Homomorphisms

Definition 1 (Ring Homomorphism). Let R and S be rings. A map $\varphi: R \to S$ is called a ring homomorphism if the following are satisfied.

- $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$.
- $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

If R and S are both unital rings, we say that φ is unital if $\varphi(1_R) = 1_S$.

Proposition 1.

- 1. If R is a ring, then $1: R \to R$ given by 1(x) = x is a ring homomorphism. If R is unital, then 1 is unital.
- 2. If $\varphi: R \to S$ and $\psi: S \to T$ are ring homomorphisms, then $\psi \circ \varphi: R \to T$ is a homomorphism. If φ and ψ are unital, then $\psi \circ \varphi$ is unital.

Homomorphisms are structure-preserving maps. The arithmetic on a ring – the plus and times – are a kind of structure, and homomorphisms are the maps which "transport" this structure to another setting. If $\varphi: R \to S$ is a ring homomorphism then in a concrete sense there is a "shadow" of R inside S. If R and S are both unital rings, then the one element is an extra bit of structure.

Proposition 2. Suppose $\varphi: R \to S$ is a ring homomorphism.

- $\bullet \ \varphi(0_R) = 0_S$
- $\varphi(-a) = -\varphi(a)$ for all $a \in R$.
- $\varphi(a-b) = \varphi(a) \varphi(b)$ for all $a, b \in R$.

Examples

- The natural projection $\pi: \mathbb{Z} \to \mathbb{Z}/(n)$ is a unital ring homomorphism.
- If R is any ring, then there is exactly one ring homomorphism $\varphi: R \to 0$, and exactly one homomorphism $\psi: 0 \to R$. Neither of these is ever unital unless R = 0.
- Let R be any unital ring. Then $\varphi: R \to \mathsf{Mat}_2(R)$ given by

$$\varphi(r) = \begin{bmatrix} 0 & 0 \\ -r & r \end{bmatrix}$$

is a ring homomorphism. Although R (and hence $\mathsf{Mat}_2(R)$) is unital, φ is not a unital homomorphism. (Why?)

Images and Kernels

Definition 2 (Image and Kernel). Let $\varphi : R \to S$ be a ring homomorphism. We define subsets of R and S as follows.

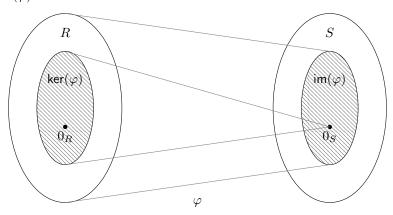
• The kernel of φ , denoted $\ker(\varphi)$, is the set

$$\ker(\varphi) = \{ r \in R \mid \varphi(r) = 0 \}.$$

• The image of φ , denoted $\operatorname{im}(\varphi)$, is the set

$$im(\varphi) = \{ s \in S \mid s = \varphi(r) \text{ for some } r \in R \}.$$

Proposition 3. If $\varphi : R \to S$ is a ring homomorphism, then $0_R \in \ker(\varphi)$ and $0_S \in \operatorname{im}(\varphi)$.



The kernel measures how badly a homomorphism fails to be injective.

Proposition 4. A ring homomorphism φ is injective if and only if $\ker(\varphi) = 0$.

Characteristic

Proposition 5. If R is a unital ring, then there is a unique unital homomorphism $\varphi : \mathbb{Z} \to R$.

We can think of the image of this map as a copy of the integers in R, with $1 = 1_R$, $2 = 1_R + 1_R$, and so on.

Definition 3 (Characteristic). Let R be a unital ring and $\varphi : \mathbb{Z} \to R$ the unique unital homomorphism. If there is a positive integer n such that $\varphi(n) = 0$, then there is a smallest such integer. We call this the characteristic of R, denoted $\operatorname{char}(R)$. That is, $\operatorname{char}(R)$ is the smallest positive natural number such that

$$\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ times}} = 0_R.$$

If no such n exists, we say that char(R) = 0.