$F = \text{field} \quad R = F[x]$ 

Division Theorem 8.2.2: Let $f(x), g(x) \in R[x]$ with $g(x) \neq 0$. Then $\exists q(x)$ and $m(x) \in R[x]$ with $\deg m(x) < \deg g(x)$ such that 

\[ f(x) = q(x)g(x) + m(x), \]

$q(x) = \text{quotient}, \quad m(x) = \text{remainder}$

$f(x) = \text{dividend}, \quad g(x) = \text{divisor}$
If \( \deg g(x) = 0 \), then \( m(x) = 0 \).

\[ \text{Proof. Suppose } \deg b < \deg g. \text{ Then } q(x) = 0 \]
and \( m(x) = b(x) \).

Suppose \( \deg b(x) \geq \deg g(x) \).
\[ b(x) = a_0 + a_1 x + \cdots + a_m x^m \quad m \geq n \]

where \( a_m \neq 0 \) with \( b_m \neq 0 \)

Let \( c = a_m / b_m \) and
\[ h(x) = f(x) - c \cdot x^{m-1} g(x) \]
\[ = (a_m x^m + \cdots) - \frac{a_m}{b_m} \cdot x^{m-m} (b_m x^m + \cdots) \]
\[ = (a_m x^m + \cdots) - (a_m x^m + \cdots) \]

Hence deg \( h(x) < \deg f(x) \).

Argue by induction on \( \deg f(x) \).

Assume inductively that there is a quotient
and remainder for \( h(x) = g'(x)g(x) + m'(x) \)

We know

\[
\begin{align*}
  v(x) &= h(x) + c x^{m-n} g(x) \\
  &= g'(x)g(x) + m'(x) + c x^{m-n} g(-x) \\
  &= (c x^{m-n} + g'(x)g(x) + m'(x))
\end{align*}
\]
\[ \varphi(x) = cx^m + \varphi'(x) \]

and \[ m(x) = m'(x). \quad \text{QED} \]

Recall the Euclidean algorithm for integers.

\[ \text{e.g., } a_0 = 86 \quad a_1 = 16 \]
Divide \( a_0 \) by \( a_1 \) and call the remainder \( a_{-1} \) \( \equiv \).

\( a_0 \) \( \equiv \) \( a_2 \) \( \equiv \).

\( a_{-1} \) \( \equiv \) \( a_3 \) \( \equiv \).

\( a_2 \) \( \equiv \) \( a_4 \) \( \equiv \).

The last nonzero remainder is the \( \text{GCD} \).
\[(86, 16) = (2) \]
\[(m, n) = (\gcd(m, n)) \quad \text{for } m, n \in \mathbb{Z}\]

Can do the same with polynomials

\[a_0 = 3x^3 + 1 \quad a_1 = x^2 + 1 \quad F = \mathbb{Q}\]
\[
\begin{array}{c}
\frac{3x^2 + 1}{x^2 + 1} \quad 3x + 1
\end{array}
\]

\[
\begin{array}{c}
3x^3 + 3x \\
-3x + 1
\end{array}
\]

\[a_2 = -3x + 1\]

Divide \(a_1\) by \(a_2\) and call the remainder \(a_3\)
$-3x + 1 \sqrt{x^2 - x^{1/3}} + 1 \frac{x^{1/3} + 1}{x^{1/3}} - \frac{1}{9}$
gcd \((3x^2 + 1, x^2 - 1)\) = \(10\)
The polynomials are relatively prime if \( \gcd(f, g) = h \), then \( h \) divides both \( f \) and \( g \) and no polynomial
of larger degree does.

A polynomial is monic if its
leading coeff. is 1.

See Thm 8.2.6
Theorem 8.3.2 \[ \text{Let } \ f(x) \in F[x] \]

Suppose \( a \in F \). Then

\[ f(a) = 0 \iff f(x) \text{ is divisible by } (x-a). \]
\[ f \in \text{obvious} \]

\[ \Rightarrow \text{ Use division algorithm} \]

\[ b(x) = g(x)(x-a) + \gamma \]

for some \( \gamma \in F \). \text{Hence} \( h(a) = \gamma \).
Hence $f(a)=0 \Rightarrow m=0 \Rightarrow b(x)=a(x\sqrt{x}-a)$

QED

We say $a$ is a zero of $b(x)$.

Theorem 8.3.7 A polynomial of degree $n$ has $\leq n$ zeros.
Proof Each zero leads to a linear factor of $f(x)$. It cannot have more than $n$ of them. QED

Theorem 8.3.10 Let $F$ be finite and let $G$ be a subgroup of $F^*$. 
Then $G$ is cyclic.

Prove that $G$ is a finite abelian group if $G$ is cyclic and $G = C_{d_1} \times C_{d_2} \times \cdots \times C_{d_m}$, where each $d_i$ is a prime power.
Let \( N = |G| = \text{gcd}(d_1, d_2, \ldots, d_m) \) and \( M = \text{lcm}(d_1, d_2, \ldots, d_m) \). Each \( x \in G \) satisfies \( x^M = 1 \), so \( x^M - 1 = 0 \). There are \( N \) elements with this property, so \( x^M - 1 \) has \( N \) factors, so \( N \leq M \).
Since \( N = 161 = d_1 d_2 \cdots d_m \), \( M \leq N \).

Hence \( M = N \). Hence the primes in the \( d_i \) are distinct and cyclic. QED.
Thm 8.3.11 \( f(x) \in \mathbb{R}[x] \subset \mathbb{C}[x] \)

If \( a + b \imath \in \mathbb{C} \) is a zero for root of \( f(x) \), then so is \( a - b \imath \).

Here \( a, b \in \mathbb{R} \).
Let \( q(x) = (x-(a+bi))(x-(a-bi)) \)

\[
= x^2 - 2ax + a^2 + b^2
\]

Divide \( f(x) \) by \( q(x) \) in \( \mathbb{R}[x] \).

\[
f(x) = g(x)(x^2 - 2ax + a^2 + b^2) + r(x)
\]

where \( r(x) = c(x + d) \)
# Mathematics

Let $c, d \in \mathbb{R}$.

For any complex numbers $a + bi$ and $c + di$,

\[
q(a + bi) g(a + bi) + (c + di) + d = 0
\]

Given the assumption

\[
c + d + b - i = 0
\]
\[ = ac + d - bc \cdot i \]

We know \( ac + d = 0 \) and \( bc = v \).

So \( f(a - b\cdot i) = 0 \), \( \Leftrightarrow \)

\( (a - b\cdot i) \) is a root of \( f(x) \), QED.
If \( f(x) \in \mathbb{F}[x] \) is irreducible, if it is not the product of 2 polynomials of smaller degree.

Example: \( x^2 + 1 \) is irreducible in \( \mathbb{R}[x] \) but not in \( \mathbb{C}[x] \).
\((x^3; i) = (x - i)(x + i) \in \mathbb{C}[x]\)

Theorem 8.4.5: Let \(f(x) \in \mathbb{C}[x]\) be irreducible and suppose \(f(x)\) divides \(g(x) h(x)\). Then \(f\) divides either \(g\) or \(h\). Assume \(b, g, h\) and \(d\) are monic.
Proof: Let \( d(x) = \gcd(f, g) \). Then
1. \( d \mid f \) since \( f \) is irreducible. Either
2. \( d = f \) or 2) \( d = 1 \).

I should have said:
If \( c = \gcd(a, b) \)
then \( c = ma + lb \).

In case 1 above, \( d = f \) divides \( g \) so \( f \) divides \( g \).

In case 2
\[1 = \mu(x)g(x) + \nu(x)\gamma(x)\]

\[h(x) = h(x)1 + (x)g(x)\]

If \(\gamma\) divides both terms on the right, so it divides \(h\).