C2 Algebra

Robin Adams

September 25, 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 (Rng)**.** A *rng* is a quintuple $(R, +, \cdot, 0)$ consisting of a set R, binary operations $+$ and $\cdot$ on R, and element $0 \in R$ such that:

1. $(R, +, 0)$ is an Abelian group.
2. The operation $\cdot$ is associative, and distributive over $+$.

Proposition 10. *In any rng we have* $x0 = 0$.

PROOF: $x0 = x(0 + 0) = x0 + x0$ and also $x0 = x0 + 0$. The result follows by the cancellation law. □

Proposition 11. *In any rng we have* $-(xy) = (-x)y = x(-y)$.

PROOF: The result $-(xy) = (-x)y$ holds because

$$xy + (-x)y = (x + (-x))y = 0y = 0 \ .$$

We prove $-(xy) = x(-y)$ similarly. □

Corollary 11.1. *In any rng,* $(-x)(-y) = xy$.

Definition 12 (Ring)**.** A *ring* consists of a rng R and an element $1 \in R$, the *unit element*, such that $\forall x \in R.x1 = 1x = x$.

Proposition 13. *In a ring R, if* $0 = 1$ *then R has only one element.*

Definition 14 (Commutative Rng)**.** A rng R is *commutative* iff $\forall x, y \in R.xy = yx$.

Definition 15 (Zero Divisor)**.** A *zero divisor* in a rng is an element x such that $x \neq 0$ but there exists $y \neq 0$ such that $xy = 0$.

Definition 16 (Integral Domain)**.** An *integral domain* is a commutative ring with no zero divisors.

Proposition 17. *The trivial ring is an integral domain.*

Lemma 18. *The integers form an integral domain.*

PROOF: Easy. □

Proposition 19. *Let R be a commutative ring. Then R is an integral domain if and only if, whenever $xy = xz$ and $x \neq 0$, then $y = z$.*

4 Ordered Integral Domains

Definition 20 (Ordered Integral Domain)**.** An *ordered integral domain* is an integral domain D with a linear order $<$ such that:

- Whenever $x < y$ then $x + z < y + z$.

- Whenever $x < y$ and $0 < z$ then $xz < yz$.

Proposition 21. *In an ordered integral domain, if $x < y$ and $z < 0$ then $yz < xz$.*

Proposition 22. *$x < y$ iff $-y < -x$.*

Definition 23 (Positive)**.** In an integral domain, we say an element a is *positive* iff $0 < a$ and *negative* iff $a < 0$.

Proposition 24. *$x < y$ iff $y - x$ is positive.*

Proposition 25. *$x < y$ iff $x - y$ is negative.*

Proposition 26. *x is positive iff $-x$ is negative.*

Proposition 27. *x is negative iff $-x$ is positive.*

Proposition 28. *The sum of two positive elements is positive.*

Proposition 29. *The product of two positive elements is positive.*

Proposition 30. *The product of two negative elements is positive.*

Proposition 31. *The product of a positive and a negative element is negative.*

Proposition 32. *If $x \neq 0$ then x^2 is positive.*

Proposition 33. *x^2 is always non-negative.*

Proposition 34. $0 < 1$

Proposition 35. $-1 < 0$

Theorem 36. *Let R be an integral domain and $P \subseteq R$ be a set such that:*

- $0 \notin P$
- *For all $x \in R$ we have $x \in P$ or $x = 0$ or $-x \in P$*
- *For all $x, y \in P$ we have $x + y \in P$*
- *For all $x, y \in P$ we have $xy \in P$*

Define $<$ on R by $x < y$ iff $y - x \in P$. Then R is an ordered integral domain under $<$ with P the set of positive elements.

Definition 37 (Absolute Value)**.** In any ordered integral domain, define

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

Proposition 38. *$|x|$ is always non-negative.*

Proposition 39. $|x| = 0$ *iff* $x = 0$

Proposition 40. $|-x| = |x|$

Proposition 41. $|x - y| = |y - x|$

Proposition 42. $|xy| = |x||y|$

Proposition 43. $-|x| \leq x \leq |x|$

Proposition 44. $|x| < u$ *iff* $-u < x < u$

Proposition 45. $|x| \leq u$ *iff* $-u \leq x \leq u$

Proposition 46 (Triangle Inequality)**.** $|x + y| \leq |x| + |y|$

Proposition 47. $||x| - |y|| \leq |x - y|$

5 Greatest Common Divisor

Theorem 48 (Division Theorem)**.** *Let a and b be integers, $a > 1$. Then there exist unique integers q and r such that $b = qa + r$ and $0 \leq r < a$.*

Proof: For existence, prove the case $b \geq 0$ by induction on b. The case $b < 0$ follows.
For uniqueness, if $qa + r = q'a + r'$ then $a|r - r'$ and $-a < r - r' < a$, hence $r - r' = 0$. So $r = r'$ and $q = q'$. □

Definition 49 (Divisibility)**.** We say a *divides* b, $a \mid b$, iff there exists c such that $b = ac$.

Proposition 50. *For every integer a we have $a \mid 0$.*

Proposition 51. *For every integer a we have $1 \mid a$.*

Proposition 52. *For every integer a we have $a \mid a$.*

Proposition 53. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proposition 54. *If $a \mid c$ and $c \neq 0$ the $|a| \leq |c|$.*

Proposition 55. *If $0 \mid a$ then $a = 0$.*

Proposition 56. *If $a \mid b$ and $b \mid a$ then $a = b$ or $a = -b$.*

Proposition 57. $a \mid ab$

Proposition 58. *If $a \mid b$ and $a \mid c$ then $a \mid b + c$.*

Proposition 59. *If $a \mid b$ and $a \mid c$ then $a \mid b - c$.*

Proposition 60. *If $a \mid 1$ then $a = 1$ or $a = -1$.*

Definition 61 (Greatest Common Divisor)**.** The integer d is the *greatest common divisor* of a and b iff d is non-negative, $d \mid a$, $d \mid b$, and whenever $x \mid a$ and $x \mid b$ then $d \mid x$.

Proposition 62. *Two integers have at most one gcd.*

Theorem 63. *Let a and b be integers that are not both 0. Then there exist integers x and y such that $xa + yb$ is the greatest common divisor of a and b.*

Proof: Take the least positive member of $\{xa + yb : x, y \in \mathbb{Z}\}$. □

Definition 64 (Relatively Prime)**.** Two integers a and b are *relatively prime* iff their gcd is 1.

Definition 65 (Prime)**.** An integer p is *prime* iff $p > 1$ and the only divisors of p are 1 and p.

An integer a is *composite* iff $a > 1$ and a is not prime.

Proposition 66. *Every integer greater than 1 is divisible by a prime.*

Theorem 67. *There are infinitely many primes.*

Proposition 68. *If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Theorem 69 (Fundamental Theorem of Arithmetic)**.** *Every integer > 1 is the product of a unique multiset of primes.*

6 Integers Modulo n

Definition 70 (Congruence)**.** Two integers a and b are *congruent* modulo n, $a \equiv b \mod n$, iff $n \mid a - b$.

Proposition 71. *Congruence modulo n is an equivalence relation.*

Proposition 72. *If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $a + c \equiv b + d \mod n$.*

Proposition 73. *If $a \equiv b \mod n$ then $-a \equiv -b \mod n$.*

Proposition 74. *If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $ac \equiv bd \mod n$.*

Definition 75. The equivalence classes with respect to congruence modulo n are called *residue classes modulo n*.

Definition 76. The set of *integers modulo n*, $\mathbb{Z}_n$, is the quotient of $\mathbb{Z}$ by congruence modulo n.

Proposition 77. *If $n > 0$ then $|\mathbb{Z}_n| = n$.*

Proposition 78. *$\mathbb{Z}_n$ is a commutative ring.*

Proposition 79. *$\mathbb{Z}_n$ is an integral domain if and only if n is prime.*

7 Field Theory

Definition 80 (Field)**.** A *field* is an integral domain such that every non-zero element has a multiplicative inverse.

Definition 81 (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 82 (Rational Numbers)**.** The field of *rational numbers* $\mathbb{Q}$ is the field of fractions of the integers.

8 Rational Numbers

Lemma 83. *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 84. The ordering on the rationals is defined by: if b and d are positive then $[(a, b)] < [(c, d)]$ iff $ad < bc$.

Theorem 85. *The relation $<$ is a linear ordering on $\mathbb{Q}$.*

Proof: Easy. □

Definition 86 (Positive)**.** A rational q is *positive* iff $0 < q$.

Definition 87 (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 88. *For any rational s, the function that maps q to $q + s$ is strictly monotone.*

Proof: Easy. □

Theorem 89. *For any positive rational s, the function that maps q to qs is strictly monotone.*

PROOF: Easy. □

Theorem 90. *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. □

9 Ordered Fields

Definition 91 (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:

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

10 The Real Numbers

Definition 92 (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 93. Given real numbers x and y, we write $x < y$ iff $x \subset y$.

Theorem 94. *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 95. *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 96 (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 $q + r < q' + r'$
$\square$

Theorem 97. *Addition is associative and commutative.*

PROOF: Easy. $\square$

Definition 98 (Zero)**.** The real number zero is $0 = \{q \in \mathbb{Q} : q < 0\}$.
It is easy to check this is a Dedekind cut.

Theorem 99. *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 100. For any real x, define

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

We prove this is a Dedekind cut.

PROOF:
⟨1⟩1. $-x \neq \emptyset$
PROOF: Pick s such that $s \notin x$. Then $-s - 1 \in -x$.
⟨1⟩2. $-x \neq \mathbb{Q}$
⟨2⟩1. PICK $r \in x$
PROVE: $-r \notin -x$
⟨2⟩2. ASSUME: for a contradiction $-r \in -x$
⟨2⟩3. PICK $s > -r$ such that $-s \notin x$
⟨2⟩4. $-s < r$
⟨2⟩5. $-s \in x$
⟨2⟩6. Q.E.D.
PROOF: This is a contradiction.
⟨1⟩3. $-x$ is closed downwards.
PROOF: Easy.
⟨1⟩4. $-x$ has no largest element.
⟨2⟩1. LET: $r \in -x$
⟨2⟩2. PICK $s > r$ such that $-s \notin x$
⟨2⟩3. PICK q such that $r < q < s$
⟨2⟩4. $r < q$ and $q \in -x$
□

Lemma 101. *For any positive integer a and integer b, there exists a natural number k such that $b < ak$.*

PROOF: Take $k = |b| + 1$. □

Lemma 102. *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 101, pick k such that $bc < adk$. Then $r < pk$. □

Lemma 103. *Let p be a positive real number. For any real x, there exists $q \in x$ such that $p + q \notin x$.*

PROOF:
⟨1⟩1. PICK rationals $r_1 \in x$ and $r_2 \notin x$
⟨1⟩2. There exists a natural number k such that $kp > r_2 - r_1$
PROOF: By Lemma 102.

$\langle 1 \rangle 3$. 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 104. *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 103.
  $\langle 2 \rangle 3$. 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 $-s \notin x$.
  $\langle 2 \rangle 6$. $p = q + (p - q) \in x + (-x)$
□

Theorem 105. *The reals form an Abelian group under addition.*

PROOF: Easy. □

Theorem 106. *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.
□

Definition 107 (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 108 (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 109. *Multiplication is commutative and associative.*

PROOF: Easy. □

Theorem 110. *Multiplication is distributive over addition.*

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

Definition 111. The real number *one* is $1 = \{q \in \mathbb{Q} : q < 1\}$.

It is easy to check this is a Dedekind cut.

Theorem 112. $0 \neq 1$

PROOF: $0 \in 1$ and $0 \notin 0$. $\square$

Theorem 113. *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 114. *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 115. *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. $\square$

11 Complete Ordered Fields

Definition 116 (Complete Ordered Field)**.** An ordered field is *complete* iff it has the least upper bound property.

Theorem 117. *The reals form a complete ordered field.*

Proof: From the results above. $\square$

Theorem 118. *Any two complete ordered fields are isomorphic.*

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

Theorem 119. *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.
$\langle 1 \rangle 2.$ $\forall q, r \in \mathbb{Q}.E(q + r) = E(q) + E(r)$
  $\langle 2 \rangle 1.$ Let: $q, r \in \mathbb{Q}$
  $\langle 2 \rangle 2.$ $E(q + r) \subseteq E(q) + E(r)$
    $\langle 3 \rangle 1.$ Let: $t \in E(q + r)$
    $\langle 3 \rangle 2.$ Let: $\epsilon = (r + s - t)/2$
    $\langle 3 \rangle 3.$ $\epsilon > 0$
    $\langle 3 \rangle 4.$ Let: $p = r - \epsilon$
    $\langle 3 \rangle 5.$ Let: $q = s - \epsilon$
    $\langle 3 \rangle 6.$ $p < r$
    $\langle 3 \rangle 7.$ $q < s$
    $\langle 3 \rangle 8.$ $p + q = t$
    $\langle 3 \rangle 9.$ $t \in E(r) + E(s)$
  $\langle 2 \rangle 3.$ $E(q) + E(r) \subseteq E(q + r)$
    Proof: If $p < q$ and $s < r$ then $p + s < q + r$.
$\langle 1 \rangle 3.$ $\forall q, r \in \mathbb{Q}.E(qr) = E(q)E(r)$
  Proof: TODO
$\langle 1 \rangle 4.$ $E(0) = 0$
  Proof: By definition.
$\langle 1 \rangle 5.$ $E(1) = 1$
  Proof: By definition.
$\langle 1 \rangle 6.$ 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 $q \notin E(q)$.

$\square$

Theorem 120 (Cantor 1873)**.** *The set ω is not equinumerous with $\mathbb{R}$.*

PROOF:

$\langle 1 \rangle 1$. LET: $f : \omega \to \mathbb{R}$

PROVE: f is not surjective.

$\langle 1 \rangle 2$. LET: z be the real number between 0 and 1 whose $n+1$st decimal place is 7 unless the $n+1$st decimal place of $f(n)$ is 7, in which case it is 6

$\langle 1 \rangle 3$. $\forall n \in \omega . f(n) \neq z$

$\square$