

# C2 Algebra

Robin Adams

August 20, 2022

## 1 Groups

**Definition 1** (Group). A *group* is a triple  $(G, \cdot, e)$  where  $G$  is a set,  $\cdot$  is a binary operation on  $G$ , and  $e \in G$ , such that:

1.  $\cdot$  is associative.
2.  $\forall x \in G. xe = ex = x$
3.  $\forall x \in G. \exists y \in G. xy = yx = e$

**Lemma 2.** *The integers  $\mathbb{Z}$  form a group under  $+$  and  $0$ .*

PROOF: Easy.  $\square$

**Lemma 3.** *In any group, inverses are unique.*

PROOF: Suppose  $y$  and  $z$  are inverses to  $x$ . Then

$$y = ey = zxy = ze = z$$

$\square$

**Definition 4.** We write  $x^{-1}$  for the inverse of  $x$ .

## 2 Abelian Groups

**Definition 5** (Abelian Group). A group  $(G, +, 0)$  is *Abelian* iff  $+$  is commutative.

When using additive notation (i.e. the symbols  $+$  and  $0$ ) for a group, we write  $-y$  for the inverse of  $y$ , and  $x - y$  for  $x + (-y)$ .

**Lemma 6.** *The integers  $\mathbb{Z}$  are Abelian.*

PROOF: Easy.  $\square$

**Lemma 7.** *The rationals  $\mathbb{Q}$  form an Abelian group under  $+$ .*

PROOF: Easy.

**Lemma 8.** *The non-zero rationals form an Abelian group under multiplication.*

PROOF: Easy.  $\square$

### 3 Ring Theory

**Definition 9** (Commutative Ring). A *commutative ring* is a quintuple  $(R, +, \cdot, 0, 1)$  consisting of a set  $R$ , binary operations  $+$  and  $\cdot$  on  $R$ , and elements  $0, 1 \in R$  such that:

1.  $(R, +, 0)$  is an Abelian group.
2. The operation  $\cdot$  is commutative, associative, and distributive over  $+$ .
3.  $\forall x \in R. x1 = x$
4.  $0 \neq 1$

**Definition 10** (Integral Domain). An *integral domain* is a ring such that, whenever  $xy = 0$ , then  $x = 0$  or  $y = 0$ .

**Lemma 11.** *The integers form an integral domain.*

PROOF: Easy.  $\square$

### 4 Field Theory

**Definition 12** (Field). A *field* is an integral domain such that every non-zero element has a multiplicative inverse.

**Definition 13** (Field of Fractions). Let  $R$  be an integral domain. The *field of fractions* of  $R$  is  $(R \times (R - \{0\})) / \sim$ , where  $(a, b) \sim (c, d)$  iff  $ad = bc$ , under the following operations:

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(ad + bc, bd)] \\ [(a, b)][(c, d)] &= [(ac, bd)] \\ 0 &= [(0, 1)] \\ 1 &= [(1, 1)] \end{aligned}$$

It is routine to check that  $\sim$  is an equivalence relation and the operations are well-defined and form a field. The additive inverse of  $[(a, b)]$  is  $[(-a, b)]$ , and the multiplicative inverse of  $[(a, b)]$  is  $[(b, a)]$ .

**Definition 14** (Rational Numbers). The field of *rational numbers*  $\mathbb{Q}$  is the field of fractions of the integers.