Theorem 6.3.2 (Factor Theorem)

Let \( f(x) \in F[x] \) be a field, and \( f(a) = 0 \) \( \iff \) \((x-a)\) is a factor of \( f(x) \).

Proof: If \( f(x) = (x-a)g(x) \) then \( f(a) = 0 \cdot g(a) = 0 \). This proves \( \Rightarrow \).

For \( \Rightarrow \), use division algorithm.

\[ f(x) = (x-a)g(x) + m \]

with \( m = \) constant.
\[ f(a) = 0 \cdot g(x) + m = m \]

Hence \( f(a) = 0 \implies m = 0 \) and \( (x-a) \mid f \cdot \quad \text{Q.E.D.} \)

When this happens we say that \( a \) is a zero of \( f \).

Conceivably \( f(x) = (x-a)^m g(x) \) where \( g(a) \neq 0 \).

Then we say that \( a \) is a zero of \( f \) with multiplicity \( m \).

\[ m \leq \deg f \]
Theorem 8.3.7: A polynomial of degree $n$ has at most $n$ zeros.

Proof: Let $a_1, a_2, \ldots, a_k$ be zeros of $f$. This means

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)g(x)$$

so $k \leq n$. QED

Let $F$ be a finite field. $\mathbb{Z}/p$ is a field iff $p$ is prime. $\mathbb{F}_p^n$ a field with $p^n$ elements (later)
Theorem 8.3.10 Let $G$ be a subgroup of $F^* = \{x \in F : x \neq 0\}$. Then $G$ is cyclic.

Proof: We know $G = G_1 \times G_2 \times \ldots \times G_n$ where each $d_i$ is a prime power.

Let $N = |G|$ and $M = \text{ lcm}(d_1, \ldots, d_n) = d_1 d_2 \ldots d_n \geq M$

Each $x \in G$ satisfies $x^M = 1$
so \( x^N - 1 = 0 \). There are \( N \) such elements so this polynomial \( N \) factors. \( N = M \).
Hence \( N = M \).

E.g. \( d_1 = 2 \), \( d_2 = 4 \), \( d_3 = 3 \)
\( N = 24 \), \( M = 12 \)
This cannot happen.

If \( M = N \), then no prime is repeated.

\[ G_0 = \mathbb{Z}_{(p_1, e_1)} \times \mathbb{Z}_{(p_2, e_2)} \times \cdots \times \mathbb{Z}_{(p_n, e_n)} \]
where the primes \( p_1, \ldots, p_n \) are distinct. This means \( G \) is cyclic. \( G = \mathbb{Z}_n \) (QED)

**Theorem 6.3.12** Let \( f(x) \in \mathbb{R}[x] \) if \( a + bi \in C \) is a root (or zero) of \( f \), so is \( a - bi \), \( a, b \in \mathbb{R} \).

**Proof** \( (x-(a+bi))(x-(a-bi)) = \cdot q(x) \)

\[= x^2 - 2ax + a^2 + b^2 \]
Divide $f$ by $g$ in $\mathbb{R}[x]$

\[ f(x) = g(x) \cdot y(x) + m(x) \]

where \( \deg m(x) < 2 \) so \( m(x) = cx + d \) for some \( c, d \in \mathbb{R} \).

If \( 0 = f(a+bi) = 0 \cdot g(a+bi) + m(a+bi) \)

\[ = c(a+bi) + d \]

\[ = ac + bi + d \]

Hence \( ac + d = 0 \) and \( bc = 0 \).

\[ f(a-bi) = 0 \cdot g(a-bi) + m(a-bi) \]

\[ = c(a-bi) + d \]
\[ -ac + d - bc i = 0 \text{ by previous calculation} \]

\[ \text{QED} \]

Recall: A polynomial in \( F[x] \) is irreducible if it is not a product of polynomials of smaller degree.

**Theorem 6.4.5:** Let \( f(x) \in F[x] \) be irreducible and \( f(x) \mid g(x) h(x) \).
Then either \( f \mid g \) or \( f \not| g \).

If \( \text{let } d(x) = \gcd (f, g) \). Then \( d \mid f \). Since \( f \) is irreducible, either

1) \( \deg d = \deg f \) so \( f = cd \) for some \( c = \text{constant} \)

2) \( \deg d = 0 \) so \( d = \text{constant} \).

In case 1), \( d \mid g \) so \( f \mid g \).

In case 2),

\[ c = m(x)f(x) + v(x)g(x) \]
multiply by $c \cdot h$

$$h = c \cdot h u f + c \cdot h u g$$

We know $f$ divides $h u g$ and $h f$, so $f \mid h$. QED

Example

$$24 = 3 \cdot 8 = 4 \cdot 6 = 2 \cdot 12$$

$$- 3 \cdot (2^3) = 2 \cdot (2 \cdot 3) = 2 \cdot (3)$$
Thm 8.4.6 Unique factorization

Any $f(x) \in F[x]$ $F$-field

is a unique product of monic irreducible factors

$f(x) = p_1(x) p_2(x) \ldots p_s(x)$

where each factor is monic and irreducible. (The $p_i$ need not be distinct.)
Proof: Argue by induction on the degree of \( f \). True for degree 1.

Assume \( f \) is monic + reducible.

\( f = gh \) where \( g \) and \( h \) are monic and

\[ \text{deg } g = \text{deg } h < \text{deg } f. \]

We know

\[ g = f_1 f_2 \cdots f_r \geq f_i \text{ are monic} \]

and \( h = f_{r+1} \cdots f_s \geq f_s \text{ irreducible} \)

\[ f = f_1 f_2 \cdots f_s \]
Suppose there is another factorization
\[ f = g_1 g_2 \cdots g_k \]
\[ p_i | g_1 g_2 \cdots g_k \text{, so it must divide } g_i \text{ for some } g_i \text{, so } p_i = g_i \text{.} \]
Divide out by this factor and get
\[ f = g_1 g_2 \cdots g_{i-1} g_{i+1} \cdots g_k \]
\[ = g_1 \cdots g_{i-1} g_{i+1} \cdots g_k / g_i \]
These factorizations are the same by induction. \[ \text{Q.E.D.} \]