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. □

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

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

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

□

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. □

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. □

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. □

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 $E : \mathbb{Z} \to \mathbb{Q}$ 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 $(D, +, \cdot, \cdot, 0, 1, <)$ such that $(D, +, \cdot, 0, 1)$ is a field, $<$ is a linear ordering on D, and:

$$\forall x, y, z. x < y \Leftrightarrow x + z < y + z$$
$$\forall x, y, z. 0 < z \Rightarrow (x < y \Leftrightarrow xz < yz)$$

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 $x \nsubseteq y$. Pick $q \in x$ such that $q \notin y$. Let $r \in y$. Then $q \nless r$ (since y is closed downwards) therefore $r < q$. Hence $r \in x$ (because x is closed downwards). □

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.
□

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

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

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 $q = r + (q - r) \in x + 0$.
□

Definition 32. For any real x, define

$$-x = \{r \in \mathbb{Q} : \exists s > r. -s \notin x\} \ .$$

We prove this is a Dedekind cut.

PROOF:
$\langle 1 \rangle 1.$ $-x \neq \emptyset$
PROOF: Pick s such that $s \notin x$. Then $-s - 1 \in -x$.
$\langle 1 \rangle 2.$ $-x \neq \mathbb{Q}$
$\langle 2 \rangle 1.$ PICK $r \in x$
PROVE: $-r \notin -x$
$\langle 2 \rangle 2.$ ASSUME: for a contradiction $-r \in -x$
$\langle 2 \rangle 3.$ PICK $s > -r$ such that $-s \notin x$
$\langle 2 \rangle 4.$ $-s < r$
$\langle 2 \rangle 5.$ $-s \in x$
$\langle 2 \rangle 6.$ Q.E.D.
PROOF: This is a contradiction.
$\langle 1 \rangle 3.$ $-x$ is closed downwards.
PROOF: Easy.

$\langle 1 \rangle 4.$ $-x$ has no largest element.

$\langle 2 \rangle 1.$ LET: $r \in -x$

$\langle 2 \rangle 2.$ PICK $s > r$ such that $-s \notin x$

$\langle 2 \rangle 3.$ PICK q such that $r < q < s$

$\langle 2 \rangle 4.$ $r < q$ and $q \in -x$

□

Lemma 33. *For any positive integer a and integer b, there exists a natural number k such that $b < ak$.*

PROOF: Take $k = |b| + 1$. □

Lemma 34. *For any positive rational p and rational r, there exists a natural number k such that $r < pk$.*

PROOF: Let $p = a/b$ and $r = c/d$ where a, b and d are positive. By Lemma 33, pick k such that $bc < adk$. Then $r < pk$. □

Lemma 35. *Let p be a positive real number. For any real x, there exists $q \in x$ such that $p + q \notin x$.*

PROOF:

$\langle 1 \rangle 1.$ PICK rationals $r_1 \in x$ and $r_2 \notin x$

$\langle 1 \rangle 2.$ There exists a natural number k such that $kp > r_2 - r_1$

PROOF: By Lemma 34.

$\langle 1 \rangle 3.$ LET: k be least such that $r_1 + kp \notin x$

$\langle 1 \rangle 4.$ $k \neq 0$

PROOF: Since $r_1 \in x$.

$\langle 1 \rangle 5.$ LET: $q = r_1 + (k-1)p$

$\langle 1 \rangle 6.$ $q \in x$

PROOF: By minimality of k.

$\langle 1 \rangle 7.$ $q + p \notin x$

□

Theorem 36. *For any real x we have $x + (-x) = 0$.*

PROOF:

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

$\langle 2 \rangle 1.$ LET: $q \in x$ and $r \in -x$

$\langle 2 \rangle 2.$ PICK $s > r$ such that $-s \notin x$

$\langle 2 \rangle 3.$ $q < -s$

$\langle 2 \rangle 4.$ $q < -r$

$\langle 2 \rangle 5.$ $q + r < 0$

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

$\langle 2 \rangle 1.$ LET: $p < 0$

$\langle 2 \rangle 2.$ PICK $q \in x$ such that $q - p/2 \notin x$

PROOF: By Lemma 35.

$\langle 2 \rangle 3.$ LET: $s = p/2 - q$

$\langle 2 \rangle 4.$ $-s \notin x$

$\langle 2\rangle 5.$ $p - q \in -x$

PROOF: Since $p - q < s$ and $-s \notin x$.

$\langle 2\rangle 6.$ $p = q + (p - q) \in x + (-x)$

$\square$

Theorem 37. *The reals form an Abelian group under addition.*

PROOF: Easy. $\square$

Theorem 38. *For any real z, the function that maps x to $x + z$ is strictly monotone.*

PROOF:

$\langle 1\rangle 1.$ ASSUME: $x < y$

$\langle 1\rangle 2.$ $x + z \subseteq y + z$

PROOF: From the definition.

$\langle 1\rangle 3.$ $x + z \neq y + z$

PROOF: By cancellation.

$\square$

Definition 39 (Absolute Value)**.** The *absolute value* of a real number x is

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

Definition 40 (Multiplication)**.** Given real numbers x, y, define the real xy by:

- If $x \geq 0$ and $y \geq 0$ then

$$xy = 0 \cup \{rs : 0 \leq r \in x, 0 \leq s \in y\}$$

- If $x \geq 0$ and $y < 0$ then $xy = -(x(-y))$
- If $x < 0$ and $y \geq 0$ then $xy = -((-x)y)$
- If $x < 0$ and $y < 0$ then $xy = (-x)(-y)$

We prove this is a Dedekind cut.

PROOF:

$\langle 1\rangle 1.$ LET: $x \geq 0$ and $y \geq 0$

$\langle 1\rangle 2.$ $xy \neq \emptyset$

PROOF: Since $-1 \in xy$

$\langle 1\rangle 3.$ $xy \neq \mathbb{Q}$

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

$\langle 2\rangle 2.$ For all r' with $0 \leq r' \in x$ and s' with $0 \leq s' \in y$ we have $r' < r$ and $s' < s$ so $r's' < rs$

$\langle 2\rangle 3.$ $rs \notin xy$

$\langle 1 \rangle 4.$ xy is closed downwards.
$\langle 2 \rangle 1.$ LET: $q \in xy$ and $r < q$
$\langle 2 \rangle 2.$ ASSUME: $0 \leq r$
$\langle 2 \rangle 3.$ PICK rationals a, b with $0 \leq a \in x$ and $0 \leq b \in y$ such that $q = ab$
$\langle 2 \rangle 4.$ $a \neq 0$ or $b \neq 0$
PROOF: Since $q \neq 0$ because $0 \leq r < q$.
$\langle 2 \rangle 5.$ ASSUME: w.l.o.g. $a \neq 0$
$\langle 2 \rangle 6.$ $r/a < b$
$\langle 2 \rangle 7.$ $r/a \in y$
$\langle 2 \rangle 8.$ $r = a(r/a) \in xy$
$\langle 1 \rangle 5.$ xy has no greatest element.
$\langle 2 \rangle 1.$ LET: $q \in xy$
PROVE: There exists $r \in xy$ such that $q < r$
$\langle 2 \rangle 2.$ ASSUME: w.l.o.g. $0 \leq q$
$\langle 2 \rangle 3.$ PICK rationals a and b with $0 \leq a \in x$ and $0 \leq b \in y$ such that $q = ab$
$\langle 2 \rangle 4.$ PICK rationals a' and b' with $a < a' \in x$ and $b < b' \in y$
$\langle 2 \rangle 5.$ $q < a'b' \in xy$
∎

Theorem 41. *Multiplication is commutative and associative.*

PROOF: Easy. ∎

Theorem 42. *Multiplication is distributive over addition.*

PROOF: See E. Mendelson. *Number Systems and the Foundations of Analysis.* Appendix F. ∎

Definition 43. The real number *one* is $1 = \{q \in \mathbb{Q} : q < 1\}$.
It is easy to check this is a Dedekind cut.

Theorem 44. $0 \neq 1$

PROOF: $0 \in 1$ and $0 \notin 0$. ∎

Theorem 45. *For any real x, $x1 = x$.*

PROOF:
$\langle 1 \rangle 1.$ LET: $x \in \mathbb{R}$
PROVE: $x1 = x$
$\langle 1 \rangle 2.$ CASE: $0 \leq x$
$\langle 2 \rangle 1.$ $x1 \subseteq x$
$\langle 3 \rangle 1.$ LET: $q \in x1$
PROVE: $q \in x$
$\langle 3 \rangle 2.$ CASE: $q < 0$
PROOF: Then $q \in x$ because $0 \leq x$.
$\langle 3 \rangle 3.$ CASE: There exist nonnegative rationals $r \in x$, $s \in 1$ such that $q = rs$
PROOF: Then $q < r \in x$ so $q \in x$.
$\langle 2 \rangle 2.$ $x \subseteq x1$

$\langle 3 \rangle 1.$ LET: $q \in x$
$\langle 3 \rangle 2.$ ASSUME: w.l.o.g. $0 \leq q$
$\langle 3 \rangle 3.$ PICK $r \in x$ with $q < r$
$\langle 3 \rangle 4.$ $0 \leq q/r < 1$
$\langle 3 \rangle 5.$ $q = r(q/r) \in x1$
$\langle 1 \rangle 3.$ CASE: $x < 0$
PROOF: Then $x1 = -((-x)1) = -(-x) = x.$
$\square$

Theorem 46. *For any nonzero real x, there is a nonzero real y such that $xy = 1$.*

PROOF: See E. Mendelson. *Number Systems and the Foundations of Analysis.* Appendix F. $\square$

Theorem 47. *For any positive real z, the function that maps x to xz is strictly monotone.*

PROOF: See E. Mendelson. *Number Systems and the Foundations of Analysis.* Appendix F. $\square$

8 Complete Ordered Fields

Definition 48 (Complete Ordered Field)**.** An ordered field is *complete* iff it has the least upper bound property.

Theorem 49. *The reals form a complete ordered field.*

PROOF: From the results above. $\square$

Theorem 50. *Any two complete ordered fields are isomorphic.*

PROOF: See A. Gleason. Fundamentals of Abstract Analysis p. 110. $\square$

Theorem 51. *Define $E : \mathbb{Q} \to \mathbb{R}$ by $E(q) = \{p \in \mathbb{Q} : p < q\}$. Then E is one-to-one and*

1. $E(q + r) = E(q) + E(r)$
2. $E(qr) = E(q)E(r)$
3. $E(0) = 0$
4. $E(1) = 1$
5. $q < r$ *iff* $E(q) < E(r)$

PROOF:
$\langle 1 \rangle 1.$ For all $q \in \mathbb{Q}$, $E(q)$ is a Dedekind cut.
PROOF: Easy.
$\langle 1 \rangle 2.$ $\forall q, r \in \mathbb{Q}. E(q + r) = E(q) + E(r)$

⟨2⟩1. LET: $q, r \in \mathbb{Q}$

⟨2⟩2. $E(q+r) \subseteq E(q) + E(r)$

⟨3⟩1. LET: $t \in E(q+r)$

⟨3⟩2. LET: $\epsilon = (r+s-t)/2$

⟨3⟩3. $\epsilon > 0$

⟨3⟩4. LET: $p = r - \epsilon$

⟨3⟩5. LET: $q = s - \epsilon$

⟨3⟩6. $p < r$

⟨3⟩7. $q < s$

⟨3⟩8. $p + q = t$

⟨3⟩9. $t \in E(r) + E(s)$

⟨2⟩3. $E(q) + E(r) \subseteq E(q+r)$

PROOF: If $p < q$ and $s < r$ then $p + s < q + r$.

⟨1⟩3. $\forall q, r \in \mathbb{Q}. E(qr) = E(q)E(r)$

PROOF: TODO

⟨1⟩4. $E(0) = 0$

PROOF: By definition.

⟨1⟩5. $E(1) = 1$

PROOF: By definition.

⟨1⟩6. E is strictly monotone.

PROOF: If $q < r$ then $E(q) \subseteq E(r)$ by transitivity of $<$ on $\mathbb{Q}$, and $E(q) \neq E(r)$ because $q \in E(r)$ and $q \notin E(q)$.

$\square$