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`

23 Lecture 23 Jun 25th 2018

23.1 Ring (Continued 3)

23.1.1 Ideals (Continued)

Proposition 64 (Ideals of $\mathbb{Z}$ are Principal Ideals)

All ideals of $\mathbb{Z}$ are of the form $\langle\, n \,\rangle$ for some $n \in \mathbb{Z}$.

Proof

Let A be an ideal of $\mathbb{Z}$. If $A = \{0\}$, then $A = \langle\, 0 \,\rangle$. Otherwise, let $a \in A$ with $a \neq 0$, and $|a|$ be the minimum. Clearly, $\langle\, a \,\rangle = a\mathbb{Z} \subseteq A$. To prove the other inclusion, let $b \in A$. By the **Division Algorithm**, *$\exists q, t \in \mathbb{Z}$ with $0 \leq r < |a|$ such that $b = qa + r$. Because A is an ideal, we have $r = b - qa \in A$. Since $|r| < |a|$ which is the minimal case, it must be that $r = 0$. Therefore $b = qa \in \langle\, a \,\rangle$ and so $A \subseteq \langle\, a \,\rangle$.* □

23.1.2 Isomorphism Theorems for Rings

Definition 38 (Ring Homomorphism)

Let R and S be rings. A mapping

$$\Theta : R \to S$$

is a ring **homomorphism** *if $\forall a, b \in R$, we have*

1. $\Theta(a+b) = \Theta(a) + \Theta(b)$
2. $\Theta(ab) = \Theta(a)\Theta(b)$
3. $\Theta(1_R) = 1_S$

Note (Remark)

$(2) \not\Longrightarrow (3)$ *because* $\Theta(1_R) \in S$ *does not necessarily have a multiplicative inverse, since* S *is a ring.*

Example 23.1.1

The mapping $k \mapsto [k]$ *from* $\mathbb{Z} \to \mathbb{Z}_n$ *is a surjective ring homomorphism.*

Example 23.1.2 (Direct Product of Rings)

If R_1, R_2 *are rings, the projection*

$$\pi_1 : R_1 \times R_2 \to R_1 \text{ defined by } \pi_1(r_1, r_2) = r_1$$

is a surjective ring homomorphism, since

1. $\pi_1(r_1 + r_2, q_1 + q_2) = r_1 + r_2 = \pi_1(r_1, q_1) + \pi_1(r_2, q_2)$;
2. $\pi_1(r_1 r_2, q_1 q_2) = r_1 r_2 = \pi_1(r_1, q_1)\pi_1(r_2, q_2)$; *and*
3. $\pi(1, 1) = 1$.

We can a similar $\pi_2 : R_1 \times R_2 \to R_2$ *such that* $(r_1, r_2) \mapsto r_2$*, and we will get that* π_2 *is also a surjective ring homomorphism.*

Proposition 65 (Properties of Ring Homomorphisms)

Let $\Theta : R \to S$ *be a ring homomorphism and let* $r \in R$*. Then*

1. $\Theta(0_R) = 0_S$
2. $\Theta(-r) = -\Theta(r)$
3. $\Theta(kr) = k\Theta(r)$
4. $\forall n \in \mathbb{N} \cup \{0\} \quad \Theta(r^n) = \Theta(r)^n$
5. $u \in R^* \implies \forall k \in \mathbb{Z} \quad \Theta(u^k) = \Theta(u)^k$

Proof

1. *Note that*
$$\Theta(r) = \Theta(0_R + r) = \Theta(0_R) + \Theta(r).$$
Therefore,
$$\Theta(0_R) = 0_S$$
as required.

2. *Note that*
$$0_S = \Theta(0_R) = \Theta(r - r) = \Theta(r) + \Theta(-r),$$
so
$$\Theta(-r) = -\Theta(r).$$

3. *Observe that*
$$\Theta(kr) = \Theta(\underbrace{r + r + \ldots + r}_{k \text{ times}}) = \underbrace{\Theta(r) + \Theta(r) + \ldots + \Theta(r)}_{k \text{ times}} = k\Theta(r)$$

Item 4 follows by induction on the definition of a ring homomorphism, and Item 5 follows as a result from Item 4 because if $u \in R^*$, then $u^{-1} \in R^*$ such that $uu^{-1} = 1_R$. □

Definition 39 (Ring Isomorphism)

*A mapping of rings $\Theta : R \to S$ is a ring **isomorphism** if Θ is a bijective ring homomorphism. In this case, we say that R and S are **isomorphic** and denote that by $R \cong S$.*

Definition 40 (Kernel and Image)

*Let $\Theta : R \to S$ be a ring homomorphism. The **kernel** of Θ is defined by*
$$\ker \Theta = \{r \in R : \Theta(r) = 0_S\}$$
*and the **image** of Θ is defined by*
$$\operatorname{im} \Theta := \Theta(R) = \{\Theta(r) : r \in R\}.$$

Proposition 66

Let $\Theta : R \to S$ be a ring homomorphism. Then

1. $\operatorname{im}\Theta \leq_r S$
2. $\ker\Theta$ *is an ideal of* R

Proof

1. $\Theta(1_R) = 1_S$ *by definition of a homomorphism so* $\Theta(1_R) \in \operatorname{im}\Theta$. *Suppose* $s_1 = \Theta(r_1)$ *and* $s_2 = \Theta(r_2)$, *then*

$$\begin{aligned} s_1 - s_2 &= \Theta(r_1) - \Theta(r_2) = \Theta(r_1 - r_2) \\ s_1 s_2 &= \Theta(r_1)\Theta(r_2) = \Theta(r_1 r_2) \end{aligned}$$

are both in $\operatorname{im}\Theta$. *By the Subring Test,* $\operatorname{im}\Theta \leq_r S$.

2. *Since* $\ker\Theta$ *is an additive subgroup of* R, *it suffices to show that* $ra, ar \in \ker\Theta$ *for all* $r \in R$ *and* $a \in \ker\Theta$. *Let* $r \in R$ *and* $a \in \ker\Theta$. *Then*

$$\Theta(ra) = \Theta(r)\Theta(a) = \Theta(r) \cdot 0 = 0$$

So $ra \in \ker\Theta$. *Similarly so,*

$$\Theta(ar) = \Theta(a)\Theta(r) = 0 \cdot \Theta(r) = 0$$

and so $ar \in \ker\Theta$. *Therefore,* $\ker\Theta$ *is an ideal of* R.

$\square$

Theorem 67 (First Isomorphism Theorem for Rings)

Let $\Theta : R \to S$ be a ring homomorphism. Then

$$R/\ker\Theta \cong \operatorname{im}\Theta.$$

Proof

Let $A = \ker\Theta$. *Since* A *is an ideal of* R, *we have that* R/A *is a ring.*

Define

$$\overline{\Theta} : R/A \to \operatorname{im} \Theta \text{ by } (r + A) \mapsto \theta(a).$$

Note that

$$r + A = s + A \iff (r - s) \in A \iff \Theta(r - s) = 0 \iff \Theta(r) = \Theta(s).$$

Therefore $\overline{\Theta}$ is well-defined and injective. Also, it is clear that $\overline{\Theta}$ is surjective. To show that $\overline{\Theta}$ is a homomorphism, note that $\forall r, s \in R$, we have

$$\begin{aligned} \overline{\Theta}(r + A + s + A) &= \overline{\Theta}(r + s + A) = \Theta(r + s) \\ &= \Theta(r) + \Theta(s) = \overline{\Theta}(r + A) + \overline{\Theta}(s + A). \end{aligned}$$

It follows that $\overline{\Theta}$ is a ring isomorphism and so

$$R/\ker \Theta \cong \operatorname{im} \Theta$$

as required. □

Exercise 23.1.1

Let $A, B \leq_r R$, where R is a ring. Prove that

1. *$A \cap B$ is the largest subring of R contained in both A and B.*
2. *If either A or B is an ideal of R, the sum*

$$A + B = \{a + b : a \in A,\, b \in B\}$$

is a subring of R, and is the smallest subring of R that contains both A and B.

Theorem 68 (Second Isomorphism Theorem for Rings)

Let A be a subring and B an ideal of a ring R. Then

1. *$A + B \leq_r R$;*
2. *B is an ideal of $A + B$;*
3. *$A \cap B$ is an ideal of A; and*
4. $$(A + B)/B \cong A/(A \cap B)$$

Theorem 69 (Third Isomorphism Theorem for Rings)

Let A and B be ideals of R with $A \subseteq B$, then ${}^{B}\!/\!{}_{A}$ is an ideal of ${}^{R}\!/\!{}_{A}$ and

$$\left({}^{R}\!/\!{}_{A} \right) \Big/ \left({}^{B}\!/\!{}_{A} \right) \cong {}^{R}\!/\!{}_{B}.$$