Intoduction to Rings

All rings in this note are commutative.

1. Basic Definitions and Examples

Ring

$(R, \cdot, +)$ $\quad$ R : *set*

$\cdot$: multiplication (it can be non-commutative)

$+$: addition

Definition: A *ring* R is a set together with two binary operations $+$ and $\cdot$ (called addition and multiplication) satisfying the following axioms:

(i) (R, $+$) forms an *abelian* group. 0 is the identity for this group, and the inverse of the ring element a will be denoted by $-a$,

(ii) (R, $\cdot$) forms a semi group (associative multiplication: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$). It may not have the identity, and if it does then the identity is 1, and has no inverse in general,

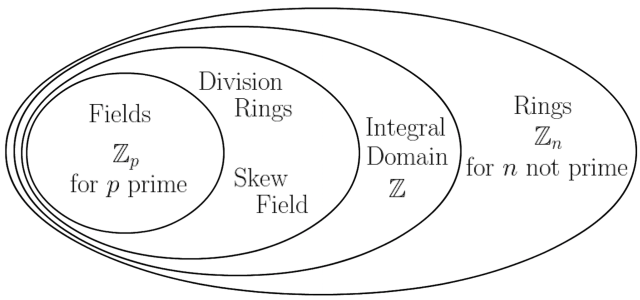
(iii) the *distributive law* $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Definition: If $(R/\{0\}, \cdot)$ has an identity and forms a group then R is a *division ring* (or *skew field*), the ring is an abelian group. If $(R, \cdot)$ is commutative then R is a *field*.

Definition: Let R be a ring

(1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(2) A commutative ring with identity $1 \neq 0$ is called an *integral domain* if R has no zero-divisor.



$$\begin{aligned} \mathbb{H}\ (\textit{Hamilton Quaternions}) &= \mathcal{L}\{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\} \\ &\cong \mathcal{L}\left\{ \begin{bmatrix} y & z \\ \bar{z} & \bar{y} \end{bmatrix} : y, z \in \mathbb{C} \right\} \\ \mathbf{i}^2 = \mathbf{j}^2 &= \mathbf{k}^2 = \mathbf{ijk} = -1 \end{aligned}$$

4 dimensional vector space over $\mathbb{R}$

Examples:

Division ring:

$Q_8 = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ $\quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$ $\quad$ is a group of order 8
Quaternions $\quad D_4 \ncong Q_8$

$$\begin{aligned}
\mathbf{i} \cdot \mathbf{ijk} = -\mathbf{jk} &= \mathbf{i}(-1) = -\mathbf{i} \\
\mathbf{jk} &= \mathbf{i} \\
-\mathbf{k} &= \mathbf{ji} \\
-\mathbf{ki} &= \mathbf{j}(-1) = -\mathbf{j} \\
\mathbf{ki} &= \mathbf{j} \\
\mathbf{k}^2 \cdot \mathbf{i} &= -1 \cdot \mathbf{i} = -\mathbf{i} = \mathbf{kj}
\end{aligned}$$

Fields: $\mathbb{C}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_p$
Division ring: $\mathbb{H}$
Integral domain: $\mathbb{R}[x], \mathbb{Z}$
Rings: $\mathbb{Z}_n$ for n not prime, $\mathbb{C}$G - group algebras $\mathbb{Z} \times \mathbb{Z}$, $\mathrm{Mat}_{n\times n}(\mathbb{C})$

Definition: Algebra is a special kind of ring. A is a ring which contains a field $F \subseteq A$ and A is a vector space over F.

$$A \cong \mathcal{L}_F\{f_1a_1 + f_2a_2 + \cdots + f_na_n : f_i \in F \text{ and } a_i \in A\}.$$

Example:

$$\begin{aligned}
\mathbb{R}Q_8 &= \text{group algebra over } \mathbb{R} \text{ of } Q_8 (\text{not the same ring as } \mathbb{H}) \\
&= \mathcal{L}_R\{\mathbf{1}, (-\mathbf{1}), \mathbf{i}, (-\mathbf{i}), \mathbf{j}, (-\mathbf{j}), \mathbf{k}, (-\mathbf{k})\} \qquad \text{dim 8 vector space over } \mathbb{R}
\end{aligned}$$

The group ring $\mathbb{R}Q_8$ is not a division ring, it is not isomorphic to $\mathbb{H}$, and has zero divisors.

2. Ring Homomorphisms and Quotient Rings

Lemma: For G be a finite group, $\mathbb{C}G \cong End(\mathbb{C}G)$.
Sketch of a proof: For $x \in \mathbb{C}G$, $\phi_x(g) = gx$

$$\begin{aligned}
\phi_x &: \mathbb{C}G \to \mathbb{C}G \\
\implies \phi &: \mathbb{C}G \to End(\mathbb{C}G)
\end{aligned}$$

Definition: Let R and T be rings.

(1) A *ring homomorphism* is a map $\phi : R \to T$ which preserves multiplication and addition structures

$$\begin{aligned}
\phi(r_1 +_R r_2) &= \phi(r_1) +_T \phi(r_2) \quad \text{for all } r_1, r_2 \in R \\
\phi(r_1 \cdot_R r_2) &= \phi(r_1) \cdot_T \phi(r_2) \quad \text{for all } r_1, r_2 \in R
\end{aligned}$$

(2) A bijective ring homomorphism is called an *isomorphism*.

Proposition: Let R and T be rings and let $\phi : R \to T$ be a homomorphism.

(1) $\ker(\phi) \subseteq R$ is an ideal of R.

(2) $\mathrm{img}(\phi) \subseteq T$ is a subring of T.

Theorem: (*The First Isomorphism Theorem for Rings*) If $\phi : R \to T$ is a homomorphism of rings, then the kernel of ϕ is an ideal of R, the image of ϕ is a subring of S and $R/\ker\phi$ is isomorphic as a ring to $\phi(R)$ ($\mathrm{img}(\phi) \cong R/\ker(\phi)$).

3. Properties of Ideals

Definition: Let A be any subset of the ring R. Let (A) denote the smallest ideal of R containing A, called the *ideal generated by A*.

The *left ideal generated by A*, such that A an anbelian group (written additively):

$$\{ra : r \in R \text{ and } a \in A\} \subseteq A$$

similarly, the *right ideal generated by A*:

$$\{ar : r \in R \text{ and } a \in A\} \subseteq A$$

and the *(two-sided) ideal generated by A*:

$$\{rar' : r, r' \in R \text{ and } a \in A\} \subseteq A.$$