

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.

5 Rational Numbers

Lemma 15. *If $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$ and b, b', d, d' are all positive then $ad < bc$ iff $a'd' < b'c'$.*

PROOF: Easy.

Definition 16. The ordering on the rationals is defined by: if b and d are positive then $[(a, b)] < [(c, d)]$ iff $ad < bc$.

Theorem 17. *The relation $<$ is a linear ordering on \mathbb{Q} .*

PROOF: Easy. \square

Definition 18 (Positive). A rational q is *positive* iff $0 < q$.

Definition 19 (Absolute Value). The *absolute value* of a rational q is the rational $|q|$ defined by

$$|q| = \begin{cases} q & \text{if } q \geq 0 \\ -q & \text{if } q \leq 0 \end{cases}$$

Theorem 20. *For any rational s , the function that maps q to $q + s$ is strictly monotone.*

PROOF: Easy. \square

Theorem 21. *For any positive rational s , the function that maps q to qs is strictly monotone.*

PROOF: Easy. \square

Theorem 22. *Define $E : \mathbb{Z} \rightarrow \mathbb{Q}$ by $E(a) = [(a, 1)]$. Then E is one-to-one and:*

1. $E(a + b) = E(a) + E(b)$
2. $E(ab) = E(a)E(b)$
3. $E(0) = 0$
4. $E(1) = 1$
5. $a < b$ iff $E(a) < E(b)$

PROOF: Easy. \square

6 Ordered Fields

Definition 23 (Ordered Field). An *ordered field* is a sextuple $(D, +, \cdot, 0, 1, <)$ such that $(D, +, \cdot, 0, 1)$ is a field, $<$ is a linear ordering on D , and:

$$\begin{aligned} \forall x, y, z. x < y &\Leftrightarrow x + z < y + z \\ \forall x, y, z. 0 < z &\Rightarrow (x < y \Leftrightarrow xz < yz) \end{aligned}$$

7 The Real Numbers

Definition 24 (Dedekind Cut). A *real number* or *Dedekind cut* is a subset x of \mathbb{Q} such that:

1. $\emptyset \neq x \neq \mathbb{Q}$
2. x is *closed downwards*, i.e. for all $q \in x$, if $r \in \mathbb{Q}$ and $r < q$ then $r \in x$.
3. x has no largest member.

Let \mathbb{R} be the set of all real numbers.

Definition 25. Given real numbers x and y , we write $x < y$ iff $x \subset y$.

Theorem 26. The relation $<$ is a linear ordering on \mathbb{R} .

PROOF: The only hard part is proving that, for any reals x and y , either $x \subseteq y$ or $y \subseteq x$.

Suppose $x \not\subseteq y$. Pick $q \in x$ such that $q \notin y$. Let $r \in y$. Then $q \not< r$ (since y is closed downwards) therefore $r < q$. Hence $r \in x$ (because x is closed downwards). \square

Theorem 27. Any nonempty set A of reals bounded above has a least upper bound.

PROOF: We prove that $\bigcup A$ is a Dedekind cut. It is then the least upper bound of A .

The set $\bigcup A$ is nonempty because A is nonempty. Pick an upper bound r for A , and a rational $q \notin r$; then $q \notin \bigcup A$, so $\bigcup A \neq \mathbb{Q}$.

$\bigcup A$ is closed downwards because every member of A is closed downwards.

$\bigcup A$ has no largest member because every member of A has no largest member. \square

Definition 28 (Addition). *Addition* $+$ on \mathbb{R} is defined by:

$$x + y = \{q + r \mid q \in x, r \in y\} .$$

We prove this is a Dedekind cut.

PROOF:

$\langle 1 \rangle 1. x + y \neq \emptyset$

PROOF: Pick $q \in x$ and $r \in y$. Then $q + r \in x + y$.

$\langle 1 \rangle 2. x + y \neq \mathbb{Q}$

$\langle 2 \rangle 1.$ PICK $q \in \mathbb{Q} - x$ and $r \in \mathbb{Q} - y$

$\langle 2 \rangle 2.$ For all $q' \in x$ we have $q' < q$

$\langle 2 \rangle 3.$ For all $r' \in y$ we have $r' < r$

$\langle 2 \rangle 4.$ For all $q' \in x$ and $r' \in y$ we have $q' + r' < q + r$

$\langle 2 \rangle 5. q + r \notin x + y$

$\langle 1 \rangle 3. x + y$ is closed downwards.

- $\langle 2 \rangle 1.$ LET: $q \in x$ and $r \in y$
- $\langle 2 \rangle 2.$ LET: $s < q + r$
- $\langle 2 \rangle 3.$ $s - q < r$
- $\langle 2 \rangle 4.$ $s - q \in y$
- $\langle 2 \rangle 5.$ $s = q + (s - q) \in x + y$
- $\langle 1 \rangle 4.$ $x + y$ has no largest member.
- $\langle 2 \rangle 1.$ LET: $q \in x$ and $r \in y$
- $\langle 2 \rangle 2.$ PICK $q' \in x$ with $q < q'$
- $\langle 2 \rangle 3.$ PICK $r' \in y$ with $r < r'$
- $\langle 2 \rangle 4.$ $q' + r' \in x + y$ and $q + r < q' + r'$

□

Theorem 29. *Addition is associative and commutative.*

PROOF: Easy. □

Definition 30 (Zero). The real number zero is $0 = \{q \in \mathbb{Q} : q < 0\}$.

It is easy to check this is a Dedekind cut.

Theorem 31. *For every real x we have $x + 0 = x$.*

PROOF:

- $\langle 1 \rangle 1.$ $x + 0 \subseteq x$

PROOF: Let $q \in x$ and $r \in 0$. Then $q + r < q$ so $q + r \in x$.

- $\langle 1 \rangle 2.$ $x \subseteq x + 0$

PROOF: Let $q \in x$. Pick $r \in x$ such that $q < r$. Then $q - r \in 0$ and $q = r + (q - r) \in x + 0$.

□