

# Rings

Giannis Tyrovolas

January 24, 2020

## 1 Introduction

In the “beautiful” mental position that is Hilary of the second year I decided to study rings. What is a ring? Why is it important? We will hopefully learn. But quite possibly not. Let’s end this section with a quote.

If you liked it then you shoulda put a ring on it - Beyonce

## 2 Recap on rings

Let’s start this section with the obvious thing we should define. The ring!

**Definition 2.1** (Ring). A ring  $(R, +, \times)$  is made of a set  $R$  (also called the carrier set) and two binary operations  $+: R \times R \longrightarrow R$ ,  $\times: R \times R \longrightarrow R$ . Such that:

1.  $(R, +)$  is an abelian group.
2.  $\times$  is associative
3.  $\times$  distributes over  $+$  i.e.  $\forall a, b, c \in R$

$$a \times (b + c) = a \times b + a \times c \text{ and } (a + b) \times c = a \times c + b \times c$$

If  $R$  has a multiplicative identity we call  $R$  *unital*

**Theorem 2.2** (Basic properties). 1. *Zero is annihilating:*  $\forall r \in R \ 0_R r = 0_R = r 0_R$

2.  $(-x)y = -xy = x(-y)$

*Proof.* 1.  $0_R r = (0_R + 0_R)r = 0_R r + 0_R r \implies 0_R r = 0_R$

2.  $xy + (-x)y = (x - x)y = 0_R y = 0_R$  Hence by the uniqueness of the inverse of  $-xy$ ,  $(-x)y = -xy$ . Similarly for  $x(-y)$

□

**Definition 2.3** (Unit group). For a *unital* ring  $R$  denote  $U(R)$  the set of  $r \in R$  with a multiplicative inverse.

**Theorem 2.4.**  $(U(R), \times)$  is a group.

*Proof.* 1. Associativity is inherited

2. Identity:  $1_R \in U(R)$  trivially.

3. Inverse: By definition of  $U(R)$

4. Closure: Let  $x, y \in U(R)$  then  $\exists x^{-1}, y^{-1} \in U(R)$ .  
Then  $(xy)(y^{-1}x^{-1}) = 1_R \implies xy \in U(R)$

□

**Definition 2.5** (Subrings). Let  $R$  be a ring and  $S \subseteq R$  such that  $S$  is a ring. Then  $S$  is a subring. If  $R$  is a unital ring and  $1_R \in S$  then  $S$  is a unital subring.

**Lemma 2.6** (Closure of intersection). Let  $\mathcal{Q}$  a set of subrings of a ring  $R$ . Then  $\bigcap_{S \in \mathcal{Q}} S$  is a subring of  $R$ .

**Definition 2.7** (Generated Subring).

$$S[\lambda_1, \dots, \lambda_n] = \bigcap \{T : T \text{ is a subring of } R \text{ and } \lambda_1, \dots, \lambda_n \in T \text{ and } S \subseteq T\}$$

**Definition 2.8** (Homomorphisms). Let  $\phi : R \longrightarrow S$  where  $R, S$  rings. And  $\forall x, y \in R$ :

$$\phi(x + y) = \phi(x) + \phi(y) \quad \text{and} \quad \phi(xy) = \phi(x)\phi(y)$$

Then  $\phi$  is a homomorphism.

If  $R, S$  are unital and  $\phi(1_R) = 1_S$  then  $\phi$  is a unital homomorphism.

**Lemma 2.9** (Inverses). Let  $\phi : R \longrightarrow S$  a homomorphism. Then  $\phi(0_R) = 0_S$  and  $\forall r \in R$ ,  $\phi(-r) = -\phi(r)$ . If  $\phi$  is unital then  $\forall x \in U(R)$ ,  $\phi(x) \in U(S)$  and  $\phi(x)^{-1} = \phi(x^{-1})$ .

*Proof.*

$$\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R) \implies \phi(0_R) = 0_S$$

$$0_S = \phi(0_R) = \phi(x) + \phi(-x) \implies \phi(-x) = -\phi(x)$$

Similarly for  $\phi(x)^{-1} = \phi(x^{-1})$

□

### 3 Integral Domains and Polynomials

**Definition 3.1** (Zero dividers).  $r \in R$  is a (left) *zero divider* if  $\exists s \in R^*$  such that  $rs = 0_R$

**Definition 3.2** (Integral Domains).  $R$  is an integral domain if it is a non-trivial, commutative, unital ring with no zero-divisors.

**Lemma 3.3.** If  $R$  is an integral domain then if  $x \in R^*$   $xy = xz \implies y = z$

*Proof.*

$$0_R = xy - xz = x(y - z) \implies y - z = 0 \implies y = z \text{ since } x \text{ is not a zero-divider}$$

□

**Theorem 3.4.** *A finite integral domain is a field.*

*Proof.* Consider  $R \longrightarrow R, x \mapsto ax$  where  $a \in R^*$ . This map is injective by cancellation. Since  $R$  is finite it is also surjective and hence  $r \in R$  such that  $ar = 1_R = ra$ . So  $a$  has an inverse and since  $a$  is arbitrary  $R$  is a field. □