Let \( F \) be a field. A monic polynomial \( d(x) \) is a greatest common divisor of \( p(x), q(x) \in F[x] \) if \( d(x) \mid p(x) \) and \( d(x) \mid q(x) \) and if for any other \( \tilde{d}(x) \) which divides \( p, q \equiv \tilde{d}(x) \mid d(x) \)

\[
d(x) = \gcd(p(x), q(x))
\]

- \( p(x), q(x) \) are relatively prime if \( \gcd(p(x), q(x)) = 1 \)

**Prop.** Let \( F \) be a field, \( p(x), q(x) \in F[x] \). There exists \( r(x), s(x) \) s.t.

\[
d(x) = \gcd(p(x), q(x)) = r(x)p(x) + s(x)q(x)
\]

Furthermore, \( \gcd(p(x), q(x)) \) is unique.

**Proof.** Very similar to th. 2.10 where \( p, q \in \mathbb{Z} \)

**Remark.** We could define an ideal in \( F[x] \)

\[
I = \langle f(x), g(x) \rangle = \{ f(x)r(x) + g(x)s(x) \mid r(x), s(x) \in F[x] \}
\]

\[
= \langle \gcd(f(x), g(x)) \rangle
\]

**Irreducible polynomials**

A non-constant poly. \( f(x) \in F[x] \) is irreducible over a field \( F \) if \( f(x) \) cannot be expressed
\( f(x) = g(x) \cdot h(x) \) with \( 0 \leq \deg(g(x)) \leq \deg(f) \)
\( 0 \leq \deg(h(x)) \leq \deg(f) \)

i.e., \( f \) is irreducible if \( f \) does not factor

(ignoring constant factors)

\[ \text{Ex} \quad x^2 - 2 \in \mathbb{Q}[x] \text{ is irreducible} \]
\[ x^2 + 1 \in \mathbb{R}[x] \text{ is irreducible} \]

\[ \text{Ex} \quad p(x) = x^5 + x^2 + 2 \text{ is irreducible over } \mathbb{Z}_3[x] \]

If \( p(x) \) were reducible. By the div. \( q/g \) \((x-a)\) is a factor

for some \( a \in \mathbb{Z}_3 \)

\( \mathbb{Z}_3 = \{0, 1, 2\} \)

\[ p(x) = (x-a)q(x) \]

for this \( a \in \mathbb{Z}_3 \implies p(a) = 0 \)

\[ p(0) = 2, \quad p(1) = 1, \quad p(2) = 2 \]

\[ \therefore \text{no elements of } \mathbb{Z}_3 \text{ are roots of } p(x) \]

\[ \therefore \text{it has no linear factors.} \]

\textbf{Lemma} \quad \text{Let } p(x) \in \mathbb{Q}[x]. \text{ Then}

\[ p(x) = \frac{n}{s} (a_0 + a_1 x + \cdots + a_n x^n) \]

where \( a_0, a_1, \ldots, a_n \in \mathbb{Z} \) and \( \gcd(r_1, s) = 1 \), \( \gcd(a_0, \ldots, a_n) = 1 \).

\textbf{Proof:}

Suppose \[ p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1} x + \cdots + \frac{b_n}{c_n} x^n \]
Take common denom. \( p(x) = \frac{1}{c_0 \cdots c_n} (d_0 + d_1 x + \cdots + d_n x^n) \)

\( d_i \in \mathbb{Z} \)

set \( d = \gcd (d_0, \ldots, d_n) \), so \( a_i = \frac{d}{d_i} \in \mathbb{Z} \)

then \( \gcd (a_0, \ldots, a_n) = 1 \)

\[ p(x) = \frac{d}{c_0 \cdots c_n} (a_0 + a_1 x + \cdots + a_n x^n) \]

let \( \frac{n}{s} \) be \( \frac{d}{c_0 \cdots c_n} \) in lowest terms.

**Theorem (Gauss's Lemma)** Let \( p(x) \in \mathbb{Z}[x] \), monic

Suppose \( p(x) = a(x) b(x) \in \mathbb{Q}[x] \) with \( \deg(a(x)) \leq \deg(p(x)) \)

\[ \deg(b) < \deg(p) \]

Then \( p(x) = a(x) b(x) \) where \( a, b \in \mathbb{Z}[x] \) and are monic with \( \deg(a) = \deg(a), \deg(b) = \deg(b) \).

Simple rev: factoring in \( \mathbb{Z}[x] \) is equivalent to factoring in \( \mathbb{Q}[x] \).

**Proof:** By last lemma may assume

\[ a(x) = \frac{c_1}{d_1} (a_0 + a_1 x + \cdots + a_m x^m) = \frac{c_1}{d_1} a(x) \]

\[ b(x) = \frac{c_2}{d_2} (b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2} b(x) \]

\[ \gcd(a_0, \ldots, a_m) = \gcd(b_0, \ldots, b_n) = 1 \]
\[ p(x) = d(x) \beta(x) = \frac{c_1 c_2}{d_1 d_2} \alpha_1(x) \beta_1(x) = \frac{c}{d} \alpha_1(x) \beta_1(x) \]

\[ : \quad d \cdot p(x) = c \cdot \alpha_1(x) \beta_1(x) \]

Case \( d = 1 \): Since \( p(x) \) is monic \( \Rightarrow \quad \text{c} = \text{am} = \text{bn} = 1 \) \( \text{and } \text{an, bn, c} \in \mathbb{Z} \)

\[ \text{c} = 1 \quad \Rightarrow \quad \text{c} = 1 = \text{am} = \text{bn} \]

\[ \begin{array}{c}
\downarrow \\
\text{c} = \text{d} = \text{am} = \text{bn} = 1 \quad \text{hence} \quad \alpha_1 \cdot \beta_1 = p(x) \\
\end{array} \quad \text{monic, in } \mathbb{Z}[x] \]

\[ \begin{array}{c}
\text{or } \quad \text{c} = 1 \quad \text{and } \text{am} = \text{bn} = -1 \\
\end{array} \quad \text{monic, in } \mathbb{Z}[x] \]

\[ \text{c} = \text{d} = 1, \\
P(x) = (-\alpha_1(x))(-\beta_1(x)) \]

\[ \text{c} = -1 \quad \text{similar...} \]

\[ \text{look for contradiction} \]

Suppose \( d \neq 1 \), \( \gcd(c, d) = 1 \)

\[ \Rightarrow \exists \text{ a prime } q \text{ s.t. } q \mid d, \text{ and } q \mid c \]

and \( \exists \text{ some } a_i \text{ s.t. } q \nmid a_i, \text{ some } b_i \text{ s.t. } q \nmid b_i \)

Let \( \overline{\alpha_1(x)} \in \mathbb{Z}_q[x], \frac{\beta_1(x)}{x} \in \mathbb{Z}_2[x] \)

Since \( q \mid d \) and \( d \cdot p(x) = c \cdot \alpha_1 \beta_1 = 0 \text{ in } \mathbb{Z}_q[x] \)

\[ \Rightarrow \overline{\alpha_1(x)} \cdot \overline{\beta_1(x)} = 0 \text{ in } \mathbb{Z}_q[x] \]

but since \( q \nmid a_i \text{ and } q \nmid b_i \quad \Rightarrow \quad \overline{\alpha_1(x)} \neq 0, \overline{\beta_1(x)} \neq 0 \]
But $\mathbb{Z}[x]$ is an integral domain (since $\mathbb{Z}$ is a field)

\[ \therefore \text{this is a contradiction.} \]

\[ \therefore d=1 \]

**Cor.** Let \( p(c) = x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x] \)

and \( a_0 \neq 0 \). If \( p(c) \) has a zero in \( \mathbb{Q} \) then \( p(c) \)
also has a zero \( \alpha \in \mathbb{Z} \), and \( d \mid a_0 \)

**Proof.** Let \( \beta \in \mathbb{Q} \) s.t. \( p(\beta) = 0 \). \( \Rightarrow p(c) \) has a linear
factor \( x-\beta \in \mathbb{Q}[x] \). By Gauss's Lemma

since \( p(c) = (x-\beta) q(c) \in \mathbb{Q}[x] \)

\[ \Rightarrow p(c) = (x-\beta) \left( x^{n-1} + \ldots + \frac{a_0}{\beta} \right) \in \mathbb{Z}[x] \]

\[ \therefore \beta \in \mathbb{Z} \quad \text{and} \quad d=\beta \quad \text{and} \quad d \mid a_0 \quad \Box \]

\[ \text{Ex.1} \quad p(c) = x^4 - 2x^3 + x + 1 \quad \text{is irreducible in} \ \mathbb{Q}[x] \]

Suppose \( p(c) = (x-d) q(c) \)

\[ \Rightarrow d \in \mathbb{Z} \quad \text{is a root of} \ p(c) \quad \text{and} \quad d \mid 1 \]

\[ \Rightarrow d = \pm 1 \]

But \( p(1) = 1, \ p(-1) = 3 \)

\[ \therefore p(c) \) has no linear factors.

\[ p(c) = (x^2 + ax + b) (x^2 + cx + d) \]

\[ = x^4 + (a+c)x^3 + (ac + b+d)x^2 + (ad + bc)x + bd \]

\[ \begin{array}{cccc}
\frac{11}{2} & \frac{7}{2} & \frac{1}{2} & \frac{1}{2} \\
\frac{11}{2} & 0 & 1 & 1
\end{array} \]
\[ d = d = 1 \] or \[ b = d = -1 \]

\[ b = d \]

\[ ad + bc = b(a + c) = 1 \]

\[ -2b = 1 \]

This is a contradiction of Gauss's lemma \( (b \in \mathbb{Z}) \).

\[ \therefore \ p \text{ is irreducible} \]

---

**Thm (Eisenstein's Criterion)**

Let \( p \) be a prime and

\[ f(x) = a_nx^n + \ldots + a_0 \in \mathbb{Z}[x] \]

If \( p \mid a_i, i=0, \ldots, n-1 \), but \( p \nmid a_n \) and \( p^2 \nmid a_0 \) then \( f \) is irreducible in \( \mathbb{Q}[x] \).

**Proof:** By Gauss's lemma it is sufficient to show \( \text{irr. in } \mathbb{Z}[x] \).

Suppose \( f(x) = (b_rx^r + \ldots + b_0)(c_sx^s + \ldots + c_0) \in \mathbb{Z}[x] \)

\[ b_i \neq 0, c_s \neq 0 \quad , r, s \leq n \]

\[ p^2 \nmid a_0 = b_0c_0 \quad \therefore \text{ Either } p \nmid b_0 \text{ or } p \nmid c_0 \]

Assume \( p \mid b_0 \), \( p \nmid c_0 \)

\[ p \mid a_n = b_rc_s \quad \therefore p \mid b_r \text{ and } p \mid c_s \]
Let $m$ be the smallest value such that $p | c_m$ (known $p | a_0$).

$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$

Not divisible by $p$

$\therefore p \nmid a_m$

By assumption of Thm, $p | a_m$ for $m < n$

$\Rightarrow m = s = n$

$\therefore f(x) = b_0 (c_n x^n + \cdots + c_0)$

$\therefore f$ is irreducible.

**Ex:**

$f(x) = 6x^5 - 9x^4 + 3x^2 + 6x - 21$

is irr by Eisenstein with $p = 3$

Since $3$ divides $9, 3, 6, 21, 3^2 = 9 + 21, 3 \times 16$

I deals in $\mathbb{F}[x]$

Let $R$ be an integral domain, an ideal $I$ is called principal if $I = \langle f \rangle = \{ f \cdot r \mid \forall r \in R \}$

An integral domain where every ideal is principal is called a principal ideal domain.

**Thm:** Let $F$ be a field. Every ideal $I$ in $\mathbb{F}[x]$ is principal, i.e. $\mathbb{F}[x]$ is a principal ideal domain.
Proof: \( I \) - ideal of \( F[x] \)

- \( I = \{0\} \implies I = \langle 0 \rangle \)

Suppose \( I \) is a non-trivial ideal, let \( f(x) \in I \) be a nonzero poly. in \( I \) of minimal degree.

If \( \deg(f(x)) = 0 \implies f(x) = c \in F[x] \), \( c \in F \)

\[ 
\therefore 1 \in I \therefore I = \langle c \rangle = \langle 1 \rangle = F[x] 
\]

Assume \( \deg(f) \geq 1 \). Let \( g(x) \) be any element of \( I \).

By the div. alg. \( \exists q, r \) s.t

\[ 
g(x) = f(x)q(x) + r(x), \quad \deg(r) < \deg(f) \]

\[ 
\therefore r(x) \in I 
\]

\( \implies \) but \( f(x) \) has minimal degree in \( I \).

\[ 
\therefore r(x) = 0 \therefore \forall g(x) \in I \quad g(x) = f(x)q(x) 
\]

\[ 
\therefore I = \langle f(x) \rangle . \quad \square 
\]