3. Rings

3.1 Rings

$(R, +, \cdot)$ where

- $(R, +)$ is a group
- Multiplicative identity: $1a = a1 = a$
- $a(bc) = (ab)c$
- $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

Properties

- $a0 = 0a = 0$
- $a(-b) = (-a)b = -(ab)$
- $(-a)(-b) = ab$

Integral Domain

> commutative ring with unity and no zero-divizors(for $a \in R$ an element $b \in R\ s.t.\ ab = 0$)

Characteristic of a ring R

> least positive integer n s.t. $nx = 0\ \forall x \in R$
> Notation: $char R$

Let R be a ring with unity 1.

- If $ord(1) = \infty$ under addition => $char R = 0$.
- If $ord(1) = n$ under addition => $char R = n$.

Proof
$n \cdot x = x + x + ... + x = 1x + 1x + ... + 1x = (n \cdot 1)x = 0x = 0\ \forall x \in R$

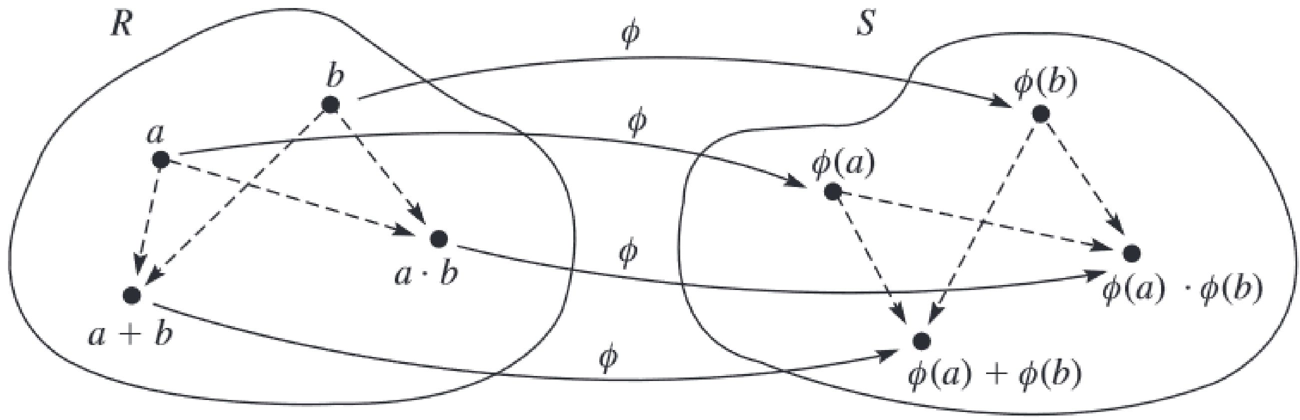
Field

> A field is a commutative ring with unity in which every nonzero element is a unit

Example

> $\mathbb{Z}_p$ for p prime

Homomorphisms



If R is a ring with unity and $char R = n > 0$ then $S < R$ is a subring isomorphic to $\mathbb{Z}_n$. If $char R = 0$ then $S \approx \mathbb{Z}$