Lecture 10

Polynomial Rings (多項式環)

What you will learn in Lecture 10

10.1 Polynomial Rings (多項式環)

10.2 The Division Algorithm (除法の算法) for Polynomial rings

10.3 Irreducible Polynomials (既約多項式)

10.1 Polynomial Rings (多項式環)

10.1 Polynomial Rings (多項式環)

In this lecture, we assume that R is a **commutative ring with identity**.

Definition 10.1

We assume that R is a **commutative ring with identity**. A **polynomial (多項式)** $f(x)$ with **indeterminate (不定元)** x **over** R is a formal sum

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

where $a_i \in R$, and $a_n \neq 0$. The a_i are **coefficients (係数)** of $f(x)$. If n is the largest nonnegative number for which $a_n \neq 0$, we say that n is the **degree (次数)** of $f(x)$ and write $\deg f(x) = n$. If all $a_i = 0$, then $f = 0$ is the **zero polynomial**, the degree of $f(x)$ is undefined or say $-\infty$. We call $f(x)$ **constant polynomial** when $\deg f(x) = 0$. **Notice that** here we call x **indeterminate** but not variable.

We will denote **the set of all polynomials** with **indeterminate** x in a ring R by $R[x]$.

10.1 Polynomial Rings (多項式環)

Two polynomials are equal exactly when their corresponding coefficients are equal; that is, if we let

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$
$$q(x) = b_0 + b_1 x + \ldots + b_m x^m$$

then $p(x) = q(x)$ if and only if $a_i = b_i$ for all $i \geq 0$.

10.1 Polynomial Rings (多項式環)

Most people are fairly familiar with polynomials by the time they begin to study abstract algebra. When **we examine polynomial expressions** such as

$$\begin{aligned} p(x) &= x^3 - 3x + 2 \\ q(x) &= 3x^2 - 6x + 5 \end{aligned}$$

we have a pretty good idea of what $p(x) + q(x)$ and $p(x)q(x)$ mean.
We just add and multiply polynomials as functions; that is,

$$\begin{aligned} (p+q)(x) &= p(x) + q(x) \\ &= (x^3 - 3x + 2) + (3x^2 - 6x + 5) \\ &= x^3 + 3x^2 - 9x + 7 \end{aligned}$$

and

$$\begin{aligned} (pq)(x) &= p(x)q(x) \\ &= (x^3 - 3x + 2)(3x^2 - 6x + 5) \\ &= 3x^5 - 6x^4 - 4x^3 + 24x^2 - 27x + 10 \end{aligned}$$

It is probably no surprise that polynomials form a ring. In this lecture we shall emphasize the algebraic structure of polynomials by studying polynomial rings. We can prove many results for polynomial rings that are similar to the theorems we proved for the integers. **Analogs of prime numbers**, the **division algorithm**, and the **Euclidean algorithm exist for polynomials**.

10.1 Polynomial Rings (多項式環)

To **show that the set of all polynomials forms a ring**, **we must first define addition and multiplication**. We define the sum of two polynomials as follows. Let

$$p(x) = a_0 + a_1 x + \cdots + a_n x_n$$
$$q(x) = b_0 + b_1 x + \cdots + b_m x_m$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = c_0 + c_1 x + \ldots + c_k x_k$$

where $c_i = a_i + b_i$ for each i.

We define the product of $p(x)$ and $q(x)$ to be

$$p(x)q(x) = c_0 + c_1 x + \cdots + c_{m+n} x_{m+n}$$

where

$$c_i = \sum_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$$

for each i. Notice that **in each case some of the coefficients may be zero.**

10.1 Polynomial Rings (多項式環)

Example 10.1
Suppose that

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

and

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

are polynomials in $\mathbb{Z}[x]$. If the coefficient of some term in a polynomial is zero, then we usually just omit that term. In this case we would write $p(x) = 3 + 2x^3$ and $q(x) = 2 - x^2 + 4x^4$.

The sum of these two polynomials is

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4$$

The product,

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7;$$

can be calculated either by determining the $c_i s$ in the definition or by simply multiplying polynomials in the same way as we have always done.

Example 10.2

Find the sum and the product of the given polynomials $p(x) = 4x - 5$ and $q(x) = 2x^2 - 4x + 2$ in the given polynomial ring $\mathbb{Z}_8[x]$.

The **sum** of $p(x)$ and $q(x)$

$$\begin{aligned} p(x) + q(x) &= (4x - 5) + (2x^2 - 4x + 2) \\ &= 2x^2 + (4 - 4)x + (-5 + 2) \\ &= 2x^2 + 5 \end{aligned}$$

The **product** of $p(x)$ and $q(x)$

$$\begin{aligned} p(x)q(x) &= (4x - 5)(2x^2 - 4x + 2) \\ &= 4x(2x^2 - 4x + 2) - 5(2x^2 - 4x + 2) \\ &= 8x^3 - 16x^2 + 8x - 10x - 10x^2 + 20x - 10 \\ &= 8x^3 - 26x^2 + 28x - 10 \\ &= 6x^2 + 4x + 6 \quad \text{(Because in } \mathbb{Z}_8[x]\text{)} \end{aligned}$$

Example 10.3
Let $p(x) = 3 + 3x^3$ and $q(x) = 4 + 4x^2 + 4x^4$ be polynomials in $\mathbb{Z}_{12}[x]$.
We know $\mathbb{Z}_{12}$ is not an integral domain.

The sum of $p(x)$ and $q(x)$ is $7 + 4x^2 + 3x^3 + 4x^4$.

The product of the two polynomials is the zero polynomial.

This example tells us that we can not expect $R[x]$ to be an **integral domain** if R is not an **integral domain**.

Theorem 10.1

Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.

Proof

Our first task is to show that $R[x]$ is an abelian group under polynomial addition.
The zero polynomial, $f(x) = 0$, is the additive identity.
Given a polynomial $p(x) = \sum_{i=0}^{m} a_i x^i$, the inverse of $p(x)$ is easily verified to be $-p(x) = \sum_{i=0}^{m}(-a_i)x^i = -\sum_{i=0}^{m} a_i x^i$.
Commutativity and associativity follow immediately from the definition of polynomial addition and from the fact that addition in R is both commutative and associative.
To show that polynomial multiplication is associative, let

$$p(x) = \sum_{i=0}^{m} a_i x^i \qquad q(x) = \sum_{i=0}^{n} b_i x^i \qquad r(x) = \sum_{i=0}^{p} c_i x^i$$

10.1 Polynomial Rings (多項式環)

Proof (cont.)

$$
\begin{aligned}
[p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right) c_{i-j}\right] x^i \\
&= \sum_{i=0}^{m+n+p}\left(\sum_{j+k+l=i} a_j b_k c_l\right) x^i \\
&= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right] x^i \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n+p}\left(\sum_{j=0}^{i} b_j c_{i-j}\right) x^i\right] \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\left(\sum_{i=0}^{n} b_i x^i\right)\left(\sum_{i=0}^{p} c_i x^i\right)\right] \\
&= p(x)[q(x)r(x)]
\end{aligned}
$$

The commutativity and distribution properties of polynomial multiplication are proved in a similar manner.

10.1 Polynomial Rings (多項式環)

Proposition

Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is an integral domain. Then $\deg p(x) + \deg q(x) = \deg(p(x)q(x))$. Furthermore, $R[x]$ is an integral domain.

Proof

Theorem 10.2

Let R be a **commutative ring with identity** and $\tau \in R$. Then we have a **ring homomorphism (環準同型)** $f_\tau\colon R[x] \to R$ defined by

$$f_\tau(p(x)) = p(\tau) = a_n\tau^n + \cdots + a_1\tau + a_0$$

where $p(x) = a_nx^n + \cdots + a_1x + a_0$.

Proof

The map $f_\tau\colon R[x] \to R$ is called the **evaluation homomorphism** at .

10.2 The Division Algorithm (除法の算法)

for Polynomial rings

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Recall that the **division algorithm (除法の算法)** for integers says that if a and b are integers with $b > 0$, then there exist **unique integers** q and r such that $a = bq + r$, where $0 \leq r < b$.

A similar theorem exists for polynomials.

The division algorithm for polynomials has several important consequences.

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Theorem 10.3

Let $f(x)$ and $g(x)$ be **polynomials** in $F[x]$, where F is a **field** and $g(x)$ is a **nonzero polynomial**. Then there exist **unique polynomials** $q(x), r(x) \in F[x]$ such that

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

where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Proof

We will first consider the existence of $q(x)$ and $r(x)$. If $f(x)$ is the zero polynomial, then

$$0 = 0 \cdot g(x) + 0$$

hence, both q and r must also be the **zero polynomial**.
Now suppose that $f(x)$ is **not the zero polynomial** and that $\deg f(x) = n$ and $\deg g(x) = m$.
If $m > n$, then we can let $q(x) = 0$ and $r(x) = f(x)$. Hence, we may assume that $m \leq n$ and proceed by induction on n. If

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

The polynomial

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

has degree less than n or is the **zero polynomial**. By induction, there exist polynomials $q'(x)$ and $r(x)$ such that

$$f'(x) = q'(x)g(x) + r(x)$$

where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. Now let

$$q(x) = q'^{(x)} + \frac{a_n}{b_m} x^{n-m}$$

Then

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

with $r(x)$ the zero polynomial or $\deg r(x) < \deg g(x)$.

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Proof (cont.)

To show that $q(x)$ and $r(x)$ are unique, suppose that there exist two other polynomials $q_1(x)$ and $r_1(x)$ such that $f(x) = g(x)q_1(x) + r_1(x)$ with $\deg r_1(x) < \deg g(x)$ or $r_1(x) = 0$, so that

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$$

and

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x):$$

If $q(x) - q_1(x)$ is not the zero polynomial, then

$$\deg(g(x)[q(x) - q_1(x)]) = \deg\big(r_1(x) - r(x)\big) \geq \deg g(x)$$

However, the degrees of both $r(x)$ and $r_1(x)$ are strictly less than the degree of $g(x)$; therefore, $r(x) = r_1(x)$ and $q(x) = q_1(x)$.

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Example 10.4
The division algorithm merely formalizes long division of polynomials, a task we have been familiar with since high school. For example, suppose that we divide $x^3 - x^2 + 2x - 3$ by $x - 2$.

$$
\begin{array}{r|l}
 & \quad x^2 + x + 4 \\
\hline
x - 2 & \quad x^3 - x^2 + 2x - 3 \\
 & \quad \underline{x^3 - 2x^2} \\
 & \qquad\quad x^2 + 2x - 3 \\
 & \qquad\quad \underline{x^2 - 2x} \\
 & \qquad\qquad\quad 4x - 3 \\
 & \qquad\qquad\quad \underline{4x - 8} \\
 & \qquad\qquad\qquad\quad 5
\end{array}
$$

Hence, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5.$

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Example 10.5

Let's work with polynomials in $\mathbb{Z}_5[x]$ and divide

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$$

by $g(x) = x^2 - 2x + 3$ to find $q(x)$ and $r(x)$ of Theorem 10.3. Notice we are in $\mathbb{Z}_5[x]$, so, for example $4x - (-3x) = 2x$.

$$
\begin{array}{r|l}
 & \quad x^2 - x - 3 \\
\hline
x^2 - 2x + 3 & \quad x^4 - 3x^3 + 2x^2 + 4x - 1 \\
 & \quad \underline{x^4 - 2x^3 + 3x^2} \\
 & \qquad\quad -x^3 - x^2 + 4x \\
 & \qquad\quad \underline{-x^3 + 2x^2 - 3x} \\
 & \qquad\qquad\quad -3x^2 + 2x - 1 \\
 & \qquad\qquad\quad \underline{-3x^2 + x - 4} \\
 & \qquad\qquad\qquad\qquad x + 3
\end{array}
$$

Thus

$$q(x) = x^2 - x - 3 \text{ and } r(x) = x + 3$$

Theorem (Remainder Theorem) 10.4

Let R be a commutative ring with identity. For $f(x) \in R[x]$ and $\tau \in R$, there exists $q(x) \in R[x]$ such that

$$f(x) = (x - \tau)q(x) + f(\tau)$$

Proof

Hint: Theorem of Division Algorithm

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Definition 10.2

Let R be a commutative ring with identity and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. For all $\tau \in R$, define

$$f(\tau) = a_0 + a_1 \tau + \cdots + a_n \tau^n.$$

when $f(\tau) = 0$, we call τ a **root (根)** or **zero** of $f(x)$.

Corollary 10.1

Let R be a commutative ring with identity. For $f(x) \in R[x]$ and $\tau \in R$, $x - \tau$ divides $f(x)$ if and only if τ is a **root** of $f(x)$.

Proof

Suppose $(x-\tau) \mid f(x)$. Then there exists $q(x) \in R[x]$ such that $f(x) = (x-\tau)q(x)$.
Hence, $f(\tau) = (\tau - \tau)q(\tau) = 0$, so τ is a root of $f(x)$.
Conversely, suppose τ is a root of $f(x)$. Then by the remainder theorem and the fact that $f(\tau) = 0$, we have $f(x) = (x-\tau)q(x)$. Consequently, $(x-\tau) \mid f(x)$.

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Example 10.6

Working again in $\mathbb{Z}_5[x]$ note that $\tau = 1$ is a root of

$$f(x) = x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x]$$

Thus by Corollary 10.1, we should be able to factor $x^4 + 3x^3 + 2x + 4$ into $(x-1)q(x)$ in $\mathbb{Z}_5[x]$. Let us find the factorization by long division

$$
\begin{array}{r|l}
 & x^3 + 4x^2 + 4x + 1 \\
\hline
x - 1 & x^4 + 3x^3 + \qquad 2x + 4 \\
 & \underline{x^4 - x^3} \\
 & \quad 4x^3 \\
 & \quad \underline{4x^3 - 4x^2} \\
 & \qquad 4x^2 + 2x \\
 & \qquad \underline{4x^2 - 4x} \\
 & \qquad\quad x + 4 \\
 & \qquad\quad \underline{x - 1} \\
 & \qquad\qquad 0
\end{array}
$$

Hence, $x^4 + 3x^3 + 2x + 4 = (x-1)(x^3 + 4x^2 + 4x + 1)$.

10.2 The Division Algorithm (除法の算法) for Polynomial rings

Example 10.6 (cont.)

Since 1 is also a root of $x^3 + 4x^2 + 4x + 1$, we can divide this polynomial by $x - 1$ and get

$$\begin{array}{r|l} & \quad x^2 + 4 \\ \hline x - 1 & x^3 + 4x^2 + 4x + 1 \\ & x^3 - x^2 \\ \hline & \qquad\quad 0 + 4x + 1 \\ & \qquad\qquad\quad 4x - 4 \\ \hline & \qquad\qquad\qquad\quad 0 \end{array}$$

Since 1 is still the root of $x^2 + 4$, we can divide again by $\mathrm{x} - 1$ and get

$$\begin{array}{r|l} & \quad x + 1 \\ \hline x - 1 & x^2 + \qquad 4 \\ & x^2 - x \\ \hline & \qquad x + 4 \\ & \qquad x - 1 \\ \hline & \qquad\quad 0 \end{array}$$

Thus $x^4 + 3x^3 + 2x + 4 = (x - 1)^3(x + 1)$ in $\mathbb{Z}_5[x]$.

10.3 Irreducible Polynomials (既約多項式)

10.3 Irreducible Polynomials (既約多項式)

Definition 10.3

A **nonconstant polynomial** $f(x) \in F[x]$ is **irreducible (既約な) over a field** F if $f(x)$ **cannot be expressed as a product of two polynomials** $g(x)$ and $h(x)$ in $F[x]$, where **the degrees of** $g(x)$ and $h(x)$ are **both smaller than the degree of** $f(x)$.

Irreducible polynomials function as the "prime numbers" of polynomial rings.

Example 10.7

The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is **irreducible** since it cannot be factored any further over the rational numbers.

Similarly, $x^2 + 1$ is **irreducible** over the real numbers.

Example 10.8

The polynomial $p(x) = x^3 + x^2 + 2$ is **irreducible** over $\mathbb{Z}_3[x]$.

Suppose that this polynomial was reducible over $\mathbb{Z}_3[x]$.

By the division algorithm there would have to be a factor of the form $x - \tau$, where τ is some element in $\mathbb{Z}_3[x]$.

Hence, it would have to be true that $p(\tau) = 0$. However,

$$
\begin{aligned}
p(0) &= 2 \\
p(1) &= 1 \\
p(2) &= 2
\end{aligned}
$$

Therefore, $p(x)$ has **no roots/zeros** in $\mathbb{Z}_3$ and must be **irreducible**.

Review for Lecture 10

- Polynomials
- Zero Polynomial
- Polynomial Rings (多項式環)
- The Division Algorithm (除法の算法) for Polynomial rings
- Remainder Theorem
- Irreducible Polynomials (既約多項式)

Assignment

Please Check https://github.com/uoaworks/Applied-Algebra

References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018

[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007

[3] **(おすすめ)** 松本 眞, 代数系への入門, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf

[4] Wikipedia

[5] Materials from internet.