Rings and Fields : Definitions

Definition

A ring is a set R, equipped with two binary operations, $+$ and $\times$, such that

0_R = identity
$-x$ = inverse of x

1/ $(R,+)$ is an Abelian Group.

1_R = identity
Inverses don't necessarily exist.

2/ $(R,\times)$ is a Monoid

3/ $a\times(b+c) = a\times b + a\times c$ **and** $(a+b)\times c = a\times c + a\times c$ $\forall\, a,b,c \in R$

$(R\ +,\times)$ is commutative if, in addition,

drop $\times$ notation

4/ $ab = ba \quad \forall\, a,b \in R$

Commutative — Non-commutative

Examples $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{Z}/n\mathbb{Z},+,\times)$, $(M_n(\mathbb{R}),+,\times)$

Definition Let R be a ring. We say $a \in R$ is invertible / a unit if $\exists\, b \in R$ such that

denoted a^{-1}

$ab = ba = 1_R$. We denote the units by R^*.

Example $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $M_n(\mathbb{R})^* = GL_n(\mathbb{R})$

Proposition $(R^*,\times)$ is a group.

Proof $(R,\times)$ a monoid $\Rightarrow$ $(R^*,\times)$ a group $\square$

<u>Observation</u> : $0_R x = (0_R + 0_R)x = 0_R x + 0_R x$

$\Rightarrow \quad 0_R x = 0_R \quad \forall x \in R$

<u>Definition</u> The trivial ring is the ring with one element.

$x = 1_R x = 0_R x = 0_R \quad \forall x \in R$

R trivial $\iff 0_R = 1_R$

<u>Definition</u>

$(R, +, \times)$ is a <u>division ring</u> iff

1/ R non-trivial

2/ $R^{*} = R \setminus \{0\}$ every non-zero element is invertible

A <u>commutative</u>, <u>division ring</u> is called a <u>field</u>.

<u>Examples</u> $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ p prime

<u>Remarkable Fact</u>: There exist non-commutative division rings.

<u>Example</u> : The <u>Quaternions</u> denoted $\mathbb{H}$.

usual vector addition

$\mathbb{H} = (\mathbb{R}^4, +, \times)$

strange non-commutative multiplication.

$$\underline{x} = \begin{pmatrix} r \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} r \\ \underline{x} \end{pmatrix}, \quad r \in \mathbb{R}, \ \underline{x} \in \mathbb{R}^3 \qquad , \quad \underline{y} = \begin{pmatrix} s \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} s \\ \underline{y} \end{pmatrix}$$

multiplication in $\mathbb{H}$ — dot product in $\mathbb{R}^3$

$$\underline{x} \times \underline{y} := \begin{pmatrix} rs - \underline{x}\cdot\underline{y} \\ r\underline{y} + s\underline{x} + \underline{x}\times\underline{y} \end{pmatrix} \in \mathbb{R}^3$$

cross product in $\mathbb{R}^3$

Remark

1/ $1_{\mathbb{H}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $0_{\mathbb{H}} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

2/ There is a more direct way to define $\times$ in $\mathbb{H}$.
$\mathbb{H} = \{\lambda 1_{\mathbb{H}} + x\underline{i} + y\underline{j} + z\underline{k} \mid \lambda, x, y, z \in \mathbb{R}\}$ and
$\underline{i}^2 = \underline{j}^2 = \underline{k}^2 = \underline{i}\underline{j}\underline{k} = -1_{\mathbb{H}}$
Historically this is where the definition of the cross product in $\mathbb{R}^3$ comes from! Very non-obvious

3/ $\mathbb{R}, \mathbb{C}, \mathbb{H}$ are the <u>only</u> finite dimensional vector spaces with structure of a division ring.

Definition Let R be a ring. R is an <u>integral domain</u> if

1/ R non-trivial
2/ R commutative
3/ $ab = 0_R \Rightarrow a = 0_R$ or $b = 0_R$

Examples $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ p prime

Non-example $M_{n\times n}(\mathbb{R})$, $n \geq 2$, $\mathbb{Z}/ab\mathbb{Z}$ $a, b > 1$

Proposition R a field $\Rightarrow$ R integral domain

Proof Exercise $\square$

Cancellation Law for Integral Domains

If R is an integral domain and $a, b, c \in R$, $a \neq 0_R$

$$ab = ac \Rightarrow b = c$$

<u>Proof</u> $ab = ac \Rightarrow ab - ac = 0_R \Rightarrow a(b-c) = 0_R$

$a \neq 0_R$

$\Rightarrow b - c = 0_R \Rightarrow b = c$ $\square$