x_i-x_j)}
\]
Irreducibility: Gauss’ Lemma

Def: \( p(x) = \sum_i p_i x^i \) is a primitive polynomial in \( \mathbb{Z}[x] \) if \( \gcd(\{p_i\}) = 1 \)

Examples:

- \( 3 - 5x^2 \in \mathbb{Z}[x] \) is primitive
- \( 3 - 6x^2 \in \mathbb{Z}[x] \) is not primitive
- \( 2 - 6x^2 \in \mathbb{Z}_{15}[x] \) is primitive (\( \gcd(2, 6) = 2 \in \mathbb{Z}_{15}^* \))

Gauss’s Lemma (III): If \( p(x) \) is irreducible over \( \mathbb{Z}[x] \) then it is irreducible over \( \mathbb{Q}[x] \)

Gauss’s Lemma (I): The product of primitive polynomials is primitive.

pf: Let \( \sum_k c_k x^k = (\sum_k a_k x^k)(\sum_k b_k x^k) \).
Assume the negation, so \( \sum_k a_k x^k \) and \( \sum_k b_k x^k \) are primitive but some prime \( p \) divides all coeffs \( c_k = \sum_i a_i b_i \).
Lemma: If $f(x) \neq 0$ in $\mathbb{F}[x]$ then $f(x) = c_f f^*(x)$, where $c_f \in \mathbb{F}$, $f^*$ is primitive in $R[x]$, unique up to unit (where $\mathbb{F}$ is the field of fractions of ring $R$)

Lemma: If $f(x) = g(x)h(x) \in R[x]$ then $c_f = uc_g c_h$ and $f^*(x) = u^{-1}g^*(x)h^*(x)$ (where $u \in R$ is a unit)

Thm: (Gauss’s Lemma) If $f(x) \in R[x]$ factors uniquely in $\mathbb{F}[x]$, then it factors uniquely in $R[x]$

pf: Assume $f(x)$ factors as $f(x) = g(x)h(x)$ in $\mathbb{F}[x]$

$f(x) \in \mathbb{F}[x] \rightarrow \{c_f, f^*(x)\} \in \mathbb{F} \times R[x]$

So $f^*(x)$ factors (up to unit) as $f^*(x) = ug^*(x)h^*(x)$ and $c_f = u'c_g c_h$
**Thm:** If there is some prime \( p \) such that \( p \mid a_i \) for \( i < n \), \( p \nmid a_n \) and \( p^2 \nmid a_0 \), then \( a(x) = \sum_{i=0}^{n} a_i x^i \) is irreducible over \( \mathbb{Q}[x] \).
Irreducibility: Counting Polynomials in $\mathbb{Z}_p[x]$

**Lemma:** If $I_p(n)$ is the number of irreducible monic polynomials over $\mathbb{Z}_p[x]$ of degree $n$, then

$$I_p(n) = \frac{1}{n} \sum_{d|n} \mu(d)p^{n/d}$$

where $\mu$ is the Möbius Mu function.

In particular $$(1 - 2p^{-n/2})/n \leq I_p(n)/p^n \leq \frac{1}{n}$$

**Example:** Count irreducible polynomials over $\mathbb{Z}_3[x]$

- There is one monic polynomial of degree 0: $a(x) = 1$
- There are three monic polynomials of degree 1: $a(x) \in \{x, x + 1, x + 2\}$
  - They are all irreducible
- There are $3^2 = 9$ monic polynomials of degree 2:
  - $a(x) \in \{x^2, x^2 + 1, x^2 + 2, x^2 + x, x^2 + x + 1, x^2 + x + 2, x^2 + 2x, x^2 + 2x + 1, x^2 + 2x + 2\}$
  - There are six combinations of the degree 1 polynomials, so there are $9-6=3$ irreducible polynomials.
- There are $3^3 = 27$ monic polynomials of degree 3
  - There are so there are $9-6=3$ irreducible polynomials.
Irreducibility: Proving Irreducibility in $\mathbb{Z}_p[x]$

**Def:** $a(x)$ is a **primitive** element in $\mathbb{Z}_p/\langle p(x) \rangle$ if it has order $p^n - 1$ - in other words, $a(x)^{p^n-1} = 1 \pmod{p(x)}$ and $a(x)^i = 1 \pmod{p(x)}$ for $i < p^n - 1$

**Def:** A polynomial is **primitive** if the element $x \in GF(p^n) = \mathbb{Z}_p/\langle p(x) \rangle$ has full order.

**Algorithm:** If there is some $a(x) \in \mathbb{Z}_p/\langle p(x) \rangle$ which has order $p^n - 1$ (a primitive element) then $p(x)$ is irreducible in $\mathbb{Z}_p$

**Note:** If $a(x) \in \mathbb{Z}_p/\langle p(x) \rangle$ has order which is not a divisor of $p^n - 1$ then $p(x)$ is reducible in $\mathbb{Z}_p$

**Example:** Show that $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible

- Find $o(x) \in \mathbb{Z}_2[x]/\langle x^4 + x^3 + x^2 + x + 1 \rangle$
  
  $x^4 \equiv x^3 + x^2 + x + 1$
  
  $x^5 = (x^4)(x) \equiv (x^3 + x^2 + x + 1)(x) = x^4 + x^3 + x^2 + x \equiv 1$
  
  So $o(x) = 5$

- Find $o(x + 1) \in \mathbb{Z}_2[x]/\langle x^4 + x^3 + x^2 + x + 1 \rangle$
  
  $(x + 1)^4 = x^4 + 1 \equiv x^3 + x^2 + x$
  
  $(x + 1)^5 = (x + 1)^4(x + 1) \equiv (x^3 + x^2 + x)(x + 1) = (x^4 + x^3 + x^2) + (x^3 + x^2 + x) = x^4 + x \equiv x^3 + x^2 + 1$
  
  $(x + 1)^8 = ((x + 1)^4)^2 = (x^3 + x^2 + x)^2 = x^6 + x^4 + x^2 \equiv x^3 + 1$
  
  So $o(x + 1) = 15$ and $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible
**Thm:** (Square-Free) If \( a(x) = p(x)^2 q(x) \) has a repeated factor, then 
\[ p(x) \mid \gcd(a(x), a'(x)) \]

**pf:** If \( a(x) = p(x)^2 q(x) \) then 
\[ a'(x) = 2p(x)p'(x)q(x) + p(x)^2 q'(x) \]
So 
\[ p(x) \mid \gcd(p(x)^2 q(x), 2p(x)p'(x) + p(x)^2 q'(x)) = \gcd(a(x), a'(x)) \]

**Examples:**

- \( a(x) = 2x^4 + 5x^3 + 7x^2 + 7x + 3 = (x + 1)^2(2x^2 + x + 3) \in \mathbb{Q}[x] \)
  
  \[ a'(x) = 8x^3 + 15x^2 + 14x + 7 \]
  So 
  \[ \gcd(a(x), a'(x)) = (x + 1) \]

- \( a(x) = x^5 - 4x^4 + 3x^3 - 2x^2 + 20x - 24 = (x - 2)^3(x^2 + 2x + 3) \in \mathbb{Q}[x] \)
  
  \[ a'(x) = 5x^4 - 16x^3 + 9x^2 - 4x + 20 \]
  So 
  \[ \gcd(a(x), a'(x)) = x^2 - 4x + 4 = (x - 2)^2 \]
Lemma: If \( p(x) \in \mathbb{Z}_p[x] \) is an irreducible degree \( n \) polynomial, then 
\[ p(x) \mid (x^{p^n} - x) \]

pf: Construct the finite field \( GF(p^n) = \mathbb{Z}_p[x]/\langle p(x) \rangle \)
The order of the group of units is \( \#GF(p^n)^* = p^n - 1 \)
So each element \( x \) has an order which is a divisor of \( p^n - 1 \) (Lagrange) ♠

Algorithm: \( \gcd(a(x), (x^{p^n} - x)) \) is the product of the factors of \( a(x) \) of degree less than or equal to \( n \).

Examples: