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`

22 Lecture 22 Jun 22 2018

22.1 Ring (Continued 2)

22.1.1 Ideals

Let R be a ring and A an additive subgroup of R. Since $(R, +)$ is abelian, we have that $A \triangleleft R$. Thus, we can talk about the additive quotient group

$$\begin{aligned} R/A &= \{r + a : r \in \mathbb{R}\} \text{ with} \\ r + A &= \{r + a : a \in A\} \end{aligned}$$

Using the properties that we know about cosets and quotient groups, we have the following proposition.

Proposition 60 (Properties of the Additive Quotient Group)

Let R be a ring and A an additive subgroup of R. For $r, s \in R$, we have

1. $r + A = s + A \iff (r - s) \in A$
2. $(r + A) + (s + A) = (r + s) + A$
3. $0 + A = A$ *is the additive identity of* R/A
4. $-(r + A) = (-r) + A$ *is the additive inverse of* $r + A$
5. $\forall k \in \mathbb{Z} \quad k(r + A) = kr + A$

This is just a translation of the properties of cosets and quotient groups, that we are familiar with, into the language of addition. You can (read: should) prove this as an exercise for yourself (read: myself).

Since R is a ring, it is natural to ask if we could make R/A into a ring[1]. A natural way to define "multiplication" in R/A is

[1] *Ideally* (see what I did there?), we would want R/A as a ring, just as we had R/A as a group.

$$(r + A)(s + A) = rs + A \quad \forall r, s \in \mathbb{R} \tag{†}$$

Note, however, that we would have

$$r + A = r_1 + A \qquad s + A = s_1 + A$$

with $r \neq r_1$ and $s \neq s_1$. In order for (†) to make sense, it is necessary that

$$r + A = r_1 + A \wedge s + A = s_1 + A \implies rs + A = r_1 s_1 + A$$

so that this "multiplication" is **well-defined**.

Proposition 61

Let A be an additive subgroup of a ring R. Then $\forall a \in A$, define

$$Ra = \{ra : r \in R\} \quad aR = \{ar : r \in R\}.$$

The following are equivalent (TFAE):

1. *$Ra \subseteq A$ and $aR \subseteq A$, $\forall a \in A$;*
2. *$\forall r, s \in R$, $(r + A)(s + A) = rs + A$ is well-defined in R/A.*

Proof

(1) $\implies$ (2): *If $r + A = r_1 + A$ and $s + A = s_1 + A$, for $r, r_1, s, s_1 \in R$, we need to show that*

$$rs + A = r_1 s_1 + A.$$

By Proposition 60, we have that $(r - r_1), (s - s_1) \in A$, and so by (1), we have

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \\ &\in (r - r_1)R + R(s - s_1) \subseteq A \end{aligned}$$

Therefore, by Proposition 60 again, we have $rs + A = r_1 s_1 + A$.

(2) $\implies$ (1): *Let $r \in R$ and $a \in A$. We have that*

$$\begin{aligned} ra + A &= (r + A)(a + A) \quad \because (2) \\ &= (r + A)(\underbrace{0}_{\text{zero of } R} + A) \quad \because a, 0 \in A \\ &= (r \cdot 0) + A \quad \because (2) \\ &= 0 + A \quad \because \textit{Proposition } 58 \\ &= A \quad \because \textit{Proposition } 60 \end{aligned}$$

Thus $ra \in A$ and so RaA. Similarly, we can show that $aR \subseteq A$. ☐

Definition 35 (Ideal)

An additive subgroup A of a ring R is called an ***ideal*** *of R if $Ra, aR \subseteq A, \forall a \in A$.*

Example 22.1.1

If R is a ring, $\{0\}$ and R are both ideals of R.

Proposition 62 (The Only Ideal with the Multiplicative Identity is the Ring Itself)

Let A be an ideal of a ring R. If $1 \in A$, then $A = R$.

This also shows that if we want a non-trivial ideal, then the ideal should not have 1.

Proof

$\forall r \in R, \because A$ is an ideal and $1 \in A$, we have $r = r \cdot 1 \in A$. It follows that $R \subseteq A \subseteq R$ and so $R = A$. ☐

Proposition 63 (Construction of the Quotient Ring)

Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with the multiplication $(r + A)(s + A) = rs + A, \forall r, s \in R$. The unity of R/A is $1 + A$.

Proof

$\because$ A is an additive subgroup of a ring R, ${}^{R}\!/_{A}$ is an additive abelian group. By Proposition 61, the multiplication on ${}^{R}\!/_{A}$ is well-defined. The multiplication is associative, since $\forall r, s, q \in R$,

$$\begin{aligned}(r+A)\big((s+A)(q+A)\big) &= (r+A)(sq+A) = (rsq+A) \\ &= (rs+A)(q+A) \\ &= \big((r+A)(s+A)\big)(q+A).\end{aligned}$$

We also have

$$(r+A)(1+A) = r+A = (1+A)(r+A)$$

and so the unity of ${}^{R}\!/_{A}$ is $1+A$. The distributive property is inherited from R. □

Definition 36 (Quotient Ring)

*Let A be an ideal of a ring R. Then the ring ${}^{R}\!/_{A}$ is called the **quotient ring** of R by A.*

Definition 37 (Principal Ideal)

*Let R be a commutative ring and A an ideal of R. If $A = aR = \{ar : r \in R\} = Ra$ for some $a \in A$, we say that A is a **principal ideal** generated by a, and denote $A = \langle\, a \,\rangle$.*

Example 22.1.2

If $n \in \mathbb{Z}$, then $\langle\; n \;\rangle = n\mathbb{Z}$ is a(n) (principal) ideal of $\mathbb{Z}$, since $\mathbb{Z}$ is commutative.

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

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

We shall prove this in the next lecture.