Definition 21.1

Let R be a commutative ring. The *ring of polynomials* $R[x]$ of variable x with coefficient in R is defined as follows.

- Elements of $R[x]$ are expressions of the form

$$p(x) = a_n x^n + a^{n-1} x_{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

  where $n \geq 0$.

- Addition in $R[x]$: if $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{m} b_i x^i$ then

$$p(x) + q(x) = \sum_{i=0}^{s} (a_i + b_i) x^i$$

  where $s = \max(m, n)$. In this formula, if $i > n$ then we take $a_i = 0$ and if $i > m$ then we take $b_i = 0$.

- Multiplication in $R[x]$: if $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{m} b_i x^i$ then

$$p(x) \cdot q(x) = \sum_{i=0}^{s} c_i x^i$$

  where $s = m + n$ and $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0$

Definition 21.2

For a polynomial $p(x) = \sum_i a_i x^i \in R[x]$ such that $p(x) \neq 0$, the *degree* $p(x)$ is the integer $n \geq 0$ such $a_n \neq 0$ and $a_i = 0$ for all $i > n$. We denote $\deg p(x) = n$. For the zero polynomial $p(x) = 0$ degree is not defined.

Theorem 21.3

Let R be an integral domain and let $p(x), q(x) \in R[x]$ be non-zero polynomials. Then

$$\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$$

Corollary 21.4

If R is an integral domain then $R[x]$ is also an integral domain.

Theorem 21.5

Let R be an integral domain. Let $p(x) = a_n x^n + \ldots + a_0$ and be a polynomial in $R[x]$ such that $p(x) \neq 0$. and a_n is a unit. Then for any $g(x) \in R[x]$ there exist unique polynomials $q(x), r(x) \in R[x]$ such that

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

where either $r(x) = 0$ or $\deg r(x) < \deg p(x)$.

Exercise. Let $p(x) = x^2 + 3x + 2$ and $g(x) = 3x^4 + 2x^2 - x + 7$ be polynomials in $\mathbb{Z}[x]$. Find the quotient and the reminder of the division of $g(x)$ by $p(x)$.

Exercise. Let $p(x) = 4x^2 + 3x + 2$ and $g(x) = 3x^4 + 2x^2 + 4x + 1$ be polynomials in $\mathbb{Z}_5[x]$. Find the quotient and the reminder of the division of $g(x)$ by $p(x)$.

Definition 21.6

Let R be an integral domain and let $p(x), g(x) \in R[x]$. We say that $p(x)$ *divides* $g(x)$ if there is $q(x) \in R[x]$ such that $g(x) = q(x)p(x)$.

Definition 21.7

Let R be an integral domain and let $p(x) \in R[x]$. We say that an element $a \in R$ is a *root* of $p(x)$ if $p(a) = 0$.

Theorem 21.8

Let R be an integral domain and let $p(x) \in R[x]$. An element $a \in R$ is a root of $p(x)$ if and only if $(x - a)$ divides $p(x)$.

Corollary 21.9

Let R be an integral domain, let $p(x) \in R[x]$ and let $a_1, \ldots, a_m \in R$ be distinct elements of R. Then $a_1, \ldots, a_m$ are roots of $p(x)$ if and only if $(x-a_1) \cdot \ldots \cdot (x-a_m)$ divides $p(x)$.

Corollary 21.10

If R is an integral domain and $p(x) \in R[x]$ is a non-zero polynomial, then $p(x)$ has at most $\deg p(x)$ distinct roots.

Corollary 21.11

Let R be an integral domain consisting of infinitely many elements. If $p(x), g(x) \in R[x]$ are polynomials such that $p(a) = g(a)$ for all $a \in R$ then $p(x) = g(x)$.

Definition 21.12

A ring R is a *principal ideal domain (PID)* if R is an integral domain and every ideal of R is principal.

Theorem 21.13

If F is a field then $F[x]$ is a PID.