Lecture 01: Recall irreducible and prime elements

Monday, January 8, 2018 10:57 AM

Today we will mainly recall some of the statements that are proved in the ring theory part of math 200a.

<u>Def.</u> Suppose A is a unital commutative ring; $a \in A$ is neither a zero-divisor nor a unit. Then

- a is called <u>prime</u> if $a \mid bc \Rightarrow (a \mid b \text{ or } a \mid c)$.
- a is called <u>irreducible</u> if $a = bc \Rightarrow (b \in A^\times \text{ or } c \in A^\times)$.

Here are some of the facts that we proved in math200a:

- Suppose A is an integral domain.
  - $a \in A$ is prime $\Rightarrow$ a is irreducible
  - $a \in A$ is prime $\Leftrightarrow$ $\langle a \rangle$ is prime
  - $a \in A$ is irreducible $\Leftrightarrow$ $\langle a \rangle$ is maximal among proper principal ideals.

<u>Cor.</u> Suppose D is a PID. Then $\operatorname{Spec}(D) = \operatorname{Max}(D) \cup \{0\}$.

<u>Pf.</u> We have proved that $\mathfrak{m} \in \operatorname{Max}(D) \Leftrightarrow D/\mathfrak{m}$ is a field.

$\Rightarrow D/\mathfrak{m}$ is an integ. domain $\Leftrightarrow \mathfrak{m} \in \operatorname{Spec}(D)$.

$D/\{0\} \simeq D$ is an integ. domain $\Rightarrow \{0\} \in \operatorname{Spec}(D)$.

Lecture 01: Review PID and associates

Monday, January 8, 2018 11:55 AM

So $\mathrm{Max}(D) \cup \{0\} \subseteq \mathrm{Spec}(D)$.

Suppose $\mathfrak{p} \in \mathrm{Spec}(D)$ and $\mathfrak{p} \neq 0$. Since D is a PID, $\mathfrak{p} = \langle p \rangle$. Since $\mathfrak{p}$ is prime, p is prime. Hence p is irreducible. Therefore

(*) $\mathfrak{p} = \langle p \rangle$ is maximal among proper principal ideals. As D is a PID, by (*), we deduce that $\mathfrak{p} \in \mathrm{Max}(D)$. ∎

<u>Lemma</u>. Suppose D is a PID. Then $a \in D$ is prime $\Leftrightarrow$ a is irreducible.

<u>Pf</u>. $(\Rightarrow)$ is true for any integral domain.

$(\Leftarrow)$ a irred. $\Rightarrow$ $\langle a \rangle$ max. among proper principal ideals

D PID

a prime. $\Leftarrow$ $\langle a \rangle \in \mathrm{Spec}(D) \Leftarrow$ $\langle a \rangle \in \mathrm{Max}(D)$

∎

<u>Def</u>. We say $a, b \in A$ are associates and write $a \sim b$ if $\exists\, u \in A^{\times}$ s.t. $a = bu$.

<u>Lemma</u>. Suppose A is an integral domain. Then

$$a \sim b \Leftrightarrow \langle a \rangle = \langle b \rangle .$$

<u>Def</u>. An integral domain D is called a Unique Factorization Domain if

Lecture 01: Review UFD

Monday, January 8, 2018 12:17 PM

any non-zero non-unit element can be written as a product of irreducibles in a unique way.

($p_1 \cdot p_2 \cdots p_m = q_1 \cdots q_n$ and p_i's and q_j's are irredu. imply that $m=n$ and $p_i \sim q_{\sigma_i}$ for some $\sigma \in S_n$; that means $p_i = u_i q_{\sigma_i}$ for some $u_i \in D^\times$.)

(*) Theorem. Suppose A is a Noeth. integral domain. Then any irreducible in A is prime $\Longleftrightarrow$ A is a UFD.

Remark. Notice that, if A is a PID, then it is a Noeth. integ. domain and any irred. is prime. So the above thm implies PID $\Rightarrow$ UFD. This statement we proved in 200a. And the proof of ($\Rightarrow$) is almost identical.

Before we get to the proof of Theorem (*), let's recall what a Noeth. ring is, Zorn's lemma, why Zorn's lemma is useful in ring theory, recall an application of Zorn's lemma.

Lecture 01: Review Zorn's lemma

Monday, January 8, 2018 12:27 PM

<u>Def.</u> Suppose $(\Sigma, \preccurlyeq)$ is a Partially Ordered Set (POSet).

A non-empty subset C of Σ is called a <u>chain</u> if

$\forall c_1, c_2 \in C$, either $c_1 \preccurlyeq c_2$ or $c_2 \preccurlyeq c_1$.

<u>Zorn's lemma</u>. Suppose $(\Sigma, \preccurlyeq)$ is a poset. Suppose any chain of Σ has an upper bound. Then Σ has a maximal element.

Zorn's lemma is useful in ring because of the following lemma:

<u>Lemma</u>. Suppose C is a chain (with respect to $\subseteq$) of ideals of a ring A. Then $\bigcup_{\mathfrak{a} \in C} \mathfrak{a} \trianglelefteq A$.

For instance we used the above lemma to prove the following important Theorem:

A : unital commutative;
$S \subseteq A$: multiplicatively close, i.e. $1 \in S$, $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.
$\mathfrak{a} \trianglelefteq A$ s.t. $\mathfrak{a} \cap S = \varnothing$

Then $\exists \mathfrak{p} \in \operatorname{Spec}(A)$ s.t. $\mathfrak{p} \supseteq \mathfrak{a}$ and $\mathfrak{p} \cap S = \varnothing$.

Lecture 01: Review Noetherian rings

Monday, January 8, 2018 12:39 PM

For ideals, we say $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{b} \subseteq \mathfrak{a}$. So in the previous theorem we are finding a prime divisor of $\mathfrak{a}$ which is still disjoint from S.

<u>Def.</u> A ring A is called Noetherian if any chain of ideals of A has a maximum element.

<u>Lemma</u>. Suppose A is a Noetherian ring, and Σ is a non-empty family (set) of ideals of A. Then Σ with respect to $\subseteq$ has a maximal element.

<u>Pf.</u> By Zorn's lemma, it is enough to show any chain of Σ has an upper bound. We do have this because of the Noetherian condition. ■

• Let $\Sigma := \{ A \subseteq \mathbb{Z} \mid \mathbb{Z} \setminus A \text{ is infinite} \}$. Then $(\Sigma, \subseteq)$ is a poset with no maximal element.

<u>Pf of Theorem ⊛</u> $(\Rightarrow)$ <u>Existence</u>. Let

$$\Sigma := \left\{ \langle a \rangle \;\middle|\; \begin{array}{l} \cdot\ a : \text{non-zero, non-unit} \\ \cdot\ a \text{ cannot be written as a prod. of irred.} \end{array} \right\}.$$

Suppose to the contrary that $\Sigma \neq \emptyset$. Since A is Noeth.,

Lecture 01: UFD criteria

Monday, January 8, 2018 12:59 PM

Σ has a maximal element. Suppose $\langle a_0 \rangle$ is a maximal element of Σ. So in particular a_0 is NOT irreducible. So $\exists\, b, c \in A$ that are not units and $a_0 = bc$. Hence $\langle a_0 \rangle \subsetneq \langle b \rangle$ and $\langle a_0 \rangle \subsetneq \langle c \rangle$. As $\langle a_0 \rangle$ is a maximal element of Σ, we deduce that $\langle b \rangle, \langle c \rangle \underset{(\mathrm{I})}{\notin} \Sigma$. Since $a_0 = bc \neq 0$, $b \neq 0$ and $c \neq 0$. So b, c are non-zero, non-units (II). Therefore $(\mathrm{I}), (\mathrm{II})$ imply that b and c can be written as products of irred. Hence $a_0 = bc$ can be written as a prod. of irred.; which is a contrad.

<u>Uniqueness</u>

$$\left.\begin{array}{l} p_1 \cdots p_m = q_1 \cdots q_n \Rightarrow p_1 \mid q_1 \cdots q_n \\ p_1 : \text{irred} \Rightarrow p_1 : \text{prime} \end{array}\right\} \Rightarrow p_1 \mid q_{\sigma_1}$$

$$\left.\begin{array}{l} \Rightarrow \langle q_{\sigma_1} \rangle \subseteq \langle p_1 \rangle \\ q_{\sigma_1} : \text{irred} \Rightarrow \langle q_{\sigma_1} \rangle \text{ max. among proper princip. ideals} \end{array}\right\} \Rightarrow \langle p_1 \rangle = \langle q_{\sigma_1} \rangle$$

$\Rightarrow p_1 \sim q_{\sigma_1}$.

$\Rightarrow p_1 = u_1 q_{\sigma_1}$ and $u_1 \in A^\times$.

$\Rightarrow p_2 \cdots p_m = u_1 q_1 \cdots \widehat{q_{\sigma_1}} \cdots q_n$.

Continue (formally use induction.)

Lecture 01: UFD criteria

Monday, January 8, 2018 1:16 PM

($\Leftarrow$) Suppose a is irreducible. So a is non-zero, non-unit.

Suppose $a \mid bc$. Hence $\exists\, d \in A$, $ad = bc$. If either $b=0$ or $c=0$, we are done. If either $b \in A^\times$ or $c \in A^\times$, we are done.

So we can and will assume that b and c are non-zero, non-units.

As A is a UFD, there are irreducibles p_i's, q_j's, and r_t's s.t.

$b = p_1 \cdots p_m$, $c = q_1 \cdots q_n$, $d = r_1 \cdots r_k$. So

$a r_1 \cdots r_k = p_1 \cdots p_m q_1 \cdots q_n$. As A is a UFD, either $a \sim p_i$ for some i or $a \sim q_j$ for some j:

$$\left.\begin{array}{l} a \sim p_i \Rightarrow a \mid p_1 \cdots p_m \Rightarrow a \mid b \\ \text{or} \\ a \sim q_j \Rightarrow a \mid q_1 \cdots q_n \Rightarrow a \mid c \end{array}\right\} \Rightarrow a \mid b \text{ or } a \mid c.$$

$\blacksquare$

So to show a ring is not a UFD, we need to find an irred. element which is not prime.