Definition 1. *Polynomial Ring* $\mathbf{R}$*[X] in* x *over the ring* $\mathbf{R}$ *is defined as set of expressions, called polynomials in* X*, of the form*

$$f(x) = a_0 + a_1x^1 + \cdots + a_mx^m$$

where $a_0, a_1, \ldots, a_n$*, the coefficients of* $p(x)$ *are elements of* $\mathbf{R}$*, and* x, x^2 *are symbols*

Definition 2. *Let* F *be a field. By the ring of polynomial in the indeterminate,* x*, written as* $\mathbf{R}$*[X], we mean the set of all symbols* $f(x) = a_0 + a_1x^1 + \cdots + a_mx^m$*, where* n *can be any nonnegative integer and where the coefficient* $a_0, a_1 + \cdots + a_n$ *are all in* F*. In order to make a ring out of* $\mathbf{F}$*[X], we must be able to recognize when the two elements in it are equal, we must add and multiply element of* $\mathbf{F}$*[X] so that the axiom defining the ring hold true for* $\mathbf{F}$*[X].*

Definition 3. *If* $f(x) = a_0 + a_1x^1 + \cdots + a_mx^m$ *and* $g(x) = b_0 + b_1x^1 + \cdots + b_mx^m$ *are in* $\mathbf{F}$*[X], then* $f(x) = g(x)$ *if and only if for every integer* $i \geq 0$*, such as* $a_i = b_i$

Definition 4. *If* $f(x) = \sum_{i=0}^{n} a_ix^i$ *and* $g(x) = \sum_{j=0}^{m} b_jx^j$*, then* $f(x) + g(x)$ *is equal*

$$\sum_{i=0}^{n} a_ix^i + \sum_{j=0}^{m} b_jx^j = \sum_{i=0}^{k}(a_i + b_j)x^k \qquad \textit{where } k = \max(n, m)$$

If $f(x)$ *or* $g(x)$ *do not contain the term* cx^t*, then assume* $c = 0, \quad k \geq t \geq 0$

Definition 5. *If* $f(x) = \sum_{i=0}^{n} a_ix^i$ *and* $g(x) = \sum_{j=0}^{m} b_jx^j$*, then* $f(x)g(x)$ *is equal*

$$\sum_{i=0}^{n} a_ix^i \sum_{j=0}^{m} b_jx^j = \sum_{i=0}^{n}\left(\sum_{j=0}^{m} a_ib_jx^{i+j}\right)$$

The definition say nothing more than: multiply two polynomials by multiplying out two symbols formally, use the relation $x^ix^j = x^{i+j}$ *and collect terms*

Definition 6. *The degree of nonzero polynomial is defined as the maximus power of a term with nonzero coefficients.*

Definition 7. *If* $f(x)$ *and* $g(x)$ *are nonzero polynomials in* $\mathbf{F}$*[X], then*

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

Proof. let $f(x) = \sum_{i=0}^{n} a_ix^i, a_n \neq 0$ and $g(x) = \sum_{j=0}^{m} b_jx^j, b_m \neq 0$ we have

$$\deg(f(x)) = n$$
$$\deg(g(x)) = m$$

let $\alpha \in \{0 \ldots n\}, \alpha \neq n$ and $\beta \in \{0 \ldots m\}, \beta \neq m$

$$\therefore \alpha < n \text{ and } \beta < m$$
$$\implies \alpha + \beta < n + m$$

From the defintion of multiplication of two polynomials

$$f(x)g(x) = \sum_{i=0}^{n} a_ix^i \sum_{j=0}^{m} b_jx^j = \sum_{i=0}^{n}\left(\sum_{j=0}^{m} a_ib_jx^{i+j}\right)$$

We need to show $a_n b_m \neq 0$, from the defintion

$$\begin{aligned}
&a_n \neq 0 \\
&b_m \neq 0 \\
&\implies a_n b_m \neq 0 \quad \because F \text{ is a integral domain} \\
&\implies \text{ the maximus power of term is } a_n b_m x^{n+m} \\
&\implies \deg(f(x)g(x)) = n + m = \deg(f(x)) + \deg(g(x))
\end{aligned}$$

□

Proof. By induction □

Definition 8. *If $f(x)$ and $g(x)$ are nonzero element in* $\mathbf{F}$*[X], then* $\deg(f(x)) \leq \deg(f(x)g(x))$

Proof. from above proof, we have

$$\begin{aligned}
\deg(f(x)) + \deg(g(x)) &= \deg(f(x)g(x)) \\
\deg(f(x)) &= \deg(f(x)g(x)) - \deg(g(x)) \\
\because \deg(g(x)) &\geq 0 \\
\therefore \deg(f(x)) &\leq \deg(f(x)g(x))
\end{aligned}$$

□

Lemma 1. *Given F is integral domain, prove $f(x)g(x) = 0 \Leftrightarrow f(x) = 0$ or $g(x) = 0$*

Proof. Proof by contradition
Assume $f(x)$ and $g(x)$ are nonzero polynomials

From the defintion of multiplication of two polynomials

$$\begin{aligned}
&f(x)g(x) = \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n} \left(\sum_{j=0}^{m} a_i b_j x^{i+j} \right) \quad a_n \neq 0, b_m \neq 0 \\
&\text{The leading term is } a_n b_m x^{n+m} \\
&\implies a_n b_m \neq 0 \quad \because F \text{ is integral domain} \\
&\implies f(x)g(x) \neq 0, \text{ therefore, that contradits our assumtion} \\
&\implies f(x) = 0 \text{ or } g(x) = 0
\end{aligned}$$

□

Proof. Proof by the degree of polynomial, need to prove F is integral domain for the formula

$$\begin{aligned}
\deg(f(x)g(x)) &= \deg(f(x)) + \deg(g(x)) \\
\deg(f(x)g(x)) &= \deg(0) = -\infty \\
\therefore \deg(f(x)) &= -\infty \text{ or } \deg(g(x)) = -\infty \\
\implies f(x) &= 0 \text{ or } g(x) = 0
\end{aligned}$$

□

Lemma 2. *Division Algorithm*
Let $f(x) = a_0 + a_1x^1 + \cdots + a_mx^m$*, there exists* $g(x)$ *and* $r(x)$ *such that*

$$f(x) = h(x)g(x) + r(x) \quad \textit{where } r(x) = 0 \textit{ or } \deg(r(x)) < \deg(g(x)), a_m \neq 0, b_n \neq 0$$

Proof. If $\deg(f(x)) < \deg(g(x))$, then we have

$$\begin{aligned} f(x) &= 0 \cdot g(x) + r(x) \\ \therefore f(x) &= r(x) \\ \therefore \deg(r(x)) &< \deg(g(x)) \end{aligned}$$

If $\deg(f(x)) \geq \deg(g(x))$
Let

$$\begin{aligned} & f_1(x) = f(x) - \frac{a_mx^m}{b_nx^n}g(x) && (1) \\ & f_1(x) = f(x) - \frac{a_mx^m}{b_nx^n}(b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + b_nx^n) \\ & f_1(x) = f(x) - \frac{a_mx^m}{b_nx^n}(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) - a_mx^m \\ & \implies \deg(f_1(x)) \leq m - 1 \end{aligned}$$

Use induction on the degree of $f_1(x)$, e.g. $m - 1$, and assume the follow hold

$$\begin{aligned} & f_1(x) = h(x)g(x) + r(x) \text{ such as } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)) && (2) \\ & f(x) - \frac{a_mx^m}{b_nx^n}g(x) = h(x)g(x) + r(x) \quad \text{from } (1), (2) \\ & f(x) = (h(x) + \frac{a_mx^m}{b_nx^n})g(x) + r(x) \\ & \implies r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)) \text{ for } \deg(f(x)) = m \\ & \therefore \text{The Division Algorithm is true} \end{aligned}$$

□

Definition 9. *Principal Idea is the ideal that generated by single element from* $\mathbf{R}$*.*
Let $a \in \mathbf{I}$ *and* $r \in \mathbf{R}$*, if* ar *or* $ra \in \mathbf{I}$*, then* ar *or* ra *is principal idea.*
For example, $2\mathbf{Z}$ *is principal ideal of* $\mathbf{Z}$

Theorem 1. *Fermat Little Theorem: $a, p \in \mathbb{Z}$, p is prime and* $\gcd(a,p) = 1$

$$a^p \equiv a \mod p$$

Proof. 1. Use induction and Binomial Theorem:

base case: $a = 1$

$$1^p \equiv 1 \mod p \quad \text{Obviously, it is true}$$

try to show $a = 2$

$$2^p \equiv 2 \mod p$$

from Binomial Theorem

$$\begin{aligned}
(1+1)^p &= \sum_{k=0}^{p} \binom{p}{k} = \binom{p}{0} + \binom{p}{1} + \dots \binom{p}{p-1} + \binom{p}{p} \\
(1+1)^p \mod p &\equiv \binom{p}{0} + \binom{p}{1} + \dots \binom{p}{p-1} + \binom{p}{p} \mod p \\
(1+1)^p \mod p &\equiv \binom{p}{0} + \binom{p}{p} \mod p \\
2^p \mod p &\equiv 2 \mod p \\
2^p &\equiv 2 \mod p \\
&\therefore \text{it hold for } a = 2
\end{aligned}$$

let assume:

$$\begin{aligned}
a^p &\equiv a \mod p \qquad (1) \\
(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \quad \text{from Binomial Theorem} \\
(a+1)^p &= \sum_{k=0}^{p} \frac{p!}{(p-k)!k!} a^k \\
(a+1)^p &= a^0 + \frac{p!}{(p-1)!1!} a^1 + \dots + \frac{p!}{(p-(p-1))!(p-1)!} a^{p-1} + a^p \\
\gcd(p, (p-k)!) = 1 &\text{ and } \gcd(p, k!) = 1 \quad \text{if } 1 \le k \le p-1 \\
(a+1)^p \mod p &\equiv a^0 + \frac{p!}{(p-1)!1!} a^1 + \dots + \frac{p!}{(p-(p-1))!(p-1)!} a^{p-1} + a^p \mod p \\
(a+1)^p \mod p &\equiv a^0 + a^p \mod p \quad \text{(All other terms contain the factor of } p\text{)} \\
(a+1)^p \mod p &\equiv 1 + a^p \mod p \\
(a+1)^p &\equiv 1 + a^p \mod p \qquad (2) \\
\left.\begin{matrix}(1)\\(2)\end{matrix}\right\} &\implies (a+1)^p = (a+1) \mod p \\
\therefore a^p &\equiv a \mod p \quad \forall a \in \mathbb{Z}, \gcd(a,p) = 1
\end{aligned}$$

$\square$

Proof. let $S = \{1, 2, \ldots, p-1\}$ then $a \cdot S = \{a, a2, \ldots, a(p-1)\}$
In $a \cdot S$, none of them is divisible by p $\because \gcd(a, p) = 1$
It is sufficient to show all of them in $a \cdot S$ are distinct.

Assume $ai \equiv aj \mod p$ where $i \neq j$, $1 \leq i, j \leq p-1$

$$\begin{aligned}
&\text{But } i \equiv j \mod p \quad \text{cancel both side by } a \\
&\text{That contracts our assumption } i \neq j \\
&\implies \text{the permuation of } S \equiv a \cdot S \mod p \\
&\implies a \cdot S \mod p \equiv S \mod p \\
&\implies a^{p-1} 1 \cdot 2 \cdot \ldots (p-1) \mod p \equiv 1 \cdot 2 \cdot \ldots p-1 \mod p \\
&\implies a^{p-1} \equiv 1 \mod p \\
&\implies a^p \equiv a \mod p
\end{aligned}$$

$\square$

Note 1. *let* $S = \{1, 2, 3, 4\}, a = 2, p = 5$
$a \cdot S = \{2, 4, 6, 8\} \mod 5$
$a \cdot S = \{2, 4, 1, 3\} \mod 5$
$a \cdot S$ *is just a different arrange of* $\{1, 2, 3, 4\}$ *as long as* $\gcd(a, p) = 1$