Lecture 25: The evaluation map; ideal; quotient; first isomorphism theorem

Friday, December 1, 2017 11:05 AM

Suppose $R_1 \subseteq R_2$ is a ring extension (that means R_1 is a subring of R_2; which is equivalent to say R_1 is closed under addition and multiplication.) For any $s \in R_2$, let $\phi_s : R_1[x] \to R_2$, $\phi_s(p(x)) := p(s)$. Then ϕ_s is a ring homomorphism.

Recall • $I \subseteq R$ is called an ideal if I is an additive subgp and $RI \subseteq I$ (and $IR \subseteq I$); that means $\forall r \in R, a \in I, ra \in I$ and $ar \in I$.

• $(R/I, +, \cdot)$ where $(x+I)+(y+I) := (x+y)+I$ and $(x+I)\cdot(y+I) := xy+I$ is a ring. It is called the quotient ring of R by I. $\pi : R \to R/I$, $\pi(a) := a+I$ is a ring homomorphism; and it is called the canonical quotient map.

The 1^{st} isomorphism theorem. Suppose $\phi : R_1 \to R_2$ is a ring homomorphism. Then

(1). $\ker \phi := \{a \in R_1 \mid \phi(a) = 0\}$ is an ideal of R_1.

. $\operatorname{Im} \phi$ is a subring of R_2.

Lecture 25: The first isomorphism theorem; the evaluation map

Friday, December 1, 2017 11:18 AM

(2) $\overline{\Phi}: R_1/\ker\phi \longrightarrow \operatorname{Im}\phi$, $\overline{\Phi}(a+\ker\phi) := \phi(a)$ is a well-def. ring homomorphism.

Quick overview of proof of (2).. $\overline{\Phi}$ is an additive gp isomorph.

$$\overline{\Phi}((a+\ker\phi)(b+\ker\phi)) = \overline{\Phi}(ab+\ker\phi) = \phi(ab)$$
$$= \phi(a)\,\phi(b)$$
$$= \overline{\Phi}(a+\ker\phi)\,\overline{\Phi}(b+\ker\phi). \qquad \square$$

So $R_1[x]/\ker\phi_s \simeq \operatorname{Im}\phi_s$.

$\ker\phi_s = \{p(x)\in R_1[x] \mid p(s)=0\}$ (and you see the relation with zeros of polynomials.)

$$\operatorname{Im}\phi_s = \underbrace{\left\{\sum_{i=0}^{n} c_i s^i \;\middle|\; c_i\in R_1\right\}}_{\text{the smallest subring of } R_2 \text{ which has } s \text{ as an element of } R_1 \text{ as a subset}} =: \underbrace{R_1[s]}_{\text{we denote it by this notation and should not be confused with ring of poly. as } s \text{ is NOT an indeterminant.}}$$

Ex. $R_1=\mathbb{Q}$, $R_2=\mathbb{C}$, $s=i$. Then

$\mathbb{Q}[i] = \left\{\sum_{k=0}^{n} c_k i^k \;\middle|\; c_k\in\mathbb{Q}\right\}$. As $i^k = \begin{cases} 1 & k\equiv 0 \pmod 4 \\ i & k\equiv 1 \pmod 4 \\ -1 & k\equiv 2 \pmod 4 \\ -i & k\equiv 3 \pmod 4 \end{cases}$,

$\mathbb{Q}[i] = \{c_0 + c_1 i \mid c_0, c_1\in\mathbb{Q}\}$.

$\ker\phi_i = \{p(x)\in\mathbb{Q}[x] \mid p(i)=0\}$. Then $x^2+1\in\ker\phi_i$ and as $i\notin\mathbb{Q}$, there is no deg 1 poly. in $\ker\phi_i$. $\square$

Lecture 25: Degree function; zero-divisor; dividing; units

Friday, December 1, 2017 11:32 AM

All rings are unital comm. unless said otherwise

<u>Def.</u> For $f(x)=\sum_{i=0}^{\infty} c_i x^i \in R[x]$, let

$$\deg f = \begin{cases} -\infty & \text{if } f=0, \\ \max\{n\in\mathbb{Z}^{\geq 0} \mid c_n\neq 0\} & \text{if } f\neq 0. \end{cases}$$

<u>Ex.</u> $4x,\ 3x^2+1 \in (\mathbb{Z}/6\mathbb{Z})[x]$,

$\deg(4x)=1$, $\deg(3x^2+1)=2$; but

$\deg((4x)(3x^2+1)) = \deg(12x^3+4x) = \deg 4x = 1.$

$\neq \deg 4x + \deg(3x^2+1)$.

This issue arises because of <u>zero-divisors</u>.

<u>Recall.</u> $a\in R$ is called a zero-divisor if $\exists c\in R\setminus\{0\}$, $ac=0$.

- In general we say $a\mid b$ if $\exists c\in R\setminus\{0\}$ s.t. $b=ac$.
- $a\in R$ is called a <u>unit</u> if $a\mid 1$; that means $\exists c\in R$, $ac=1$. The set of all units is denoted by either $U(R)$ or $R^\times$. $(R^\times,\cdot)$ is a group.
- A ring D is called an <u>integral domain</u> if D does not have a non-zero zero-divisor, and $0\neq 1$.
- A ring F is called a field if $F\setminus\{0\}=F^\times$.

Lecture 25: Integral domain and field

Friday, December 1, 2017 1:08 PM

<u>Lemma</u>. (1) A field is an integral domain.

(2) A finite integral domain is a field.

<u>Pf</u>. (1) $\left.\begin{array}{l} ab=0 \\ a\neq 0 \Rightarrow a\in F^{\times} \Rightarrow a^{-1}\in F \end{array}\right\} \Rightarrow b = a^{-1}(ab) = 0$.

Here we are using $r\cdot 0 = 0$; which can be proved as follows $r\cdot 0 = r\cdot(0+0) = r\cdot 0 + r\cdot 0$

(2) $\forall a\in D\setminus\{0\}$, let $l_a : D\to D$, $l_a(b) := ab$.

<u>Claim</u>. l_a is 1-1.

<u>Pf</u>. $l_a(b_1) = l_a(b_2) \Rightarrow ab_1 = ab_2 \Rightarrow a(b_1-b_2)=0$

$\left.\begin{array}{l} a(b_1-b_2)=0 \\ a\neq 0 \\ \text{no non-zero zero-divisor in } D \end{array}\right\} \Rightarrow b_1 - b_2 = 0 \Rightarrow b_1 = b_2$.

Since D is finite and l_a is 1-1, l_a is onto. So

$\exists a'\in D$, $l_a(a') = 1$. Hence $aa' = 1$; which means $a\in D^{\times}$.

■

Going back to the degree function;

<u>Lemma</u>. Suppose D is an integral domain. Then, for any $f,g\in D[x]$, $\deg fg = \deg f + \deg g$.

(Here we are using the convention that $-\infty + n = -\infty$ $\forall n\in\mathbb{Z}$, and $(-\infty)+(-\infty) = -\infty$.)

Lecture 25: Degree function; zero-divisor and units of D[x]

Friday, December 1, 2017 1:22 PM

Pf. If either $f=0$ or $g=0$, then $fg=0$; and so

$$\text{LHS} = -\infty \quad \text{and} \quad \text{RHS} = -\infty.$$

Suppose $f, g \neq 0$. So $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $a_n \neq 0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ and $b_m \neq 0$. (a_n is called the leading coefficient of f.) Then

$$f(x)\,g(x) = a_n b_m x^{n+m} + \text{terms of deg} < m+n.$$

$$\left.\begin{array}{l} a_n \neq 0,\ b_m \neq 0 \\ D: \text{integral domain} \end{array}\right\} \Rightarrow a_n b_m \neq 0. \text{ And so } \deg fg = n+m = \deg f + \deg g.$$

■

Cor. If D is an integral domain, then $D[x]$ is an integral domain.

Pf. $f(x)\,g(x) = 0 \Rightarrow \deg fg = -\infty \Rightarrow \deg f + \deg g = -\infty$

$\Rightarrow$ either $\deg f = -\infty$ or $\deg g = -\infty$

$\Rightarrow f=0$ or $g=0$. ■

Cor. $D[x]^\times = D^\times$

Pf. $f(x)\,g(x) = 1 \Rightarrow \deg f + \deg g = 0 \Rightarrow \deg f = \deg g = 0$

$f, g \in D$ and $f \cdot g = 1 \Rightarrow f \in D^\times$. And clearly $D^\times \subseteq D[x]^\times$. ■

Lecture 25: Units of a polynomial ring; a historical remark on ideals.

Friday, December 1, 2017 11:37 PM

We will prove that

<u>Proposition</u>. $R[x]^\times = \{a_0+a_1x+\cdots+a_nx^n \mid a_0\in R^\times,\ a_1,\dots,a_n$ are nilpotent $\}$

(a is called <u>nilpotent</u> if $a^k=0$ for some $k\in\mathbb{Z}^+$.)

But prove this we need to know a bit more about ideals.

We'd like to define prime and maximal ideals. Before that let's make a pseudo-historical remark on <u>ideals</u>.

Say we'd like to attack Fermat's last conjecture; and suppose for integers x,y,z that are pairwise coprime we have $x^p+y^p=z^p$ where p is an odd prime. Then

$x^p = z^p-y^p = (z-y)(z-\zeta y)\cdots(z-\zeta^{p-1}y)$. If $\mathbb{Z}[\zeta]$ is a UFD ; that means any non-zero, non-unit element can be written as a prod. of primes in an essentially unique way, then

$z-y=x_1^p,\ z-\zeta y=x_2^p,\ \dots,\ z-\zeta^{p-1}y=x_p^p$. And one can get a contradiction (in an elementary, but not quite easy way.) Kummer

and Dedekind noticed that, if instead of numbers, one works with ideals

Lecture 25: A historical note

Sunday, December 3, 2017 10:36 PM

then in rings similar to $\mathbb{Z}[\zeta]$ in the lack of unique factorization of elements we still have unique factorization of <u>ideals</u>. And in fact Kummer called it <u>ideal numbers</u>; and its generalization by Dedekind was called ideal. In order to make sense of this we need to define <u>prime ideal</u>. And it will be done in the next lecture.