More definitions and examples

<u>Basic properties</u>

Let R be a ring.

① $0\cdot a = a\cdot 0 = 0 \quad \forall a\in R$

$\ulcorner\; 0+0=0 \implies 0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$

$$\begin{aligned} 0\cdot a + (-0\cdot a) &= 0\cdot a + 0\cdot a + (-0\cdot a) \\ 0 &= 0\cdot a + 0 \\ 0 &= 0\cdot a \quad \lrcorner \end{aligned}$$

② $(-a)\cdot b = a\cdot(-b) = -(a\cdot b) \quad \forall a,b\in R$

$\ulcorner\; a\cdot b + -(a\cdot b) = 0 \leftarrow$ By definition

$a\cdot b + (-a)\cdot b = (a+(-a))\cdot b = 0\cdot b = 0$

$\implies -(a\cdot b) = (-a)\cdot b \quad \lrcorner$

③ $(-a)\cdot(-b) = a\cdot b \quad \forall a,b\in R$

$\ulcorner\; (-a)\cdot(-b) = -\big(a\cdot(-b)\big) = -(-(a\cdot b))$

$-(a\cdot b) + -(-(a\cdot b)) = 0$

But. $-(a\cdot b) + a\cdot b = 0 \implies a\cdot b = -(-(a\cdot b)) \quad \lrcorner$

④ If R has 1, then 1 is unique and $-a = (-1)\cdot a$

$\ulcorner\; 1 = 1\cdot 1' = 1'$

Additive inverses are unique $\implies a + \overbrace{(-1)\cdot a}^{=-a} = 1\cdot a + (-1)\cdot a = (1+(-1))\cdot a$

$= 0\cdot a = 0 \quad \lrcorner$

Defn: We say a non-zero element $a \in R$ is a <u>zero divisor</u> if $\exists\, b \neq 0$ s.t. $a \cdot b = 0$

Example: $M_2(\mathbb{R})$

Recall $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Example 2: $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$$

Claim: If $\bar{0} \neq \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is not a zero divisor, then it is a unit.

Pf: If $a \in \mathbb{Z}$, $a \neq 0$ relatively prime to n.

then Euclid's Algorithm constructs $x, y \in \mathbb{Z}$ s.t.

$$a \cdot x + n \cdot y = 1$$

$$\Longrightarrow \bar{a} \cdot \bar{x} = \bar{1} \in \mathbb{Z}/n\mathbb{Z}.$$

On the other hand, if $\gcd(a,n) > 1$, then say $\gcd(a,n) = d$.

Then $n = d \cdot q$

Then $\bar{a} \cdot \bar{q} = \bar{n} = \bar{0}$ $\square$

Cor: If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field.

PF: If $0 < m < n$ and n is prime,

then $\gcd(m,n) = 1$ $\square$

Ex: $\mathbb{Z}/2\mathbb{Z}$ is a field, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ is not a field

(check $\bar{2} \cdot \bar{2} = \bar{0}$)

Claim: If $a \in R$ is a zero divisor,

then it is not a unit.

PF: Say $b \neq 0$ and $a \cdot b = 0$

If $\exists c \in R$ s.t. $a \cdot c = 1 = c \cdot a$

then $c \cdot a \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$

$= (c \cdot a) \cdot b = 1 \cdot b = b \rightarrow\leftarrow$

$\square$

Notation: If R is a ring w/ $1 \neq 0$

we denote the set of units by

$$R^\times := \{ a \in R \mid \exists b \in R \text{ s.t. } a \cdot b = b \cdot a = 1 \}$$

$R^\times$ is the group of units of R.

Claim: $(R^\times, \cdot)$ is a group.

Pf: • $1 \in R^\times$ $(1 \cdot 1 = 1)$

and $\forall a \in R^\times$, $a \cdot 1 = 1 \cdot a = a$.

• Associativity follows from associativity for $\cdot$ in R

• $\forall a \in R^\times$, by definition $\exists b \in R$

s.t. $a \cdot b = b \cdot a = 1$

But this implies $b \cdot a = a \cdot b = 1 \Longrightarrow b \in R^\times$ $\square$

Note: A field F is a comm ring w/ $1 \neq 0$

s.t. $F^\times = F \setminus \{0\}$

Defn: We say a comm. ring R w/ $1 \neq 0$

is an integral domain if it has no zero divisors

Non-example: $\mathbb{Z}/4\mathbb{Z}$ is not an int. dom.

$M_2(\mathbb{R})$ is not an int. dom.

Example: $\mathbb{Z}$ is an integral domain.

Prop: Cancellation

Let R be a ring, $a, b, c \in R$

Suppose a is not a zero divisor

If $ab = ac$, then $b = c$

Pf: If $a \neq 0$, then $a \cdot (b-c) = 0$

Since a is not a zero divisor $\Longrightarrow b-c=0$

$\Longrightarrow b=c$ $\square$

Example: $\mathbb{Z}/4\mathbb{Z}$

$\bar{2} \cdot \bar{2} = \bar{0}$, $\bar{2} \cdot \bar{0} = \bar{0}$ But $\bar{2} \neq \bar{0}$

Cor: If R is a finite (as a set) integral domain then R is a field.

Pf: Fix $a \in R$, $a \neq 0$

Define a map

$$f_a : R \longrightarrow R$$
$$x \longmapsto a \cdot x$$

Claim: f_a is an injective map by cancellation.

Suppose $f_a(x) = f_a(y) \Longrightarrow x = y$
$ax = ay$

By Pigeonhole Principle f_a is also surjective

$\Longrightarrow \exists\, x \in R$ s.t. $a \cdot x = 1$

$\Longrightarrow a \in R^{\times} \Longrightarrow R$ is a field $\square$

<u>Defn</u>: A <u>subring</u> S of a ring R is a subgroup that is closed under multiplication.

That is $S \subset R$ s.t.

① $\forall a,b \in S \quad a+b \in S$ (closure under $+$)

② $0 \in S$

③ $\forall a \in S, \ -a \in S$

S is a subgroup

④ $\forall a,b \in S \quad a \cdot b \in S$ (closure under $\cdot$)

<u>Subgroup Criterion</u> If $S \subset R$ is a subset of a ring s.t.

① $S \neq \emptyset$

② $\forall a,b \in S \quad a-b \in S$

③ $\forall a,b \in S \quad a \cdot b \in S$

Then S is a subring.

<u>Pf</u>: Suppose $a \in S$.

$\Longrightarrow \ a-a=0 \in S$ ✓

$\Longrightarrow \ 0-a=-a \in S$ ✓

$\Longrightarrow$ If $a,b \in S$, then $a+b=a-(-b) \in S$ ✓

and $a \cdot b \in S$

$\square$

Examples: $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$ $(\mathbb{Z} \subset \mathbb{R})$ are subrings.

- $2\mathbb{Z} \subset \mathbb{Z}$ is a subring

  In fact $n \cdot \mathbb{Z} \subset \mathbb{Z}$ is a subring.

- $C[0,1] \subset \mathcal{F} := \{f : [0,1] \to \mathbb{R}\}$ is a subring.

Q: What do subrings of fields look like?

Defn: If F is a field and $F' \subset F$ is a subring s.t.

1. $1 \in F'$
2. $\forall a \in F'$, $a^{-1} \in F'$

then we say F' is a subfield of F

Warning: Not all subrings of fields are subfields!

e.g. $\mathbb{Z} \subset \mathbb{R}$

Claim: If $R \subset F$ is a subring of a field w/ $1 \in R$

then R is an integral domain.