3. Rings

3.1 Rings

Definition -- Ring

Let $(R, +, \cdot)$ be a set annointed with 2 operations. This is a ring if

- $(R, +)$ is a group with identity 0
- Multiplicative identity: $1a = a1 = a$
- $a(bc) = (ab)c$
- $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

R is **commutative** if $\cdot$ is commutative

Properties

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

Examples

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are rings. You can check the properties
2. $\mathbb{Z}/n\mathbb{Z}$ -- the integers modulo n also form a ring
3. The polynomial ring $R[x] = \{a_n \cdot x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \ : \ a_i \in R\}$
4. Gaussian integers $\mathbb{Z}[i] = \{a + bi \ : \ a, b, \in \mathbb{Z}\}$

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

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

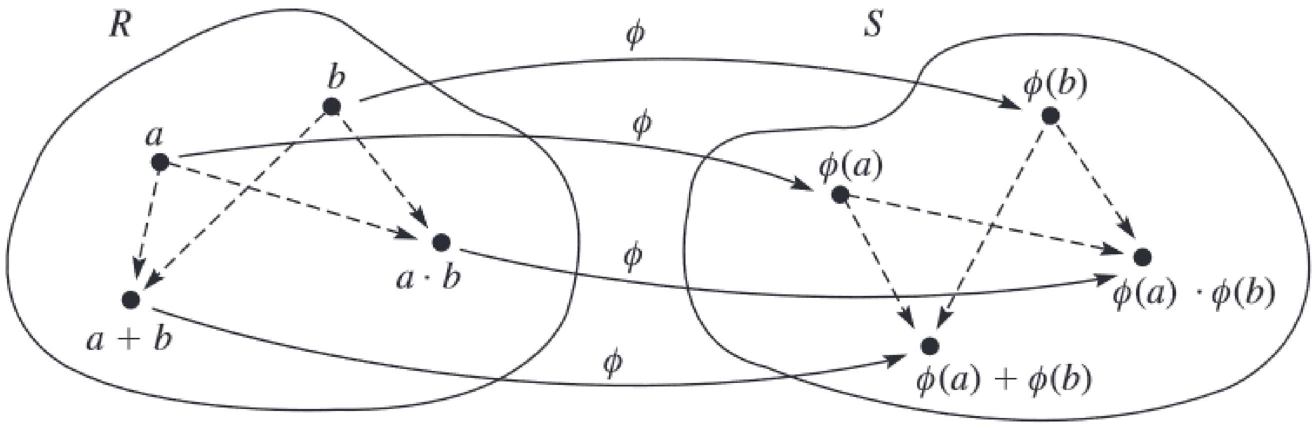
Field

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

Examples

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. $\mathbb{Z}$ is not a field because not every element has an inverse (We can't divide here)
3. $\mathbb{Z}/\mathbb{Z}p$ 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 $S \approx \mathbb{Z}$