Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on: `https://japorized.github.io/TeX_notes`

27 Lecture 27 Jul 06th 2018

27.1 Polynomial Ring

27.1.1 Polynomials

Definition 48 (Polynomials)

Let R be a ring and x a variable. Let

$$R[x] = \left\{ f(x) = \sum_{i=0}^{m} a_i x^i : m \in \mathbb{N} \cup \{0\},\, a_i \in R, 0 \leq i \leq m \right\}.$$

Each element in $R[x]$ is called a ***polynomial*** *in x over R. If $a_m \neq 0$, we say that $f(x)$ has* ***degree*** *m, denoted by $\deg f = m$, and we say that a_m is the* ***leading coefficient*** *of $f(x)$.*

If $\deg f = 0$, then $f(x) = a_0 \in R$. In this case, we call $f(x)$ a ***constant polynomial****. Note if*

$$f(x) = 0 \iff a_0 = a_1 = ... = a_m = 0,$$

we define $\deg 0 = -\infty$, and $f(x)$ is called a ***zero polynomial****.*

For

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \ldots + b_n x^n$$

in $R[x]$. If $m \leq n$, we can define $a_i = 0$ for $m + 1 \leq i \leq n$. Then the addition and multiplication on $R[x]$ can be defined as

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n \\ f(x)g(x) &= (a_0 + a_1 x + \ldots + a_m x^m)(b_0 + b_1 x + \ldots + b_n x^n) \\ &= a_0 b_0 + (a_1 b_0 + a_1 b_0)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \ldots \\ &\quad + (a_m b_m)x^{m+n} \\ &= c_0 + c_1 x + \ldots + c_{m+n} x^{m+n} \end{aligned}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0$.

Proposition 81 (Ring is a Subring of Its Polynomial Ring)

Let R be a ring and x a variable.

1. *$R[x]$ is a ring*
2. *R is a subring of $R[x]$*
3. *If $Z = Z(R)$ denote the center of R, then the center of $R[x]$ is $Z[x]$. In particular, x is in the center of $R[x]$.*

Proof

1. ***Checking all 9 properties**: Let*

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_m x^m \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n \\ h(x) &= d_0 + d_1 x + \ldots + d_k x^k \end{aligned}$$

be in $R[x]$.

- *(**Closed under addition and multiplication**) Suppose, WLOG, that $m \leq n$. Let $a_i = 0$ for $m + 1 \leq i \leq n$. Then*

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n$$

and we observe that $a_i + b_i \in R$ for $0 \leq i \leq n$ since R is a ring. And so $f(x) + g(x) \in R[x]$. Also, we have

$$f(x)g(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0 \in R$ for $1 \leq i \leq$

$m+n$. And so $f(x)g(x) \in R[x]$.

- *(**Commutativity of Addition**) Suppose, WLOG, that $m \leq n$. Let $a_i = 0$ for $m+1 \leq i \leq n$. Then*

$$\begin{aligned} f(x)+g(x) &= (a_0+b_0)+(a_1+b_1)x+\ldots+(a_n+b_n)x^n \\ &= (b_0+a_0)+(b_1+a_1)x+\ldots+(b_n+a_n)x^n \\ &= g(x)+f(x) \end{aligned}$$

- *(**Zero and Unity**) It is clear that the zero and unity of R are the zero and unity of $R[x]$ respectively, since only*

$$f(x)+0 = f(x) = 0+f(x)$$

and

$$1f(x) = f(x) = f(x) \cdot 1.$$

- *(**Associativity**) Suppose, WLOG, that $m \leq n \leq k$. Let $a_i = b_j = 0$ for $m+1 \leq i \leq k$ and $n+1 \leq j \leq k$. Then*

$$\begin{aligned} & f(x)+[g(x)+h(x)] \\ &= f(x)+[(b_0+d_0)+(b_1+d_1)x+\ldots+(b_k d_k)x^k] \\ &= (a_0+b_0+d_0)+(a_1+b_1+d_1)x+\ldots+(a_k+b_k+d_k)x^k \\ &= [(a_0+b_0)+(a_1+b_1)x+\ldots+(a_k+b_k)x^k]+d(x) \\ &= [f(x)+g(x)]+h(x) \end{aligned}$$

and if we use the summation notation for $f(x), g(x)$ and $h(x)$, we *have*

$$\begin{aligned}
f(x)[g(x)d(x)] &= f(x)\left[\left(\sum_{j=0}^{n} b_j x^j\right)\left(\sum_{l=0}^{k} d_l x^l\right)\right] \\
&= \left[\sum_{i=0}^{m} a_i x^i\right]\left[\sum_{j=0}^{n}\sum_{l=0}^{k} b_j d_l x^{j+l}\right] \\
&= \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{l=0}^{k} a_i b_j d_l x^{i+j+k} \\
&= \left[\sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j}\right]\left[\sum_{l=0}^{k} d_l x^l\right] \\
&= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right)\right] h(x) \\
&= [f(x)g(x)]h(x)
\end{aligned}$$

- (***Inverse***) *Since R is a ring, and in particular an additive ring, for each $a_i \in R$, $0 \leq i \leq m$, we have that $\exists(-a_i) \in R$ such that $a_i + (-a_i) = 0$. Particularly, we have that*

  $$-f(x) = (-a_0) + (-a_1)x + (-a_2)x^2 + \ldots + (-a_m)x^m$$

  is the inverse of $f(x) \in R[x]$.

- (***Distributivity***) *Again, using the summation notation, since R is a ring, we have*

  $$\begin{aligned}
  &f(x)[g(x) + h(x)] \\
  &= \left[\sum_{i=0}^{m} a_i x^i\right]\left[\sum_{j=0}^{n} b_j x^j + \sum_{l=0}^{k} d_l x^l\right] \\
  &= \left[\sum_{i=0}^{m} a_i x^i\right]\left[\sum_{j=0}^{k} (b_j + d_j) x^j\right] \\
  &= \sum_{i=0}^{m}\sum_{j=0}^{k} a_i(b_j + d_j)x^{i+j} = \sum_{i=0}^{m}\sum_{j=0}^{k} (a_i b_j + a_i d_j)x^{i+j} \\
  &= \sum_{i=0}^{m}\sum_{j=0}^{k} a_i b_j x^{i+j} + \sum_{i=0}^{m}\sum_{j=0}^{k} a_i d_j x^{i+j} \\
  &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j} + \sum_{i=0}^{m}\sum_{j=0}^{k} a_i d_j x^{i+j} \\
  &= f(x)g(x) + f(x)d(x).
  \end{aligned}$$

  Proof for the other side is similar.

With that, we have that $R[x]$ is a ring.

2. *We already have that R is a ring, and so it suffices to prove that $R \subseteq R[x]$. This is, however, rather simple, since $\forall r \in R$, we have that r is a constant polynomial, and so $r \in R[x]$, and therefore $R \subseteq R[x]$.*

3. *Let*

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m \in Z[x] \\ g(x) &= b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n \in R[x]. \end{aligned}$$

We have that

$$f(x)g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j}.$$

Since $a_i \in Z$ for $0 \leq i \leq n$, we have

$$f(x)g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} b_j a_i x^{i+j} = \sum_{j=0}^{n} \sum_{i=0}^{m} b_j a_i x^{j+i} = g(x)f(x)$$

for any $g(x) \in R[x]$. And so $Z[x] = Z(R[x])$.

For $\supseteq$, $f(x) \in Z(R[x]) \implies \forall b \in R \subseteq R[x]$ we have $f(x)b = bf(x)$. It follows that

$$\forall 0 \leq i \leq n \quad a_i b = b a_i$$

and so $a_i \in Z(R)$, which implies that $Z(R[x]) \subseteq Z[x]$. Therefore, $Z(R[x]) = Z[x]$.

$\square$

Warning

Althought $f(x) \in R[x]$ can be used to define a function from $R \to R$, the polynomial is not the same as the function it defines. For example, if $R = \mathbb{Z}_2$, then $\mathbb{Z}_2[x]$ is an infinite set, but there are only 4 different functions from $\mathbb{Z}_2 \to \mathbb{Z}_2$

Proposition 82 (Polynomial Ring is an Integral Domain)

Let R be an integral domain. Then

1. *$R[x]$ is an integral domain.*

2. *If* $f(x) \neq 0$ *and* $g(x) \neq 0$ *in* $R[x]$, *then*[1]

$$\deg(fg) = \deg f + \deg g$$

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

[1] In order to preserve this for when we have the case of $\deg 0$, we have to define $\deg 0 = -\infty$. Otherwise, say if we define $\deg 0 = -1$, then if $\deg f = -1$, then $\deg(fg) = \deg f + \deg g$ would imply that $\deg g = -2$, which is undefined.

Proof

We shall prove (1) *and* (2) *together.*

1 & 2. *Suppose* $f(x) \neq 0 \neq g(x) \in R[x]$, *say*

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_m x^m \quad a_m \neq 0 \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n \quad b_n \neq 0. \end{aligned}$$

Then

$$f(x)g(x) = a_m b_n x^{m+n} + \ldots a_0 b_0.$$

Now since R *is an integral domain, we have that* $a_m b_n \neq 0$ *and so* $f(x)g(x) \neq 0$. *Thus* $R[x]$ *is an integral domain. Moreover, we see that*

$$\deg(fg) = m + n = \deg f + \deg g.$$

3. *Suppose that* $u(x) \in R[x]$ *is a unit of* $R[x]$ *with inverse* $u^{-1}(x)$ *which we shall write as* $v(x)$. *Since* $u(x)v(x) = 1$, *by* (2), *we have that*

$$\deg u + \deg v = \deg 1 = 0. \tag{27.1}$$

Now by (1), $R[x]$ *is an integral domain, and so since* $u(x)v(x) = 1$, *we have that* $u(x) \neq 0 \neq v(x)$. *Therefore,* $\deg u, \deg v \geq 0$, *which implies that we must have* $\deg u = 0 = \deg v$ *from Equation* (27.1). *Therefore, units in* $R[x]$ *are from* R^*.

$\square$

Note

Recall that $\mathbb{Z}_n$ *is an integral domain if and only if* $n = p$ *a prime. If* $n \neq p$, *then, e.g., for* $\mathbb{Z}_4[x]$, *we have*

$$2x \cdot 2x = 4x^2 = 0$$

and so

$$\deg(2x) + \deg(2x) \neq \deg(4x^2) = \deg(2x \cdot 2x).$$

27.1.2 Factorization of Polynomials

Definition 49 (Division of Polynomials)

Let R be a commutative ring and $f(x), g(x) \in R[x]$. We say that $f(x)$ divides $g(x)$, denoted as $f(x) \mid g(x)$ if $\exists q(x) \in R[x]$ such that

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

Definition 50 (Monic Polynomial)

Let R be a commutative ring and $f(x) \in R[x]$. $f(x)$ is monic if its leading coefficient is 1.

We shall prove the following proposition next class.

Proposition

Let R be an integral domain, and $f(x)$, $g(x) \in R[x]$ be monic polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.