WHAT IS A RING

Kechao Chen

April 2021

A ring is an extension of the abelian group in the sense that a ring consists of both the commutative + ("addition") operation of an abelian group and a \times ("multiplication") operation (whose symbol is often neglected in practice). These properties can be defined naturally on the endomorphisms of any abelian groups.

Addition on $\operatorname{End}_{\mathsf{Abel}}A$ is inherited from the addition of A in the sense that for all $\phi, \psi \in \operatorname{End}_{\mathsf{Abel}}A$, there is a

$$\phi + \psi : a \mapsto \phi \, a + \psi \, a$$

One can easily check that indeed $\phi + \psi \in \text{End}_{\mathsf{Abel}} A$.

$$(\phi + \psi)(a + b) = \phi(a + b) + \psi(a + b)$$

$$= \phi a + \phi b + \psi a + \psi b$$

$$= \phi a + \psi a + \phi b + \psi b$$

$$= (\phi + \psi) a + (\phi + \psi) b$$

Notice that the commutativity of A is necessary, otherwise $\phi + \psi$ would not have been a group homomorphism. That is, addition cannot be defined on $\operatorname{End}_{\mathsf{Grp}}G$. The additive identity of $\operatorname{End}_{\mathsf{Abel}}A$ is the trivial map 0 and the inverse of ϕ is $-\phi$ defined by

$$-\phi: a \mapsto -(\phi a)$$

Which is yet another map that is a homomorphism if and only if A is abelian.

The multiplication operation is defined by the natural composition of homomorphisms in $\operatorname{End}_{\mathsf{Abel}}A.$

$$\psi \times \phi := \psi \circ \phi$$

Therefore the multiplicative identity is the identity map $id \in End_{Abel}A$.

The two operations of a ring corresponds naturally by the two distributive properties.

$$\theta \times (\phi + \psi) = \theta \times \phi + \theta \times \psi$$

and

$$(\phi + \psi) \times \theta = \phi \times \theta + \psi \times \theta$$

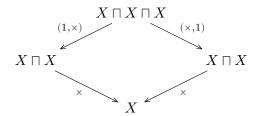
This is because for all $a \in A$,

$$\begin{aligned} \theta \times (\phi + \psi) \, a &= \theta \times (\phi \, a + \psi \, a) \\ &= \theta \times \phi \, a + \theta \times \psi \, a \\ &= (\theta \times \phi + \theta \times \psi) \, a. \end{aligned}$$

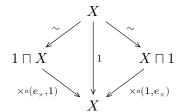
The right distributive property is given by the same reasoning.

The following commutative diagrams categorize the additional axioms of the *ring object*, making it an extension of the abelian group object. (A ring object is the information $(+, e_+, -, \times, e_\times)$.)

• Multiplicative associativity:



• Multiplicative identity:



• Left distributivity:

• Right distributivity:

Some may question the choice of using $\operatorname{End}_{\mathsf{Abel}}A$ instead of $\operatorname{Aut}_{\mathsf{Abel}}A$ as the multiplicative structure for a ring. This is because addition is not well defined on the automorphisms of abelian groups.

A simple explanation is that $\operatorname{Aut}_{\mathsf{Abel}} A$ does not contain the trivial map 0 that is the identity of the abelian group. In fact, $\operatorname{Aut}_{\mathsf{Abel}} A$ is not even closed under addition. Given that $1 \in \operatorname{Aut}_{\mathsf{Abel}} A$, one can always construct maps

$$m1 := \underbrace{1 + \dots + 1}_{m} : g \mapsto mg.$$

In particular, lcm(|a|, |b|) id maps both a and b onto the identity, which is not an isomorphism.

A ring is a division ring if $\operatorname{End}_{\mathsf{Abel}} A \setminus \{0\} = \operatorname{Aut}_{\mathsf{Abel}} A$. One can then show that $\operatorname{End}_{\mathsf{Abel}} A$ is a division ring if and only if all elements other than the identity of A have the same order.

A commutative division ring is a *field*.

On the other hand, a weaker notion of a ring is that of a pseudo-ring. Take an arbitrary ring R, $mR := \{mr : m \in \mathbb{Z}, r \in R\}$ is a ring if and only if for some $r \in R$, mr = 1, otherwise mR is a ring without multiplicative identity, making it a pseudo-ring.