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 definition 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 $a_nb_m \neq 0$, from the definition

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

□

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 definition 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 $f(x) = a_0 + a_1 x^1 + \cdots + a_m x^m$, there exists $g(x)$ and $r(x)$ such that

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

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

$$\begin{aligned}
&f_1(x) = f(x) - \frac{a_m x^m}{b_n x^n} g(x) \qquad (1) \\
&f_1(x) = f(x) - \frac{a_m x^m}{b_n x^n} (b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + b_n x^n) \\
&f_1(x) = f(x) - \frac{a_m x^m}{b_n x^n} (b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}) - a_m x^m \\
&\implies \deg(f_1(x)) \leq m - 1
\end{aligned}$$

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

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

□

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.*

Example 1. $2\mathbf{Z}$ *is principal ideal of* $\mathbf{Z}$ *or* $n\mathbf{Z}$ *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:

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 $i \neq j$, $1 \leq i, j \leq p-1$

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

□

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* $\gcd(a,p) = 1$

Definition 10. *Legendra Symbol*

p is old prime, $a \in \mathbb{Z}$

$$\left(\frac{a}{q}\right) = \begin{cases} +1 & : a^{\frac{p-1}{2}} \mod p \equiv 1 \\ 0 & : a^{\frac{p-1}{2}} \mod p \equiv 0 \\ -1 & : a^{\frac{p-1}{2}} \mod p \equiv p-1 \end{cases}$$

Proof. write your proof here □

Definition 11. *Gauss Lemma*

Proof. write your proof here □