Prop Let $F$ be a field, $q(x), p(x) \in F[x]$. Then 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 proof for $p, q \in \mathbb{Z}$.

Irreducible Poly nomials

A non-constant poly. $f(x) \in F[x]$ is irreducible over a field $F$ if $f(x)$ cannot be expressed as
\[ f(x) = g(x)h(x) \quad \text{with} \quad 0 \leq \deg(g(x)) < \deg(f) \]
\[ 0 \leq \deg(h(x)) < \deg(f) \]

i.e. $f$ irreducible iff $f$ does not factor.

Think prime numbers for Poly. ring.

Example $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible

$\mathbb{Q}[x]$ is irreducible

Example $x^2 + 1 \in \mathbb{R}[x]$ is irreducible

Example $p(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3[x]$

Suppose $p(x)$ were reducible over $\mathbb{Z}_3[x]$
By div alg \((x-a)\) is a factor for some \(a \in \mathbb{Z}_3\)

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

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

for this \(a\), \(p(a) = 0\)

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

\(\therefore p(x)\) is irreducible since \(0, 1, 2\) are not roots.

**Lemma**

Let \(p(x) \in \mathbb{Q}[x]\). Then

\[
p(x) = \frac{r}{s}\left(a_0 + a_1x + \cdots + a_nx^n\right)
\]

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

**Proof:**

Suppose

\[
p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n
\]

Rewrite

\[
p(x) = \frac{1}{c_0 \cdots c_n}\left(d_0 + \cdots + d_nx^n\right)
\]

Set \(d = \gcd(d_0, \ldots, d_n)\) then \(\forall i, a_i = \frac{d_i}{d} \in \mathbb{Z}\)

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

\[
p(x) = \frac{d}{c_0 \cdots c_n}\left(a_0 + a_1x + \cdots + a_nx^n\right)
\]

Writing \(\frac{d}{c_0 \cdots c_n}\) in lowest terms as \(\frac{r}{s}\) this gives

\[
p(x) = \frac{r}{s}\left(a_0 + \cdots + a_nx^n\right).
\]
**Theorem (Gauss's Lemma):** Let \( p(x) \in \mathbb{Z}[x] \), monic

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

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

**Simple Version:** If \( p(x) \) poly in \( \mathbb{Z}[x] \) factors in \( \mathbb{Q}[x] \) it also factors in \( \mathbb{Z}[x] \).

**Proof:** By last lemma may assume

\[
\alpha(x) = \frac{c_1}{d_1} \left( a_0 + a_1 x + \ldots + a_m x^m \right) = \frac{c_1}{d_1} \alpha_1(x)
\]
\[
\beta(x) = \frac{c_2}{d_2} \left( b_0 + b_1 x + \ldots + b_n x^n \right) = \frac{c_2}{d_2} \beta_1(x)
\]

\[
g(c(d(a_0, \ldots, a_m)) = \gcd(b_0, \ldots, b_n) = 1.
\]

\[
p(x) = \alpha(x) \beta(x) = \frac{c_1 c_2}{d_1 d_2} \alpha_1(x) \beta_1(x) = \frac{c}{d} \alpha_1(x) \beta_1(x)
\]

\[
\therefore \quad d \ p(x) = C \alpha_1(x) \beta_1(x)
\]

**Case \( d = 1 \):** Since \( p(x) \) is monic \( \Rightarrow \)
\( C \ a m b n = 1 \) monic

\[
C, a, m, b \in \mathbb{Z} \quad \Rightarrow \quad C = 1 \text{ or } C = -1 \quad \Rightarrow \quad p(x) = \alpha(x) \beta(x)
\]
Let \( am = bn = -1 \) \( \Rightarrow \) \( p(x) \left( - \alpha_i(x) \right) \left( - \beta_i(x) \right) \)

\( c = -1 \) similar

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

\( \Rightarrow \exists \) prime \( q \) s.t. \( q \mid d \) and \( q + c \)

and also \( \exists \) some \( a_i \) s.t. \( q \mid a_i \), and some \( b_i \) s.t. \( q \mid b_i \);

let \( \alpha_i(x) \in \mathbb{Z}_q[x] \), \( \beta_i(x) \in \mathbb{Z}_q[x] \)

Since \( q \mid d \), \( \Rightarrow \) \( \alpha_i(x) \cdot \beta_i(x) = 0 \) in \( \mathbb{Z}_q[x] \).

But since \( q \mid a_i \) \( q \mid b_i \), \( \alpha_i(x) \neq 0 \) and \( \beta_i(x) \neq 0 \) \( \Rightarrow \) \( \mathbb{Z}_q[x] \) is an integral domain (since \( \mathbb{Z}_q \) is a field)

\( \Rightarrow \) this is a contradiction \( \Rightarrow \) \( d = 1 \).

**Corollary** Let \( p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_q[x] \), \( a_0 \neq 0 \).

If \( p(x) \) has a zero in \( \mathbb{Z}_q \) then \( p(x) \) also has a zero \( \alpha \in \mathbb{Z}_q \). Further more \( \alpha \mid a_0 \).

**Proof:**

Let \( \alpha \in \mathbb{Z}_q \) s.t. \( p(\alpha) = 0 \) \( \Rightarrow \) \( p(x) \) a linear factor \( x - \alpha \)

By Gauss's Lemma since \( \gcd (p(x)) = (x - \alpha) q(x) \) in \( \mathbb{Z}_q[x] \)

\[ p(x) = (x - \alpha) \left( x^{n-1} + \cdots + \frac{a_0}{\alpha} \right) \in \mathbb{Z}_q[x] \]

\( \Rightarrow \) \( \alpha \mid a_0 \).