Ring of polynomials over a field:

\[ f = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n \]

Say that:

\[ \text{deg}(f) = n, \]

leading coefficient is \( a_n \)

\[ \text{deg}(0) = -\infty \]

\[ \text{deg}(1) = 0 \quad \text{if} \quad a \in K^\times = K \setminus \{0, 1\} \quad \text{(constant polynomial)} \]

Example:

\[ f(x) = \pi^{15} x^3 + 2 x^2 - x + \sqrt{2} \]

\[ \text{deg}(f) = 3 \]

leading coeff. is \( \pi^{15} \)

Proposition:

If \( f, g \in K[x] \)

\[ \text{deg}(fg) = \text{deg}(f) + \text{deg}(g) \]

\[ \text{deg}(f+g) \leq \max \{ \text{deg}(f), \text{deg}(g) \} \]

Proof:

\[ f = \sum_{i=0}^{n} a_i x^i \quad g = \sum_{j=0}^{m} b_j x^j \]

\[ fg = \sum_{i,j} a_i b_j x^{i+j} \quad \max \{n, m\} \]

\[ \Rightarrow \text{deg}(fg) = n + m \]

\[ f+g = \sum_{i} (a_i + b_i) x^i \]

\[ \Rightarrow \text{deg}(f+g) = \max \{a, b\} \quad \Rightarrow \text{deg}(f+g) = \max \{n, m\} \]
**Corollary:** \( (K\bar{K}^x)^x = K^x \)

**Proof:** \( K^x \subseteq (K\bar{K}^x)^x \)

If \( f(x) \in (K\bar{K}^x)^x \) then there exists \( f^{-1} \) such that

\[ 1 = f(x) \cdot f^{-1}(x) \]

\[ \Rightarrow 0 = \deg(1) = \deg(f \cdot f^{-1}) = \deg(f) + \deg(f^{-1}) \]

since \( \deg > 0 \)

\[ \Rightarrow \deg(f) = 0 \]

\[ \Rightarrow f \in K \Rightarrow f \in K^x. \]

**Def:** Say that \( f \in K\bar{K}^x \) is irreducible if \( \deg(f) > 0 \) and whenever \( f = gh \) either \( g \in K^x \) or \( h \in K^x \).

**Example:** \( K = \mathbb{R} \)

\( f(x) = x^2 + 1 \) is irreducible:

if \( f = gh \) then \( \deg(g) > 0 \) or \( \deg(h) > 0 \) is not possible.

\( K = \mathbb{C} \), \( f(x) = x^2 + 1 \) has no real roots.
Theorem. Any \( f \in \mathbb{K}[x] \), \( \deg(f) > 0 \) is a product of irreducible polynomials, unique up to multiplication by a unit, that is:

\[ f = p_1 \cdots p_k = q_1 \cdots q_l \]

with \( k = l \) and after reindexing \( P_1 = q_1 q_i \) for some \( q_i \in \mathbb{K}^* \).

Remark: Similar to prime factorization in \( \mathbb{Z} \), similar proof.

Proof:

existence: induction on degree.

If \( \deg(f) = 1 \), we're done since \( f \) must be irreducible.

Suppose true if \( f \in \mathbb{K}[x] \) and \( \deg(f) \leq n \).

Let \( g \in \mathbb{K}[x] \) have degree \( n+1 \).

If \( f \) is irreducible we're done otherwise.

\[ g = f \cdot h \]

applying IH we can write \( f \cdot h \) as a product of irreducibles.

Uniqueness: almost, similar to case of primes in \( \mathbb{Z} \).
Def. If \( f, g \in K[x] \) say that \( h(y) \in \overline{K[x]} \)
such that \( fh = g \).

Proposition: \( \forall f, d \in K[x], \deg(d) \geq 0 \).

Then \( \exists q, r \in K[x] \) s.t.

\[
f = qd + r \quad \text{where} \quad deg(r) < deg(d).
\]

Proof: This is polynomial long division. \( \Box \)

Example: \( f(x) = 2x^4 + x^3 - 2x^2 + 2x + 1 \) \( K = \mathbb{Z}_3 \)
\[
d(x) = x^2 + 2
\]

\[
\begin{array}{r|cccc}
\multicolumn{2}{l}{2x^2 + x} \\
\hline
x^2 + 2 & 2x^4 + x^3 - 2x^2 + 2x + 1 \\
\hline
& 2x^4 + 2x^3 \\
\hline
& - (2x^4 + 2x^3) \\
\hline
& x^3 - 6x^2 + 2x + 1 \\
\hline
& - (x^3 + 2x) \\
\hline
& 1
\end{array}
\]

So \( 2x^4 + x^3 - 2x^2 + 2x + 1 = (2x^2 + x)(x^2 + 2) + 1 \) in \( \mathbb{Z}_3[x] \)
Def. \( \forall f, g \in \mathbb{K}[x] \), \( \gcd(f, g) \) is the \( k \in \mathbb{K}[x] \) s.t.

\[ \forall h_1, h_2, h_3 \in \mathbb{K}[x] \text{ such that } h_1 + h_2 = h_3 \text{ then } k \mid h_3 \text{ as well} \]

Theorem. \( \forall f, g \in \mathbb{K}[x] \) \( \exists h \) \( \gcd(f, g) \) exists and

\[ \gcd(f, g) = sf + tg \text{ for some } s, t \in \mathbb{K}[x] \]

Proof. omitted: use long division (see 1.8.16 in text)

Def. For \( f, g \in \mathbb{K}[x] \), let

\[ (f, g) \in \mathbb{K}[x] \]

be defined by

\[ (f, g) = \{ sf + tg \mid s, t \in \mathbb{K}[x] \} \]

called ideal generated by \( f \) and \( g \)

Proposition. \( (f, g) \in \mathbb{K}[x] \) is a subring (without \( 1 \)) of \( \mathbb{K}[x] \)

and if \( h \in (f, g) \) then

\[ h + (f, g) \subseteq (f, g) \]

Proof. exercise.
**Proposition**: If \( p \) is irreducible, and \( pf \equiv g \pmod{p} \), then \( p|f \) or \( p|g \).

**Proof**: If \( p \nmid f \) then since \( p \) is irreducible we must have \( \gcd(f, p) = 1 \).

\[ \Rightarrow \quad \exists s, t \quad \text{s.t.} \quad 1 = sf + tp \]

\[ \Rightarrow \quad g = sfg + tpg \]

\[ p \text{ divides } pg \quad p \text{ divides } f \]

\[ \Rightarrow \quad p \text{ divides } g \]

\[ \square \]