Thm 8.4.7  \( f \in \mathbb{F}[x] \) has degree 2 or 3 then \( f \) is reducible \( \iff \) it has a zero.

Pf. One of the factors must have degree 1 \( \Box \).

Thm 9.4.11 (Rational roots theorem)

Let \( f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x] \)

\[ = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0 \]
Suppose \( a \in \mathbb{Q} \) is a zero of \( f \) let \( a = n/s \) with \( n, s \in \mathbb{Z} \)
and \( \gcd(n, s) = 1 \)

Then \( m \mid c_0 \) and \( s \mid c_n \).

Example: \( f(x) = 2x^3 + x^2 - 1 \). If \( f \) can be
factored \( \mathbb{Q} \), let \( a = n/s \) be a zero
\( m \mid 1 \) \( \Rightarrow \) \( m = \pm 1 \)
\( s \mid 2 \) \( \Rightarrow \) \( s = \pm 1 \) or \( \pm 2 \)

\( a = \pm 1 \) or \( \pm 1/2 \) \( f(a) \neq 0 \) in each case

Hence \( f \) is irreducible
Proof: \( f(a) = C_m \left( \frac{a}{2} \right)^n + C_{m-1} \left( \frac{a}{2} \right)^{n-1} + \ldots + C_0 = 0 \)

Multiply by \( 2^n \) and get

\[ C_m M^n + C_{m-1} M^{n-1} S + \ldots + C_1 M S^{n-1} + C_0 S^n = 0 \]

\[ C_m M^n + S(\text{even}) = 0 \]

Hence \( C_m \) is divisible by \( S \).

\[ C_0 S^n + S(\text{even}) = 0 \]

So \( C_0 \) is divisible by \( M \).

Q.E.D.
Def 8.4.14 Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$

The content of $f$ is

$$c = \gcd(a_n, a_{n-1}, \ldots, a_0)$$

$f(x)$ is primitive if its content is 1.

Ramesh Lemma 8.4.15 If $f$ and $g$

are primitive, so is $fg$.

Proof Suppose $fg$ is not primitive.

Let $p$ be a prime dividing all
The coefficients of $fg$

We have a ring homomorphism

$$\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x] = \text{domain}$$

$$\begin{array}{c}
\mathbb{Z} \\
\mathbb{Z}/p\mathbb{Z} \\
0
\end{array}$$

$$\begin{array}{c}
l \\
g \\
fg
\end{array}$$

Since $\mathbb{Z}/p\mathbb{Z}[x]$ is a domain, $\bar{f} \cdot \bar{g}$ is $0$. So one of them has coefficients divisible by $p$. But both are primitive. CONTRADICTION. Q.E.D.
Theorem 3.4.16 \( f \in \mathbb{Z}[x] \) factors over \( \mathbb{Q} \) if and only if it factors over \( \mathbb{Z} \).

**Example** \( f(x) = 6x^4 + 4x^2 - 3x - 2 \)

\[
= (3x^2 + 1)(4x^2 - 2)
= (3x^2 + 2)(2x^2 - 1)
\]

**Proof** Let \( f(x) = g(x)h(x) \in \mathbb{Q}[x] \)

where \( \deg f = n \), \( \deg h = s > 0 \)

\( \deg g = m > 0 \), \( m + s = n \)

We will show that \( g(x) \) and \( h(x) \in \mathbb{Z}[x] \) with the same degrees and \( g, h \in \mathbb{Z} \).
We can assume WLOG that \( f \) is primitive.

Let \( a = \text{LCM} \left( \text{denominators of } f \right) \) be the coefficients of \( g \).

Let \( b = \text{LCM} \left( \text{denominators of } h \right) \).

This means \( a \cdot g \in \mathbb{Z}[x] \) and \( b \cdot h \in \mathbb{Z}[x] \).

Let \( c = \text{content of } a \cdot g \), so

\[ a \cdot g = c \cdot g, \] where \( g \in \mathbb{Z}[x] \) is primitive.

and \( b \cdot h = d \cdot h \), where \( h \in \mathbb{Z}[x] \) is primitive.
The content of $abf$ is $a b$

By Gauss’ lemma, $g_1, h_1$ is primitive, so its content is $1$ and content of $cq, dh$, is $c d$

$abf = c d g_1, h_1$

so $ab = c d$

$f = g_1, h_1$ \quad QED$

Example: $f(x) = x^4 - 5x^2 + 6x + 1$

The only possible zeroes are $\pm 1$

$f(\pm 1) \neq 0$
If $f$ is reducible, then
\[
f = (x^2 + ax + b)(x^2 + cx + d)
\]
\[
= x^4 + (a+c)x^3 + (ac+d+b)x^2 + (ad+bc)x + bd
\]
so $a + c = 0$, $b = d = \pm 1$
\[
ac + b + d = -5 \implies bc + ad = \pm(a + c) = 0
\]
so $bc + ad = 0$
\[
bc + ad = b^2 \implies \text{CONTRADICTION}
\]
$f(x)$ is irreducible.
Theorem 6.4.19 Eisenstein's criterion

Let \( f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x] \)

It is irreducible if

1) \( p \nmid a_n \)
2) \( p \mid a_i \) for \( i < n \)
3) \( p^2 \nmid a_0 \)

Example: \( x^2 + 2px + p^2 = (x + p)^2 \) satisfies 1) and 2) but not 3)
Proof: Suppose
\[ \phi(x) = (b_n x^n + \cdots + b_0) (c_0 x^0 + \cdots + c) \]
with \( b_n, c_i \in \mathbb{Z} ; n, i \neq 0 ; n + i = n \).

Let \( b_0 = a_0 \) be divisible by \( \phi \) but not by \( \phi^2 \).

So \( \phi \) divides \( b_0 = c_0 \). But not both.

Suppose \( \phi \) is divisible by \( \phi \).

Let \( m \) be the smallest integer with \( \phi \mid b_m \).

Let \( a_m = b_m c_0 + b_{m-1} c_1 + \cdots + b_0 c_m \).
$b_i$ is div by $p$ for $i < m$
but $b_m$ and $c_0$ are not div by $p$.

Hence $a_m$ is not div by $p$.

CONTRADICTION

QED

Example: Let $f(x) = \frac{x^p - 1}{x - 1}$

$p = \text{prime}$

$f(x)$ is the $p$th cyclotomic polynomial.

$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{i=0}^{p} (i) \frac{x^i}{x}$
\[ \sum_{i=1}^{p} (\frac{1}{i}) x^{i-1} = x^{p-1} + p x^{p-2} + \frac{(p)}{2} x^{p-3} + \ldots + p \]

\[ = \text{Eisenstein polynomial} \]

so \( f(x) \) is irreducible.

Theorem 8.4.24 Let \( f \in \mathbb{Z}[x] \)

and let \( \bar{f} \in \mathbb{Z}/p[\bar{x}] \) be its mod \( p \) reduction. Assume \( \bar{f} \) and \( f \) have the same degree. If \( \bar{f} \)

is irreducible over \( \mathbb{Z}/p \), then
If \( f \) is irreducible over \( \mathbb{Q} \), then
\[
\overline{f} = \overline{g} \overline{h}
\]
and
\[
\overline{f} = \overline{g} \overline{h} \quad \text{i.e. } \overline{f} \text{ is reducible over } \mathbb{Z}/p.
\]

QED

Example: \( f = 3x^4 - 6x^3 + 10x^2 - 5x + 9 \)

\( p = 2 \)
\[
\overline{f} = x^4 + x + 1
\]
\( \overline{f}(0) = 1 \)
\( \overline{f}(1) = 1 \)

\( \overline{f} \) has no zeros
Can also show it cannot be
f can be factored as
\[ f = (x^3 + ax + b)(x^2 + cx + d) \]

\[ \implies \text{CONTRADICTION} \]

Hence \( f \) is irreducible.

So \( f \) is irreducible.