Previously.

- Ring Homomorphisms
- First Isomorphism Theorem for Rings

This Section.

- Polynomial Rings

Exercise 1. We encountered $\mathbb{R}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \geq 0,\ a_i \in \mathbb{R}\}$ briefly before. It is a ring under polynomial addition and multiplication.

(a) Give some example elements of $\mathbb{R}[x]$.

(b) What's the additive identity of $\mathbb{R}[x]$?

(c) What's the multiplicative identity of $\mathbb{R}[x]$?

(d) How would you define $\mathbb{Z}[x]$? $\mathbb{Q}[x]$?

(e) What do elements of $\mathbb{Z}_3[x]$ look like?

Definition. Let R be a ring. We denote the set of polynomials over R by $R[x]$ where

$$R[x] := \{r_0 + r_1x + r_2x^2 + \cdots + r_nx^n \mid n \in \mathbb{Z}_{\geq 0} \text{ and } r_i \in R\ \forall\ 0 \leq i \leq n\}.$$

Any particular element $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ in $R[x]$ is called a polynomial, the elements $a_i \in R$ are called the coefficients of f.

Note. The variable x is called an indeterminate it is a symbol representing a position in the list.

Theorem. Let R be a ring with unity. For $f, g \in R[x]$ such that

$$f = a_0 + a_1x + a_2x^2 + \cdots \text{ and } g = b_0 + b_1x + b_2x^2 + \cdots$$

define the operations

- $f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$
- $f \cdot g = c_0 + c_1x + c_2x^2 + \cdots$ where

$$c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0 = \sum_{k=0}^{i} a_kb_{i-k}.$$

Then $(R[x], +, \cdot)$ is a ring with unity.

Exercise 2. Let $f = 3 + 2x + 4x^2$ and $g = x - 3x^2 + 2x^3$. Compute the coefficient of x^4 in $f \cdot g$ using the formula for c_4.

Exercise 3. In $\mathbb{Z}_3[x]$ compute $(x + 2)^4$.

Definition. Let R be a ring with unity. For $f, g \in R[x]$ such that

$$f = a_0 + a_1x + a_2x^2 + \cdots \text{ and } g = b_0 + b_1x + b_2x^2 + \cdots$$

define the items:

- We call two polynomials `equal` if the corresponding coefficients are equal.
  That is, $f = g$ means that $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$, $\ldots$.
- We call a_0 the `constant term` or `constant coefficient`.
- A polynomial of the form $f = a_0$ is a `constant polynomial`.
- The `zero` of $R[x]$ is ____________ and the `unity` is ____________.
- The `negative` of $f = a_0 + a_1x + a_2x^2 + \cdots$ is $-f = -a_0 - a_1x - a_2x^2 - \cdots$

Definition. Let R be a ring with unity. For $f \in R[x]$ such that

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad a_n \neq 0,$$

define the following:

- Since $a_n \neq 0$, we say that the `degree` of f is n and write $\deg(f) = n$.
- We call a_n the `leading coefficient` of f.
- If the leading coefficient of f is 1, we call f `monic`.

Theorem 4.1.1. Let R be a ring and let x be an indeterminate over R. Then

1. $R[x]$ is a ring.

2. R is the subring of all constant polynomials in $R[x]$.

3. If $Z = Z(R)$ denotes the center of R, then the center of $R[x]$ is $Z[x]$.

4. In fact, x is in the center of $R[x]$.

5. If R is commutative, then $R[x]$ is commutative.

Definition.

- If $\deg(f) = 1$, we call f a linear polynomial.
- If $\deg(f) = 2$, we call f a ____________ polynomial.
- If $\deg(f) = 3$, we call f a ____________ polynomial.
- If $\deg(f) = 4$, we call f a ____________ polynomial.
- If $\deg(f) = 5$, we call f a ____________ polynomial.

Exercise 4. Consider $S = \{f \in \mathbb{Z}[x] \ : \ f(1) = 0\}$. Is S a subring or an ideal of $\mathbb{Z}[x]$?

Exercise 5. Show that $(x) = \{xf \mid f \in \mathbb{Z}[x]\}$ is an ideal of $\mathbb{Z}[x]$ and that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

Theorem 4.1.2. Let R be a domain. Then

1. $R[x]$ is a domain.

2. If $f \neq 0$ and $g \neq 0$ in $R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$.

3. The units in $R[x]$ are the units in R.

Exercise 6. As a non-example to the previous theorem, consider $f = 1 + 2x$ in $\mathbb{Z}_4[x]$.

(a) Verify that $\mathbb{Z}_4$ is not a domain.

(b) Compute f^2 to see $\deg(f^2) \neq 2\deg(f)$.

(c) Find some zero divisors in $\mathbb{Z}_4[x]$.

Division Algorithm (Theorem 4.1.4). Let R be any ring and let f and g be polynomials in $R[x]$. Assume $f \neq 0$ and that the leading coefficient of f is a unit in R. Then there exist unique $q, r \in R[x]$ such that

1. $g = qf + r$.
2. Either $r = 0$ or $\deg r < \deg f$.

Exercise 7. Use long division to find q and r given $f = x^2 + 1$ and $g = x^4 + 3x^3 + x + 1$ in $\mathbb{Z}[x]$.

Factor Theorem (Theorem 4.1.6(1). Let R be a commutative ring, $a \in R$, and $f \in R[x]$. Then $f(a) = 0$ if and only if $f = (x - a)g$ for some $g \in R[x]$.
(Remainder Theorem) Moreover, in general, when dividing f by $x - a$, we get $f = (x - a)q + f(a)$. That is, the remainder when dividing f by $x - a$ is $f(a) \in R$.

Exercise 8. Consider $R = \mathbb{Z}_6$ and $f = x^3 - x$.
Notice $f(0) = f(1) = f(2) = f(3) = f(4) = f(5) = 0$. Thus

- $f = (x - 0)(\underline{\hspace{3cm}})$
- $f = (x - 1)(\underline{\hspace{3cm}})$
- $f = (x - 2)(\underline{\hspace{3cm}})$
- $f = (x - 3)(\underline{\hspace{3cm}})$
- $f = (x - 4)(\underline{\hspace{3cm}})$
- $f = (x - 5)(\underline{\hspace{3cm}})$

Question 9. Does this mean $f = x(x - 1)(x - 2)(x - 3)(x - 4)(x - 5)$?

Corollary. Let R be a commutative ring, $a \in R$, and $\phi_a : R[x] \to R$ the evaulation map at a. Then

$$\ker(\phi_a) = (x-a) = \{(x-a)g \mid g \in R[x]\}$$

and $R[x]/(x-a) \cong R$.

Definition. Let $f \in R[x]$ and $a \in R$. We call a a root or f if the following conditions (which are all equivalent) are true:

1. $f(a) = 0$.
2. $f = (x-a)g$ for some $g \in R[x]$.
3. f is in the principal ideal $(x-a)$.

If $a \in R$ is a root of f, we say it has multiplicity $m \in \mathbb{Z}_{>0}$ if $f = (x-a)^m q$ and $q(a) \neq 0$.

Example. What's the multiplicity of $a = -1$ as a root of $f = t^4 + t^3 + t + 1 \in \mathbb{Z}_7[t]$?

Theorem 4.1.8. Let R be an integral domain and let f be a nonzero polynomial of degree n in $R[x]$. Then f has at most n roots in R.

Rational Roots Theorem (Theorem 4.1.9). Let $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}[x]$ with $a_0, a_n \neq 0$. Then every root of f in $\mathbb{Q}$ is of the form $\frac{c}{d}$ where $c \mid a_0$ and $d \mid a_n$.

Example. Factor the following as much as possible in $\mathbb{Q}[x]$.

(a) $2\,x^3 - 7\,x^2 - 7\,x + 12$

(b) $x^4 + 5x^3 - 4x^2 + 3x$

(c) $12\,x^4 - 44\,x^3 + 39\,x^2 + 8\,x - 12$