C2 Algebra

Robin Adams

October 15, 2022

1 Groups

Definition 1.1 (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 1.2. *The integers $\mathbb{Z}$ form a group under $+$ and 0.*

Proof: Easy. □

Lemma 1.3. *In any group, inverses are unique.*

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

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

□

Definition 1.4. We write x^{-1} for the inverse of x.

2 Abelian Groups

Definition 2.1 (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 2.2. *The integers $\mathbb{Z}$ are Abelian.*

Proof: Easy. □

Lemma 2.3. *The rationals $\mathbb{Q}$ form an Abelian group under $+$.*

Proof: Easy.

Lemma 2.4. *The non-zero rationals form an Abelian group under multiplication.*

Proof: Easy. □

3 Ring Theory

Definition 3.1 (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 3.2. *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 3.3. *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 3.3.1. *In any rng,* $(-x)(-y) = xy$.

Definition 3.4 (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 3.5. *In a ring R, if $0 = 1$ then R has only one element.*

Definition 3.6. Let n be an integer. In any ring, we write just n for $n1$.

Definition 3.7 (Commutative Rng)**.** A rng R is *commutative* iff $\forall x, y \in R. xy = yx$.

Definition 3.8 (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 3.9 (Integral Domain)**.** An *integral domain* is a commutative ring with no zero divisors.

Example 3.10.

1. The trivial ring is an integral domain.
2. The integers form an integral domain.
3. The rationals form an integral domain.

Proposition 3.11. *Let R be a commutative ring. Then R is an integral domain if and only if, whenever $xy = xz$ and $x \neq 0$, then $y = z$.*

Definition 3.12 (Boolean Ring)**.** A *Boolean rng* is a rng R such that $\forall x \in R. x^2 = x$

Example 3.13. $\mathbb{Z}_2$ is a Boolean rng.

Proposition 3.14. *In any Boolean rng we have $x + x = 0$ for all x*

PROOF: We have $x = x^2 = (-x)^2 = -x$. ∎

Proposition 3.15. *Every Boolean rng is commutative.*

PROOF: We have

$$\begin{aligned}(x+y)^2 &= x+y \\ &= x^2+y^2 \\ \therefore x^2+xy+yx+y^2 &= x^2+y^2 \\ \therefore xy+yx &= 0 \\ \therefore xy &= -(yx) \\ &= yx\end{aligned}$$

∎

Definition 3.16 (Characteristic)**.** The *characteristic* of an integral domain is the least positive integer n such that $n = 0$, or 0 if there is no such n.

Example 3.17. 1. The characteristic of $\mathbb{Z}$ is 0.

2. The characteristic of $\mathbb{Z}_n$ is n.

Proposition 3.18. *The characteristic of an integral domain is either 0, 1 or a prime.*

PROOF:
$\langle 1\rangle 1$. LET: D be any integral domain of characteristic $n > 1$.
$\langle 1\rangle 2$. ASSUME: for a contradiction $n = ab$ with $a, b > 1$
$\langle 1\rangle 3$. $ab = 0$ in D
$\langle 1\rangle 4$. $a = 0$ or $b = 0$ in D
$\langle 1\rangle 5$. Q.E.D.
  PROOF: This contradicts the minimality of n.
∎

Theorem 3.19. *An integral domain D has characteristic 0 iff $\{n1 : n \in \mathbb{N}\}$ is infinite.*

PROOF:
$\langle 1\rangle 1$. If D has characteristic $p > 0$ then $\{n1 : n \in \mathbb{N}\}$ is finite.
  $\langle 2\rangle 1$. ASSUME: the characteristic of D is $p > 0$
    PROVE: For all $n \in \mathbb{N}$ there exists $k < p$ such that $n1 = k1$ in D
  $\langle 2\rangle 2$. LET: $n \in \mathbb{N}$
  $\langle 2\rangle 3$. LET: q, r be the integers such that $n = qp + r$ with $0 \leq r < p$
  $\langle 2\rangle 4$. $n1 = r1$
    PROOF:

$$\begin{aligned}n1 &= q(p1) + r1 \\ &= q0 + r1 \\ &= r1\end{aligned}$$

$\langle 1\rangle 2$. If $\{n1 : n \in \mathbb{N}\}$ is finite then D has non-zero characteristic.
  $\langle 2\rangle 1$. ASSUME: $\{n1 : n \in \mathbb{N}\}$ is finite.

$\langle 2\rangle 2$. PICK a positive integer p such that $p1 = k1$ for some non-negative $k < p$
$\langle 2\rangle 3$. $(p-k)1 = 0$ and $p - k > 0$
□

Proposition 3.20. *For any integral domain D, the set $\{n1 : n \in \mathbb{Z}\}$ is a subdomain.*

Proposition 3.21. *For any integral domain D of characteristic 0, the mapping that sends n to $n1$ is an embedding of $\mathbb{Z}$ in D.*

Corollary 3.21.1. *The integers are the unique integral domain D up to isomorphism with characteristic 0 such that D has no proper subdomains.*

4 Polynomials

Definition 4.1 (Polynomial)**.** Let D be an integral domain. The set $D[x]$ of *polynomials* over D is the set of sequences in D that are eventually zero. We write the sequence (a_n) as $a_0 + a_1 x + \cdots + a_m x^m$ if $a_n = 0$ for all $n > m$. The element a_i is called the ith *coefficient*, or the *coefficient* of x^i.

Definition 4.2 (Degree)**.** The *degree* of a non-zero polynomial p is the largest integer n such that the coefficient of x^n is non-zero. This coefficient is the *leading coefficient* of p.

Definition 4.3 (Addition)**.** Addition of polynomials is defined by: $(a_n)+(b_n) = (a_n + b_n)$.

Definition 4.4 (Multiplication)**.** Multiplication of polynomials is defined by: $(\sum_n a_n x^n)(\sum_n b_n x^n) = \sum_n (\sum_{m=0}^n a_m b_{n-m}) x^n$.

Theorem 4.5. *Under these operations, $D[x]$ is an integral domain.*

5 Ordered Integral Domains

Definition 5.1 (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 5.2. *In an ordered integral domain, if $x < y$ and $z < 0$ then $yz < xz$.*

Proposition 5.3. $x < y$ *iff* $-y < -x$.

Proposition 5.4. *Any subdomain of an ordered integral domain is an ordered integral domain under the restriction of $<$.*

Definition 5.5 (Positive)**.** In an integral domain, we say an element a is *positive* iff $0 < a$ and *negative* iff $a < 0$.

Proposition 5.6. *$x < y$ iff $y - x$ is positive.*

Proposition 5.7. *$x < y$ iff $x - y$ is negative.*

Proposition 5.8. *x is positive iff $-x$ is negative.*

Proposition 5.9. *x is negative iff $-x$ is positive.*

Proposition 5.10. *The sum of two positive elements is positive.*

Proposition 5.11. *The product of two positive elements is positive.*

Proposition 5.12. *The product of two negative elements is positive.*

Proposition 5.13. *The product of a positive and a negative element is negative.*

Proposition 5.14. *If $x \neq 0$ then x^2 is positive.*

Proposition 5.15. *x^2 is always non-negative.*

Proposition 5.16. $0 < 1$

Proposition 5.17. $-1 < 0$

Theorem 5.18. *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 5.19 (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 5.20. *$|x|$ is always non-negative.*

Proposition 5.21. *$|x| = 0$ iff $x = 0$*

Proposition 5.22. $|-x| = |x|$

Proposition 5.23. $|x - y| = |y - x|$

Proposition 5.24. $|xy| = |x||y|$

Proposition 5.25. $-|x| \leq x \leq |x|$

Proposition 5.26. $|x| < u$ *iff* $-u < x < u$

Proposition 5.27. $|x| \leq u$ *iff* $-u \leq x \leq u$

Proposition 5.28 (Triangle Inequality)**.** $|x+y| \leq |x| + |y|$

Proposition 5.29. $||x| - |y|| \leq |x - y|$

Proposition 5.30. *Any ordered integral domain has characteristic 0.*

Proof: For any positive integer n we have $0 < n$ and so $n \neq 0$. □

Theorem 5.31. *Let D be an ordered integral domain. Then the following are equivalent.*

1. $D \cong \mathbb{Z}$
2. *The set of positive elements of D is* $\{n1 : n \in \mathbb{Z}^+\}$
3. *The set of positive elements of D is well-ordered by $<$.*

Theorem 5.32. *Let D be an ordered integral domain. Then $D[x]$ is an ordered integral domain under: $p(x) < q(x)$ iff $q(x) - p(x)$ is positive, where a polynomial is positive iff its leading coefficient is positive.*

Definition 5.33 (Monic Polynomial)**.** A polynomial is *monic* iff its leading coefficient is 1.

Theorem 5.34. *Let D be an integral domain. Let $f, g \in D[x]$ with f a monic polynomial of degree ≥ 1. Then there exist unique polynomials $q, r \in D[x]$ such that $g = fq + r$ and either $r = 0$ or $\deg r < \deg f$.*

Proof:
⟨1⟩1. Let: $f \in D[x]$ be a monic polynomial of degree $k \geq 1$
⟨1⟩2. 0 and 0 are the unique polynomials such that $0 = f0 + 0$
⟨1⟩3. For any $n \in \mathbb{N}$ and polynomial g of degree n, there exist polynomials $q, r \in D[x]$ such that $g = fq + r$ and either $r = 0$ or $\deg r < \deg f$
  ⟨2⟩1. For any ppolynomial g of degree $< k$, there exist polynomials $q, r \in D[x]$ such that $g = fq + r$ and either $r = 0$ or $\deg r < \deg f$
   Proof: Take $q = 0$ and $r = g$.
  ⟨2⟩2. Let $n \in \mathbb{N}$ with $k \leq n$. Assume for any polynomial g of degree $\leq n$, there exist polynomials $q, r \in D[x]$ such that $g = fq + r$ and either $r = 0$ or $\deg r < \deg f$. Then for any polynomial g of degree $n + 1$, there exist polynomials $q, r \in D[x]$ such that $g = fq + r$ and either $r = 0$ or $\deg r < \deg f$
   ⟨3⟩1. Let: $n \in \mathbb{N}$
   ⟨3⟩2. Assume: For any polynomial g of degree n, there exist polynomials $q, r \in D[x]$ such that $g = fq + r$ and either $r = 0$ or $\deg r < \deg f$.

⟨3⟩3. LET: g be a polynomial of degree $n+1$
⟨3⟩4. LET: a_{n+1} be the leading coefficient of g
⟨3⟩5. LET: $h(x) = g(x) - a_{n+1}x^{n+1-k}f(x)$
⟨3⟩6. Either $h = 0$ or $\deg h \leq n$
⟨3⟩7. PICK polynomials q, r with $h = fq + r$ and either $r = 0$ or $\deg r < k$
⟨3⟩8. $g(x) = f(x)(q(x) + a_{n+1}x^{n+1-k}) + r(x)$
⟨1⟩4. If $fq + r = fq' + r'$; either $r = 0$ or $\deg r < \deg f$; and either $r' = 0$ or $\deg r' < \deg f$; then $q = q'$ and $r = r'$
⟨2⟩1. $f(q - q') = r' - r$ and $r' - r$ is either 0 or has degree $< \deg f$
⟨2⟩2. $q - q' = 0$
⟨2⟩3. $r = r'$
□

Definition 5.35 (Polynomial Function)**.** Given $f(x) \in D[x]$ and $a \in D$, define $f(a) \in D$ in the obvious way.

Definition 5.36 (Root)**.** A *root* of a polynomial $p(x) \in D[x]$ is an element $a \in D$ such that $p(a) = 0$.

Theorem 5.37. *Let $p(x) \in D[x]$ and $a \in D$. Then $p(a) = 0$ iff there exists $q(x) \in D[x]$ such that $p(x) = q(x)(x - a)$.*

PROOF:
⟨1⟩1. If $p(x) = q(x)(x - a)$ then $p(a) = 0$
⟨1⟩2. If $p(a) = 0$ then there exists q such that $p(x) = q(x)(x - a)$
⟨2⟩1. ASSUME: $p(a) = 0$
⟨2⟩2. LET: q and r be the polynomials such that $p(x) = q(x)(x - a) + r(x)$ where $r = 0$ or $\deg r < 1$
⟨2⟩3. LET: $r(x) = c$, a constant
⟨2⟩4. $c = 0$
PROOF:

$$\begin{aligned} p(a) &= 0 \\ \therefore q(a)(a - a) + c &= 0 \\ \therefore c &= 0 \end{aligned}$$

⟨2⟩5. $p(x) = q(x)(x - a)$
□

Corollary 5.37.1. *A polynomial of degree n has at most n distinct roots.*

Corollary 5.37.2. *Let D be an infinite integral domain and $f, g \in D[x]$. Then $f = g$ iff f and g determine the same function $D \to D$.*

PROOF: If f and g determine the same function then $f - g$ has infinitely many roots, hence $f - g = 0$. □

Theorem 5.38 (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 5.39 (Divisibility)**.** We say a *divides* b, $a \mid b$, iff there exists c such that $b = ac$.

Proposition 5.40. *For every integer a we have $a \mid 0$.*

Proposition 5.41. *For every integer a we have $1 \mid a$.*

Proposition 5.42. *For every integer a we have $a \mid a$.*

Proposition 5.43. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proposition 5.44. *If $a \mid c$ and $c \neq 0$ the $|a| \leq |c|$.*

Proposition 5.45. *If $0 \mid a$ then $a = 0$.*

Proposition 5.46. *If $a \mid b$ and $b \mid a$ then $a = b$ or $a = -b$.*

Proposition 5.47. $a \mid ab$

Proposition 5.48. *If $a \mid b$ and $a \mid c$ then $a \mid b + c$.*

Proposition 5.49. *If $a \mid b$ and $a \mid c$ then $a \mid b - c$.*

Proposition 5.50. *If $a \mid 1$ then $a = 1$ or $a = -1$.*

Definition 5.51 (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 5.52. *Two integers have at most one gcd.*

Theorem 5.53. *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 5.54 (Relatively Prime)**.** Two integers a and b are *relatively prime* iff their gcd is 1.

Definition 5.55 (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 5.56. *Every integer greater than 1 is divisible by a prime.*

Theorem 5.57. *There are infinitely many primes.*

Proposition 5.58. *If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Theorem 5.59 (Fundamental Theorem of Arithmetic)**.** *Every integer > 1 is the product of a unique multiset of primes.*

6 Integers Modulo n

Definition 6.1 (Congruence)**.** Two integers a and b are *congruent* modulo n, $a \equiv b \mod n$, iff $n \mid a - b$.

Proposition 6.2. *Congruence modulo n is an equivalence relation.*

Proposition 6.3. *If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $a+c \equiv b+d \mod n$.*

Proposition 6.4. *If $a \equiv b \mod n$ then $-a \equiv -b \mod n$.*

Proposition 6.5. *If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $ac \equiv bd \mod n$.*

Definition 6.6. The equivalence classes with respect to congruence modulo n are called *residue classes modulo n*.

Definition 6.7. The set of *integers modulo n*, $\mathbb{Z}_n$, is the quotient of $\mathbb{Z}$ by congruence modulo n.

Proposition 6.8. *If $n > 0$ then $|\mathbb{Z}_n| = n$.*

Proposition 6.9. *$\mathbb{Z}_n$ is a commutative ring.*

Proposition 6.10. *$\mathbb{Z}_n$ is an integral domain if and only if n is prime.*

7 Field Theory

Definition 7.1 (Field)**.** A *field* is a non-trivial integral domain such that every non-zero element has a multiplicative inverse.

Definition 7.2 (Field of Fractions)**.** Let R be a non-trivial integral domain. The *field of fractions* or *quotient field* of R is $(R \times (R - \{0\}))/\sim$, where $(a, b) \sim (c, d)$ iff $ad = bc$, under the following operations:

$$\begin{aligned}
[(a, b)] + [(c, d)] &= [(ad + bc, bd)] \\
[(a, b)][(c, d)] &= [(ac, bd)] \\
0 &= [(0, 1)] \\
1 &= [(1, 1)]
\end{aligned}$$

We prove that the relation $\sim$ is an equivalence relation, the operations are well-defined, and this structure is a field.

PROOF:
$\langle 1 \rangle 1.$ $\sim$ is an equivalence relation.
  $\langle 2 \rangle 1.$ $\sim$ is reflexive on R^2.
    $\langle 3 \rangle 1.$ LET: $a, b \in R$ with $b \neq 0$
    $\langle 3 \rangle 2.$ $ab = ab$
    $\langle 3 \rangle 3.$ $(a, b) \sim (a, b)$
  $\langle 2 \rangle 2.$ $\sim$ is symmetric.

$\langle 3\rangle 1.$ LET: $a, b, c, d \in R$ with $b \neq 0$ and $d \neq 0$
$\langle 3\rangle 2.$ ASSUME: $(a, b) \sim (c, d)$
$\langle 3\rangle 3.$ $ad = bc$
$\langle 3\rangle 4.$ $cb = da$
PROOF: Since R is commutative.
$\langle 3\rangle 5.$ $(c, d) \sim (a, b)$
$\langle 2\rangle 3.$ $\sim$ is transitive.
$\langle 3\rangle 1.$ LET: $a, b, c, d, e, f \in R$ with $b \neq 0$, $d \neq 0$ and $f \neq 0$
$\langle 3\rangle 2.$ ASSUME: $(a, b) \sim (c, d) \sim (e, f)$
$\langle 3\rangle 3.$ $ad = bc$
$\langle 3\rangle 4.$ $cf = de$
$\langle 3\rangle 5.$ $adf = bcf$
$\langle 3\rangle 6.$ $bcf = bde$
$\langle 3\rangle 7.$ $adf = bde$
$\langle 3\rangle 8.$ $af = be$
PROOF: Proposition 3.11.
$\langle 1\rangle 2.$ Addition is well-defined.
$\langle 2\rangle 1.$ If $b \neq 0$ and $d \neq 0$ then $bd \neq 0$
PROOF: Since R has no zero-divisors.
$\langle 2\rangle 2.$ ASSUME: $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$
$\langle 2\rangle 3.$ $ab' = a'b$
$\langle 2\rangle 4.$ $cd' = c'd$
$\langle 2\rangle 5.$ $(ad + bc)b'd' = (a'd' + b'c')bd$
PROOF:

$$\begin{aligned}(ad + bc)b'd' &= ab'dd' + bb'cd' \\ &= a'bdd' + bb'cd' \\ &= (a'd' + b'c')bd\end{aligned}$$

$\langle 2\rangle 6.$ $(ad + bc, bd) \sim (a'd' + b'c', b'd')$
$\langle 1\rangle 3.$ Multiplication is well-defined.
$\langle 2\rangle 1.$ If $b \neq 0$ and $d \neq 0$ then $bd \neq 0$
$\langle 2\rangle 2.$ ASSUME: $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$
$\langle 2\rangle 3.$ $ab' = a'b$
$\langle 2\rangle 4.$ $cd' = c'd$
$\langle 2\rangle 5.$ $ab'cd' = a'bc'd$
$\langle 2\rangle 6.$ $(ac, bd) \sim (a'c', b'd')$
$\langle 1\rangle 4.$ The axioms of a field are satisfied.
$\langle 2\rangle 1.$ Addition is commutative.
PROOF: $[(a, b)] + [(c, d)] = [(c, d)] + [(a, b)] = [(ad + bc, bd)]$
$\langle 2\rangle 2.$ Addition is associative.
PROOF:

$$\begin{aligned}[(a, b)] + ([(c, d)] + [(e, f)]) &= [(a, b)] + [(cf + de, df)] \\ &= [(adf + bcf + bde, bdf)] \\ &= [(ad + bc, bd)] + [(e, f)] \\ &= ([(a, b)] + [(c, d)]) + [(e, f)]\end{aligned}$$

$\langle 2\rangle 3.$ $x + 0 = x$

PROOF:

$$\begin{aligned}[(a,b)] + [(0,1)] &= [(a1 + b0, b1)] \\ &= [(a,b)]\end{aligned}$$

$\langle 2\rangle 4.$ For all x, there exists y such that $x + y = 0$

PROOF:

$$\begin{aligned}[(a,b)] + [(-a,b)] &= [(ab - ab, b^2)] \\ &= [(0, b^2)] \\ &= [(0,1)]\end{aligned}$$

since $(0, b^2) \sim (0,1)$.

$\langle 2\rangle 5.$ Multiplication is commutative.

PROOF: $[(a,b)][(c,d)] = [(c,d)][(a,b)] = [(ac, bd)]$

$\langle 2\rangle 6.$ Multiplication is associative.

PROOF: $[(a,b)]([(c,d)][(e,f)]) = ([(a,b)][(c,d)])[(e,f)] = [(ace, bdf)]$

$\langle 2\rangle 7.$ $x1 = x$

PROOF: $[(a,b)][(1,1)] = [(a1, b1)] = [(a,b)]$

$\langle 2\rangle 8.$ For all $x \neq 0$, there exists y such that $xy = 1$

$\langle 3\rangle 1.$ LET: $a, b \in R$ with $b \neq 0$ and $(a,b) \nsim (0,1)$

$\langle 3\rangle 2.$ $a \neq 0$

$\langle 3\rangle 3.$ $[(a,b)][(b,a)] = [(1,1)]$

PROOF: Since $(ab, ab) \sim (1,1)$

$\langle 2\rangle 9.$ Multiplication is distributive over addition.

PROOF:

$$\begin{aligned}[(a,b)]([(c,d)] + [(e,f)]) &= [(a,b)][(cf + de, df)] \\ &= [(acf + ade, bdf)] \\ &= [(abcf + abde, b^2 df)] \\ &= [(ac, bd)] + [(ae, bf)] \\ &= [(a,b)][(c,d)] + [(a,b)][(e,f)]\end{aligned}$$

$\langle 2\rangle 10.$ $0 \neq 1$

PROOF: Since $(0,1) \nsim (1,1)$

$\square$

Definition 7.3 (Rational Numbers)**.** The field of *rational numbers* $\mathbb{Q}$ is the field of fractions of the integers.

Theorem 7.4. *Every finite integral domain with at least two elements is a field.*

PROOF: Let D be a non-trivial finite integral domain. Let $x \in D$. The map that sends y to xy is an injective map $D \to D$, hence a bijection by the Pigeonhole Principle. Therefore there exists y such that $xy = 1$. $\square$

Corollary 7.4.1. *For any integer $n > 1$, we have $\mathbb{Z}_n$ is a field if and only if n is prime.*

Theorem 7.5. *Let a_0, a_1, ..., a_{k-1} be integers. If x is a rational number such that $x^k + a_{k-1}x^{k-1} + \cdots + a_0 = 0$ then x is an integer.*

PROOF:
⟨1⟩1. PICK integers p, q such that $x = p/q$ with $\gcd(p, q) = 1$
⟨1⟩2. $p^k + a_{k-1}qp^{k-1} + \cdots + a_0 q^k = 0$
⟨1⟩3. $q = 1$
  ⟨2⟩1. ASSUME: for a contradiction q has a prime factor r
  ⟨2⟩2. $r \mid a_{k-1}qp^{k-1} + \cdots + a_0 q^k$
  ⟨2⟩3. $r \mid p^k$
  ⟨2⟩4. $r \mid p$
  ⟨2⟩5. Q.E.D.
    PROOF: This contradicts the fact that $\gcd(p, q) = 1$.
□

Corollary 7.5.1. *There is no rational number q such that $q^2 = 2$.*

7.1 Subfields

Definition 7.6 (Subfield)**.** Let $(E, +_E, \cdot_E)$ and $(F, +_F, \cdot_F)$ be fields. Then E is a *subfield* of F if and only if $E \subseteq F$, $+_E = +_F \upharpoonright E^2$ and $\cdot_E = \cdot_F \upharpoonright E^2$.

Proposition 7.7. *Let $(F, +_F, \cdot_F)$ be a field and $E \subseteq F$. If E contains a non-zero element and is closed under subtraction and division (i.e. whenever $x, y \in E$ and $y \neq 0$ then $x/y \in E$), then $(E, +_F \upharpoonright E^2, \cdot_F \upharpoonright E^2)$ is a subfield of F.*

PROOF:
⟨1⟩1. $1 \in E$
  ⟨2⟩1. PICK $a \in E$ with $a \neq 0$
  ⟨2⟩2. $a/a \in E$
⟨1⟩2. $0 \in E$
  PROOF: Since $0 = 1 - 1$
⟨1⟩3. $\forall x \in E. -x \in E$
  PROOF: Since $-x = 0 - x$
⟨1⟩4. E is closed under addition.
  PROOF: For $x, y \in E$, we have $x + y = x - (-y) \in E$.
⟨1⟩5. $\forall x \in E - \{0\}. x^{-1} \in E$
  PROOF: Since $x^{-1} = 1/x$.
⟨1⟩6. E is closed under multiplication.
  PROOF: For $x, y \in E$, if $y = 0$ then $xy = 0 \in E$. Otherwise $xy = x/y^{-1} \in E$.
□

Definition 7.8 (Prime Field)**.** A field is *prime* iff it contains no proper subfield.

Definition 7.9 (Integers and Rational Numbers of a Field)**.** In any field F, the *integers* of F are the elements of the form $n1$ for $n \in \mathbb{Z}$.

The *rational numbers* of F are the elements of the form m/n where m and n are integers of F with $n \neq 0$.

Proposition 7.10. *For any field F, the rational numbers of F form a subfield of F which is minimal (i.e. a subfield of every other subfield of F).*

Proposition 7.11. *If F has characteristic 0 then the rationals of F are isomorphic to $\mathbb{Q}$.*

Corollary 7.11.1. *In any ordered field F, the rationals of F are isomorphic to $\mathbb{Q}$.*

Theorem 7.12. *The prime fields are $\mathbb{Z}_p$ for p prime and $\mathbb{Q}$.*

PROOF:
$\langle 1 \rangle 1$. Every $\mathbb{Z}_p$ is prime.
PROOF: If F is a subfield of $\mathbb{Z}_p$ then F contains every integer and so is $\mathbb{Z}_p$.
$\langle 1 \rangle 2$. $\mathbb{Q}$ is a prime field.
PROOF: If F is a subfield of $\mathbb{Q}$ then F contains every integer, hence contains m/n for m and n integers with $n \neq 0$, and so is $\mathbb{Q}$.
$\langle 1 \rangle 3$. For p prime, if F is a prime field of characteristic p then $F \cong \mathbb{Z}_p$.
$\langle 2 \rangle 1$. If F is any field of characteristic p then $\mathbb{Z}_p$ is a subfield of F.
$\langle 3 \rangle 1$. Define $\phi : \mathbb{Z}_p \to F$ by $\phi(k) = k1$
$\langle 3 \rangle 2$. ϕ is injective.
PROOF: Since $k1 \neq l1$ for $0 \leq k, l < p$.
$\langle 3 \rangle 3$. ϕ preserves addition.
PROOF: If $k + l \cong m(\mod p)$ then $k1 + l1 = m1$ in F.
$\langle 3 \rangle 4$. ϕ preserves multiplication.
PROOF: If $kl \cong m(\mod p)$ then $(k1)(l1) = m1$ in F.
$\langle 1 \rangle 4$. If F is a prime field of characteristic 0 then $F \cong \mathbb{Q}$.
$\langle 2 \rangle 1$. If F is any field of characteristic 0 then $\mathbb{Q}$ is a subfield of F.
□

8 Rational Numbers

Lemma 8.1. *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 8.2. The ordering on the rationals is defined by: if b and d are positive then $[(a, b)] < [(c, d)]$ iff $ad < bc$.

Theorem 8.3. *The relation $<$ is a linear ordering on $\mathbb{Q}$.*

PROOF: Easy. □

Definition 8.4 (Positive)**.** A rational q is *positive* iff $0 < q$.

Definition 8.5 (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 8.6. *For any rational s, the function that maps q to $q+s$ is strictly monotone.*

PROOF: Easy. □

Theorem 8.7. *For any positive rational s, the function that maps q to qs is strictly monotone.*

PROOF: Easy. □

Theorem 8.8. *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 9.1 (Ordered Field)**.** An *ordered field* is an ordered integral domain $(D, +, \cdot, 0, 1, <)$ such that $(D, +, \cdot, 0, 1)$ is a field.

Theorem 9.2. *The quotient field F of an ordered integral domain D is an ordered field under: $[(a, b)]$ is positive iff $ab > 0$ in D. The canonical imbedding $D \hookrightarrow F$ is strictly monotone.*

PROOF:
$\langle 1\rangle 1$. LET: D be an ordered integral domain and F its quotient field.
$\langle 1\rangle 2$. Define a fraction $[(a, b)]$ to be positive iff $ab > 0$
  $\langle 2\rangle 1$. LET: $a, b, c, d \in D$ with $b \neq 0 \neq d$
  $\langle 2\rangle 2$. ASSUME: $(a, b) \sim (c, d)$ and $ab > 0$
    PROVE: $cd > 0$
  $\langle 2\rangle 3$. $ad = bc$
  $\langle 2\rangle 4$. CASE: $d > 0$
    $\langle 3\rangle 1$. $abd > 0$
    $\langle 3\rangle 2$. $b^2c > 0$
    $\langle 3\rangle 3$. $c > 0$
    $\langle 3\rangle 4$. $cd > 0$
  $\langle 2\rangle 5$. CASE: $d < 0$
    $\langle 3\rangle 1$. $abd < 0$
    $\langle 3\rangle 2$. $b^2c < 0$
    $\langle 3\rangle 3$. $c < 0$

$\langle 3\rangle 4.$ $cd > 0$
$\langle 1\rangle 3.$ 0 is not positive.
PROOF: Since $0 \times 1 \not> 0$.
$\langle 1\rangle 4.$ For any $x \in F$, either x is positive or $x = 0$ or $-x$ is positive.
$\langle 2\rangle 1.$ LET: $x = [(a, b)]$
$\langle 2\rangle 2.$ Either $ab > 0$ or $ab = 0$ or $ab < 0$
$\langle 2\rangle 3.$ If $ab < 0$ then $-x$ is positive.
PROOF: Since $-x = [(-a, b)]$ and $-ab > 0$.
$\langle 1\rangle 5.$ If x and y are positive then $x + y$ is positive.
$\langle 2\rangle 1.$ LET: $x = [(a, b)]$ and $y = [(c, d)]$
$\langle 2\rangle 2.$ ASSUME: $ab > 0$ and $cd > 0$
$\langle 2\rangle 3.$ $x + y = [(ad + bc, bd)]$
$\langle 2\rangle 4.$ $(ad + bc)bd > 0$
$\langle 1\rangle 6.$ If x and y are positive then xy is positive.
$\langle 2\rangle 1.$ LET: $x = [(a, b)]$ and $y = [(c, d)]$
$\langle 2\rangle 2.$ ASSUME: $ab > 0$ and $cd > 0$
$\langle 2\rangle 3.$ $xy = [(ac, bd)]$
$\langle 2\rangle 4.$ $acbd > 0$
$\langle 1\rangle 7.$ For $a, b \in D$, if $a < b$ then $[(a, 1)] < [(b, 1)]$
PROOF: We have $[(a - b, 1)]$ is positive because $a - b > 0$.
□

Corollary 9.2.1. *The rationals are an ordered field under $p/q < r/s$ iff $ps < rq$ for q, s positive.*

Theorem 9.3. *The relation $p/q < r/s$ iff $ps < qr$ for q, s positive is the only relation that makes $\mathbb{Q}$ into an ordered field.*

PROOF: If $\mathbb{Q}$ is an ordered field under $<$ then, for q, s positive:

$$p/q < r/s \Leftrightarrow ps < qr$$
$$\Leftrightarrow$$

Proposition 9.4. *In any ordered field, if $x \neq 0$, then $x > 0$ iff $x^{-1} > 0$.*

PROOF:
$\langle 1\rangle 1.$ If $x > 0$ then $x^{-1} > 0$
PROOF: If $x^{-1} \leq 0$ then $xx^{-1} = 1 \leq 0$.
$\langle 1\rangle 2.$ If $x^{-1} > 0$ then $x > 0$
PROOF: From $\langle 1\rangle 1$ since $(x^{-1})^{-1} = x$.
□

Corollary 9.4.1. *In any ordered field, if $x \neq 0$, then $x < 0$ iff $x^{-1} < 0$.*

Proposition 9.5. *In any ordered field, if $y > 0$ and $v > 0$ then $x/y < u/v$ iff $xv = yu$.*

PROOF: Multiplying by yv or by $y^{-1}v^{-1}$. □

Proposition 9.6. *In any ordered field, if $y \neq 0$ then $|x/y| = |x|/|y|$.*

PROOF: Since $|x/y||y| = |x|$. □

Corollary 9.6.1. *In any ordered field, if $y \neq 0$ then $|y^{-1}| = 1/|y|$.*

Proposition 9.7 (Density)**.** *In any ordered field, if $x < y$ then $x < (x+y)/2 < y$.*

PROOF: If $x < y$ then $2x < x + y$ so $x < (x + y)/2$, and $x + y < 2y$ so $(x + y)/2 < y$. □

Proposition 9.8 (Cauchy-Schwarz Inequality)**.** *Let F be an ordered field. Let $a_1, \ldots, a_n, b_1, \ldots, b_n \in F$. Then*

$$(a_1 b_1 + \cdots + a_n b_n)^2 \leq (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) \ .$$

PROOF:
⟨1⟩1. $\sum_{i=1}^n \sum_{j=1}^n (a_i b_j - a_j b_i)^2 = 2 \sum_{i=1}^n a_i^2 \sum_{j=1}^n b_j^2 - 2 \left(\sum_{i=1}^n a_i b_i\right)^2$
PROOF:

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^n (a_i b_j - a_j b_i)^2 &= \sum_{i=1}^n \sum_{j=1}^n a_i^2 b_j^2 - 2 \sum_{i_1}^n \sum_{j=1}^n a_i b_j a_j b_i + \sum_{i=1}^n \sum_{j=1}^n a_j^2 b_i^2 \\ &= 2 \sum_{i=1}^n a_i^2 \sum_{j=1}^n b_j^2 - 2 \left(\sum_{i=1}^n a_i b_i \right)^2 \end{aligned}$$

⟨1⟩2. Q.E.D.
PROOF: Since a sum of squares must be ≥ 0.
□

Definition 9.9 (Cut)**.** Let F be an ordered field. A *cut* in F is a pair (A, B) of subsets of F such that:

1. A and B are nonempty.
2. $A \cup B = F$
3. $\forall x \in A . \forall y \in B . x < y$

Definition 9.10 (Gap)**.** Let F be an ordered field. A *gap* in F is a cut (A, B) in F such that A has no maximum element and B has no minimum element.

Proposition 9.11. *Let (A, B) be a cut in an ordered field F. Then (A, B) is a gap if and only if A has no supremum.*

PROOF:
⟨1⟩1. If A has a supremum then (A, B) is not a gap.
⟨2⟩1. LET: s be the supremum of A
⟨2⟩2. CASE: $s \in A$
PROOF: In this case s is the maximum element of A.
⟨2⟩3. CASE: $s \in B$
PROOF: In this case s is the minimum element of B.
⟨1⟩2. If (A, B) is not a gap then A has a supremum.

PROOF: If A has a maximum element then it is a supremum of A, and if B has a minimum element then it is a supremum of A.
□

Proposition 9.12. *Let (A, B) be a cut in an ordered field F. Then (A, B) is a gap if and only if B has no infimum.*

PROOF: Dual. □

Definition 9.13 (Cut Determined by an Element)**.** Let F be an ordered field and $c \in F$. The cuts *determined* by c are $(\{x \in F : x \leq c\}, \{x \in F : x > c\})$ and $(\{x \in F : x \leq c\}, \{x \in F : x > c\})$.

Definition 9.14 (Complete Ordered Field)**.** A *complete ordered field* is an ordered field with no gaps.

Theorem 9.15. *Let F be an ordered field. The following are equivalent.*

1. *F is complete.*
2. *Every nonempty subset of F bounded above has a supremum.*
3. *Every nonempty subset of F bounded below has an infimum.*

PROOF:
$\langle 1\rangle 1$. $1 \Rightarrow 2$
  $\langle 2\rangle 1$. ASSUME: F is complete
  $\langle 2\rangle 2$. LET: A be a nonempty subset of F bounded above.
  $\langle 2\rangle 3$. LET: $A_1 = \{x \in F : \exists y \in A. x \leq y\}$
  $\langle 2\rangle 4$. LET: $B = F - A_1$
  $\langle 2\rangle 5$. (A_1, B) is a cut.
    $\langle 3\rangle 1$. $A_1 \neq \emptyset$
      $\langle 4\rangle 1$. PICK $a \in A$
        PROOF: A is nonempty ($\langle 2\rangle 2$).
      $\langle 4\rangle 2$. $a - 1 \in A_1$
    $\langle 3\rangle 2$. $B \neq \emptyset$
      $\langle 4\rangle 1$. PICK an upper bound u for A
        PROOF: A is bounded above ($\langle 2\rangle 2$).
      $\langle 4\rangle 2$. $u + 1 \in B$
    $\langle 3\rangle 3$. $A_1 \cup B = F$
      PROOF: By $\langle 2\rangle 4$.
    $\langle 3\rangle 4$. $\forall x \in A_1. \forall y \in B. x < y$
      PROOF: If $x \in A_1$ and $y \leq x$ then $y \in A_1$.
  $\langle 2\rangle 6$. (A_1, B) is not a gap.
    PROOF: By $\langle 2\rangle 1$.
  $\langle 2\rangle 7$. CASE: A_1 has a maximum element.
    $\langle 3\rangle 1$. LET: s be the maximum of A_1.
    $\langle 3\rangle 2$. $s \in A$
      $\langle 4\rangle 1$. PICK $x \in A$ such that $s \leq x$

⟨4⟩2. $x \in A_1$
⟨4⟩3. $x \leq s$
PROOF: By the maximality of s.
⟨4⟩4. $x = s$
⟨3⟩3. s is an upper bound for A.
PROOF: Since $A \subseteq A_1$.
⟨3⟩4. s is the maximum element of A.
⟨3⟩5. s is the supremum of A.
⟨2⟩8. CASE: B has a minimum element.
⟨3⟩1. LET: s be the minimum element in B.
⟨3⟩2. s is an upper bound for A
PROOF: For all $x \in A$ we have $x \in A_1$ and so $x < s$.
⟨3⟩3. For any upper bound u for A we have $s \leq u$
⟨4⟩1. LET: u be an upper bound for A.
⟨4⟩2. $u \notin A_1$
⟨5⟩1. ASSUME: for a contradiction $u \in A_1$
⟨5⟩2. $u < s$
⟨5⟩3. PICK y such that $u < y < s$
⟨5⟩4. CASE: $y \in A_1$
⟨6⟩1. PICK $x \in A$ such that $y \leq x$
⟨6⟩2. $u < x$
⟨6⟩3. Q.E.D.
PROOF: This contradicts ⟨4⟩1.
⟨5⟩5. CASE: $y \in B$
PROOF: This contradicts ⟨3⟩1.
⟨4⟩3. $u \in B$
⟨4⟩4. $s \leq u$
PROOF: By minimality of s.
⟨1⟩2. $2 \Rightarrow 1$
PROOF: By Proposition 9.11
⟨1⟩3. $1 \Rightarrow 3$
PROOF: Similar to ⟨1⟩1.
⟨1⟩4. $3 \Rightarrow 1$
PROOF: By Proposition 9.12.
□

Definition 9.16 (Archimedean)**.** An ordered field F is *Archimedean* if and only if, for all positive $x, y \in F$, there exists $n \in \mathbb{Z}^+$ such that $nx > y$.

Lemma 9.17. *The rational numbers are Archimedean.*

PROOF: Let $p = a/b$ and $r = c/d$ where a, b and d are positive. Let $n = bc + 1$. Then $bc < adn$ so $r < pn$. □

Example 9.18. The quotient field of $\mathbb{Z}[x]$ is not Archimedean, since $n1 < x$ for all $n \in \mathbb{Z}^+$.

Theorem 9.19. *Let F be an ordered field. Then F is Archimedean if and only if the set of integers in F is not bounded above.*

PROOF:
$\langle 1\rangle 1$. If F is Archimedean then the set of integers in F is not bounded above.
  $\langle 2\rangle 1$. ASSUME: F is Archimedean.
  $\langle 2\rangle 2$. For every integer y in F, there exists an integer n such that $n1 > y$.
  $\langle 2\rangle 3$. The integers in F have no upper bound.
$\langle 1\rangle 2$. If the set of integers in F is not bounded above then F is Archimedean.
  $\langle 2\rangle 1$. ASSUME: The set of integers in F is not bounded above.
  $\langle 2\rangle 2$. LET: $x, y \in F$ be positive.
  $\langle 2\rangle 3$. PICK an integer n such that $n1 > y/x$
  $\langle 2\rangle 4$. $nx > y$
□

Corollary 9.19.1. *Let F be an ordered field. Then F is Archimedean if and only if, for every positive $z \in F$, there exists a positive integer n such that $1/n < z$.*

Theorem 9.20. *Let F be an Archimedean ordered field. Let $x \in F$. Then there exists a unique integer n such that $n \leq x < n + 1$.*

PROOF:
$\langle 1\rangle 1$. There exists an integer n such that $n \leq x < n + 1$
  $\langle 2\rangle 1$. PICK a positive integer j such that $-x < j$.
    PROOF: By the Archimedean property applied to $-x$.
  $\langle 2\rangle 2$. LET: h be the least positive integer such that $x + j < h$.
    PROOF: By the Archimedean property applied to $x + j$.
  $\langle 2\rangle 3$. LET: $n = h - j - 1$
  $\langle 2\rangle 4$. $x < n + 1$
  $\langle 2\rangle 5$. $x \geq n$
    PROOF: Since $h - 1 \leq x + j$ by the minimality of h and the fact that $0 < x + j$.
$\langle 1\rangle 2$. If m and n are integers with $m \leq x < m + 1$ and $n \leq x < n + 1$ then $m = n$
  $\langle 2\rangle 1$. $m < n + 1$
  $\langle 2\rangle 2$. $m \leq n$
  $\langle 2\rangle 3$. $n < m + 1$
  $\langle 2\rangle 4$. $n \leq m$
□

Definition 9.21 (Floor)**.** In any Archimedean ordered field, the *floor* of x, $\llcorner x \lrcorner$, is the integer such that $\llcorner x \lrcorner \leq x < \llcorner x \lrcorner + 1$.

Theorem 9.22. *Every complete ordered field is Archimedean.*

PROOF:
$\langle 1\rangle 1$. LET: F be a complete ordered field.
$\langle 1\rangle 2$. ASSUME: for a contradiction the integers of F are bounded above.
$\langle 1\rangle 3$. LET: u be the supremum of the integers of F
$\langle 1\rangle 4$. $u < \llcorner u \lrcorner + 1$

$\langle 1\rangle 5.$ $\llcorner u \lrcorner + 1 \leq u$
  PROOF: Since u is an upper bound for the integers of F.
$\langle 1\rangle 6.$ Q.E.D.
  PROOF: This is a contradiction.
□

Definition 9.23 (Dense)**.** Let F be an ordered field and $A \subseteq F$. Then A is *dense* in F if and only if, for all $x, y \in F$ with $x < y$, there exists $z \in A$ with $x < z < y$.

Theorem 9.24. *Let F be an ordered field. Then F is Archimedean if and only if the rational numbers are dense in F.*

PROOF:
$\langle 1\rangle 1.$ If F is Archimedean then the rationals are dense in F.
  $\langle 2\rangle 1.$ LET: F be an Archimedean ordered field.
  $\langle 2\rangle 2.$ LET: $x, y \in F$ with $x < y$.
  $\langle 2\rangle 3.$ LET: n be the least positive integer such that $1/n < y - x$.
  $\langle 2\rangle 4.$ LET: $k = \llcorner nx + 1 \lrcorner$
  $\langle 2\rangle 5.$ $nx < k \leq nx + 1$
  $\langle 2\rangle 6.$ $x < k/n < y$
$\langle 1\rangle 2.$ If the rationals are dense in F then F is Archimedean.
  $\langle 2\rangle 1.$ ASSUME: The rationals are dense in F.
  $\langle 2\rangle 2.$ LET: $x \in F$
    PROVE: There exists an integer n such that $x < n$
  $\langle 2\rangle 3.$ ASSUME: w.l.o.g. $x > 0$
  $\langle 2\rangle 4.$ PICK
□

Lemma 9.25. *Let F be an Archimedean ordered field. Let $x \in F$. Then x is the supremum of $A = \{q \in F : q \text{ is rational}, q < x\}$.*

PROOF:
$\langle 1\rangle 1.$ x is an upper bound for A.
$\langle 1\rangle 2.$ For any upper bound u for A we have $x \leq u$
  $\langle 2\rangle 1.$ LET: u be an upper bound for A.
  $\langle 2\rangle 2.$ ASSUME: for a contradiction $u < x$.
  $\langle 2\rangle 3.$ PICK a rational q with $u < q < x$.
    PROOF: Theorem 9.24.
  $\langle 2\rangle 4.$ $q \in A$ and $u < q$
  $\langle 2\rangle 5.$ Q.E.D.
    PROOF: This contradicts $\langle 2\rangle 1$.
□

10 The Real Numbers

Definition 10.1 (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 10.2. For any rational number u, let $u_{\mathbb{R}} = \{x \in \mathbb{Q} : x < u\}$.

Proposition 10.3. $\forall u \in \mathbb{Q}.u_{\mathbb{R}} \in \mathbb{R}$

PROOF:
$\langle 1 \rangle 1.$ LET: $u \in \mathbb{Q}$
$\langle 1 \rangle 2.$ $u_{\mathbb{R}} \neq \emptyset$
  PROOF: Since $u - 1 \in u_{\mathbb{R}}$.
$\langle 1 \rangle 3.$ $u_{\mathbb{R}} \neq \mathbb{Q}$
  PROOF: Since $u \notin u_{\mathbb{R}}$.
$\langle 1 \rangle 4.$ $u_{\mathbb{R}}$ is closed downwards.
  PROOF: If $x < y < u$ then $x < u$.
$\langle 1 \rangle 5.$ $u_{\mathbb{R}}$ has no largest member.
  PROOF: If $x \in u_{\mathbb{R}}$ then $x < (x + u)/2 \in u_{\mathbb{R}}$.
$\square$

Definition 10.4. Given real numbers x and y, we write $x < y$ iff $x \subset y$.

Theorem 10.5. *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). $\square$

Theorem 10.6. *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 10.7 (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 10.8. *Addition is associative and commutative.*

PROOF: Easy. □

Theorem 10.9. *For every real x we have $x + 0_{\mathbb{R}} = x$.*

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 10.10. 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: $-r \notin -x$

⟨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 10.11. *Let ϵ be a positive real number. For any real x, there exists $q \in x$ such that $q + \epsilon$ is an upper bound for x but not the least upper bound for x.*

PROOF:
⟨1⟩1. PICK a rational $a_1 \in x$ such that if x has a least upper bound s then $a_1 > s - \epsilon$.
⟨1⟩2. LET: k be least such that $a_1 + k\epsilon$ is an upper bound for x
PROOF: By Lemma 9.17.
⟨1⟩3. $a_1 + k\epsilon$ is an upper bound for x that is not the least upper bound for x
⟨1⟩4. $a_1 + (k-1)\epsilon \in x$
□

Theorem 10.12. *For any real x we have $x + (-x) = 0$.*

PROOF:
⟨1⟩1. $x + (-x) \subseteq 0$
⟨2⟩1. LET: $q \in x$ and $r \in -x$
⟨2⟩2. PICK $s > r$ such that $-s \notin x$
⟨2⟩3. $q < -s$
⟨2⟩4. $q < -r$
⟨2⟩5. $q + r < 0$
⟨1⟩2. $0 \subseteq x + (-x)$
⟨2⟩1. LET: $p < 0$
⟨2⟩2. PICK $q \in x$ such that $q - p/2 \notin x$
PROOF: By Lemma 10.11.
⟨2⟩3. LET: $s = p/2 - q$
⟨2⟩4. $-s \notin x$
⟨2⟩5. $p - q \in -x$
PROOF: Since $p - q < s$ and $-s \notin x$.
⟨2⟩6. $p = q + (p - q) \in x + (-x)$
□

Theorem 10.13. *The reals form an Abelian group under addition.*

PROOF: Easy. ∎

Theorem 10.14. *For any real z, the function that maps x to $x + z$ is strictly monotone.*

PROOF:
⟨1⟩1. ASSUME: $x < y$
⟨1⟩2. $x + z \subseteq y + z$
  PROOF: From the definition.
⟨1⟩3. $x + z \neq y + z$
  PROOF: By cancellation.
∎

Definition 10.15 (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 10.16 (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:
⟨1⟩1. LET: $x \geq 0$ and $y \geq 0$
⟨1⟩2. $xy \neq \emptyset$
  PROOF: Since $-1 \in xy$
⟨1⟩3. $xy \neq \mathbb{Q}$
  ⟨2⟩1. PICK $r \in \mathbb{Q} - x$ and $s \in \mathbb{Q} - y$
  ⟨2⟩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 $r's' < rs$
  ⟨2⟩3. $rs \notin xy$
⟨1⟩4. xy is closed downwards.
  ⟨2⟩1. LET: $q \in xy$ and $r < q$
  ⟨2⟩2. ASSUME: $0 \leq r$
  ⟨2⟩3. PICK rationals a, b with $0 \leq a \in x$ and $0 \leq b \in y$ such that $q = ab$
  ⟨2⟩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 10.17. *Multiplication is commutative and associative.*

PROOF: Easy. □

Theorem 10.18.

$$\forall x, y, z \in \mathbb{R}. x(y + z) = xy + xz$$

PROOF:
$\langle 1 \rangle 1$. LET: $x, y, z \in \mathbb{R}$
$\langle 1 \rangle 2$. CASE: $x, y, z > 0$
$\langle 2 \rangle 1$. $xy > 0$
$\langle 2 \rangle 2$. $xz > 0$
$\langle 2 \rangle 3$. $y + z > 0$
$\langle 2 \rangle 4$. $x(y + z) > 0$
$\langle 2 \rangle 5$. $xy + xz > 0$
$\langle 2 \rangle 6$. $x(y + z) \subseteq xy + xz$
$\langle 3 \rangle 1$. LET: $q \in x(y + z)$
$\langle 3 \rangle 2$. ASSUME: w.l.o.g. $0 < q$
PROOF: Otherwise $q \in xy$ and $0 \in xz$ so $q \in xy + xz$
$\langle 3 \rangle 3$. PICK $a \in x$, $b \in y$ and $c \in z$ such that $0 < a$, $0 < b+c$ and $q = a(b+c)$
$\langle 3 \rangle 4$. $ab \in xy$
$\langle 4 \rangle 1$. CASE: $b \leq 0$
PROOF: Then $ab \leq 0$ so $ab \in xy$
$\langle 4 \rangle 2$. CASE: $b > 0$
PROOF: Then $ab \in xy$ by definition.
$\langle 3 \rangle 5$. $ac \in xz$
PROOF: Similar.
$\langle 3 \rangle 6$. $q \in xy + xz$
$\langle 2 \rangle 7$. $xy + xz \subseteq x(y + z)$
$\langle 3 \rangle 1$. LET: $q \in xy + xz$
$\langle 3 \rangle 2$. CASE: $\exists a, a_1 \in x. \exists b \in y. \exists c \in z. (a, b, c, a_1 > 0 \land q = ab + a_1 c)$
$\langle 4 \rangle 1$. LET: $a_2 = \max(a, a_1)$
$\langle 4 \rangle 2$. $q \leq a_2(b + c)$

⟨4⟩3. $q \in x(y+z)$

⟨3⟩3. CASE: $\exists a \in x. \exists b \in y. \exists u \leq 0. q = ab + u$

⟨4⟩1. $ab + u \leq ab$

⟨4⟩2. $ab + u \in xy$

⟨4⟩3. CASE: $ab + u \leq 0$

PROOF: $ab + u \in x(y+z)$

⟨4⟩4. CASE: $ab + u > 0$

⟨5⟩1. PICK $a' \in x$, $b' \in y$ such that $0 < a'$, $0 < b'$ and $ab + u = a'b'$

⟨5⟩2. $b' \in y + z$

⟨5⟩3. $a'b' \in x(y+z)$

⟨3⟩4. CASE: $\exists u \leq 0. \exists a \in x. \exists c \in z. q = u + ac$

PROOF: Similar.

⟨3⟩5. CASE: $\exists u, u' \leq 0. q = u + u'$

⟨4⟩1. $u + u' \leq 0$

⟨4⟩2. $u + u' \in x(y+z)$

⟨1⟩3. CASE: $x = 0$ or $y = 0$ or $z = 0$

PROOF: Then $x(y+z) = xy + xz = 0$

⟨1⟩4. CASE: $x < 0$ and $y > 0$ and $z > 0$

PROOF:

$$\begin{aligned} x(y+z) &= -((-x)(y+z)) \\ &= -((-x)y + (-x)z) && (\langle 1\rangle 2) \\ &= -(-(xy) + -(xz)) \\ &= xy + xz \end{aligned}$$

⟨1⟩5. CASE: $x > 0$ and $y < 0$ and $z > 0$

⟨2⟩1. $z = -y$

⟨3⟩1. $x(y+z) = 0$

⟨3⟩2. $xy + xz = 0$

⟨2⟩2. $z > -y$

PROOF:

$$\begin{aligned} xy + xz &= xy + (x(-y + y + z)) \\ &= -(x(-y)) + x(-y) + x(y+z) && (\langle 1\rangle 2) \\ &= x(y+z) \end{aligned}$$

⟨2⟩3. $z < -y$

PROOF:

$$\begin{aligned} xy + xz &= -(x(-y)) + xz \\ &= -(x(z - y - z)) + xz \\ &= -(xz + x(-y - z)) + xz && (\langle 1\rangle 2) \\ &= -xz - x(-y - z) + xz \\ &= -x(-y - z) \\ &= x(y+z) \end{aligned}$$

⟨1⟩6. CASE: $x > 0$ and $y < 0$ and $z < 0$

PROOF:

$$\begin{aligned} x(y+z) &= -(x(-y-z)) \\ &= -(x(-y)) - (x(-z)) && (\langle 1\rangle 2) \\ &= xy + xz \end{aligned}$$

$\langle 1\rangle 7$. CASE: $x < 0$ and $y < 0$ and $z > 0$

$\langle 2\rangle 1$. CASE: $y = -z$

PROOF: Then $x(y+z) = xy + xz = 0$.

$\langle 2\rangle 2$. CASE: $y > -z$

PROOF:

$$\begin{aligned} x(y+z) &= -((-x)(y+z)) \\ &= -((-x)y) - ((-x)z) && (\langle 1\rangle 5) \\ &= --((-x)(-y)) + xz \\ &= xy + xz \end{aligned}$$

$\langle 2\rangle 3$. CASE: $y < -z$

PROOF:

$$\begin{aligned} x(y+z) &= (-x)(-y-z) \\ &= (-x)(-y) + (-x)(-z) && (\langle 1\rangle 5) \\ &= xy + xz \end{aligned}$$

$\langle 1\rangle 8$. CASE: $x < 0$ and $y < 0$ and $z < 0$

PROOF:

$$\begin{aligned} x(y+z) &= (-x)(-y-z) \\ &= (-x)(-y) + (-x)(-z) && (\langle 1\rangle 2) \\ &= xy + xz \end{aligned}$$

$\square$

Definition 10.19. The real number *one* is $1 = \{q \in \mathbb{Q} : q < 1\}$.

It is easy to check this is a Dedekind cut.

Theorem 10.20. $0 \neq 1$

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

Theorem 10.21. *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 $q \in x$.

⟨2⟩2. $x \subseteq x1$

⟨3⟩1. LET: $q \in x$

⟨3⟩2. ASSUME: w.l.o.g. $0 \leq q$

⟨3⟩3. PICK $r \in x$ with $q < r$

⟨3⟩4. $0 \leq q/r < 1$

⟨3⟩5. $q = r(q/r) \in x1$

⟨1⟩3. CASE: $x < 0$

PROOF: Then $x1 = -((-x)1) = -(-x) = x$.

□

Theorem 10.22. *For any nonzero real x, there is a nonzero real y such that $xy = 1$.*

PROOF:

⟨1⟩1. CASE: $x > 0$

⟨2⟩1. LET: $y = \{q \in \mathbb{Q} : q \leq 0\} \cup \{1/q : q \text{ is an upper bound of } x \text{ but not the least upper bound of } x\}$

⟨2⟩2. $y \in \mathbb{R}$

⟨3⟩1. $y \neq \emptyset$

PROOF: Since $-1 \in y$.

⟨3⟩2. $y \neq \mathbb{Q}$

PROOF: Pick a positive integer $q \in x$. Then $1/q \notin y$.

⟨3⟩3. y is closed downwards.

PROOF: Easy.

⟨3⟩4. y has no largest member.

⟨4⟩1. LET: $q \in y$

PROVE: There exists $r \in y$ such that $q < r$

⟨4⟩2. CASE: $q \leq 0$

⟨5⟩1. PICK a rational r that is an upper bound of x but not the least upper bound of x

⟨5⟩2. $q < 1/r \in y$

⟨4⟩3. CASE: $q > 0$

⟨5⟩1. $1/q$ is an upper bound of x but not the least upper bound of x

⟨5⟩2. PICK $r < 1/q$ such that r is an upper bound of x but not the least upper bound of x

⟨5⟩3. $q < 1/r \in y$

⟨2⟩3. $0 < y$

PROOF: Easy

⟨2⟩4. $xy = 1$

⟨3⟩1. $xy \subseteq 1$

⟨4⟩1. LET: $q \in xy$

⟨4⟩2. ASSUME: w.l.o.g. $q > 0$

⟨4⟩3. PICK $r \in x$ and $s \in y$ such that $r > 0$, $s > 0$ and $q = rs$

⟨4⟩4. $1/s$ is an upper bound of x

⟨4⟩5. $r < 1/s$

⟨4⟩6. $rs < 1$

⟨3⟩2. $1 \subseteq xy$

⟨4⟩1. LET: q be a rational with $0 < q < 1$

$\langle 4\rangle 2$. Pick $r \in x$ with $0 < r$

$\langle 4\rangle 3$. $(1-q)r > 0$

$\langle 4\rangle 4$. Pick $a \in x$ such that $a > 0$ and $a + (1-q)r$ is an upper bound for x but not the least upper bound for x

$\langle 4\rangle 5$. Let: $w = a + (1-q)r$

$\langle 4\rangle 6$. $w - a = (1-q)r < (1-q)w$

$\langle 4\rangle 7$. $qw < a$

$\langle 4\rangle 8$. $w < a/q$

$\langle 4\rangle 9$. a/q is an upper bound of x and not the least upper bound of x.

$\langle 4\rangle 10$. $q/a \in y$

$\langle 4\rangle 11$. $q = a(q/a) \in xy$

$\langle 1\rangle 2$. Case: $x < 0$

$\langle 2\rangle 1$. Pick y such that $(-x)y = 1$

Proof: By $\langle 1\rangle 1$.

$\langle 2\rangle 2$. $x(-y) = 1$

$\square$

Theorem 10.23. *For any positive real z, the function that maps x to xz is strictly monotone.*

Proof:

$\langle 1\rangle 1$. Let: $0 < z$ and $x < y$

$\langle 1\rangle 2$. $y - x > 0$

$\langle 1\rangle 3$. $z(y-x) > 0$

Proof: Definition of multiplication.

$\langle 1\rangle 4$. $zx < zy$

$\square$

11 Complete Ordered Fields

Definition 11.1 (Complete Ordered Field)**.** An ordered field is *complete* iff it has the least upper bound property.

Theorem 11.2. *The reals form a complete ordered field.*

Proof: From the results above. $\square$

Theorem 11.3. *Any two complete ordered fields are isomorphic.*

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

Theorem 11.4. *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 $q \notin E(q)$.
□

Theorem 11.5 (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
$\langle 1 \rangle 3$. $\forall n \in \omega.f(n) \neq z$
□