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 $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0$

Note. Let R be a commutative ring. Any polynomial $p(x) = a_n x^n + a_{n-1}x_{n-1} + \ldots + a_0$ defines a function $\overline{p}\colon R \to R$ given by $\overline{p}(r) = a_n r^n + a_{n-1}r^{n-1} + \ldots + a_0$. In general it may happen that $p(x)$, $q(x)$ are different polynomials, but the functions $\overline{p}$, $\overline{q}$ they define are the same.

For example, take $p(x) = 0$, $q(x) = x^2 + x \in \mathbb{Z}_2[x]$. Then $p(x) \neq q(x)$. On the other hand, consider the functions $\overline{p}, \overline{q}\colon \mathbb{Z}_2 \to \mathbb{Z}_2$. We have $\overline{p}(0) = 0 = \overline{q}(0)$ and $\overline{p}(1) = 0 = \overline{q}(1)$, so $\overline{p} = \overline{q}$.

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

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

Proof. If $\deg p(x) = n$ and $\deg q(x) = m$ then $p(x) = a_n x^n + \ldots + a_0$ $p(x) = b_m x^m + \ldots + b_0$ for some $a_i, b_i \in R$ such that $a_n \neq 0$, $b_m \neq 0$. Then

$$p(x) \cdot q(x) = a_n b_m x^{m+n} + \ldots + a_0 b_0$$

Since R is an integral domain, thus $a_n b_m \neq 0$, so $\deg(p(x) \cdot q(x)) = m + n$. □

Example. Theorem 21.3 is not true when R is not an integral domain. Take e.g. $p(x) = 2x+1,\ q(x) = 3x+1 \in \mathbb{Z}_6[x]$. Then $\deg p(x) = p(x) = 1$ and $\deg(p(x) \cdot q(x)) = \deg(5x+1) = 1$.

Corollary 21.4

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

Proof. If $p(x), q(x) \in R[x]$ are non-zero polynomials, then by Theorem 21.3 $\deg(p(x) \cdot q(x))$ is defined, so $p(x) \cdot q(x) \neq 0$. □

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 $\deg r(x) < \deg p(x)$.

Note. We say that $q(x)$ is the *quotient* and $r(x)$ is the *reminder* of the division of $g(x)$ by $p(x)$.

Proof of Theorem 21.5. To show existence of $q(x)$ and $r(x)$, we argue by induction with respect to $\deg g(x)$. If $g(x) = 0$ or $\deg g(x) < \deg p(x)$ then we take $q(x) = 0$ and $r(x) = g(x)$. Next, assume that for any polynomial $g'(x)$ of degree smaller than m we can find $q(x)$ and $r(x)$ as in the theorem, and let $g(x) = b_m x^m + \ldots + b_0$ be a polynomial such that $\deg g(x) = m \geq n = \deg p(x)$. Let

$$g(x) = b_m x^m + \ldots + b_0$$

Using the assumption that a_n is a unit in R, take the polynomial

$$s(x) = g(x) - (b_m a_n^{-1})p(x) \cdot x^{m-n}$$

We have:

$$\begin{aligned} s(x) =& g(x) - (b_m a_n^{-1})p(x) \cdot x^{m-n} \\ &= (b_m x^m + b_{m-1}x^{m-1} + \ldots) - (b_m a_n^{-1})(a_n x^n + a_{n-1}x^{n-1} + \ldots) \cdot x^{m-n} \\ &= (b_m x^m + b_{m-1}x^{m-1} + \ldots) - ((b_m a_n^{-1} a_n)x^m + (b_m a_n^{-1} a_{n-1})x^{m-1} + \ldots) \\ &= (b_m x^m + b_{m-1}x^{m-1} + \ldots) - (b_m x^m + (b_m a_n^{-1} a_{n-1})x^{m-1} + \ldots) \\ &= ((b_{m-1} - b_m a_n^{-1} a_{n-1})x^{m-1} + \ldots) \end{aligned}$$

This shows that $\deg s(x) \leq m$ and so, by the inductive assumption, we have $s(x) = q'(x)p(x) + r'(x)$ for some $q'(x), r'(x) \in R[x]$ such that either $r'(x) = 0$ or $\deg r'(x) < \deg p(x)$. This gives:

$$\begin{aligned} g(x) &= s(x) + (b_m a_n^{-1})p(x) \cdot x^{m-n} \\ &= (q'(x)p(x) + r'(x)) + (b_m a_n^{-1})p(x) \cdot x^{m-n} \\ &= (q'(x) + (b_m a_n^{-1})x^{m-n})p(x) + r'(x) \end{aligned}$$

Thus we can take $q(x) = q'(x) + (b_m a_n^{-1})x^{m-n}$ and $r(x) = r'(x)$.

For uniqueness, assume that $g(x) = q_1(x)p(x) + r_1(x)$ and $g(x) = q_2(x)p(x) + r_2(x)$ for some $p_1(x), p_2(x), r_1(x), r_2(x) \in R[x]$. Then

$$0 = (q_1(x) - q_2(x))p(x) + (r_1(x) - r_2(x))$$

or equivalently

$$(q_1(x) - q_2(x))p(x) = -(r_1(x) - r_2(x))$$

If $q_1(x) \neq q_2(x)$ then degree of the left hand side is greater or equal to $\deg p(x)$, which is greater than the degree of the right hand side. Since this is impossible, we get $q_1(x) = q_2(x)$. This implies that $r_1(x) = r_2(x)$. □

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 $p(x)$.

Proof. By Theorem 21.5 we have

$$p(x) = q(x)(x - a) + r(x)$$

for some $q(x), r(x) \in R[x]$ where $r(x) = b$ for some $b \in R$. This gives:

$$p(a) = q(a)(a - a) + b = b$$

Thus $p(a) = 0$ if and only if $b = 0$. In such case $p(x) = q(x)(x - a)$. □

Corollary 21.9

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

Proof. If $(x - a_1) \cdot \ldots \cdot (x - a_m)$ divides $p(x)$ then

$$p(x) = q(x) \cdot (x - a_1) \cdot \ldots \cdot (x - a_m)$$

for some $q(x) \in R[x]$. Then $p(a_i) = 0$ for $i = 1, \ldots, m$, so $a_1, \ldots, a_m$ are roots of $p(x)$. Conversely, assume that $a_1, \ldots, a_m$ are roots of $p(x)$. By Theorem 21.8 we have

$$p(x) = q_1(x) \cdot (x - a_1)$$

for some $q_1 \in R[x]$. This gives:

$$0 = p(a_2) = q_1(a_2) \cdot (a_2 - a_1)$$

Since $a_1 \neq a_2$, we have $a_2 - a_1 \neq 0$. Thus, since R is an integral domain, we obtain that $q_1(a_2) = 0$. Applying Theorem 21.8 to the polynomial $q_1(x)$ we obtain that

$$q_1(x) = q_2(x) \cdot (x - a_2)$$

for some $q_2(x) \in R[x]$, and so

$$p(x) = q_2(x) \cdot (x - a_2) \cdot (x - a_1)$$

Continuing this argument inductively, we obtain that

$$p(x) = q(x) \cdot (x - a_1) \cdot \ldots \cdot (x - a_m)$$

for some $q(x) \in R[x]$. □

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.

Proof. If $a_1, \ldots, a_m$ are distinct roots of $p(x)$ then by Corollary 21.9 we have

$$p(x) = q(x) \cdot (x - a_1) \cdot \ldots \cdot (x - a_m)$$

Then $\deg p(x) = \deg q(x) + m$, so $m \leq \deg p(x)$. □

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 $p(x) = g(x)$.

Proof. Assume that $p(a) = g(a)$ for all $a \in R$. Take $f(x) = p(x) - g(x)$. Then $f(a) = 0$ for all $a \in R$. Since consists of infinitely many elements, thus $f(a)$ has infinitely many roots. By 21.10 this is possible only if $f(x) = 0$, i.e. $p(x) = g(x)$. □

Recall that if R a commutative ring, then an ideal $J \triangleleft R$ is principal if J is generated by a single element. Thank is, there is $a \in R$ such that

$$J = \langle a \rangle = \{ar \mid r \in R\}$$

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.

Example. Every field is a PID. Indeed, if F is a field then the only ideals of F are $\{0\} = \langle 0 \rangle$ and $F = \langle 1 \rangle$.

Example. The ring of integers $\mathbb{Z}$ is a PID. Indeed, let $J \triangleleft \mathbb{Z}$. If $J = \{0\}$ then $J = \langle 0 \rangle$. If $J \neq \{0\}$, let a be the smallest positive integer such that $a \in J$. We will show that $J = \langle a \rangle$. Indeed, assume that $b \in J$. We have $b = qa + r$ for some $q, r \in \mathbb{Z}$ such that $0 \geq r < a$. Since $r = b - qa$, thus $r \in J$. Since a is the smallest positive element of J, we must have $r = 0$. Thus $b = qa$, and so $b \in \langle a \rangle$. This shows that $J \subseteq \langle a \rangle$. Also, since $a \in J$, thus $\langle a \rangle \subseteq J$. This gives $J = \langle a \rangle$.

Example. The ring $\mathbb{Z}[x]$ is not a PID. Take for example the ideal $\langle 2, x \rangle \triangleleft \mathbb{Z}[x]$ generated by the constant polynomial $p(x) = 2$ and the polynomial $q(x) = x$. Elements of $\langle 2, x \rangle$ are polynomials $g(x) = a_n x^n + \ldots + a_0$ such that a_0 is an even number. The ideal $\langle 2, x \rangle$ is not principal. Indeed, assume that $\langle 2, x \rangle = \langle f(x) \rangle$ for some $f(x) \in \mathbb{Z}[x]$. Since $2 \in \langle 2, x \rangle$, thus $f(x)$ must divide 2. This means that $f(x)$ is a constant polynomial, and $f(x) = 1, -1, 2$ or 2. If $f(x) = \pm 1$ then $\langle f(x) \rangle = \mathbb{Z}[x] \neq \langle 2, x \rangle$. Also, if $f(x) = \pm 2$, then $\langle f(x) \rangle$ consists of polynomials whose all coefficients are even. Thus $\langle f(x) \rangle \neq \langle 2, x \rangle$.

Theorem 21.13

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

Note. Theorem 21.13 can be considered as a generalization of Theorem 21.8 as follows. For $a \in F$ consider the homomorphism $\varphi\colon F[x] \to F$ given by $\varphi(p(x)) = p(a)$. Then $\mathrm{Ker}(\varphi)$ is an ideal of $F[x]$ consisting of polynomials $g(x)$ such that $g(a) = 0$. Theorem 21.8 says that every such polynomial is a multiple of $(x - a)$, so $\mathrm{Ker}(\varphi)$ is a principal ideal, $\mathrm{Ker}(\varphi) = \langle (x - a) \rangle$. Now, if $J \triangleleft F[x]$ is an arbitrary ideal, then there is a homomorphism $\varphi\colon F[x] \to S$ for some ring S such that $J = \mathrm{Ker}(\varphi)$. Theorem 21.13 says that $\mathrm{Ker}(\varphi) = \langle p(x) \rangle$ for some $p(x) \in F[x]$.

Proof of Theorem 21.13. Let $J \triangleleft F[x]$. If $J = \{0\}$ then $J = \langle 0 \rangle$. Assume then that $J \neq \{0\}$. Let $p(x)$ be a non-zero polynomial of the smallest degree, such that $p(x) \in J$. We will show that $J = \langle p(x) \rangle$.

Let $f(x) \in J$. We need to show that $f(x) = q(x)p(x)$ for some $q(x) \in F[x]$. Since F is a field, the coefficient of the highest degree term of $p(x)$ is a unit, so by Theorem 21.5 we have $f(x) = q(x)p(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg p(x)$. Assume that $r(x) \neq 0$. Then $r(x) = f(x) - q(x)p(x) \in J$, which is impossible, since by assumption $p(x)$ is a polynomial of the smallest degree in J. Thus $r(x) = 0$ and so $f(x) = q(x)p(x)$. □