**Def.** A homomorphism of rings \( f: R \rightarrow S \) is a function such that

\[
\begin{align*}
\phi(xy) &= f(x)f(y), \\
\phi(x) &= f(x)
\end{align*}
\]

If \( R, S \) have \( 1 \), say \( f \) is unital if \( f(1) = 1 \).

An **isomorphism** is a bijective ring homomorphism.

**Example:** \( f: \mathbb{Z} \rightarrow \mathbb{Z} \)

\[
\begin{align*}
m &\mapsto [m]
\end{align*}
\]

- If \( R \) is a ring with \( 1 \), there is a (unital) ring homomorphism

\[
f: \mathbb{Z} \rightarrow R \quad f(m) = \frac{1_R + 1_R + \cdots + 1_R}{m}
\]

**Proposition.** Let \( R, S \) be commutative rings with \( 1 \),

\( f: R \rightarrow S \) is a unital ring homomorphism.

Then there is a unique unital ring homomorphism

\( \psi: R[x] \rightarrow S \)

such that

\[
\psi(ax) = f(a) \qquad \forall \ a \in R
\]

and

\( \psi(x) = x \).

**Proof.** Define \( \psi \left( \sum r_i x^i \right) = \sum f(r_i) \cdot a^i \). This is a unital ring homomorphism (check!).

On the other hand, if \( \psi \) is a ring homomorphism,

\( \psi(\sum r_i x^i) = \sum \psi(r_i) \psi(x^i) \),

the above formula is the only option.
Corollary: If \( R \) is a comm. ring \( -(1, \neq 0) \) and \( R \) is unique ring

homomorphism \( \text{ev}_a : \mathbb{R}[x] \to R \)

with \( \text{ev}_a(r) = r \) and \( \text{ev}_a(x) = a \). It is given by \( \text{ev}_a(\sum r_i x^i) = \sum r_i a^i \).

Proof: Apply previous, with \( f = \text{id} : R \to R \), then \( \text{ev}_a = f_{a, 1} \).

This view of \( \text{ev}_a \) as a function \( p(a) = \text{ev}_a(p) \).

Now let \( K \) be a field.

Say that \( a \in K \) is a root of \( p \) if \( p(a) = 0 \).

Proposition: Let \( p \in K[x] \), \( f \in K[x] \) st.

\[ p(x) = g(x)(x-a) + p(a) \]

Proof: Using long division, we find

\[ \exists q, r \in K[x] \quad \text{st.} \quad p(x) = \overline{g(x)}(x-a) + \overline{r(x)} \]

with \( \deg(r) < \deg(x-a) = 1 \) is constant

Since \( \overline{p(a)} = \overline{g(a)}(a-a) + \overline{r(a)} = 0 \) \( \Rightarrow r = p(a) \). \( \square \)

Corollary: \( a \) is a root of \( p \) \( \Rightarrow x-a \) divides \( p \).
Example: \( x^2 + 1 \in \mathbb{R}[x] \triangleq \mathbb{C}[x] \).

ined in \( \mathbb{K}[x] \) in \( \mathbb{C} \) an root \( i = \sqrt{-1} \)

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

Def.: The multiplicity of a root \( a \) of \( p(x) \)

is the number of times \( (x - a) \) appears in a factorization of \( p(x) \) into irreducibles.

Corollary: If \( p(x) \in \mathbb{K}[x] \) has degree \( n \), then it has at most \( n \) roots in \( \mathbb{K} \), counting multiplicities.

Proof.

Let \( a_1, \ldots, a_n \) be the roots of \( p(x) \) with multiplicity \( m_1, \ldots, m_n \).

Then the factorization of \( p(x) \) into irreducibles is of the form

\[ p(x) = (x - a_1)^{m_1} \cdots (x - a_n)^{m_n} q_1 \cdots q_s \]

where

\[ n = \deg(p) = m_1 + m_2 + \cdots + m_n + \deg(q_1) + \cdots + \deg(q_s) \]

\[ > m_1 + m_2 + \cdots + m_n. \]
Theorem: Let $K$ be a finite field, $|K|=n$. Then $K^*$ is cyclic.

Proof: Let $m \in \mathbb{N}$ smallest natural number such that $a^m = 1 \not\in K^*$ (note: $m = \text{lcm}\{\text{gcd}(a)\} \in K^*$). Since $1K^m = 1 \implies m \mid |K^*| = n-1 \implies m \leq n-1$.

On the other hand, every $a \in K^*$ is a root of $x^m - 1$.

So by previous corollary, $\#\text{roots} = n-1 \leq \deg(x^m-1) = m$.

Therefore $m = n-1$.

Now we need to see that there is always an element of order $\text{lcm}\{\text{gcd}(a)\} \in K^*$.

Follow from the following lemma. 

Lemma: Let $G$ be a finite abelian group and $m$ the smallest natural number such that $g^m = e \iff g \in G$. Then there is an element $g \in G$ such that $o(g) = m$. 

Proof. First note that since $G$ is abelian then if $\text{gcd}(o(a), o(b)) = 1 \implies o(ab) = o(a) o(b)$
(check!)

So, if $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is the prime factorization, it is enough to find elements $y_i \in G$ with $o(y_i) = p_i^{e_i}$.

To do this, first we let $x_i \in G$ be an element such that $x_i$ is a power of $p_i$ in $o(x_i)$.

Let $n_i = o(x_i) / p_i^{e_i}$. Then letting $y_i = x_i^{n_i}

we have $o(y_i) = \frac{o(x_i)}{n_i} = p_i^{e_i}$.

Now let $g = y_1 y_2 \cdots y_r$ we have $o(g) = o(y_1) o(y_2) \cdots o(y_r) = p_1^{e_1} \cdots p_r^{e_r}$. $\Box$