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`

24 Lecture 24 Jun 27th 2018

24.1 Rings (Continued 4)

24.1.1 Isomorphism Theorems for Rings (Continued)

Theorem 70 (Chinese Remainder Theorem)

Let A and B be ideals of R.

1. $A + B = R \implies {}^{R}\!/_{(A \cap B)} \cong {}^{R}\!/_{A} \times {}^{R}\!/_{B}$
2. $A + B = R \wedge A \cap B = \{0\} \implies R \cong {}^{R}\!/_{A} \times {}^{R}\!/_{B}$

Proof

It suffices to prove (1) *since if* (1) *is true and* $A \cap B = \{0\}$, *then* (2) *immediately follows.*

Define

$$\Theta : R \to {}^{R}\!/_{A} \times {}^{R}\!/_{B} \qquad r \mapsto (r + A, r + B)$$

Then Θ is a ring homomorphism [1].

[1]

Exercise 24.1.1
Prove that Θ is a ring homomorphism.

Proof (Θ is a ring homomorphism)

$\forall r, s \in R$, *we have*

$$\begin{aligned}\Theta(rs) &= (rs + A, rs + B) \\ &\overset{(*)}{=} (r + A, r + B)(s + A, s + B) \\ &= \Theta(r)\Theta(s)\end{aligned}$$

where $(*)$ *is by Proposition 63. Also by the same proposition, we have*

$$\Theta(1) = (1 + A, 1 + B).$$

Then,

$$\begin{aligned}\Theta(r+s) &= (r+s+A, r+s+B) \\ &\overset{(\dagger)}{=} (r+A, r+B) + (s+A, s+B) \\ &= \Theta(r) + \Theta(s)\end{aligned}$$

where $(\dagger)$ *is by Proposition 60.*

Note that $\ker\Theta = A \cap B$*, since*

$$\ker\Theta = \{r \in R : \Theta(r) = (A, B)\} = \{r \in A \wedge r \in B\} = A \cap B.$$

To show that Θ *is surjective, let* $(s + A, t + B) \in {}^{R}\!/_{A} \times {}^{R}\!/_{B}$ *with* $s, t \in R$*. Since* $A + B = R$*,* $\exists a \in A$*,* $\exists b \in B$ *such that* $a + b = 1$*. Let* $r = sb + ta$*. Then*

$$\begin{aligned}s - r &= s - sb - ta = s(1-b) - ta = sa - ta = (s-t)a \in A \\ t - r &= t - sb - ta = t(1-a) - sb = tb - sb = (t-s)b \in B\end{aligned}$$

and so by Proposition 60,

$$s + A = r + A \text{ and } t + B = r + B.$$

Therefore

$$\Theta(r) = (r + A, r + B) = (s + A, t + B),$$

and so Θ *is surjecive. Then by the Theorem 67,*

$${}^{R}\!/_{(A \cap B)} \cong {}^{R}\!/_{A} \times {}^{R}\!/_{B}.$$

□

Why is Theorem 70 called the Chinese Remainder Theorem?

Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Then we know that

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}.$$

Also, $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ since $1 = ma + nb$ for some $a, b \in \mathbb{Z}$ by **Bezout's Lemma**. And so:

Corollary 71

1. *If $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then*

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

i.e.

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

2. *If $m, n \in \mathbb{N}$ with $m, n \geq 2$ and $\gcd(m, n) = 1$, then*

$$\phi(mn) = \phi(m)\phi(n)$$

*where $\phi(m) = |\mathbb{Z}_m^*|$ is **Euler's ϕ-function**.*

Let p be a prime. Recall that one consequence of Lagrange's Theorem is that every group G of order p is cyclic, i.e. $G \cong C_p$.

An analogous notion in rings is the following:

Proposition 72 (Ring With Prime Order Is Isomorphic to Integer Modulo Prime)

If R is a non-trivial ring with $|R| = p$ where p is prime, then $R \cong \mathbb{Z}_p$.

Proof

Define

$$\Theta : \mathbb{Z}_p \to R \qquad [k] \mapsto k \cdot 1_R.$$

Note that since R is an additive group with $|R| = p$, by Lagrange's Theorem, $o(1_R) = 1$ or p. Since R is non-trivial, we have that $1_R \neq 0$ by the remark on the definition of a trivial ring, and so $o(1_R) \neq 1$. Thus $o(1_R) = p$. Then, by Proposition 59, we have

$$[k] = [m] \iff p \mid (k - m) \iff (k - m)1_R = 0 \iff k \cdot 1_R = m \cdot 1_R$$

in R. Thus, Θ is well-defined and injective. Θ is also a ring homomorphism [2].

[2]

Exercise 24.1.2
Prove that Θ is a ring homomorphism.

Proof (Θ is a ring homomorphism)
$\forall [a], [b] \in \mathbb{Z}$, *we have*

$$\begin{aligned}\Theta([a][b]) = \Theta([ab]) &= ab \cdot 1_R \\ &= (a \cdot 1_R)(b \cdot 1_R) = \Theta([a])\Theta([b]).\end{aligned}$$

$$\Theta([1]) = 1 \cdot 1_R = 1_R$$

and

$$\begin{aligned}\Theta([a] + [b]) = \Theta([a + b]) &= (a + b) \cdot 1_R \\ &= a \cdot 1_R + b \cdot 1_R = \Theta([a]) + \Theta([b]).\end{aligned}$$

So Θ is a ring homomorphism.

Now because $|\mathbb{Z}_p| = p = |R|$ *and Θ is injective, Θ must be surjective. Therefore Θ is a ring isomorphism and hence* $R \cong \mathbb{Z}_p$ *as required.* □

24.2 Commutative Rings

24.2.1 Integral Domain and Fields

Definition 41 (Units)

Let R be a ring. We say that $u \in R$ *is a* ***unit*** *if u has a multiplicative inverse in R, and denote it by* u^{-1}. *We have*

$$uu^{-1} = 1 = u^{-1}u$$

Note

If u is a unit in R, and $r, s \in R$, we have

$$ur = us \implies r = s \quad \textit{(Right Cancellation)}$$
$$ru = su \implies r = s \quad \textit{(Left Cancellation)}$$

*Let R^* denote the set of all units in R. We know that the definition of a ring is that R is "almost" a group under multiplication except that its elements do not necessarily have multiplicative inverses. Since R^*R is the set that contains all units, i.e. all elements with multiplicative inverses in R, we have that $(R^*, \cdot)$ is a group. This is called the **Group of Units** of R.*

Example 24.2.1

Note that 2 is a unit in $\mathbb{Q}$, but it is not a unit in $\mathbb{Z}$. We have that

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \text{ and } \mathbb{Z}^* = \{\pm 1\}$$

Example 24.2.2

*Consider the ring of **Gaussian Integers**,*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\} \subseteq \mathbb{C}.$$

Then[3]

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}.$$

[3] Proof to be added once A4 is over.

Definition 42 (Division Ring and Field)

*A non-trivial ring R is a **division ring** if*

$$R^* = R \setminus \{0\}.$$

*A commutative division ring is a **field**.*

Example 24.2.3

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields but $\mathbb{Z}$ is not.

Example 24.2.4

$\mathbb{Z}_n$ is a field $\iff$ n is prime.

Remark

If R is a division ring or a field, then its only ideals are $\{0\}$ or R, since if $A \neq \{0\}$ is an ideal of R, then $\exists a \in A$, $a \neq 0$, such that $1 = aa^{-1} \in A$, which implies that $A = R$ by Proposition 62.

This remark is not as useful or spectacular within this course, but it will be once we go into PMATH348 contents.

Remark

It can be shown that every finite division ring is a field, and this is known as Wedderburn's Theorem.

NOTE THAT if $n = ab$ for some integer n with $0 < a, b < n$, then in $\mathbb{Z}$ we have

$$[a][b] = [n] = [0]$$

but $[a] \neq [0] \neq [b]$ by our definition of a, b.

Definition 43 (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 $ab = 0$.*