Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on: `https://japorized.github.io/TeX_notes`

26 Lecture 26 Jul 04th 2018

26.1 Commutative Rings (Continued 2)

26.1.1 Prime Ideals and Maximal Ideals

Definition 45 (Prime Ideals)

Let R be a commutative ring. An ideal $P \neq R$ is a prime ideal of R if $r, s \in R$ satisfy: $rs \in R \implies r \in P$ or $s \in P$.

Example 26.1.1

For $n \in \mathbb{N} \setminus \{1\}$, $n\mathbb{Z} = \langle n \rangle$ is a prime ideal if and only if n is prime.

Proposition 77 (Ideal is Prime $\iff$ Quotient of Ring by Ideal is an Integral Domain)

If R is a commutative ring, then an ideal $P \neq R$ of R is a prime ideal if and only if R/P is an integral domain.

Proof

Since R is commutative, so is R/P. Since $P \neq R$, we know that $1 \notin P$ [1]*, i.e. $0 + P = P \neq 1 + P$, and so R/P is a non-trivial ring.*

To prove ($\implies$), let $(r + P)(s + P) = 0 + P = P$. Since P is an ideal[2]*, we have that $rs + P = P$ and so $rs \in P$. WLOG, since P is a prime ideal, if $r \in P$, then $r + P = P$. And so R/P is an integral domain.*

[1] See Proposition 62.

[2] See Proposition 61.

To prove ($\Longleftarrow$), *let* $rs \in P$. *Then since* P *is an ideal,*

$$(r+P)(s+P) = rs + P = P.$$

Since R/P *is an integral domain, either*

$$r + P = P \text{ or } s + P = P$$

so $r \in P$ *or* $s \in P$, *which implies that* P *is a prime ideal.* $\square$

Definition 46 (Maximal Ideals)

Let R *be a (commutative) ring. An ideal* $M \neq R$ *or* R *is a maximal ideal if* $\forall A$ *that is an ideal of* R, *we have that*

$$M \subseteq A \subseteq R \implies A = M \text{ or } A + R.$$

Proposition 78 (Ideal is Maximal $\iff$ Quotient of Ring by Ideal is a Field)

If R *is a commutative ring, then an ideal* $M \neq R$ *is a maximal ideal if and only if* R/M *is a field.*

Proof

Similar to the proof of Proposition 77, R/M *is a nontrivial commutative ring. Let* $r \in R$.

($\implies$) *Suppose* M *is a maximal ideal. Since* R/M *is non-trivial, let* $r + M \neq 0 + M \in R/M$. *Let* $\langle\ r\ \rangle = rR$ *Note that* $r \notin M$ *and* $r \in \langle\ r\ \rangle + M$. *Thus,* $M \subsetneq \langle\ r\ \rangle + M$. *Since* M *is maximal and* M *is a proper subset of* $\langle\ r\ \rangle + M$, *we have that* $\langle\ r\ \rangle + M = R$. *In particular, we have* $1 \in \langle\ r\ \rangle + M$ *and so* $\exists s \in R$ *and* $m \in M$ *such that* $1 = rs + m$. *Thus*

$$1 + M = rs + M = (r+M)(s+M).$$

Therefore $s + M$ *is the multiplicative inverse of* $r + M$, *and so* R/M *is a field.*

($\Longleftarrow$) *Since* R/M *is a non-trivial field, we know* $0 + M \neq 1 + M$.

Therefore $M \neq R$. Suppose A is an ideal such that $M \subsetneq A \subseteq R$. Choose $r \in A \setminus M$. Since $r \notin M$ and so $r + M \neq 0 + M$ and R/M is a field, we have that $\exists s + M \in R/M$ such that $(r+M)(s+M) = 1 + M$. Since M is an ideal, we have

$$rs + M = 1 + M \implies \exists m \in M \quad 1 = rs + m.$$

Since $r, m \in A$ and A is an ideal, we have that $1 \in A$ and so $A = R$, implying that M is maximal. □

Combining Proposition 74, Proposition 77, and Proposition 78, we get the following corollary.

Corollary 79 (Maximal Ideals of a Commutative Rings are Prime)

Every maximal ideal of a commutative ring is a prime ideal.

Note

The converse of Corollary 79 is not true.

Example 26.1.2

In $\mathbb{Z}$, $\{0\}$ is a prime ideal, but is clearly not maximal.

26.1.2 Fields of Fractions

Recall that every subring of a field is an integral domain. The converse is actually true[3], i.e. every integral domain R is isomorphic to a subring of a field F.

[3] This is in comparison with Proposition 74.

Let R be an integral domain and $D = R \setminus \{0\}$. Consider

$$X = R \times D = \{(r, s) : r \in R, s \in D\}$$

We say that

$$(r, s) \equiv (r_1, s_1) \in X \iff rs_1 = r_1 s \tag{26.1}$$

Example 26.1.3

Show that Equation (26.1) *is an equivalence relation.*

1. $(r, s) \equiv (r, s)$
2. $(r, s) \equiv (r_1, s_1) \iff (r_1, s_1) \equiv (r, s)$
3. $(r, s) \equiv (r_1, s_1) \wedge (r_1, s_1) \equiv (r_2, s_2) \implies (r, s) = (r_2, s_2)$

Note that using the above idea, we can construct the smallest field that contains $\mathbb{Z}$, and that field is $\mathbb{Q}$. Motivated by this idea, we make the following definition.

Definition 47 (Fraction)

*Let R be an integral domain, $D = R \setminus \{0\}$, and $X = R \times D$. The **fraction**, $\frac{r}{s}$ to be the equivalent class $[(r, s)]$ of the pair $(r, s) \in X$.*

Let F denote the set of all these fractions, i.e.

$$F = \{[(r, s)] : r \in R, s \in D\} = \{\frac{r}{s} : r \in R, s \in R \setminus \{0\}\}.$$

The addition and multiplication of F are defined by

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + sr_1}{ss_1}$$
$$\frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

where we note that $ss_1 \neq 0$ since $s, s_1 \in R \setminus \{0\}$ and R is an integral domain.

It can be shown that F is a field[4]. Also, we have $R \cong R' = \frac{r}{1} : r \in R\} \subseteq F$.

[4] Prove this as an easy exercise to ease yourself with the concept.

Exercise 26.1.1
Prove that F is a field.

Theorem 80 (Field of Fractions)

*Let R be an integral domain. Then there is a field F containing fractions $\frac{r}{s}$ with $r, s \in R$ and $s \neq 0$. By identifying that $r = \frac{r}{1}$, for any $r \in R$, we have that R is a subring of F. The field F is called the **field of fractions** of R.*

Note

We can generalize $D = R \setminus \{0\}$ to any subset $D \subseteq R$ satisfying

1. $1 \in D$
2. $0 \notin D$
3. $a, b \in D \implies ab \in D$