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
4.2 Properties of the Real Numbers 19
4.3 The Extended Real Number System 22

5 Complex Analysis **25**

I Linear Algebra **29**

6 Vector Spaces **31**

7 Real Inner Product Spaces **33**

8 Complex Inner Product Spaces **35**
8.1 Hilbert Spaces 36

9 Lie Algebras **37**
9.1 Lie Algebar Homomorphisms 38

II More Algebra **39**

10 Lie Groups **41**

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.
$\langle 1 \rangle 2$. $(-x)y < (-x)z$
$\langle 1 \rangle 3$. $-(xy) < -(xz)$
$\langle 1 \rangle 4$. $xz < xy$
□

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.
□

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. □

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.
$\langle 1 \rangle 3$. $xy^{-1} < yy^{-1} = 1$
$\langle 1 \rangle 4$. $y^{-1} = x^{-1}xy^{-1} < x^{-1}1 = x^{-1}$
□

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.
$\langle 1 \rangle 4$. $s \neq \mathbb{Q}$

$\langle 2\rangle 1.$ Pick an upper bound u for E.
$\langle 2\rangle 2.$ Pick $q \notin u$
Prove: $q \notin s$
$\langle 2\rangle 3.$ $\forall \alpha \in E.\alpha \subseteq u$
$\langle 2\rangle 4.$ $s \subseteq u$
$\langle 2\rangle 5.$ $q \notin s$
$\langle 1\rangle 5.$ s is closed downwards.
$\langle 2\rangle 1.$ Let: $q \in s$ and $r < q$.
$\langle 2\rangle 2.$ Pick $\alpha \in E$ such that $q \in \alpha$.
$\langle 2\rangle 3.$ $r \in \alpha$
$\langle 2\rangle 4.$ $r \in s$
$\langle 1\rangle 6.$ s has no greatest element.
$\langle 2\rangle 1.$ Let: $q \in s$
$\langle 2\rangle 2.$ Pick $\alpha \in E$ such that $q \in \alpha$.
$\langle 2\rangle 3.$ Pick $r \in \alpha$ such that $q < r$.
$\langle 2\rangle 4.$ $r \in s$
$\square$

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:
$\langle 1\rangle 1.$ $\alpha + \beta$ is nonempty.
Proof: Since α and β are nonempty.
$\langle 1\rangle 2.$ $\alpha + \beta \neq \mathbb{Q}$
$\langle 2\rangle 1.$ Pick $q \in \mathbb{Q} - \alpha$ and $r \in \mathbb{Q} - \beta$.
Prove: $q + r \notin \alpha + \beta$
$\langle 2\rangle 2.$ Assume: for a contradiction $q + r \in \alpha + \beta$.
$\langle 2\rangle 3.$ Pick $x \in \alpha$ and $y \in \beta$ such that $q + r = x + y$
$\langle 2\rangle 4.$ $x < q$
$\langle 2\rangle 5.$ $y < r$
$\langle 2\rangle 6.$ $x + y < q + r$
$\langle 2\rangle 7.$ Q.E.D.
Proof: This is a contradiction.
$\langle 1\rangle 3.$ $\alpha + \beta$ is closed downwards.
$\langle 2\rangle 1.$ Let: $q \in \alpha$, $r \in \beta$ and $x < q + r$
$\langle 2\rangle 2.$ $x - q < r$
$\langle 2\rangle 3.$ $x - q \in \beta$
$\langle 2\rangle 4.$ $x \in \alpha + \beta$
$\langle 1\rangle 4.$ $\alpha + \beta$ has no greatest element.
$\langle 2\rangle 1.$ Let: $q \in \alpha$ and $r \in \beta$.
Prove: $q + r$ is not greatest in $\alpha + \beta$.
$\langle 2\rangle 2.$ Pick $q' \in \alpha$ with $q < q'$ and $r' \in \beta$ with $r < r'$.
$\langle 2\rangle 3.$ $q + r < q' + r' \in \alpha + \beta$

□

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

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

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 $r < (q + r)/2 \in q^*$.
□

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 $q < r$
  $\langle 2 \rangle 3.$ $q = r + (q - r) \in \alpha + 0^*$
□

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 $-q \in \beta$

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

Proposition 4.11. *Given $\alpha, \beta, \gamma \in R$, if $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$.*

PROOF:
$\langle 1 \rangle 1.$ $\alpha + \beta \subseteq \alpha + \gamma$
PROOF: Immediate from definitions.
$\langle 1 \rangle 2.$ $\alpha + \beta \neq \alpha + \gamma$
PROOF: If $\alpha + \beta = \alpha + \gamma$ then $\beta = \gamma$ by cancellation.
$\square$

Definition 4.12. Given cuts α and β, define $\alpha\beta$ by:

$$\alpha\beta = \begin{cases} \{p \in \mathbb{Q} : \exists r \in \alpha . \exists s \in \beta (p \leq rs \wedge r > 0 \wedge s > 0\} & \text{if } \alpha > 0^* \text{ and } \beta > 0^* \\ (-\alpha)(-\beta) & \text{if } \alpha < 0^* \text{ and } \beta < 0^* \\ -((-\alpha)\beta) & \text{if } \alpha < 0^* \text{ and } \beta > 0^* \\ -(\alpha(-\beta)) & \text{if } \alpha > 0^* \text{ and } \beta < 0^* \\ 0^* & \text{if } \alpha = 0^* \text{ or } \beta = 0^* \end{cases}$$

Proposition 4.13. *For any cuts α and β, we have $\alpha\beta$ is a cut.*

PROOF:
$\langle 1 \rangle 1$. If $\alpha > 0^*$ and $\beta > 0^*$ then $\alpha\beta$ is a cut.
  $\langle 2 \rangle 1$. $\alpha\beta \neq \emptyset$
    $\langle 3 \rangle 1$. PICK $q \in \alpha$ and $r \in \beta$ such that $q, r \notin 0^*$
    $\langle 3 \rangle 2$. ASSUME: w.l.o.g. $0 < q$ and $0 < r$.
      PROOF: Since α and β have no greatest element.
    $\langle 3 \rangle 3$. $qr \in \alpha\beta$
  $\langle 2 \rangle 2$. $\alpha\beta \neq \mathbb{Q}$
    $\langle 3 \rangle 1$. PICK $r \notin \alpha$ and $s \notin \beta$
      PROVE: $rs \notin \alpha\beta$
    $\langle 3 \rangle 2$. ASSUME: for a contradiction $rs \in \alpha\beta$.
    $\langle 3 \rangle 3$. PICK $r' \in \alpha$ and $s' \in \beta$ such that $rs \leq r's'$ and $r' > 0$ and $s' > 0$.
    $\langle 3 \rangle 4$. $r' < r$ and $s' < s$
    $\langle 3 \rangle 5$. $r's' < rs$
    $\langle 3 \rangle 6$. Q.E.D.
      PROOF: This is a contradiction.
  $\langle 2 \rangle 3$. $\alpha\beta$ is closed downwards.
    $\langle 3 \rangle 1$. LET: $p \in \alpha\beta$ and $p' < p$
    $\langle 3 \rangle 2$. PICK $r \in \alpha$ and $s \in \beta$ such that $p \leq rs$, $r > 0$ and $s > 0$
    $\langle 3 \rangle 3$. $p' \leq rs$
    $\langle 3 \rangle 4$. $p' \in \alpha\beta$
  $\langle 2 \rangle 4$. $\alpha\beta$ has no greatest element.
    $\langle 3 \rangle 1$. LET: $p \in \alpha\beta$
    $\langle 3 \rangle 2$. PICK $r \in \alpha$ and $s \in \beta$ such that $p \leq rs$, $r > 0$ and $s > 0$.
    $\langle 3 \rangle 3$. PICK $r' \in \alpha$ and $s' \in \beta$ with $r < r'$ and $s < s'$.
    $\langle 3 \rangle 4$. $p < r's' \in \alpha\beta$
$\langle 1 \rangle 2$. For any cuts α and β, we have $\alpha\beta$ is a cut.
  PROOF: Since if α is a cut then $-\alpha$ is a cut.
$\square$

Proposition 4.14. *For any cuts α and β we have $\alpha\beta = \beta\alpha$.*

PROOF: Easy from the definitions. $\square$

Proposition 4.15. *For any cuts α, β and γ we have*

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma \ .$$

PROOF:
$\langle 1\rangle 1$. CASE: α, β and γ are all positive.
PROOF: In this case $\alpha(\beta\gamma) = (\alpha\beta)\gamma = \{p \in \mathbb{Q} : \exists r \in \alpha.\exists s \in \beta.\exists t \in \gamma.(p \leq rst \wedge r > 0 \wedge s > 0 \wedge t > 0)\}$.
$\langle 1\rangle 2$. CASE: One of α, β or γ is 0^*.
PROOF: Then $\alpha(\beta\gamma) = (\alpha\beta)\gamma = 0^*$.
$\langle 1\rangle 3$. CASE: α and β are positive, γ is negative.
PROOF:

$$\begin{aligned}
\alpha(\beta\gamma) &= \alpha(-(\beta(-\gamma))) \\
&= -(\alpha(\beta(-\gamma))) \\
&= -((\alpha\beta)(-\gamma)) && (\langle 1\rangle 1) \\
&= (\alpha\beta)\gamma
\end{aligned}$$

$\langle 1\rangle 4$. CASE: α is positive, β is negative, γ is positive.
PROOF:

$$\begin{aligned}
\alpha(\beta\gamma) &= \alpha(-((-\beta)\gamma)) \\
&= -(\alpha((-\beta)\gamma)) \\
&= -((\alpha(-\beta))\gamma) && (\langle 1\rangle 1) \\
&= (-(\alpha(-\beta)))\gamma \\
&= (\alpha\beta)\gamma
\end{aligned}$$

$\langle 1\rangle 5$. CASE: α is positive, β and γ are negative.
PROOF:

$$\begin{aligned}
\alpha(\beta\gamma) &= \alpha((-\beta)(-\gamma)) \\
&= (\alpha(-\beta))(-\gamma) && (\langle 1\rangle 1) \\
&= (-(\alpha\beta))(-\gamma) \\
&= (\alpha\beta)\gamma
\end{aligned}$$

$\langle 1\rangle 6$. CASE: α is negative, β and γ are positive.
PROOF: Similar to $\langle 1\rangle 3$.
$\langle 1\rangle 7$. CASE: α is negative, β is positive, γ is negative.
PROOF:

$$\begin{aligned}
\alpha(\beta\gamma) &= \alpha(-(\beta(-\gamma))) \\
&= (-\alpha)(\beta(-\gamma)) \\
&= ((-\alpha)\beta)(-\gamma) && (\langle 1\rangle 1) \\
&= (-(\alpha\beta))(-\gamma) \\
&= (\alpha\beta)\gamma
\end{aligned}$$

$\langle 1\rangle 8$. CASE: α and β are negative, γ is positive.
PROOF: Similar to $\langle 1\rangle 5$.
$\langle 1\rangle 9$. CASE: α, β and γ are all negative.

PROOF:

$$\begin{aligned}\alpha(\beta\gamma) &= \alpha(-(-\beta)(-\gamma)) \\ &= -((-\alpha)((-\beta)(-\gamma))) \\ &= -(((-\alpha)(-\beta))(-\gamma)) && (\langle 1\rangle 1) \\ &= -((\alpha\beta)(-\gamma)) \\ &= (\alpha\beta)\gamma\end{aligned}$$

□

Proposition 4.16. *For any cut α we have $\alpha 1^* = \alpha$.*

PROOF:
⟨1⟩1. CASE: α is positive.
 ⟨2⟩1. $\alpha 1^* \subseteq \alpha$
 ⟨2⟩2. $\alpha \subseteq \alpha 1^*$
⟨1⟩2. CASE: $\alpha = 0^*$
⟨1⟩3. CASE: α is negative.
□

Theorem 4.17. *There exists an ordered field with the least upper bound property.*

Proposition 4.18. *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.
⟨1⟩9. Q.E.D.
 PROOF: ⟨1⟩2, ⟨1⟩4 and ⟨1⟩8 form a contradiction.
□

Theorem 4.19. *Any two complete ordered fields are isomorphic.*

Definition 4.20. Let $\mathbb{R}$ be the complete ordered field. We call its elements *real numbers.*

4.2 Properties of the Real Numbers

Theorem 4.21. *$\mathbb{Q}$ is a subfield of $\mathbb{R}$.*

Theorem 4.22 (Archimedean Property)**.** *Let $x, y \in \mathbb{R}$ with $x > 0$. There exists a positive integer n such that $nx > y$.*

PROOF:
⟨1⟩1. LET: $A = \{nx : n \in \mathbb{Z}^+\}$
⟨1⟩2. ASSUME: for a contradiction there is no positive integer n such that $nx > y$.
⟨1⟩3. y is an upper bound for A.
⟨1⟩4. LET: $\alpha = \sup A$
⟨1⟩5. $\alpha - x$ is not an upper bound for A.
⟨1⟩6. PICK a positive integer m such that $\alpha - x < mx$
⟨1⟩7. $\alpha < (m+1)x \in A$
⟨1⟩8. Q.E.D.
PROOF: This contradicts ⟨1⟩4.
□

Theorem 4.23. *$\mathbb{Q}$ is dense in $\mathbb{R}$.*

PROOF:
⟨1⟩1. LET: $x, y \in \mathbb{R}$ with $x < y$
⟨1⟩2. PICK a positive integer n such that

$$n(y-x) > 1 \ .$$

PROOF: Archimedean property.
⟨1⟩3. PICK a positive integer m_1 such that $m_1 > nx$
PROOF: Archimedean property.
⟨1⟩4. PICK a positive integer m_2 such that $m_2 > -nx$
PROOF: Archimedean property.
⟨1⟩5. $-m_2 < nx < m_1$
⟨1⟩6. LET: m be the integer such that

$$m - 1 \leq nx < m \ .$$

⟨1⟩7. $nx < m \leq 1 + nx < ny$
⟨1⟩8. $x < m/n < y$
□

Theorem 4.24. *For every real number $x > 0$ and positive integer n, there exists a unique positive real number y such that $y^n = x$.*

PROOF:
⟨1⟩1. There exists a real $y > 0$ such that $y^n = x$.
⟨2⟩1. LET: $E = \{t \in \mathbb{R}^+ : t^n < x\}$
⟨2⟩2. LET: $y = \sup E$
⟨3⟩1. $E \neq \emptyset$
⟨4⟩1. LET: $t = x/(x+1)$
⟨4⟩2. $0 < t < 1$
⟨4⟩3. $t^n < t < x$
⟨4⟩4. $t \in E$
⟨3⟩2. $x + 1$ is an upper bound for E.
⟨4⟩1. LET: $t > x + 1$
⟨4⟩2. $t^n > t > x$
⟨4⟩3. $t \notin E$

⟨2⟩3. $y^n = x$
⟨3⟩1. $y^n \not< x$
⟨4⟩1. ASSUME: for a contradiction $y^n < x$.
⟨4⟩2. PICK h such that $0 < h < 1$ and

$$h < \frac{x - y^n}{n(y+1)^{n-1}} \ .$$

⟨4⟩3. $(y+h)^n - y^n < x - y^n$
PROOF:

$$\begin{aligned}(y+h)^n - y^n &= ((y+h) - y)\sum_{i=0}^{n-1}(y+h)^{n-1-i}y^i \\ &= h\sum_{i=0}^{n-1}(y+h)^{n-1-i}y^i \\ &\leq hn(y+h)^{n-1} \\ &\leq hn(y+1)^{n-1} \\ &< x - y^n\end{aligned}$$

⟨4⟩4. $(y+h)^n < x$
⟨4⟩5. $y + h \in E$
⟨4⟩6. Q.E.D.
PROOF: This contradicts the fact that y is an upper bound for E.
⟨3⟩2. $y^n \not> x$
⟨4⟩1. ASSUME: for a contradiction $y^n > x$
⟨4⟩2. LET:

$$k = \frac{y^n - x}{ny^{n-1}}$$

⟨4⟩3. $0 < k < y$
⟨4⟩4. $y - k$ is an upper bound for E.
⟨5⟩1. LET: $t \geq y - k$
⟨5⟩2. $y^n - t^n \leq y^n - x$
PROOF:

$$\begin{aligned}y^n - t^n &\leq y^n - (y-k)^n \\ &= (y - (y-k))\sum_{i=0}^{n-1} y^{n-i}(y-k)^i \\ &= k\sum_{i=0}^{n-1} y^{n-i}(y-k)^i \\ &\leq kny^{n-1} \\ &= y^n - x\end{aligned}$$

⟨5⟩3. $t^n \geq x$
⟨5⟩4. $t \notin E$
⟨4⟩5. Q.E.D.
PROOF: This contradicts the fact that y is the least upper bound of E.
⟨1⟩2. If y and y' are positive reals with $y^n = y'^n$ then $y = y'$.

PROOF: Since the function that sends y to y^n is strictly monotone.
□

Definition 4.25 (nth Root)**.** Given any real number $x > 0$ and positive integer n, the *nth root* of x, denoted $x^{1/n}$, is the unique positive real such that

$$(x^{1/n})^n = x \quad .$$

We write $\sqrt{x}$ for $x^{1/2}$.

Proposition 4.26. *Let a and b be positive real numbers and n a positive integer. Then*

$$(ab)^{1/n} = a^{1/n}b^{1/n} \quad .$$

PROOF: Since $(a^{1/n}b^{1/n})^n = ab$. □

4.3 The Extended Real Number System

Definition 4.27 (Extended Real Number System)**.** The *extended real number system* is the set $\mathbb{R} \cup \{+\infty, -\infty\}$.

We extend the ordering $\leq$ to the extended reals by defining

$$-\infty < x < +\infty$$

for every $x \in \mathbb{R}$.

We extend $+$, $\cdot$ and $/$ to partial operations on the extended real by defining:

$$
\begin{aligned}
x + (+\infty) &= +\infty & (x \in \mathbb{R}) \\
x + (-\infty) &= -\infty & (x \in \mathbb{R}) \\
(+\infty) + x &= +\infty & (x \in \mathbb{R}) \\
(+\infty) + (+\infty) &\text{ is undefined} & \\
(+\infty) + (-\infty) &\text{ is undefined} & \\
(-\infty) + x &= -\infty & (x \in \mathbb{R}) \\
(-\infty) + (+\infty) &\text{ is undefined} & \\
(-\infty) + (-\infty) &\text{ is undefined} & \\
x \cdot (+\infty) &= +\infty & (x \in \mathbb{R}) \\
x \cdot (-\infty) &= -\infty & (x \in \mathbb{R}) \\
(+\infty) \cdot x &= +\infty & (x \in \mathbb{R}) \\
(+\infty) \cdot (+\infty) &\text{ is undefined} & \\
(+\infty) \cdot (-\infty) &\text{ is undefined} & \\
(-\infty) \cdot x &= -\infty & (x \in \mathbb{R}) \\
(-\infty) \cdot (+\infty) &\text{ is undefined} & \\
(-\infty) \cdot (-\infty) &\text{ is undefined} & \\
x/(+\infty) &= 0 & (x \in \mathbb{R}) \\
x/(-\infty) &= 0 & (x \in \mathbb{R}) \\
(+\infty)/x &\text{ is undefined} & (x \in \mathbb{R}) \\
(+\infty)/(+\infty) &\text{ is undefined} & \\
(+\infty)/(-\infty) &\text{ is undefined} & \\
(-\infty)/x &\text{ is undefined} & (x \in \mathbb{R}) \\
(-\infty)/(+\infty) &\text{ is undefined} & \\
(-\infty)/(-\infty) &\text{ is undefined} &
\end{aligned}
$$

Chapter 5

Complex Analysis

Definition 5.1 (Complex Numbers)**.** A *complex number* is a pair of real numbers. We write $\mathbb{C}$ for the set of complex numbers.

Define $+$ and $\cdot$ on $\mathbb{C}$ by:

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

Theorem 5.2. *The complex numbers form a field.*

Theorem 5.3. *The function that maps a to $(a,0)$ is an embedding of $\mathbb{R}$ in $\mathbb{C}$.*

Definition 5.4.

$$i = (0,1)$$

Lemma 5.5.

$$(a,b) = a+ib$$

PROOF: Since $(a,0)+(0,1)(b,0)=(a,b)$. □

Lemma 5.6.

$$i^2 = -1$$

PROOF: Immediate from definitions. □

Definition 5.7 (Complex Conjugate)**.** For any complex number z, the *complex conjugate* $\overline{z}$ is defined by

$$\overline{a+ib} = a-ib \qquad (a,b\in\mathbb{R}) \ .$$

Definition 5.8 (Real Part)**.** For any complex number z, the *real part* of z, denoted $\mathrm{Re}(z)$, is defined by

$$\mathrm{Re}(a+ib) = a \qquad (a,b\in\mathbb{R}) \ .$$

Definition 5.9 (Imaginary Part)**.** For any complex number z, the *imaginar part* of z, denoted $\mathrm{Im}(z)$, is defined by

$$\mathrm{Im}(a+ib) = b \qquad (a, b \in \mathbb{R}) \ .$$

Theorem 5.10. *For all $z, w \in \mathbb{C}$ we have*

$$\overline{z+w} = \overline{z} + \overline{w} \ .$$

PROOF:

$$\begin{aligned} \overline{(a+ib)+(c+id)} &= \overline{(a+c)+i(b+d)} \\ &= (a+c) - i(b+d) \\ &= (a-ib)+(c-id) \\ &= \overline{a+ib} + \overline{c+id} \end{aligned}$$

$\square$

Theorem 5.11. *For all $z, w \in \mathbb{C}$ we have*

$$\overline{zw} = \overline{z} \cdot \overline{w} \ .$$

PROOF:

$$\begin{aligned} \overline{(a+ib)(c+id)} &= \overline{(ac-bd)+i(ad+bc)} \\ &= (ac-bd) - i(ad+bc) \\ &= (a-ib)(c-id) \\ &= \overline{a+ib} \cdot \overline{c+id} \end{aligned}$$

$\square$

Theorem 5.12. *For all $z \in \mathbb{C}$ we have*

$$\mathrm{Re}(z) = \frac{1}{2}(z+\overline{z}) \ .$$

PROOF:

$$\begin{aligned} (a+ib) + \overline{a+ib} &= (a+ib)+(a-ib) \\ &= 2a \\ &= 2\,\mathrm{Re}(a+ib) \end{aligned}$$

$\square$

Theorem 5.13. *For all $z \in \mathbb{C}$ we have*

$$\mathrm{Im}(z) = \frac{1}{2i}(z-\overline{z}) \ .$$

PROOF:

$$\begin{aligned} (a+ib) - \overline{a+ib} &= (a+ib)-(a-ib) \\ &= 2ib \\ &= 2i\,\mathrm{Im}(a+ib) \end{aligned}$$

$\square$

Theorem 5.14. *For all $z \in \mathbb{C}$ we have $z\overline{z}$ is a non-negative real.*

PROOF:

$$\begin{aligned}(a+ib)(\overline{a+ib}) &= (a+ib)(a-ib)\\ &= a^2+b^2 \qquad \square\end{aligned}$$

Theorem 5.15. *For any $z \in \mathbb{C}$, if $z\overline{z} = 0$ then $z = 0$.*

PROOF: Let $z = a + ib$. Then $z\overline{z} = a^2 + b^2 = 0$ iff $a = b = 0$. $\square$

Definition 5.16 (Absolute Value)**.** For $z \in \mathbb{C}$, the *absolute value* of z is

$$|z| = (z\overline{z})^{1/2} \ .$$

Proposition 5.17. *For x a non-negative real we have $|x| = x$.*

PROOF: Since $|x| = \sqrt{x^2} = x$. $\square$

Proposition 5.18. *For x a negative real we have $|x| = -x$.*

PROOF: Since $|x| = \sqrt{x^2} = -x$. $\square$

Theorem 5.19. *For any complex number z we have $|z| \geq 0$.*

PROOF: Immediate from definition. $\square$

Theorem 5.20. *For any complex number z, if $|z| = 0$ then $z = 0$.*

PROOF: From Theorem 5.15. $\square$

Theorem 5.21. *For any complex number z we have*

$$|\overline{z}| = |z| \ .$$

PROOF: Immediate from definitions. $\square$

Theorem 5.22. *For any complex numbers z and w we have*

$$|zw| = |z||w| \ .$$

PROOF:

$$\begin{aligned}|zw| &= \sqrt{zw\overline{zw}}\\ &= \sqrt{z\overline{z}}\sqrt{w\overline{w}} && \text{(Proposition 4.26)}\\ &= |z||w| && \square\end{aligned}$$

Theorem 5.23. *For any complex number z we have*

$$|\operatorname{Re} z| \leq |z|$$

PROOF: Let $z = a + ib$. Then

$$|\operatorname{Re} z| = \sqrt{a^2} \leq \sqrt{a^2+b^2} \ . \square$$

Theorem 5.24. *For any complex numbers z and w we have*

$$|z + w| \leq |z| + |w| \ .$$

PROOF:
$$
\begin{aligned}
|z+w|^2 &= (z+w)(\overline{z}+\overline{w}) \\
&= z\overline{z} + z\overline{w} + \overline{z}w + w\overline{w} \\
&= |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 && \text{(Theorem 5.12)} \\
&\leq |z|^2 + 2|z\overline{w}| + |w|^2 && \text{(Theorem 5.23)} \\
&= |z|^2 + 2|z||w| + |w|^2 && \text{(Theorem 5.22)} \\
&= (|z|+|w|)^2 && \square
\end{aligned}
$$

Theorem 5.25 (Schwarz Inequality)**.** *Let $a_1, \ldots, a_n, b_1, \ldots, b_n$ be complex numbers. Then*
$$\left|\sum_{j=1}^{n} a_j \overline{b_j}\right|^2 \leq \sum_{j=1}^{n} |a_j|^2 \sum_{j=1}^{n} |b_j|^2 \ .$$

PROOF:
⟨1⟩1. LET: $A = \sum_{j=1}^{n} |a_j|^2$
⟨1⟩2. LET: $B = \sum_{j=1}^{n} |b_j|^2$
⟨1⟩3. LET: $C = \sum_{j=1}^{n} a_j \overline{b_j}$
⟨1⟩4. ASSUME: w.l.o.g. $B > 0$
PROOF: If $B = 0$ then $b_1 = \cdots = b_n = 0$ and both sides of the inequality are 0.
⟨1⟩5. $\sum_{j=1}^{n} |Ba_j - Cb_j|^2 = B(AB - |C|^2)$
PROOF:
$$
\begin{aligned}
\sum_{j=1}^{n} |Ba_j - Cb_j|^2 &= \sum_{j=1}^{n} (Ba_j - Cb_j)(B\overline{a_j} - \overline{Cb_j}) \\
&= B^2 \sum_{j=1}^{n} |a_j|^2 - B\overline{C} \sum_{j=1}^{n} a_j \overline{b_j} - BC \sum_{j=1}^{n} \overline{a_j} b_j + |C|^2 \sum_{j=1}^{n} |b_j|^2 \\
&= B^2 A - 2B|C|^2 + B|C|^2 \\
&= B(AB - |C|^2)
\end{aligned}
$$
⟨1⟩6. $B(AB - |C|^2) \geq 0$
⟨1⟩7. $AB \geq |C|^2$
$\square$

Part I

Linear Algebra

Chapter 6

Vector Spaces

Chapter 7

Real Inner Product Spaces

Definition 7.1 (Inner Product)**.** Given $\vec{x}, \vec{y} \in \mathbb{R}^k$, define the *inner product* $\vec{x} \cdot \vec{y}$ by

$$(x_1, \ldots, x_k) \cdot (y_1, \ldots, y_k) = x_1 y_1 + \cdots + x_k y_k \quad .$$

Definition 7.2 (Norm)**.** Define the *norm* of a vector $\vec{x} \in \mathbb{R}^k$ by

$$\|\vec{x}\| = \sqrt{\vec{x} \cdot \vec{x}} \quad .$$

Proposition 7.3.

$$\|\vec{x}\| \geq 0$$

PROOF: Immediate from the definition. □

Proposition 7.4. *If* $\|\vec{x}\| = 0$ *then* $\vec{x} = \vec{0}$.

PROOF: If $\|\vec{x}\| = 0$ then $x_1^2 + \cdots + x_n^2 = 0$ so $x_1 = \cdots = x_n = 0$. □

Proposition 7.5. *For* $\alpha \in \mathbb{R}$ *and* $\vec{x} \in \mathbb{R}^k$,

$$\|\alpha \vec{x}\| = |\alpha| \|\vec{x}\| \quad .$$

PROOF: Easy. □

Proposition 7.6. *For* $\vec{x}, \vec{y} \in \mathbb{R}^k$, *we have*

$$\|\vec{x} \cdot \vec{y}\| \leq \|\vec{x}\| \|\vec{y}\| \quad .$$

PROOF: By the Schwarz inequality. □

Proposition 7.7. *For* $\vec{x}, \vec{y} \in \mathbb{R}^k$ *we have*

$$\|\vec{x} + \vec{y}\| \leq \|\vec{x}\| + \|\vec{y}\| \quad .$$

PROOF:

$$\begin{aligned}
\|\vec{x}+\vec{y}\|^2 &= (\vec{x}+\vec{y})\cdot(\vec{x}+\vec{y}) \\
&= \vec{x}\cdot\vec{x} + 2\vec{x}\cdot\vec{y} + \vec{y}\cdot\vec{y} \\
&\leq \|\vec{x}\|^2 + 2\|\vec{x}\|\|\vec{y}\| + \|\vec{y}\|^2 && \text{(Proposition 7.6)} \\
&= (\|\vec{x}\| + \|\vec{y}\|)^2 && \square
\end{aligned}$$

Corollary 7.7.1. *For $\vec{x}, \vec{y}, \vec{z} \in \mathbb{R}^k$ we have*

$$\|\vec{x}-\vec{z}\| \leq \|\vec{x}-\vec{y}\| + \|\vec{y}-\vec{z}\| \ .$$

Chapter 8

Complex Inner Product Spaces

Definition 8.1 (Inner Product)**.** Let V be a complex vector space. An *inner product* on V is a function $\langle\ ,\ \rangle : V^2 \to \mathbb{C}$ such that, for all $x, y, z \in V$ and $\alpha \in \mathbb{C}$:

- $\langle y, x\rangle = \overline{\langle x, y\rangle}$
- $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$
- $\langle \alpha x, y\rangle = \overline{\alpha}\langle x, y\rangle$
- $\langle x, x\rangle \geq 0$
- If $\langle x, x\rangle = 0$ then $x = 0$.

An *inner product space* consists of a complex vector space V and an inner product on V.

Definition 8.2 (Norm)**.** Let V be an inner product space and $x \in V$. The *norm* of x is

$$\|x\| = \sqrt{\langle x, x\rangle}\ .$$

Proposition 8.3. *An inner product space is a metric space under*

$$d(x, y) = \|x - y\|\ .$$

Definition 8.4 (Bounded)**.** Let V_1 and V_2 be inner product spaces and $T : V_1 \to V_2$ a linear transformation. Then T is *bounded* iff $\{\|T(x)\| : \|x\| = 1\}$ is bounded above.

Proposition 8.5. *Every linear transformation between finite dimensional inner product spaces is bounded.*

Definition 8.6 (Outer Product)**.** Let V be an inner product space and $|\psi\rangle, |\phi\rangle \in V$. The *outer product* of $|\psi\rangle$ and $|\phi\rangle$ is

$$|\psi\rangle\langle\phi| : V \to V\ .$$

8.1 Hilbert Spaces

Definition 8.7 (Hilbert Space)**.** A *Hilbert space* is a complete inner product space.

Theorem 8.8 (Completeness Relation)**.** *Let $\mathcal{H}$ be a Hilbert space. Let $\{|e_n\rangle\}_{n\in\mathbb{N}}$ be a countable orthonormal basis for $\mathcal{H}$. Then*

$$\sum_{n=0}^{\infty} |e_n\rangle \langle e_n| = I \ .$$

PROOF:
⟨1⟩1. LET: $|\psi\rangle \in \mathcal{H}$
⟨1⟩2. LET: $|\psi\rangle = \sum_{n=0}^{\infty} \alpha_n |e_n\rangle$
⟨1⟩3. $\sum_{n=0}^{\infty} \langle e_n|\phi\rangle |e_n\rangle = |\psi\rangle$
PROOF:

$$\begin{aligned}\sum_{n=0}^{\infty} \langle e_n|\phi\rangle |e_n\rangle &= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \alpha_m \langle e_n|e_m\rangle |e_n\rangle \\ &= \sum_{n=0}^{\infty} \alpha_n |e_n\rangle \\ &= |\psi\rangle \end{aligned}$$ □

□

Definition 8.9 (Separable)**.** A Hilbert space is *separable* iff it has a countable dense orthonormal basis.

Chapter 9

Lie Algebras

Definition 9.1 (Lie Algebra)**.** Let K be a field. A *Lie algebra* $\mathcal{L}$ over K consists of a vector space $\mathcal{L}$ over K and an operation

$$[\ ,\ ] : \mathcal{L}^2 \to \mathcal{L}\ ,$$

the *Lie bracket* or *commutator*, such that, for all $x, y, z \in \mathcal{L}$ and $\alpha \in K$:

$$\begin{aligned}
[x+y, z] &= [x, z] + [y, z] \\
[x, y+z] &= [x, y] + [x, z] \\
[\alpha x, y] &= \alpha[x, y] \\
[x, x] &= 0 \\
[x, [y, z]] + [y, [z, x]] + [z, [x, y]] &= 0 \qquad \text{(Jacobi identity)}
\end{aligned}$$

Lemma 9.2. *If K has characteristic 0 then the condition $[x, x] = 0$ can be replaced with $[x, y] = -[y, x]$.*

Proposition 9.3. *The commutator is determind by its values on any basis for $\mathcal{L}$.*

Example 9.4. $\mathbb{R}^3$ with the cross product is a real Lie algebra.

Example 9.5. For any $n \geq 0$, we have $GL(n, K)$ is a Lie algebra over K under

$$[A, B] = AB - BA\ .$$

Definition 9.6 (Linear Lie Algebra)**.** A *linear Lie algebra* over K is a Lie algebra over K that is a subalgebra of $GL(n, K)$ for some n.

Example 9.7 (Special Linear Algebra)**.** The *special Linear algebra* $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \mathrm{tr} = 0\}$ is a real linear Lie algebra.

Example 9.8 (Orthogonal Lie Algebra)**.** The *orthogonal Lie algebra* $SO(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : A \text{ is skew-symmetric}\}$ is a real linear Lie algebra.

Example 9.9. Let $u(n)$ be the set of all skew-Hermitian $n \times n$-matrices as a real Lie algebra.

Let $su(n) = u(n) \cap SL(n, \mathbb{R})$.

Proposition 9.10. *$SU(2)$ is spanned by the* Pauli matrices

$$\sigma_x = \frac{1}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad \sigma_y = \frac{1}{2}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_z = \frac{1}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

which satisfy

$$\begin{aligned} [\sigma_x, \sigma_y] &= \sigma_z \\ [\sigma_y, \sigma_z] &= \sigma_x \\ [\sigma_z, \sigma_x] &= \sigma_y \end{aligned}$$

9.1 Lie Algebar Homomorphisms

Definition 9.11 (Homomorphism)**.** Let L_1 and L_2 be Lie algebras over the same field. A *Lie algebra homomorphism* $\phi : L_1 \to L_2$ is a linear transformation such that

$$\phi([x, y]) = [\phi(x), \phi(y)]$$

for all $x, y \in L_1$.

Lemma 9.12. *Every bijective Lie algebra homomorphism is an isomorphism.*

Definition 9.13 (Representation)**.** Let L be a real (complex) Lie algebra. A *representation* of L is a Lie algebra homomorphism $L \to GL(n, \mathbb{R})$ ($GL(n, \mathbb{C})$) for some n.

Example 9.14. The linear transformation $\mathbb{R}^3 \to su(2)$ defined by

$$i \mapsto \sigma_x, j \mapsto \sigma_y, k \mapsto \sigma_z$$

is a representation of $\mathbb{R}^3$.

Part II

More Algebra

Chapter 10

Lie Groups

Definition 10.1 (Lie Group)**.** A *Lie group G* is a group G that is also an analytic differentiable manifold such that the group operation and inverse operation are analytic.

A *homomorphism of Lie groups* is a group homomorphism that is an analytic function.

Lemma 10.2. *Every bijective Lie group homomorphism is an isomorphism.*

Definition 10.3 (Unitary Group)**.** The *unitary group $U(n)$* is the Lie group of all $n \times n$ unitary matrices.

Definition 10.4 (Special Unitary Group)**.** The *special unitary group $SU(n)$* is the Lie group of all $n \times n$ unitary matrices with determinant 1.

Definition 10.5 (Lie Subgroup)**.** Let G be a Lie group. A *Lie subgroup* of G is a subgroup that is also an analytic submanifold of G.

Example 10.6. $U(n)$ and $SU(n)$ are Lie subgroups of $GL(n, \mathbb{C})$.