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`

21 Lecture 21 Jun 20th 2018

21.1 Rings (Continued)

21.1.1 Rings (Continued)

Note (Notation)

Given a ring R, to distinguish the difference between multiples in addition and in multiplication, for $n \in \mathbb{N} \wedge a \in R$, we write

$$na = \underbrace{a + a + \ldots + a}_{n \text{ times}}$$

and

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}}$$

respectively. Also, we will define

$$(-n)a = \underbrace{(-a) + (-a) + \ldots + (-a)}_{n \text{ times}}$$

and

$$a^{-n} = \left(a^{-1}\right)^n$$

if a^{-1} exists.

Note

Recall that for a group G and $g \in G$, we have $g^0 = 1$, $g^1 = g$, and

$\left(g^{-1}\right)^{-1} = g$. *Thus for addition, we have*

$$\begin{array}{ccc} \text{integer} & & \\ \uparrow & & \\ 0 \cdot a = 0 & & 1 \cdot a = a \\ \downarrow & & \\ \text{zero in } R & & \end{array}$$

$$-(-a) = a$$

Also, by Proposition 5, if $n, m \in \mathbb{Z}$, *we have*

$$m \cdot a + n \cdot a = (m+n) \cdot a$$
$$n(ma) = (nm)a$$
$$n(a+b) = na + nb$$

Proposition 58 (More Properties of Rings)

Let R *be a ring and* $r, s \in \mathbb{R}$.

This is a problem in A4.

1. *If* 0 *is the zero of* R, *then* $0 \cdot r = 0 = r \cdot 0$; [1]
2. $-r(s) = -(rs) = r(-s)$;
3. $(-r)(-s) = rs$;
4. $\forall m, n \in \mathbb{Z}$, $(mr)(ns) = (mn)(rs)$.

[1] i.e. all the 0's are zeros of R.

Definition 32 (Trivial Ring)

A ***trivial ring*** *is a ring of only one element. In this case, we have* $1 = 0$, *i.e. the unity is the zero and vice versa.*

Remark

If R *is a ring with* $R \neq \{0\}$, *since* $r = r \cdot 1$ *for all* $r \in R$, *we have* $1 \neq 0$. *Otherwise, if* $1 = 0$, *then* $r = r \cdot 1 = r \cdot 0 = 0$, *i.e.* $R = \{0\}$.

Example 21.1.1

Let $R_1, R_2, \ldots, R_n$ *be rings. We define component-wise operation on the* *product*

$$R_1 \times R_2 \times \ldots \times R_n$$

as follows:

$$(r_1, r_2, ..., r_n) + (s_1, s_2, ..., s_n) = (r_1 + s_1, r_2 + s_2, ..., r_n + s_n)$$
$$(r_1, r_2, ..., r_n)(s_1, s_2, ..., s_n) = (r_1 s_1, r_2 s_2, ..., r_n s_n)$$

We can check that $R_1 \times R_2 \times \ldots \times R_n$ *is a ring with the zro being* $(0, 0, ..., 0)$ *and the unity being* $(1, 1, ..., 1)$. *This set*

$$R_1 \times R_2 \times \ldots \times R_n$$

is called the ***direct product*** *of* $R_1, R_2, ..., R_n$.

Definition 33 (Characteristic of a Ring)

If R is a ring, we define the ***characteristic*** *of R, denoted by* $\mathrm{ch}(R)$, *in terms of the order of* 1_R *in the additive group* $(R, +)$, *by*

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

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean that $\forall r \in R$, $kr = 0$.

By Proposition 58, we have

$$kr = k(1_R \cdot r) = (k1_R) \cdot r$$

and so $kR = 0$ if and only if $k1_R = 0$. Then, since $(R, +)$ is a group, by Proposition 13 and Proposition 14, it follows that:

Proposition 59 (Implications of the Characteristic)

Let R be a ring and $k \in \mathbb{Z}$.[2]

1. $\mathrm{ch}(R) = n \in \mathbb{N} \implies (kR = 0 \iff n \mid k)$
2. $\mathrm{ch}(R) = 0 \implies (kR = 0 \iff k = 0)$

[2] This is why we defined $\mathrm{ch}(R) = 0$ if $o(1_R) = \infty$

Example 21.1.2

Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ has characteristic 0. For $n \in \mathbb{N}$ with $n \geq 2$, the ring $\mathbb{Z}_n$ has characteristic n.

21.1.2 Subring

Definition 34 (Subring)

A subset S of a ring R is a subring if S is a ring itself (under the same operations: addition and multiplication).

Unlike subgroups, since there is no proper suggestion of a symbolic representation, I shall use $S \leq_r R$ to denote that S is a subring of R, in comparison to $\leq$ for subgroups, which has no subscript. Note that this is purely for keeping my writing succinct, and so the subscript r is used simply to indicate that the $\leq$ symbol is for denoting a subring and should not be confused with other r's that may be used in a proof. This notation is also not used in class, and should be avoided during materials outside of this set of notes.

Note that properties (2), (3), (7) and (9) from Definition 31 are automatically satisfied. Thus, to show that S is a subring, it suffices to show the following:

Subring Test

1. $0, 1 \in S$
2. $s, t \in S \implies (s - t), st \in S$

Example 21.1.3

We have the following chain of commutative rings:

$$\mathbb{Z} \leq_r \mathbb{Q} \leq_r \mathbb{R} \leq_r \mathbb{C}$$

Example 21.1.4

If R is a ring, the center $Z(R)$ of R is defined as

$$Z(R) = \{z \in R : zr = rz, r \in R\}.$$

Note taht $0, 1 \in Z(R)$. Also, if $s, t \in Z(R)$, then $\forall r \in R$,

$$(s - t)r = sr - tr = rs - rt = r(s - t)$$

and so $(s - t) \in Z(R)$. Also,

$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$

and so $st \in Z(R)$. By the Subring Test, $Z(R) \leq_r R$.

Example 21.1.5

Let

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

It can be shown that $\mathbb{Z}[i] \leq_r \mathbb{C}$, and is called the ring of ***Gaussian integers****.*[3]

[3] Proof that the Gaussian integers is a subring is in A4, which shall be included after the assignment is over.