Math 171 Class Notes

Lucas Garron

March 29, 2011

Mar 29, 2011

Reals

We will state several axioms. Any set with these properties is called the *set of real numbers*. (HW: Show that the set is unique).

Axiom Structure

1. Field Axoms (algebra), $+, \cdot$
2. Order Axioms, $>$
3. Completeness Axioms, related to limits

Algebraic structures:

Definition 1 *Semigroup.* A semigroup $(G, *)$ is a set G with a map $* : G \times G \to G$ $(*(g, g') = g*g'$ - $g, g' \in G)$
$*$ should be associative. $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$
There is an identity $e \in G$ such that $g * e = g = e * g$ for all $g \in G$.

Lemma 1 *The identity in a semigroup is unique.* Suppose both e and e' are identity elements. Then $e = e * e' = e'$.

Definition 2 *Commutative (or Abelian) Semigroup* A commutative semigroup is a semigroup $(G, *)$ such that $g * g' = g' * g$ for all $g, g' \in G$.

Definition 3 *Left inverse.* If $(G, *)$ is a semigroup, $g \in G$ is a left inverse for g is an element $g' \in G$ such that $g' * g = e$.

Definition 4 *Right inverse.* Same with $g * g' = e$.

Definition 5 *Invertible* $g \in G$ if it has a left inverse and a right inverse.

Lemma 2 *If $(G, *)$ is a semigroup and $g \in G$ is invertible, then any left inverse equals any right inverse.* Suppose $g \in G$, a a left inverse, r a right inver for g. Then $a = a * e = a * (g * b) = (a * g) * b = e * b = b$

Definition 6 *Group* A group $(G, *)$ is a semigroup all of whose elements are invertible.

Definition 7 *Commutative Group* A commutative group is a group if $g*g' = g'*g$ for all $g, g' \in G$.

Definition 8 *Field.* A field $(\mathbb{F}, +, \cdot)$ is a set F and two maps

1. $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$
2. $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

...such that $(\mathbb{F}, +)$ is a commutative group, $(F, \cdot)$ is a commutative semigroup.
0 in the identity of $(\mathbb{F}, +)$, 1 in the identity of $(\mathbb{F}, +)$, every $x \in \mathbb{F}$ $(x \neq 0)$ is invertible in $(F, \cdot)$, $1 \neq 0$, and the distributive law holds: $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ for all $x, y, z \in = \mathbb{F}$.

Lemma 3 *If $\mathbb{F}$ is a field, then for all $x \in \mathbb{F}, x \cdot 0 = 0$.*

Notation 1 *The inverse of x in $(\mathbb{F}, +)$ is written as $-x$. For $(\mathbb{F}, \cdot)$, $x^{-1} = \frac{1}{x}$*

Proof of Lemma: $0 = x \cdot 0 + (-(x \cdot 0)) = x \cdot (0 + 0) + (-(x \cdot 0)) = (x \cdot 0) + (x \cdot 0) + (-(x \cdot 0)) = (x \cdot 0) + ((x \cdot 0) + (-(x \cdot 0))) = (x \cdot 0) + 0 = x \cdot 0$

Example 1 *Other algebraic statements:*
$-x = (-1) \cdot x$ $(x \in \mathbb{F})$
$(-x) \cdot (-y) = x \cdot y$ $(x, y \in \mathbb{F})$

Example 2 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/2\mathbb{Z}$

Order Axioms

Definition 9 *Ordered Field* An ordered field $\mathbb{F}, +, \cdot, P$ is a field $(\mathbb{F}, +, \cdot)$ and a subset P of $\mathbb{F}$ such that:

1. $x \in \mathbb{F} \Rightarrow$ exactly one of the following holds: $x \in P, -x \in P, x = 0$
2. $x, y \in P \Rightarrow x + y \in Y, x \cdot y \in P$

P is called the positive elements of $\mathbb{F}$.

Example 3 $\mathbb{R}, \mathbb{Q}, \{a + b\sqrt{2} : a, b \in Q\} \subset \mathbb{R}$

Lemma 4 *$1 \in P$.* Proof: By 1. of the definition, exactly one of the following holds: $1 = 0, 1 \in P, -1 \in P$.
Since we have a field, $1 \neq 0$.
Assume $-1 \in P$. Then $(-1) \cdot (-1) = 1 \in P$ by 2. Contradiction.

Definition 10 *We write $x > y$ if $x - y \in P$*

Definition 11 *We write $x < y$ if $y - x \in P$* This has the usual properties. (Note: $x \in P$ means $x > 0$, $x \notin P$ means $x < 0$) (e.g. $x > y \Rightarrow x + z > y + z$, $x, y, z \in \mathbb{F}$)

Completeness

Problem: Fields like $\mathbb{Q}$ have sequences that don't converge inside the field.

Definition 12 *Upper bound, lower bound* Suppose $\mathbb{F}$ is an ordered field and $A \subset \mathbb{F}$. We say that $x \in \mathbb{F}$ is an upper bound for A if $a \in A \Rightarrow a \leq x$ (lower bound: $a \geq x$)

Definition 13 *Least upper bound* Suppose $A \subset \mathbb{F}, A \neq \emptyset$. We say that $x \in A$ is a least upper bound for A if:

1. x is an upper bound of A
2. if y is an upper bound of A, then $y \geq x$

Definition 14 *Greatest upper bound* Complementary definition.

Lemma 5 *If $A \subset \mathbb{F}, A \neq \emptyset$ has a least upper bound, it is unique.* Suppose not, $x, y \in \mathbb{F}$ are both least upper bounds. Then $x \leq y, y \leq x \Rightarrow x = y$

Notation 2 *If it exists, then the unique least upper bound is denoted $supA$ (supremum)*

Notation 3 *Greatest lower bound: $infA$ (infimum)*

Definition 15 *Reals* The reals are the ordered field $(\mathbb{R}, +, \cdot, P)$ such that if $A \subset \mathbb{R}, A \neq \emptyset$ and A has an upper bound, then A has a least upper bound.

Example 4 *In $\mathbb{Q}$, truncated decimal expansions of $\sqrt{2}$ have no least upper bound. In $\mathbb{R}$, they do.*