

Lecture 12 (Quotient Rings, Polynomial Rings)

A bijective homomorphism of rings is called a ring isomorphism. If there is an isomorphism $\varphi : R \rightarrow S$, we say R is isomorphic to S and write $R \cong S$.

Theorem 12.1 (First Isomorphism Theorem) Suppose $\varphi : R \rightarrow S$ is a homomorphism of rings.

Then $\ker \varphi$ an ideal of R , $\text{im } \varphi$ is a subring of S and the natural map $\bar{x} \mapsto \varphi(x)$ is an isomorphism $\pi : R/\ker \varphi \cong \text{im } \varphi$.

Proof We have already shown $\ker \varphi$ an ideal of R , $\text{im } \varphi$ is a subring of S . Any pair of elements in $R/\ker \varphi$ is of the form \bar{x}, \bar{y} for some $x, y \in R$. We have

$$\begin{aligned}\bar{x} &= \bar{y} \\ \Leftrightarrow x &\equiv y \pmod{\ker \varphi} \\ \Leftrightarrow x - y &\in \ker \varphi \\ \Leftrightarrow \varphi(x - y) &= 0 \\ \Leftrightarrow \varphi(x) - \varphi(y) &= 0 \\ \Leftrightarrow \varphi(x) &= \varphi(y)\end{aligned}$$

This shows $\pi(\bar{x}) = \varphi(x)$ is well defined and defines a bijection from $R/\ker \varphi$ to $\text{im } \varphi$.

It remains to show it respects addition and multiplication in and thus is a ring homomorphism.

$$\begin{aligned}\pi(\bar{x} + \bar{y}) &= \pi(\overline{x + y}) \quad (\text{addition in the quotient ring}) \\ &= \varphi(x + y) \quad (\text{definition of } \pi) \\ &= \varphi(x) + \varphi(y) \quad (\varphi \text{ respects addition}) \\ &= \pi(\bar{x}) + \pi(\bar{y}) \quad (\text{definition of } \pi).\end{aligned}$$

So π respect addition. We deduce similarly it preserves multiplication:

$$\begin{aligned}\pi(\bar{x}\bar{y}) &= \pi(\overline{xy}) \quad (\text{multiplication in the quotient ring}) \\ &= \varphi(xy) \quad (\text{definition of } \pi) \\ &= \varphi(x)\varphi(y) \quad (\varphi \text{ respects multiplication}) \\ &= \pi(\bar{x})\pi(\bar{y}) \quad (\text{definition of } \pi).\end{aligned}$$

□

Rambling Definition 12.2 (Polynomials) Suppose R is a ring and x an indeterminate. Let us define the ring $R[x]$ of polynomials in x with coefficients in R .

A polynomial in x with coefficients in R is any finite formal sum

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$

with all $a_i \in R$, and where terms with $a_i = 0$ may be omitted or retained at will. If an expression for a polynomial contains a term a_0 , this called the constant term. If there is no term a_0 present the constant term is 0. If there is a term a_ix^i , then we say the coefficient of x^i is a_i , if there is no such term the coefficient of x^i is 0. We declare two polynomials equal if their sequences of coefficients coincide. Thus there is a 1-1 correspondence between polynomials and infinite sequences (a_0, a_1, a_2, \dots) of elements of R which are 0 except for finitely many values of i . We let $R[x]$ be the set of all such polynomials.

So for example in $\mathbb{Z}[x]$, $2 + 5x^2 + 4x^4 = 2 + 0x + 5x^2 + 4x^4 + 0x^5$ has coefficients of x , x^3 and all x^i , $i \geq 5$ equal to 0.

We add two polynomials in $R[x]$ in the usual way, by adding coefficients of like term. We multiply two such polynomials by multiplying out formally distributing multiplication over addition using relations

$$a_ix^ib_jx^j = a_ib_jx^{i+j}$$

and combining terms of like degree by adding their coefficients. These operations can be described simply in terms of sequence of coefficients.

Suppose $a(x)$ has sequence of coefficients (a_0, a_1, a_2, \dots) and $b(x)$ has sequence of coefficients (b_0, b_1, b_2, \dots) . Then the sequence of coefficients of $a(x) + b(x)$ is the sequence $(a_0 + b_0, a_1 + b_1, \dots)$ obtained by adding corresponding terms and their product $a(x)b(x)$ is the polynomial $c(x)$ whose sequence of coefficients is (c_0, c_1, c_2, \dots) , where

$$c_n = \sum_{i+j=n, i, j \geq 0} a_ib_j.$$

It is easily checked that $R[x]$ is a ring.

Note The usual convention of omitting terms $0x^i$, $i \geq 1$ when writing polynomials identifies R as the subring of constant polynomials in $R[x]$.

More Observations and Conventions

- The zero of $R[x]$ is the constant 0 polynomial.
- The ring $R[x]$ is commutative if and only if R is commutative.
- If $R[x]$ has an identity element if and only if R does.
- If R has an identity we put $1x^i = x^i$ and view x and its powers as elements of $R[x]$.

Definition 12.3 If $a(x) \in R[x]$ is not the constant 0 polynomial then we can write

$$a(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_n \neq 0$$

In this case we put $\deg a(x) = n$.

We declare $\deg 0 = -\infty$.

For $a = a(x), b = b(x) \in R[x]$,

$$\begin{aligned} \deg(a(x) + b(x)) &\leq \max \{ \deg a(x), \deg b(x) \} \\ \deg(a(x)b(x)) &\leq \deg a(x) + \deg b(x) \end{aligned}$$

Lemma 12.4 We have

$$\deg a(x)b(x) = \deg a(x) + \deg b(x)$$

for all polynomials $a(x), b(x) \in R[x]$ if and only if R has no zero divisors.

Proof Suppose $a(x), b(x) \in R[x]$. Set $n = \deg a(x)$, $m = \deg b(x)$. We will have $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$ if either of $a(x)$ or $b(x)$ is the 0 polynomial. Otherwise both $n \geq 0$ and $m \geq 0$. So $a(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, and $b(x) = b_0 + b_1x + \cdots + b_mx^m$, $a_m \neq 0$. Then the coefficient of x_i in $a(x)b(x)$ is 0 for $i \geq m + n$ and the coefficient of x^{n+m} is a_nb_m . This coefficient will be nonzero and $\deg a(x)b(x) = \deg a(x) + \deg b(x)$ if and only if $a_nb_m \neq 0$. This will be the case for all such polynomials if and only if R has no zero divisors. \square

From the proof we see the product of two non-zero polynomials in $R[x]$ is non-zero if R has no zero divisors.

Corollary If R has no zero divisors neither does $R[x]$. \square

An integral domain is a commutative ring with identity with no zero divisors. We know that R is commutative and has an identity element if $R[x]$ is commutative and has an identity element.

Proposition 12.5 If R is an integral domain so is $R[x]$.

Proof Follows from the corollary and the remarks above. □