Lecture 16: Recall rings ideals and factor rings

Wednesday, December 5, 2018 5:43 PM

we start with recalling definition of ideal and factor ring:

<u>Def.</u> Suppose A is a unital (commutative) ring. $I \subseteq A$ is called an ideal of A if $\forall a, b \in I$, $a+b \in I$ and

$$\forall r \in A,\ a \in I,\ ra \in I,\ ar \in I.$$

We write $I \triangleleft A$. (When A is not commutative, left and right ideals are defined as well where the 2^{nd} condition is replaced with $\forall r \in A, a \in I \Rightarrow ra \in I$ and $\forall r \in A, a \in I, \Rightarrow ar \in I$, respectively).

• Suppose $I \triangleleft A$. Then on the additive group A/I one can define the following binary operation: $(a_1+I)(a_2+I) := a_1a_2+I$.

Here is why it is well-define: $a_i + I = a_i' + I \Rightarrow a_i - a_i' \in I$

$$\Rightarrow a_1a_2 - a_1'a_2' = a_1a_2 - a_1'a_2 + a_1'a_2 - a_1'a_2'$$
$$= \underbrace{(a_1-a_1')}_{\text{in } I} a_2 + a_1' \underbrace{(a_2-a_2')}_{\text{in } I} \in I \Rightarrow a_1a_2 + I = a_1'a_2' + I.$$

One can check that $(A/I, +, \cdot)$ is a unital (comm.) ring.

• Suppose $f: A \to A'$ is a ring homo.; that means f is a gp homo. and it preserves multipication. Then the following is a commuting diagram (The 1^{st} isomo. theorem)

$$\begin{tikzcd}
a \arrow[r, mapsto] \arrow[d, mapsto] & f(a) \\
a+\ker f \arrow[ur, mapsto] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowright"] & \operatorname{Im} f \subseteq A' \\
A/\ker f \arrow[ur, "\bar{f}"', "\sim"] &
\end{tikzcd}$$

Going back to ring of poly.; an extremely useful way of studying it is by viewing them as functions:

<u>Evaluation map</u>. Suppose $A \subseteq B$ is a ring extension. For $b \in B$, let $\phi_b : A[x] \to B$, $\phi_b(f(x)) := f(b)$. Then ϕ_b is a ring homomorphism. Image of ϕ_b is $\{\sum_{i=0}^{n} a_i b^i \mid a_i \in A, n \in \mathbb{Z}^{\geq 0}\}$, which is the smallest subring of B that has A as a subset and contains b. We denote such ring by $A[b]$. <u>Warning</u>. This notation is similar to poly. ring, and one has to distinguish them from the content. $\ker \phi_b = \{f(x) \in A[x] \mid \underset{(b \text{ is a zero of } f)}{f(b) = 0}\}$.

By the 1^{st} isom. $A[b] \simeq A[x]/\{f(x) \in A[x] \mid f(b) = 0\}$.

Lecture 16: Evaluation maps

Wednesday, December 5, 2018 12:46 AM

<u>Ex</u>. Show that $\mathbb{Q}[x]/\langle x^2+1\rangle \simeq \mathbb{Q}[i] = \{a+bi \mid a,b\in\mathbb{Q}\}$.

<u>Pf</u>. Consider the evaluation map at i. Then

- $\operatorname{Im}\phi_i = \{\sum_{j=0}^{n} r_j (i)^j \mid r_j\in\mathbb{Q},\ n\in\mathbb{Z}^{\geq 0}\}$

$$\left.\begin{array}{l} i^2=-1 \\ i^3=-i \\ i^4=1 \end{array}\right\} \Rightarrow \quad = \{a+bi \mid a,b\in\mathbb{Q}\} = \mathbb{Q}[i].$$

- $\ker\phi_i = \{f(x)\in\mathbb{Q}[x] \mid f(i)=0\}$

For instance $x^2+1\in\ker\phi_i$. If $f(x)\in\ker\phi_i$, then

by long division $f(x) = (x^2+1)\,q(x) + r(x)$,

$q(x), r(x)\in\mathbb{Q}[x]$, $\deg r < \deg(x^2+1) = 2$.

Hence $\exists\, a,b\in\mathbb{Q}$ s.t. $r(x) = ax+b$.

We plug in i at both sides:

$$0 = f(i) = \underbrace{(i^2+1)}_{0}\,q(i) + r(i) = ai+b$$

So $a=b=0$; therefore $r(x)=0$ and $f(x)\in\langle x^2+1\rangle$.

<u>Def./Remark</u>. For a non-empty subset X of a ring A, $\langle X\rangle$ denotes the smallest ideal of A that contains X as a subset.

Lecture 16: Finitely generated ideals

Wednesday, December 5, 2018 12:56 AM

Notice that this is a similar notation as the subgroup generated by X, and one has to understand which one is which from the content.

(Since intersection of a family of ideals is an ideal,

$$\langle X\rangle = \bigcap_{\substack{X\subseteq I\\ I\trianglelefteq A}} I$$ is the smallest ideal of A that contains X as a subset.)

<u>Lemma</u>. For a unital commutative ring A, $a_1,\ldots,a_n\in A$,

(*) $\langle a_1,\ldots,a_n\rangle = \{r_1a_1+\cdots+r_na_n \mid r_1,\ldots,r_n\in A\}$.

In particular, a <u>principal ideal</u> $\langle a\rangle = \{ra \mid r\in A\}$.

<u>Pf</u>. Suppose $a_1,\ldots,a_n\in I$ and $I\trianglelefteq A$. Then

$\forall r_1,\ldots,r_n\in A,\ r_1a_1,\ldots,r_na_n\in I \Rightarrow r_1a_1+\cdots+r_na_n\in I.$

$\Rightarrow \text{RHS}\subseteq I \Rightarrow \text{RHS}\subseteq \bigcap_{\substack{a_1,\ldots,a_n\in I\\ I\trianglelefteq A}} I = \langle a_1,\ldots,a_n\rangle$.

One can easily check that the RHS is an ideal of A; and

$a_i = 0\cdot a_1+\cdots+0\cdot a_{i-1}+1\cdot a_i+0\cdot a_{i+1}+\cdots+0\cdot a_n\in \text{RHS}$

$\Rightarrow \langle a_1,\ldots,a_n\rangle\subseteq \text{RHS}$. And we get (*).)

Lecture 16: The degree function

Thursday, November 29, 2018 1:31 PM

<u>Def</u>. For $f(x) \in A[x]$, we let $\deg f = -\infty$ if $f=0$, and

$\deg f = n$ if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ and $a_n \neq 0$.

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

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

The main reason for $\deg f_1 f_2 \neq \deg f_1 + \deg f_2$ is the existence of <u>zero-divisors</u>.

<u>Def</u>. Suppose A is a unital commutative ring.

(1) $a \in A \setminus \{0\}$ is called a <u>zero-divisor</u> if $\exists\, b \in A \setminus \{0\}$ s.t. $ab = 0$.

(2) For $a, b \in A$, we say $a \mid b$ if $\exists\, c \in A$ s.t. $b = ac$.

(this is equivalent to say $\langle b \rangle \subseteq \langle a \rangle$.)

(3) $a \in A$ is called a <u>unit</u> if $a \mid 1$; this means $\exists\, b \in A$, $ab = ba = 1$.

<u>Def</u>. A non-trivial unital commutative ring D is called an <u>integral domain</u> if it has no zero-divisors. (Here non-trivial

means not zero.)

Def. A non-trivial unital commutative ring F is called a field if any non-zero element of F is a unit in F.

Lemma. (1) The set of units of a ring R is denoted by $R^\times$; and $(R^\times, \cdot)$ is a group.

(2) The set of zero-divisors of a unital commutative ring A is denoted by $D(A)$; and $D(A) \cap A^\times = \emptyset$. In particular any field is an integral domain.

Pf. (1) $a, b \in R^\times \Rightarrow \exists\, a', b' \in R$ s.t. $aa' = bb' = 1$; and so
$a'a = b'b = 1$

$(ab)(b'a') = (b'a')(ab) = 1$, which implies $ab \in R^\times$.

. $a \in R^\times \Rightarrow \exists\, a' \in R$ s.t. $aa' = 1 = a'a \Rightarrow a' \in R^\times$ and it is multiplicative inverse of a. . $1 \cdot 1 = 1 \Rightarrow 1 \in R^\times$.

(2) Suppose $a \in D(A) \cap A^\times$. Then $\exists\, b \in A \setminus \{0\}$ s.t. $ab = 0$ and $\exists\, a' \in A$ s.t. $aa' = 1$. So $b = (a'a)b = a'(ab) = 0$ which is a contradiction. To show the 2^{nd} part of claim

Lecture 16: Integral domains and fields

Wednesday, December 5, 2018 8:49 AM

we first notice that, since F is a field, it is a non-trivial ring. Then we observe that $D(F) \subseteq F \setminus (F^\times \cup \{0\})$ as $D(F) \cap F^\times = \emptyset$ and $0 \notin D(F)$, which implies $D(F) = \emptyset$. ■

We notice that $\mathbb{Z}$ is an integral domain, but it is not a field. So an integral domain is not necessarily a field.

Nevertheless under additional conditions we might get such an implication:

<u>Proposition</u>. A finite integral domain is a field.

<u>Pf</u>. $\forall a \in D \setminus \{0\}$, let $l_a : D \to D$, $l_a(b) = ab$.

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

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

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

Since D is finite and l_a is 1-1, l_a is onto. So $\exists b \in D$ s.t. $l_a(b) = 1$; hence $\exists\, b \in D$, $ab = 1$, which means $a \in D^\times$.

We also mention that D is non-trivial as it is an int. domain. ■

Lecture 16: Polynomial rings

Wednesday, December 5, 2018 9:06 AM

<u>Remark</u>. When D is a finite dimensional k-vector space for some field k and multiplication in D is k-linear (we call such a ring a k-algebra), the above argument still works:

$$\left.\begin{array}{l} D: \text{integral domain} \\ D: \text{finite dimensional} \\ \quad k\text{-algebra} \end{array}\right\} \Rightarrow D \text{ is a field.}$$

<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 $-\infty + n = -\infty$ for any $n \in \mathbb{Z}$ and $(-\infty)+(-\infty) = -\infty$.)

<u>Pf.</u> If either $f=0$ or $g=0$, then $fg=0$; and so $\text{LHS} = -\infty$ and $\text{RHS} = -\infty$.

- Suppose $f \neq 0$ and $g \neq 0$. 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 <u>leading coefficient</u> of f). Then

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

Lecture 16: Deg function; zero-divisors and units

Wednesday, December 5, 2018 9:17 AM

$$\left.\begin{array}{l} a_n \neq 0,\ b_m \neq 0 \\ \text{no zero-divisor} \end{array}\right\} \Rightarrow a_n b_m \neq 0. \text{ And so } \deg fg = n+m$$
$$= \deg f + \deg g.$$
$\blacksquare$

<u>Cor.</u> If D is an integral domain, then $D[x]$ is an integral domain.

<u>Pf.</u> $f.g = 0 \Rightarrow \deg fg = -\infty \Rightarrow \deg f + \deg g = -\infty$

$$\Rightarrow \deg f = -\infty \text{ or } \deg g = -\infty$$

$$\Rightarrow f = 0 \text{ or } g = 0. \quad \blacksquare$$

<u>Cor.</u> If D is an integral domain, then $D[x]^\times = D^\times$.

<u>Pf.</u> $f.g = 1 \Rightarrow \deg fg = 0 \Rightarrow \deg f + \deg g = 0$

$$\Rightarrow \left\{\begin{array}{l} \deg f, \deg g \in \mathbb{Z}^{\geq 0} \\ \deg f + \deg g = 0 \end{array}\right\} \Rightarrow \deg f = \deg g = 0$$

$$\Rightarrow \left.\begin{array}{l} f, g \in D \\ f.g = 1 \end{array}\right\} \Rightarrow f \in D^\times. \quad \blacksquare$$

As it was pointed out earlier, parts of algebra has been developed to solve Fermat's last conjecture. Roughly idea was; write

$$z^p = x^p - y^p = (x-y)(x-\zeta y)\cdots(x-\zeta^{p-1}y) \text{ where } \zeta = e^{\frac{2\pi i}{p}},$$

Lecture 16: Prime and maximal ideals

Wednesday, December 5, 2018 3:27 PM

if in $\mathbb{Z}[\zeta]$ we had prime elements and could write any element as a prod. of primes and made sure that $x-\zeta^i y$ to be relatively prime, then $x-y=z_0^p$, $x-\zeta y=z_1^p$, $\ldots$, $x-\zeta^{p-1}y=z_{p-1}^p$ for some $z_i\in\mathbb{Z}[\zeta]$. And we had a chance of getting a contradiction. This is what Kummer did. He further realized that, though in general we do not get the desired unique factor., if we change to ideals we do get such a result; that is why he called ideals, ideal numbers. Later they were studied extensively for other rings, and the word "number" got dropped.

Def. Suppose A is a unital commutative.

(1) $\mathfrak{p}\trianglelefteq A$ is called a prime ideal if

- $\mathfrak{p}$ is proper and $ab\in\mathfrak{p}\Rightarrow a\in\mathfrak{p}$ or $b\in\mathfrak{p}$.

The set of all prime ideals of A is denoted by $\mathrm{Spec}(A)$.

(2) $\mathfrak{m}\trianglelefteq A$ is called a maximal ideal if

- $\mathfrak{m}$ is proper and ($\mathfrak{m}\subsetneq J\subseteq A$, $J\trianglelefteq A\Rightarrow J=A$)

The set of all maximal ideals of A is denoted by $\mathrm{Max}(A)$.