Encyclopaedia of Mathematics and Physics

Robin Adams

Contents

1 Relations **5**

2 Order Theory **7**

3 Field Theory **9**

3.1 Ordered Fields 11

4 Real Analysis **13**

4.1 Construction of the Real Numbers 13

Chapter 1

Relations

Definition 1.1 (Antisymmetric)**.** A relation R on a set A is *antisymmetric* iff, whenever xRy and yRx, then $x = y$.

Definition 1.2 (Transitive)**.** A relation R on a type A is *transitive* iff, whenever xRy and yRz, then xRz.

Chapter 2

Order Theory

Definition 2.1 (Linear Order). A *linear order* on a set A is a binary relation $\leq$ on A that is transitive, antisymmetric and:

$$\forall x, y \in A. x \leq y \vee y \leq x \ .$$

A *linearly ordered set* is a pair $(A, \leq)$ where A is a set and $\leq$ is a binary relation on A.

We write $x < y$ for $x \leq y$ and $x \neq y$.

Definition 2.2 (Upper Bound). Let S be a linearly ordered set, $u \in S$ and $E \subseteq S$. Then u is an *upper bound* in E iff $\forall x \in E. x \leq u$. We say E is *bounded above* iff it has an upper bound.

The *up-set* of E, denoted $E \uparrow$, is the set of upper bounds of E.

Definition 2.3 (Lower Bound). Let S be a linearly ordered set, $l \in S$ and $E \subseteq S$. Then u is an *lower bound* in E iff $\forall x \in E. l \leq x$. We say E is *bounded below* iff it has a lower bound.

The *down-set* of E, denoted $E \downarrow$, is the set of lower bounds of E.

Definition 2.4 (Supremum). Let S be a linearly ordered set, $u \in S$ and $E \subseteq S$. Then u is the *least upper bound* or *supremum* of E iff u is an upper bound for E and, for any upper bound u' for E, we have $u \leq u'$.

Definition 2.5 (Infimum). Let S be a linearly ordered set, $l \in S$ and $E \subseteq S$. Then l is the *greatest lower bound* or *infimum* of E iff l is a lower bound for E and, for any lower bound l' for E, we have $l' \leq l$.

Definition 2.6 (Least Upper Bound Property). A linearly ordered set S has the *least upper bound property* iff every nonempty subset of S that is bounded above has a least upper bound.

Proposition 2.7. *Let S be a linearly ordered set and $E \subseteq S$.*

1. *If $E \downarrow$ has a supremum l, then l is the infimum of E.*

2. If $E\uparrow$ has an infimum u, then U is the supremum of E.

PROOF:
⟨1⟩1. If $E\downarrow$ has a supremum l, then l is the infimum of E.
⟨2⟩1. l is a lower bound for E.
⟨3⟩1. LET: $x \in E$
⟨3⟩2. x is an upper bound for $E\downarrow$.
PROOF: For all $y \in E\downarrow$ we have $y \leq x$.
⟨3⟩3. $l \leq x$
⟨2⟩2. For any lower bound l' for E, we have $l' \leq l$.
PROOF: Since l is an upper bound for $E\downarrow$.
⟨1⟩2. If $E\uparrow$ has an infimum u, then u is the supremum of E.
PROOF: Dual.
□

Corollary 2.7.1. *A linearly ordered set has the least upper bound property if and only if every nonempty set bounded below has an infimum.*

Definition 2.8 (Closed Downwards)**.** Let S be a linearly ordered set and $E \subseteq S$. Then E is *closed downwards* iff, whenever $x \in E$ and $y < x$, then $y \in E$.

Definition 2.9 (Closed Upwards)**.** Let S be a linearly ordered set and $E \subseteq S$. Then E is *closed upwards* iff, whenever $x \in E$ and $x < y$, then $y \in E$.

Definition 2.10 (Greatest)**.** Let S be a linearly ordered set and $u \in S$. Then u is *greatest* in S iff $\forall x \in S.x \leq u$.

Definition 2.11 (Least)**.** Let S be a linearly ordered set and $l \in S$. Then l is *least* in S iff $\forall x \in S.l \leq x$.

Proposition 2.12. *Let $\leq$ be a linear order on a set S and $E \subseteq S$. Then $\leq \cap E^2$ is a linear order on E.*

PROOF: Easy. □

Given a linearly ordered set $(S, \leq)$ and $E \subseteq S$, we write just E for the linearly ordered set $(E, \leq \cap E^2)$.

Chapter 3

Field Theory

Definition 3.1 (Field)**.** A *field* F consists of a set F, two operations $+, \cdot : F^2 \to F$ and an element $0 \in F$ such that:

- $+$ is commutative.
- $+$ is associative.
- $\forall x \in F. x + 0 = x$
- $\forall x \in F. \exists y \in F. x + y = 0$
- $\cdot$ is commutative.
- $\cdot$ is associative.
- There exists $1 \in F$ such that $1 \neq 0$ and $\forall x \in F. x1 = x$ and $\forall x \in F. x \neq 0 \Rightarrow \exists y \in F. xy = 1$
- *Distributive Law* $\forall x, y, z \in F. x(y + z) = xy + xz$

Proposition 3.2. *In any field F, the element 0 is the unique element such that $\forall x \in F. x + 0 = x$.*

Proof: If 0 and $0'$ both have this property then $0 = 0 + 0' = 0'$. □

Proposition 3.3. *In any field F, given $x \in F$, there is a unique $y \in F$ such that $x + y = 0$.*

Proof: If $x + y = x + y' = 0$ then

$$\begin{aligned} y &= y + 0 \\ &= y + x + y' \\ &= 0 + y' \\ &= y' \end{aligned}$$

□

Definition 3.4. Let F be a field. Let $x \in F$. We denote by $-x$ the unique element of F such that $x + (-x) = 0$.

Given $x, y \in F$, we write $x - y$ for $x + (-y)$.

Proposition 3.5. *In any field F, if $x + y = x + z$ then $y = z$.*

PROOF: If $x + y = x + z$ we have

$$\begin{aligned} -x + x + y &= -x + x + z \\ \therefore 0 + y &= 0 + z \\ \therefore y &= z \end{aligned}$$

∎

Proposition 3.6. *In any field F, we have $-(-x) = x$.*

PROOF: Since $x + (-x) = 0$. ∎

Proposition 3.7. *In any field F, the element 1 such that $\forall x \in F. x1 = x$ is unique.*

PROOF: If 1 and $1'$ both have this property then $1 = 1 \cdot 1' = 1'$. ∎

Proposition 3.8. *In any field F, given $x \in F$ with $x \neq 0$, the element y such that $xy = 1$ is unique.*

PROOF: If y and y' both have this property then we have

$$\begin{aligned} y &= y1 \\ &= yxy' \\ &= 1y' \\ &= y' \end{aligned}$$

∎

Definition 3.9. In any field F, if $x \neq 0$, we write x^{-1} for the unique element such that $xx^{-1} = 1$.

We write x/y for xy^{-1}.

Proposition 3.10. *In any field F, if $xy = xz$ and $x \neq 0$ then $y = z$.*

PROOF:

$$\begin{aligned} y &= 1y \\ &= x^{-1}xy \\ &= x^{-1}xz \\ &= 1z \\ &= z \end{aligned}$$

∎

Proposition 3.11. *In any field F, if $x \neq 0$ then $x^{-1} \neq 0$ and $(x^{-1})^{-1} = x$.*

PROOF: Since $xx^{-1} = 1$. ∎

Proposition 3.12. *In any field F, we have $x0 = 0$.*

PROOF:

$$\begin{aligned} x0 + 0 &= x0 \\ &= x(0 + 0) \\ &= x0 + x0 \\ \therefore 0 &= x0 \end{aligned} \qquad \square$$

Proposition 3.13. *In any field F, if $xy = 0$ then $x = 0$ or $y = 0$.*

PROOF: If $xy = 0$ and $x \neq 0$ then we have $y = x^{-1}xy = x^{-1}0 = 0$. $\square$

Proposition 3.14. *In any field F, we have $(-x)y = -(xy)$.*

PROOF:

$$\begin{aligned} xy + (-x)y &= (x + (-x))y \\ &= 0y \\ &= 0 && \text{(Proposition 3.12)}\square \end{aligned}$$

Corollary 3.14.1. *In any field F, we have $(-x)(-y) = xy$.*

PROOF:

$$\begin{aligned} (-x)(-y) &= -(x(-y)) \\ &= -(-(xy)) \\ &= xy && \text{(Proposition 3.6)}\square \end{aligned}$$

3.1 Ordered Fields

Definition 3.15 (Ordered Field)**.** An *ordered field F* consists of a field F and a linear order $\leq$ on F such that:

- For all $x, y, z \in F$, if $y < z$ then $x + y < x + z$
- For all $x, y \in F$, if $x > 0$ and $y > 0$ then $xy > 0$.

We call x *positive* iff $x > 0$ and *negative* iff $x < 0$.

Example 3.16. $\mathbb{Q}$ is an ordered field.

Proposition 3.17. *In any ordered field, if x is positive then $-x$ is negative.*

PROOF: If $x > 0$ then $0 = x + (-x) > 0 = (-x) = -x$. $\square$

Proposition 3.18. *In any ordered field, if $y < z$ and x is positive then $xy < xz$.*

PROOF: If $y < z$ then we have

$$\begin{aligned} 0 &< z - y \\ \therefore 0 &< x(z - y) \\ &= xz - xy \\ \therefore xy &< xz \end{aligned} \qquad \square$$

Proposition 3.19. *In any ordered field, if $y < z$ and x is negative then $xy > xz$.*

PROOF:
$\langle 1 \rangle 1$. $-x$ is positive.
$\langle 1 \rangle 2$. $(-x)y < (-x)z$
$\langle 1 \rangle 3$. $-(xy) < -(xz)$
$\langle 1 \rangle 4$. $xz < xy$
$\square$

Proposition 3.20. *In any ordered field, if $x \neq 0$ then $x^2 > 0$.*

PROOF:
$\langle 1 \rangle 1$. If $x > 0$ then $x^2 > 0$.
PROOF: Proposition 3.18.
$\langle 1 \rangle 2$. If $x < 0$ then $x^2 > 0$.
PROOF: Proposition 3.19.
$\square$

Corollary 3.20.1. *In any ordered field, we have $1 > 0$.*

Proposition 3.21. *In any ordered field, if x is positive then x^{-1} is positive.*

PROOF: If $x^{-1} < 0$ then we would have $1 = xx^{-1} < x0 = 0$ contradicting Corollary 3.20.1. $\square$

Proposition 3.22. *In any ordered field, if $0 < x < y$ then $y^{-1} < x^{-1}$.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: $0 < x < y$
$\langle 1 \rangle 2$. x^{-1} and y^{-1} are positive.
PROOF: Proposition 3.21.
$\langle 1 \rangle 3$. $xy^{-1} < yy^{-1} = 1$
$\langle 1 \rangle 4$. $y^{-1} = x^{-1}xy^{-1} < x^{-1}1 = x^{-1}$
$\square$

Chapter 4

Real Analysis

4.1 Construction of the Real Numbers

Definition 4.1 (Cut)**.** A *cut* is a subset α of $\mathbb{Q}$ such that:

- $\emptyset \neq \alpha \neq \mathbb{Q}$
- α is closed downwards.
- α has no greatest element.

In this section, we write R for the set of all cuts.

Proposition 4.2. *R is linearly ordered by $\subseteq$.*

PROOF: The only difficult part is to prove that, for any cuts α and β, either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.
$\langle 1 \rangle 1$. ASSUME: $\alpha \nsubseteq \beta$
PROVE: $\beta \subseteq \alpha$
$\langle 1 \rangle 2$. PICK $q \in \alpha$ such that $q \notin \beta$
$\langle 1 \rangle 3$. LET: $r \in \beta$
$\langle 1 \rangle 4$. $q \nless r$
$\langle 1 \rangle 5$. $r < q$
$\langle 1 \rangle 6$. $r \in \alpha$
□

Proposition 4.3. *R has the least upper bound property.*

PROOF:
$\langle 1 \rangle 1$. LET: $E \subseteq R$ be nonempty and bounded above.
$\langle 1 \rangle 2$. LET: $s = \bigcup E$
PROVE: s is a cut.
$\langle 1 \rangle 3$. $\emptyset \neq s$
PROOF: Since E is nonempty and every element of E is nonempty.
$\langle 1 \rangle 4$. $s \neq \mathbb{Q}$

⟨2⟩1. PICK an upper bound u for E.
⟨2⟩2. PICK $q \notin u$
PROVE: $q \notin s$
⟨2⟩3. $\forall \alpha \in E. \alpha \subseteq u$
⟨2⟩4. $s \subseteq u$
⟨2⟩5. $q \notin s$
⟨1⟩5. s is closed downwards.
⟨2⟩1. LET: $q \in s$ and $r < q$.
⟨2⟩2. PICK $\alpha \in E$ such that $q \in \alpha$.
⟨2⟩3. $r \in \alpha$
⟨2⟩4. $r \in s$
⟨1⟩6. s has no greatest element.
⟨2⟩1. LET: $q \in s$
⟨2⟩2. PICK $\alpha \in E$ such that $q \in \alpha$.
⟨2⟩3. PICK $r \in \alpha$ such that $q < r$.
⟨2⟩4. $r \in s$
□

Definition 4.4 (Addition)**.** Given cuts α and β, we define

$$\alpha + \beta = \{q + r : q \in \alpha, r \in \beta\} \ .$$

Proposition 4.5. *Given cuts α and β, we have $\alpha + \beta$ is a cut.*

PROOF:
⟨1⟩1. $\alpha + \beta$ is nonempty.
PROOF: Since α and β are nonempty.
⟨1⟩2. $\alpha + \beta \neq \mathbb{Q}$
⟨2⟩1. PICK $q \in \mathbb{Q} - \alpha$ and $r \in \mathbb{Q} - \beta$.
PROVE: $q + r \notin \alpha + \beta$
⟨2⟩2. ASSUME: for a contradiction $q + r \in \alpha + \beta$.
⟨2⟩3. PICK $x \in \alpha$ and $y \in \beta$ such that $q + r = x + y$
⟨2⟩4. $x < q$
⟨2⟩5. $y < r$
⟨2⟩6. $x + y < q + r$
⟨2⟩7. Q.E.D.
PROOF: This is a contradiction.
⟨1⟩3. $\alpha + \beta$ is closed downwards.
⟨2⟩1. LET: $q \in \alpha$, $r \in \beta$ and $x < q + r$
⟨2⟩2. $x - q < r$
⟨2⟩3. $x - q \in \beta$
⟨2⟩4. $x \in \alpha + \beta$
⟨1⟩4. $\alpha + \beta$ has no greatest element.
⟨2⟩1. LET: $q \in \alpha$ and $r \in \beta$.
PROVE: $q + r$ is not greatest in $\alpha + \beta$.
⟨2⟩2. PICK $q' \in \alpha$ with $q < q'$ and $r' \in \beta$ with $r < r'$.
⟨2⟩3. $q + r < q' + r' \in \alpha + \beta$

$\square$

Proposition 4.6. *Addition is commutative and associative on R.*

Proof: Immediate from definitions and the fact that addition is commutative and associative on $\mathbb{Q}$. $\square$

Definition 4.7. For any $q \in \mathbb{Q}$, let $q^* = \{r \in \mathbb{Q} : r < q\}$.

Proposition 4.8. *For any $q \in \mathbb{Q}$, we have q^* is a cut.*

Proof:
$\langle 1 \rangle 1.$ $q^* \neq \emptyset$
  Proof: Since $q - 1 \in q^*$.
$\langle 1 \rangle 2.$ $q^* \neq \mathbb{Q}$
  Proof: Since $q \notin q^*$.
$\langle 1 \rangle 3.$ q^* is closed downwards.
  Proof: Immediate from definition.
$\langle 1 \rangle 4.$ q^* has no greatest element.
  Proof: For all $r \in q^*$ we have $r < (q + r)/2 \in q^*$.
$\square$

Proposition 4.9. *For any cut α we have $\alpha + 0^* = \alpha$.*

Proof:
$\langle 1 \rangle 1.$ $\alpha + 0^* \subseteq \alpha$
  $\langle 2 \rangle 1.$ Let: $q \in \alpha$ and $r \in 0^*$
    Prove: $q + r \in \alpha$
  $\langle 2 \rangle 2.$ $r < 0$
  $\langle 2 \rangle 3.$ $q + r < q$
  $\langle 2 \rangle 4.$ $q + r \in \alpha$
$\langle 1 \rangle 2.$ $\alpha \subseteq \alpha + 0^*$
  $\langle 2 \rangle 1.$ Let: $q \in \alpha$
  $\langle 2 \rangle 2.$ Pick $r \in \alpha$ such that $q < r$
  $\langle 2 \rangle 3.$ $q = r + (q - r) \in \alpha + 0^*$
$\square$

Proposition 4.10. *For any cut α, there exists a cut β such that $\alpha + \beta = 0$.*

Proof:
$\langle 1 \rangle 1.$ Let: $\beta = \{p \in \mathbb{Q} : \exists r > 0. -p - r \notin \alpha\}$
$\langle 1 \rangle 2.$ β is a cut.
  $\langle 2 \rangle 1.$ $\beta \neq \emptyset$
    $\langle 3 \rangle 1.$ Pick $q \notin \alpha$
    $\langle 3 \rangle 2.$ $-q - 1 \in \beta$
  $\langle 2 \rangle 2.$ $\beta \neq \mathbb{Q}$
    $\langle 3 \rangle 1.$ Pick $q \in \alpha$
      Prove: $-q \notin \beta$
    $\langle 3 \rangle 2.$ Assume: for a contradiction $-q \in \beta$

⟨3⟩3. PICK $r > 0$ such that $q - r \notin \alpha$
⟨3⟩4. $q - r < q$
⟨3⟩5. Q.E.D.
PROOF: This contradicts the fact that α is closed downwards.
⟨2⟩3. β is closed downwards.
⟨3⟩1. LET: $p \in \beta$ and $q < p$.
⟨3⟩2. PICK $r > 0$ such that $-p - r \notin \alpha$
⟨3⟩3. $-p - r < -q - r$
⟨3⟩4. $-q - r \notin \alpha$
⟨3⟩5. $q \in \beta$
⟨2⟩4. β has no greatest element.
⟨3⟩1. LET: $p \in \beta$
⟨3⟩2. PICK $r > 0$ such that $-p - r \notin \alpha$
⟨3⟩3. $-(p + r/2) - r/2 \notin \alpha$
⟨3⟩4. $p + r/2 \in \beta$
⟨1⟩3. $\alpha + \beta \subseteq 0^*$
⟨2⟩1. LET: $p \in \alpha$ and $q \in \beta$.
⟨2⟩2. PICK $r > 0$ such that $-q - r \notin \alpha$.
⟨2⟩3. $p < -q - r$
⟨2⟩4. $p + q < -r$
⟨2⟩5. $p + q < 0$
⟨2⟩6. $p + q \in 0^*$
⟨1⟩4. $0^* \subseteq \alpha + \beta$
⟨2⟩1. LET: $v \in 0^*$
⟨2⟩2. LET: $w = -v/2$
⟨2⟩3. $w > 0$
⟨2⟩4. PICK an integer n such that $nw \in \alpha$ and $(n + 1)w \notin \alpha$.
⟨2⟩5. LET: $p = -(n + 2)w$
⟨2⟩6. $p \in \beta$
⟨2⟩7. $v = nw + p$
⟨2⟩8. $v \in \alpha + \beta$
□

Theorem 4.11. *There exists an ordered field with the least upper bound property.*

Proposition 4.12. *There is no rational p such that $p^2 = 2$.*

PROOF:
⟨1⟩1. ASSUME: for a contradiction $p^2 = 2$.
⟨1⟩2. PICK integers m, n not both even such that $p = m/n$.
⟨1⟩3. $m^2 = 2n^2$
⟨1⟩4. m is even.
⟨1⟩5. PICK an integer k such that $m = 2k$.
⟨1⟩6. $4k^2 = 2n^2$
⟨1⟩7. $2k^2 = n^2$
⟨1⟩8. n is even.

$\langle 1 \rangle 9$. Q.E.D.

PROOF: $\langle 1 \rangle 2$, $\langle 1 \rangle 4$ and $\langle 1 \rangle 8$ form a contradiction.

$\square$