Definition: A maximal ideal of a commutative ring R is a proper ideal M of R such that if there exists an ideal I satisfying $M \subset I \subset R$, then either $I = M$ or $I = R$.

Theorem: Let R be a commutative ring with identity M an ideal in R. Then M is a maximal ideal if and only if R/M is a field.

Proof: Suppose M is a maximal ideal in R. We want to show that R/M is a field. Since R is a commutative ring with identity, then R/M is also commutative ring with identity. It remains to show that for every $a+M \neq 0_R + M$, there exists a $b \in R$ such that

$(a+M)(b+M) = 1_R + M \Rightarrow ab + M = 1_R + M$.

Let $I = \bigcup_{r \in R} (ar + M) = \{ar + m : r \in R, m \in M\}$. We want to show that $M \subsetneq I$ and we also show that I is an ideal of R. For the first, let $m \in M$ be arbitrary. Then $m = a \cdot 0_R + m \in I \Rightarrow M \subset I$. Now let $a \in R \setminus M$. Then $a = a \cdot 1_R + 0_R \in I \Rightarrow M \neq I \Rightarrow M \subsetneq I$. Next, we show that $I \trianglelefteq R$. We use the subring test:

- $0_R = a \cdot 0_R + 0_R \in I$
- $(ar_1 - m_1) - (ar_2 - m_2) = a(r_1 - r_2) - (m_1 - m_2) \in I$.
- $\forall s \in R, ar, m \in I \Rightarrow s(ar, m) = a(sr) + sm \in I \Rightarrow I$ is an ideal.

Since M is a maximal ideal $I = R \Rightarrow 1_R \in I$, i.e there exists a $b \in R$ such that $1 = ab + m$ for some $m \in M$. Therefore, R/M is a field.

On the other hand, assume that R/M is a field. Let $I \trianglelefteq R$ such that $M \subset I \subset R$. If $I = M$, then we are done. We now want to show that $I = R$. Let $a \in I \setminus M$. Then $a + M \neq 0 + M = 0_{R/M}$. Because R/I is a field, there exists a $b \notin M$ such that $(a+M)(b+M) = ab + M = 1 + M$. Thus, there exists an $m \in M$ such that $\underbrace{ab}_{\in I} + \underbrace{m}_{\in I} = 1$, and $1 \in I$. Therefore, $I = R$, so M is the maximal ideal of R.

Polynomial Rings and The Division Algorithm.

Theorem (Division Algorithm): Let $f(x)$ and $g(x)$ be polynomials in $F[x]$ where F is a field and $g(x)$ is a nonzero polynomial. Then there exists unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

where either $\deg(r(x)) < \deg(g(x))$, or $r(x)$ is the zero polynomial.

Example: Let $\alpha \in F$ and let $g(x) = x - \alpha$. Let $f(x) \in F[x]$. Then by the Division Algorithm, there exists $q(x), r(x)$ such that

$$f(x) = q(x)(x-\alpha) + r(x) \text{ and either } r(x) = 0, \text{ or}$$

$\deg(r(x)) < \deg(g(x))$. If $r(x) = b$ for some $b \in F$, then substituting α, we have $f(\alpha) = q(\alpha)(\alpha - \alpha) + b \Rightarrow f(\alpha) = b$, where $f(\alpha)$ is the remainder. This is called the Remainder Theorem.

The Remainder Theorem: Let F be a field and let $p(x) \in F[x]$. When $p(x)$ is divided by a polynomial $ax - b$, then the remainder is $p(\frac{b}{a})$.

Definition: Let $f(x), g(x) \in F[x]$ be polynomial.

- We say that $g(x)$ divides $f(x)$, i.e. $g(x) \mid f(x)$ or $g(x)$ is a factor of $f(x)$ if there exists a $h(x) \in F[x]$ such that $f(x) = g(x)h(x)$

- A root α of $f(x)$ has multiplicity n if $(x-\alpha)^n \mid f(x)$, but $(x-\alpha)^{n+1} \nmid f(x)$.

The Factor Theorem: Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F[x]$ if and only if $x-\alpha$ is a factor of $p(x) \in F[x]$.

Proof: By the remainder theorem, α is a root of $p(x)$ if and only if $p(\alpha)=0$ if and only if $p(x) = q(x)(x-\alpha)$ if and only if $x-\alpha \mid p(x)$.

Corollary: Let F be a field. A nonzero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F

Proof: We will use induction on $p(x)$. If $\deg(p(x))=0$, then $p(x)$ is a constant polynomial with no roots. Let $\deg(p(x)) = n > 0$. If $p(x)$ has no roots, then we are done. On the other hand, if α is a zero of $p(x)$, with multiplicity $k \geq 1$. Then $p(x) = (x-\alpha)^k h(x)$ where $\deg(h(x)) = n-k. \Rightarrow (x-\alpha) \nmid h(x)$. If $p(x)$ has no other root that it has roots $\alpha, \alpha, \dots, \alpha$ (k times), then we are done. Otherwise, $p(x)$ has a root $\beta \neq \alpha$. By the Factor Theorem, we have

$$p(\beta) = (\underbrace{\beta-\alpha}_{\beta-\alpha \neq 0_F})^k h(\beta) = 0 \quad \Rightarrow (\beta-\alpha)^k \neq 0_F \quad] \; *$$

Multiply $*$ $(\beta-\alpha)^k \Rightarrow h(\beta) = 0 \Rightarrow \beta$ has root of $h(x)$.

By the inductive hypothesis, $h(x)$ has at most $n-k$ roots and so $p(x)$ has at most $k+(n-k) = n$ roots.