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`

25 Lecture 25 Jun 29th 2018

25.1 Commutative Rings (Continued)

25.1.1 Integral Domain and Fields (Continued)

Recall the definition of a **zero divisor**.

Definition (Zero Divisor)

*Let R be a non-trivial ring. If $0 \neq a \in R$, then a is called a **zero divisor** if $\exists 0 \neq b \in R$ such that $ab = 0$.*

Example 25.1.1

$[2], [3], [6]$ in $\mathbb{Z}_6$ are all zero divisors since

$$[0] = [2][3] = [4][3] = [6][2].$$

Example 25.1.2

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor in $M_n(\mathbb{R})$ since

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Proposition 73 (Ring Cancellations and Zeros)

Let R be a ring. TFAE:

1. $\forall ab = 0 \in R \quad a = 0 \vee b = 0$;

2. $\forall ab = ac \in R \wedge a \neq 0 \implies b = c$;
3. $\forall ba = ca \in R \wedge a \neq 0 \implies b = c$.

Proof

It suffices to prove $(1) \iff (2)$, *since* $(1) \iff (3)$ *would have a similar argument.*

$(1) \implies (2)$: *Let* $ab = ac$ *with* $a \neq 0$. *Then* $a(b-c) = 0$. *Then by* (1), *since* $a \neq 0$, $(b-c) = 0 \iff b = c$.

$(2) \implies (1)$: *Let* $ab = 0 \in R$. *We now have 2 cases:*

Case 1 *If* $a = 0$, *we are done.*

Case 2 *If* $a \neq 0$, *then* $ab = 0 = a \cdot 0$, *and so by* (2), $b = 0$.

□

With that, we can make the following definition.

Definition 44 (Integral Domain)

A commutative ring $R \neq \{0\}$ *(i.e. non-trivial ring) is called an* ***integral domain*** *if it has* ***no zero divisor***, *i.e. if* $ab = 0 \in R$ *then* $a = 0$ *or* $b = 0$.

Example 25.1.3

$\mathbb{Z}$ *is an integral domain since* $ab = 0 \implies a = 0$ *or* $b = 0$.

Example 25.1.4

Note that if p *is prime, then* $p \mid ab \implies p \mid a \vee p \mid b$, *i.e.* $[a][b] = [0]$ *in* $\mathbb{Z}_p \implies [a] = 0$ *or* $[b] = 0$. *So* $\mathbb{Z}_p$ *is an integral domain.*

However, for n *not prime, with* $n = ab$, *if we have* $n = ab$ *such that* $1 < a, b < n$, *then*

$$[a][b] = [0] \text{ in } \mathbb{Z}_n$$

but neither $[a]$ *nor* $[b]$ *is* $[0]$.

With that, we have that $\mathbb{Z}_n$ *is an integral domain if and onoly if* n *is prime.*

Proposition 74 (Fields are Integral Domains)

Every field is an integral domain.

Proof

$\forall a, b \in R$, *where* R *is a field, such that* $ab = 0$, *we want to show that* $a = 0$ *or* $b = 0$. *We have 2 cases:*

Case 1: $a = 0$. *There is nothing to do since the proof is complete.*

Case 2: $a \neq 0$. *Since* $a \neq 0 \in R$, *we know that* $\exists a^{-1} \in R$ *since* R *is a field. And so*

$$b = a^{-1}ab = a^{-1} \cdot 1 = 0$$

Therefore, by definition, the field R *is an integral domain.* □

Note

Using the proof from above, we can show that every subring of a field is an integral domain[1].

[1] This will become useful in PMATH348

Note

The converse of Proposition 74 is not true. As shown in Example 25.1.3, $\mathbb{Z}$ *is an integral domain but not a field.*

However, we have the following partial converse:

Proposition 75 (Finite Integral Domains are Fields)

Every ***finite*** *integral domain is a field.*

Proof

Let R be a finite integral domain, say $|R| = n \in \mathbb{N}$. Let

$$R = \{r_1, r_2, ..., r_n\}.$$

Then for some $a \in R$ such that $a \neq 0$, by Proposition 73, the set

$$\{ar_1, ar_2, ..., ar_n\}$$

have distinct elements. Since R is finite and so $|aR| = n$, and $aR \subseteq R$, we have that $aR = R$. In particular, $\exists 1 \in aR$ such that $1 = ab$ for some $b \in R$ [2]. It follows that $ab = 1 = ba$ since R is commutative, which then implies that a is a unit. Therefore, R is a field. □

[2] We can prove for a more general case by not assuming that R is a commutative ring: We can find $c \in R$ such that $1 = ca$. Then

$$b = (ca)b = c(ab) = c.$$

Recall that the characteristic of a ring R, denoted by $\text{ch}(R)$, is the order of the unity, 1_R, in $(R, +)$, and write

$$\text{ch}(R) = \begin{cases} 0 & o(1_R) = \infty \\ n & o(1_R) = n \in \mathbb{N} \end{cases}$$

Proposition 76 (Integral Domains have Zero or Prime Characteristics)

The characteristic of any integral domain is 0 or a prime p.

Proof

Let R be an integral domain. We have 2 cases:

Case 1: $\text{ch}(R) = 0$. *Our job is done.*

Case 2: $\text{ch}(R) = n \in \mathbb{N}$. *Suppose $n \neq p$ a prime, and say $n = ab$ for some $a, b \in R$ such that $1 < a, b < n$. If 1 is the unity of R, then by Proposition 58, we have*

$$ab = (a \cdot 1)(b \cdot 1) = (ab)(1) = n(1) = 0.$$

Since R is an integral domain, we have that either

$$a \cdot 1 = 0 \text{ or } b \cdot 1 = 0.$$

This contradicts that fact that n is the characteristic. Therefore, n must be prime. □

Note

Let R be an integral domain with $\mathrm{ch}(R) = p$ a prime. For $a, b \in R$, by the ***Binomial Theorem****, we have*

$$(a+b)^p = \sum_{i=1}^{p} \binom{p}{i} a^{p-i} b^i.$$

Since p is prime, we have $p \mid \binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$ for $1 \leq i \leq p-1$. Therefore, since $\mathrm{ch}(R) = p$, we have that

$$(a+b)^p = a^p + b^p$$

This is known as the Freshman's Dream.