Lecture 08: Ideals

Wednesday, April 18, 2018 8:36 AM

In order to solve Fermat's last conjecture Kummer worked with the ring $\mathbb{Z}[\zeta_n] = \{a_0 + \zeta_n a_1 + \cdots + \zeta_n^{n-1} a_{n-1} \mid a_i \in \mathbb{Z}\}$ where $\zeta_n = e^{\frac{2\pi i}{n}}$. He realized that in this ring, numbers might be written as products of prime in different ways. But when he worked with "ideal numbers", he could write them as product of "prime ideal number" in a unique way. Later Dedekind and Noether extended these concepts to all rings; and now we talk about ideals and prime ideals.

Def. Suppose R is a ring. We say $I \subseteq R$ is an ideal if

(1) I is a subring, (2) $\forall r \in R$, $\forall a \in I$, $ra \in I$ and $ar \in I$.

We write $I \lhd R$.

Lemma. Suppose R is a ring and $\emptyset \neq I \subseteq R$. Then $I \lhd R$ if and only if (1) $\forall a, b \in I$, $a - b \in I$ (2) $\forall a \in I$, $r \in R$, $ra, ar \in I$.

Pf. ($\Rightarrow$) Since I is a subring, (1) holds; since $I \lhd R$, (2) holds.

($\Leftarrow$) We only need to say why I is a subring. By the subring

criterion it is enough to show $\forall a,b \in I$, $a-b \in I$ and $a \cdot b \in I$;

And both are direct consequeces of our assumptions. ∎

Ex. $I \lhd \mathbb{Z} \iff I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Pf. ($\Leftarrow$). $a, b \in n\mathbb{Z} \Rightarrow n|a,\ n|b \Rightarrow n|a-b \Rightarrow a-b \in n\mathbb{Z}$.

- $\left.\begin{matrix} a \in n\mathbb{Z} \\ r \in \mathbb{Z} \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} n|a \\ r \in \mathbb{Z} \end{matrix}\right\} \Rightarrow n|ar$ and $n|ra \Rightarrow \left\{\begin{matrix} ar \in n\mathbb{Z}. \\ ra \in n\mathbb{Z}. \end{matrix}\right.$

($\Rightarrow$). If $I = 0$, we are done.

. If $I \neq 0$, let $n \in I \setminus \{0\}$. Then $\pm n \in I$. And so I has a positive integer. Let $n_0 = \min I \cap \mathbb{Z}^+$. Then $n_0\mathbb{Z} \subseteq I$.

Claim. $n_0\mathbb{Z} = I$.

Pf of claim. For $m \in I$, by the division algorithm,

$\exists q, r \in \mathbb{Z}$ s.t. $m = n_0 q + r$, $0 \leq r < n_0$.

And so $r = m - n_0 q \in I \cap [0, n_0 - 1)$ · (*)

Since $n_0 = \min I \cap \mathbb{Z}^+$, by (*) $r = 0$. And so

$m = n_0 q \in n_0\mathbb{Z}$. ∎

Lecture 08: Finitely generated Ideals

Wednesday, April 18, 2018 10:49 AM

Ex. Ideals generated by $a_1, \dots, a_n \in R$ in a unital commutative ring:

We say I is the ideal generated by $a_1, \dots, a_n$ if I is the smallest ideal of R that contains $a_1, \dots, a_n$. We denote it by $\langle a_1, \dots, a_n \rangle$.

Claim. $\langle a_1, \dots, a_n \rangle = \{ r_1 a_1 + \dots + r_n a_n \mid r_i \in R \}$.

Pf. Let's call the right hand side by J.

Step 1. If $I \lhd R$ and $a_1, \dots, a_n \in I$, then $J \subseteq I$.

Pf. $a_i \in I \Rightarrow \forall r_i \in R,\ r_i a_i \in I$

$\Rightarrow r_1 a_1 + \dots + r_n a_n \in I$. And so $J \subseteq I$.

Step 2. $J \lhd R$.

Pf. $\left(\sum_{i=1}^n r_i a_i\right) - \left(\sum_{i=1}^n r_i' a_i\right) = \sum_{i=1}^n \underbrace{(r_i - r_i')}_{\text{in } R} a_i \in J$.

$\forall r \in R,\ r\left(\sum_{i=1}^n r_i a_i\right) = \sum_{i=1}^n (r r_i) a_i \in J$.

Since R is commutative,

$$\left(\sum_{i=1}^n r_i a_i\right) r = r \left(\sum_{i=1}^n r_i a_i\right) \in J.$$

Step 3. $a_1, \dots, a_n \in J$.

Pf. Since R is unital, $1 \cdot a_i = a_i \in J$. ∎

Lecture 08: Kernels are ideals

Wednesday, April 18, 2018 10:58 AM

Def. • An ideal is called principal if it is generated by 1 element.

• An integral domain is called a Principal Ideal Domain (PID) if any ideal is principal.

Ex. $\mathbb{Z}$ is a PID.

Lemma. Suppose $f: R_1 \to R_2$ is a ring homomorphism. Kernel of f is $\ker f = \{ r_1 \in R_1 \mid f(r_1) = 0 \}$. Then $\ker f \lhd R_1$.

Pf. • $a, b \in \ker f \Rightarrow f(a) = 0 \,,\ f(b) = 0$

$$\Rightarrow f(a-b) = f(a) - f(b) = 0$$

$$\Rightarrow a - b \in \ker f.$$

• $a \in \ker f \,,\ r \in R \Rightarrow f(ar) = f(a) f(r) = 0 \cdot f(r) = 0$

$$\Rightarrow ar \in \ker f.$$

Similarly $f(ra) = f(r) f(a) = f(r) \cdot 0 = 0 \Rightarrow ra \in \ker f.$

And so $\ker f \lhd R_1$. ■

Using an ideal we can construct a new ring; that is called the factor ring of R by I and it is denoted by R/I.

Lecture 08: Factor rings

Wednesday, April 18, 2018 11:08 AM

Proposition. Suppose $I \lhd R$. Let $R/_I := \{r+I \mid r \in R\}$ be the set of all the (additive) cosets of I in R. Then $(R/_I, +, \cdot)$ is a ring where

- $(a+I)+(b+I) := (a+b)+I$,
- $(a+I)(b+I) := ab+I$.

(we will continue next time.)