Examples of ring homomorphisms

(a) $\mathrm{Hom}_{\text{rings}}(\mathbb{Z}, R) = \{\chi_R\}$

(b) $\mathrm{Hom}_{\text{rings}}(\mathbb{Z}, \mathbb{Z}) = \{id_{\mathbb{Z}}\}$ Identity map on $\mathbb{Z}$.

(c) Consider the family of rings R_i, $i \in I$

$\prod_{i\in I} R_i$ is a ring

Multiplicative identity is $(1_{R_i})_{i\in I}$

In particular, $R_i = R$ $\forall i \in I$, then R^I is a ring. The map

$$R_i \longrightarrow \prod_{i\in I} R_i$$
$$x \longmapsto (1_R, \dots, \underset{\substack{\uparrow \\ i^{th}\text{ position}}}{x}, \dots)$$

is not an ring homomorphism because it does not preserve the '+' operation on the Abelian group.

Subring: A is a subring of R if $A \subseteq R$, and (i) A is a ring, (ii) $1_A = 1_R$

Illustrative examples:

(a) If I is infinite

$$\coprod_{i\in I} R_i \subset \prod_{i\in I} R_i$$

is not a subring because the identity element is absent

(b) If I is finite, then

$$\coprod_{i\in I} R_i = \prod_{i\in I} R_i$$

(c) Group G is abelian. Consider the set

$\mathrm{End}(G) = \{f : G \to G \mid f \text{ is group homomorphism}\}$

$f, g \in \mathrm{End}(G)$, $\quad f+g : G \longrightarrow G$
$$x \longmapsto f(x) + g(x)$$

One can show that $f+g \in End(G)$ 4

$f \circ g : G \to G$

$(End(G), +, \circ)$ is a ring with the multiplicative identity being the identity map.

(d) $\mathbb{Z}_n = \{0, 1, 2, \dots n-1\}$, with the operations

$$a +_n b = r(a+b)$$
$$a \cdot_n b = r(a \cdot b)$$

$r(x)$ is the remainder obtained when dividing x by n.

Show that $(\mathbb{Z}_n, +_n, \cdot_n)$ is a ring.

(e) Consider the ring R, and the matrices of dimension $m \times n$ with entries in R. The matrices belong to

$$R^{\{1, 2, \dots m\} \times \{1, 2 \dots n\}}$$

The above set is a ring with the same operations component wise.

Special elements: Units $R^\times = (R^*, \cdot)^\times$

For the ring $\mathbb{Z}_n$, the units ~~of~~ are $\{m \mid \gcd(m,n) = 1\}$

Example:

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$
$$\mathbb{Z}_4^\times = \{1, 3\} \Rightarrow |\mathbb{Z}_n^*| = \phi(n).$$

Generally,

$$\left(\prod_{i \in I} R_i\right)^\times = \prod_{i \in I} R_i^\times$$

$$\Rightarrow (R^I)^\times = (R^\times)^I$$

Note: $(\mathbb{Z}_4^*, \cdot)$ is not cancellative because $2 \cdot_4 2 = 0$.

$\not\Rightarrow 2 = 0$

Field: A ring R is a field if $(R^*, \cdot)$ is a commutative group. If $(R^*, \cdot)$ is a group which is not commutative, then $(R, +, \cdot)$ is called a division ring.

Examples: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields.

Given a ring $(R, +, \cdot)$ show that

$$(R^*, \cdot) \text{ is a monoid} \iff (R^*, \cdot) \text{ is cancellative.}$$

Also, it can be shown that

$$\text{if } a \cdot b = 0 \implies a = 0 \text{ or } b = 0$$

Zero divisor: In a ring $(R, +, \cdot)$, if $a \in R$, then a is called a zero divisior if $a \neq 0$, and $\exists\, b \neq 0$ such that $a \cdot b = 0$.

Note: A zero divisor cannot be a unit.

$$\left.\begin{matrix} \text{If } a \in R^{\times}, \\ a \neq 0,\ b \neq 0 \end{matrix}\right\} \text{ and } a \cdot b = 0 \implies a^{-1} \cdot a \cdot b = 0$$

$$\implies b = 0$$

(contradiction)

When is a finite monoid a group?

Ans: A finite cancellative monoid is a group.

Outline of the proof: use the map f_a

$$M \xrightarrow{f_a} M$$

$$x \longmapsto ax$$

Show that f_a is injective which implies f_a is bijective. In addition show that for every element in M there exists a inverse and it is unique.

$(\mathbb{Z}_n^*, +_n, \cdot_n)$ is a field only when n is prime. (Prove)