Economics 204

Lecture 2, July 28, 2009

Section 1.4, Cardinality (Cont.)

Theorem 1 (Cantor) *$2^{\mathbf{N}}$, the set of all subsets of $\mathbf{N}$, is* not *countable.*

Proof: Suppose $2^{\mathbf{N}}$ is countable. Then there is a bijection $f : \mathbf{N} \to 2^{\mathbf{N}}$. Let $A_m = f(m)$. We create an infinite matrix, whose $(m, n)^{th}$ entry is 1 if $n \in A_m$, 0 otherwise:

$$
\begin{array}{c}
\mathbf{N}
\end{array}
$$

$$
\begin{array}{cccc|cccccc}
 & & & & 1 & 2 & 3 & 4 & 5 & \cdots \\
\hline
 & A_1 & = & \emptyset & \mathbf{0} & 0 & 0 & 0 & 0 & \cdots \\
 & A_2 & = & \{1\} & 1 & \mathbf{0} & 0 & 0 & 0 & \cdots \\
2^{\mathbf{N}} & A_3 & = & \{1,2,3\} & 1 & 1 & \mathbf{1} & 0 & 0 & \cdots \\
 & A_4 & = & \mathbf{N} & 1 & 1 & 1 & \mathbf{1} & 1 & \cdots \\
 & A_5 & = & 2\mathbf{N} & 0 & 1 & 0 & 1 & \mathbf{0} & \cdots \\
 & & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

Now, on the main diagonal, change all the 0s to 1s and vice versa:

$$
\begin{array}{cccc|cccccc}
 & & & & & & \mathbf{N} & & & \\
 & & & & 1 & 2 & 3 & 4 & 5 & \cdots \\
\hline
 & A_1 & = & \emptyset & \mathbf{1} & 0 & 0 & 0 & 0 & \cdots \\
 & A_2 & = & \{1\} & 1 & \mathbf{1} & 0 & 0 & 0 & \cdots \\
2^{\mathbf{N}} & A_3 & = & \{1,2,3\} & 1 & 1 & \mathbf{0} & 0 & 0 & \cdots \\
 & A_4 & = & \mathbf{N} & 1 & 1 & 1 & \mathbf{0} & 1 & \cdots \\
 & A_5 & = & 2\mathbf{N} & 0 & 1 & 0 & 1 & \mathbf{1} & \cdots \\
 & & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

The coding on the diagonal represents a subset of $\mathbf{N}$ which differs from each of the A_m, contradiction. It is important that we go along the diagonal. We need to define a set $A \subseteq \mathbf{N}$ which is different from $f(1), f(2), \ldots$. To define a set, we need to specify exactly what its elements are, and we do this by taking one entry from each column and one entry from each row. The entry from column n tells us whether or not n is in the set, and the entry in row m is used to ensure that $A \neq A_m$.

More formally, let

$$
t_{mn} = \begin{cases} 1 & \text{if } n \in A_m \\ 0 & \text{if } n \notin A_m \end{cases}
$$

Let $A = \{m \in \mathbf{N} : t_{mm} = 0\}$. (*Aside: this is the set described by changing all the codings on the diagonal.*)

$$
\begin{aligned}
m \in A &\Leftrightarrow t_{mm} = 0 \\
&\Leftrightarrow m \notin A_m \\
1 \in A &\Leftrightarrow 1 \notin A_1 \text{ so } A \neq A_1 \\
2 \in A &\Leftrightarrow 2 \notin A_2 \text{ so } A \neq A_2 \\
&\vdots \\
m \in A &\Leftrightarrow m \notin A_m \text{ so } A \neq A_m
\end{aligned}
$$

Therefore, $A \neq f(m)$ for any m, so f is not onto, contradiction. ■

Message: There are fundamentally more subsets of $\mathbf{N}$ *than elements of* $\mathbf{N}$. *One can show that* $2^{\mathbf{N}}$ *is numerically equivalent to* $\mathbf{R}$*, so there are fundamentally more real numbers than rational numbers.*

Section 1.5: Algebraic Structures

Field Axioms

A *field* $\mathcal{F} = (F, +, \cdot)$ is a 3-tuple consisting of a set F and two binary operations $+, \cdot : F \times F \to F$ such that

1. Associativity of $+$:

$$\forall_{\alpha,\beta,\gamma \in F}\ (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

2. Commutativity of $+$:

$$\forall_{\alpha,\beta \in F}\ \alpha + \beta = \beta + \alpha$$

3. Existence of additive identity:

$$\exists!_{0 \in F}\, ((1 \neq 0) \wedge (\forall_{\alpha \in F}\ \alpha + 0 = 0 + \alpha = \alpha))$$

(*Aside: This says that* 0 *behaves like zero in the real numbers; it need not be zero in the real numbers.*)

4. Existence of additive inverse:

$$\forall_{\alpha \in F} \exists !_{(-\alpha) \in F} \ \alpha + (-\alpha) = (-\alpha) + \alpha = 0$$

(Aside: We wrote $\alpha + (-\alpha)$ rather than $\alpha - \alpha$ because substraction has not yet been defined. In fact, we define $\alpha - \beta$ to be $\alpha + (-\beta)$.)

5. Associativity of $\cdot$:

$$\forall_{\alpha, \beta, \gamma \in F} \ (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

6. Commutativity of $\cdot$:

$$\forall_{\alpha, \beta \in F} \ \alpha \cdot \beta = \beta \cdot \alpha$$

7. Existence of multiplicative identity:

$$\exists !_{1 \in F} \forall_{\alpha \in F} \ \alpha \cdot 1 = 1 \cdot \alpha = \alpha$$

(Aside: This says that 1 behaves like one in the real numbers; it need not be one in the real numbers.)

8. Existence of multiplicative inverse:

$$\forall_{\alpha \in F, \alpha \neq 0} \exists !_{\alpha^{-1} \in F} \ \alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$$

(Aside: We define $\frac{\alpha}{\beta} = \alpha \beta^{-1}$.)

9. Distributivity of multiplication over addition:

$$\forall_{\alpha, \beta, \gamma \in F} \ \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

The point is that any property that follows from the definition of field (the "Field Axioms") must apply to any field

Examples of Fields:

- **R**

- $\mathbf{C} = \{x + iy : x, y \in \mathbf{R}\}$. $i^2 = -1$, so

$$(x + iy)(w + iz) = xw + ixz + iwy + i^2 yz = (xw - yz) + i(xz + wy)$$

- $\mathbf{Q}$: $\mathbf{Q} \subset \mathbf{R}$, $\mathbf{Q} \neq \mathbf{R}$. $\mathbf{Q}$ is closed under $+, \cdot$, taking additive and multiplicate inverses; the field axioms are inherited from the field axioms on $\mathbf{R}$, so $\mathbf{Q}$ is a field.

- $\mathbf{N}$ is not a field: no additive identity.

- $\mathbf{Z}$ is not a field; no multiplicative inverse for 2.

- $\mathbf{Q}(\sqrt{2})$, the smallest field containing $\mathbf{Q} \cup \{\sqrt{2}\}$. Take $\mathbf{Q}$, add $\sqrt{2}$, and close up under $+$, $\cdot$, taking additive and multiplicative inverses. One can show

$$\mathbf{Q}(\sqrt{2}) = \{q + r\sqrt{2} : q, r \in \mathbf{Q}\}$$

For example,

$$\left(q + r\sqrt{2}\right)^{-1} = \frac{q}{q^2 - 2r^2} - \frac{r}{q^2 - 2r^2}\sqrt{2}$$

- A *finite field*: $F_2 = (\{0, 1\}, +, \cdot)$ where

$$\begin{array}{rclcl@{\qquad}rclcl} & & 0+0 & = & 0 & & & 0\cdot 0 & = & 0 \\ 0+1 & = & 1+0 & = & 1 & 0\cdot 1 & = & 1\cdot 0 & = & 0 \\ & & 1+1 & = & 0 & & & 1\cdot 1 & = & 1 \end{array}$$

(*"Arithmetic mod 2"*)

Vector Space Axioms

Abstract definition of objects that "behave like $\mathbf{R}^n$"

A *vector space* is a 4-tuple $(V, F, +, \cdot)$ where V is a set of elements, called *vectors*, F is a field, $+$ is a binary operation on V called vector addition, and $\cdot : F \times V \to V$ is called scalar multiplication, satisfying

1. Associativity of $+$:

$$\forall_{x,y,z\in V}\ (x+y)+z=x+(y+z)$$

2. Commutativity of $+$:

$$\forall_{x,y\in V}\ x+y=y+x$$

3. Existence of vector additive identity:

$$\exists!_{0\in V}\forall_{x\in V}\ x+0=0+x=x$$

   (*Note that* $0\in V$ *and* $0\in F$ *are different.*)

4. Existence of vector additive inverse:

$$\forall_{x\in V}\exists!_{(-x)\in V}\ x+(-x)=(-x)+x=0$$

   (*We define* $x-y$ *to be* $x+(-y)$*.*)

5. Distributivity of scalar multiplication over vector addition:

$$\forall_{\alpha\in F,x,y\in V}\ \alpha\cdot(x+y)=\alpha\cdot x+\alpha\cdot y$$

6. Distributivity of scalar multiplication over scalar addition:

$$\forall_{\alpha,\beta\in F,x\in V}\ (\alpha+\beta)\cdot x=\alpha\cdot x+\beta\cdot x$$

7. Associativity of $\cdot$:

$$\forall_{\alpha,\beta\in F,x\in V}\ (\alpha\cdot\beta)\cdot x=\alpha\cdot(\beta\cdot x)$$

8. Multiplicative identity:

$$\forall_{x\in V}\ \ 1\cdot x=x$$

   (*Note that* 1 *is the multiplicative identity in* F*;* $1\notin V$)

Examples of vector spaces:

1. $\mathbf{R}^n$ over $\mathbf{R}$.

2. $\mathbf{R}$ is a vector space over $\mathbf{Q}$:

$$\text{(scalar multiplication) } q \cdot r = qr \text{ (product in } \mathbf{R}\text{)}$$

   $\mathbf{R}$ is not finite-dimensional over Q, i.e. $\mathbf{R}$ is not $\mathbf{Q}^n$ for any $n \in \mathbf{N}$.

3. $\mathbf{R}$ is a vector space over $\mathbf{R}$.

4. $\mathbf{Q}(\sqrt{2})$ is a vector space over $\mathbf{Q}$. As a vector space, it is $\mathbf{Q}^2$; as a field, you need to take the funny field multiplication.

5. $\mathbf{Q}(\sqrt[3]{2})$, as a vector space over $\mathbf{Q}$, is $\mathbf{Q}^3$.

6. $(F_2)^n$ is a *finite* vector space over F_2.

7. $C([0,1])$, the space of all continuous functions from $[0,1]$ to $\mathbf{R}$, is a vector space over $\mathbf{R}$.

   - vector addition:

     $$(f+g)(t) = f(t) + g(t)$$

     (*We define the function $f+g$ by specifying what value it takes for each $t \in [0,1]$.*)

   - scalar multiplication:

     $$(\alpha f)(t) = \alpha(f(t))$$

   - vector additive identity: 0 is the function which is identically zero: $0(t) = 0$ for all $t \in [0,1]$.

   - vector additive inverse:

     $$(-f)(t) = -(f(t))$$

Section 1.6: Axioms for R

1. $\mathbf{R}$ is a field with the usual operations $+$, $\cdot$, additive identity 0, and multiplicative identity 1.

2. **Order Axiom:** There is a complete ordering $\leq$, i.e. $\leq$ is reflexive, transitive, antisymmetric ($\alpha \leq \beta, \beta \leq \alpha \Rightarrow \alpha = \beta$) with the property that

$$\forall_{\alpha,\beta\in\mathbf{R}} \ (\alpha \leq \beta) \vee (\beta \leq \alpha)$$

The order is compatible with $+$ and $\cdot$, i.e.

$$\forall_{\alpha,\beta,\gamma\in\mathbf{R}} \begin{cases} \alpha \leq \beta & \Rightarrow \quad \alpha+\gamma \leq \beta+\gamma \\ \alpha \leq \beta, 0 \leq \gamma & \Rightarrow \quad \alpha\gamma \leq \beta\gamma \end{cases}$$

$\alpha \geq \beta$ means $\beta \leq \alpha$.

$\alpha < \beta$ means $\alpha \leq \beta$ and $\alpha \neq \beta$.

3. **Completeness Axiom:** Suppose $L, H \subseteq \mathbf{R}$, $L \neq \emptyset \neq H$ satisfy

$$\forall_{\ell\in L, h\in H} \ \ell \leq h$$

Then

$$\exists_{\alpha\in\mathbf{R}}\forall_{\ell\in L, h\in H} \ \ell \leq \alpha \leq h$$

$$\begin{array}{ccc} & \alpha & \\ L & \downarrow & H \\ ----) & \cdot & (---- \end{array}$$

The Completeness Axiom differentiates $\mathbf{R}$ *from* $\mathbf{Q}$*:* $\mathbf{Q}$ *satisfies all the axioms for* $\mathbf{R}$ *except the Completeness Axiom*

The most useful consequence of the Completeness Axiom (and often used as an alternative axiom) is the <u>*Supremum Property*</u>*.*

Definition 2 Suppose $X \subseteq \mathbf{R}$. We say u is an *upper bound* for X if

$$\forall_{x \in X}\ x \leq u$$

and ℓ is a *lower bound* for X if

$$\forall_{x \in X}\ \ell \leq x$$

X is bounded above if there is an upper bound for X, and bounded below if there is a lower bound for X.

Definition 3 Suppose X is bounded above. The *supremum* of X, written $\sup X$, is the smallest upper bound for X, i.e. $\sup X$ satisfies

$$\forall_{x \in X}\ \sup X \geq x \ \ \text{(sup is an upper bound)}$$

$$\forall_{y < \sup X} \exists_{x \in X}\ x > y \text{ (there is no smaller upper bound)}$$

Analogously, suppose X is bounded below. The *infimum* of X, written $\inf X$, is the greatest lower bound for X, i.e. $\inf X$ satisfies

$$\forall_{x \in X}\ \inf X \leq x \ \ (\inf X \text{ is a lower bound})$$

$$\forall_{y > \inf X} \exists_{x \in X}\ x < y \text{ (there is no greater lower bound)}$$

(Not in book) If X is not bounded above, write $\sup X = \infty$. If X is not bounded below, write $\inf X = -\infty$. $\sup \emptyset = -\infty$, $\inf \emptyset = +\infty$.

The Supremum Property: Every nonempty set of real numbers which is bounded above has a supremum, which is a real number. Every nonempty set of real numbers which is bounded below has an infimum, which is a real number.

Caution: $\sup X$ *need not be an element of* X*. For example,* $\sup(0,1) = 1 \notin (0,1)$.

Theorem 4 (Theorem 6.8, plus ...) *The Supremum Property and the Completeness Axiom are equivalent.*

Proof: Assume the Completeness Axiom. Let $X \subseteq \mathbf{R}$ be a nonempty set which is bounded above. Let U be the set of all upper bounds for X. Since X is bounded above, $U \neq \emptyset$. If $x \in X$ and $u \in U$, $x \leq u$ since u is an upper bound for X. So

$$\forall_{x \in X, u \in U}\ x \leq u$$

By the Completeness Axiom,

$$\exists_{\alpha \in \mathbf{R}} \forall_{x \in X, u \in U}\ x \leq \alpha \leq u$$

α is an upper bound for X, and it is less than or equal to every other upper bound for X, so it is the least upper bound for X, so $\sup X = \alpha \in \mathbf{R}$. The case in which X is bounded below is similar. Thus, the Supremum Property holds.

Conversely, assume the Supremum Property. Suppose $L, H \subseteq \mathbf{R}$, $L \neq \emptyset \neq H$, and

$$\forall_{\ell \in L, h \in H}\ \ell \leq h$$

Since $L \neq \emptyset$ and L is bounded above (by any element of H), $\alpha = \sup L$ exists and is real. By the definition of supremum, α is an upper bound for L, so

$$\forall_{\ell \in L}\ \ell \leq \alpha$$

Suppose $h \in H$. Then h is an upper bound for L, so by the definition of supremum, $\alpha \leq h$. Therefore, we have shown that

$$\forall_{\ell \in L, h \in H}\ \ell \leq \alpha \leq h$$

so the Completeness Axiom holds. ■

Theorem 5 (Archimedean Property, Theorem 6.10 + ...)

$$\forall_{x,y\in\mathbf{R},y>0}\exists_{n\in\mathbf{N}}\ ny = \underbrace{(y+\cdots+y)}_{n\ times} > x$$

Theorem 6 (Intermediate Value Theorem) *Suppose $f : [a,b] \to \mathbf{R}$ is continuous, and $f(a) < d < f(b)$. Then there exists $c \in (a,b)$ such that $f(c) = d$.*

Proof: Later, we will give a slick proof. Here, we give a bare-hands proof using the Supremum Property. Let

$$B = \{x \in [a,b] : f(x) < d\}$$

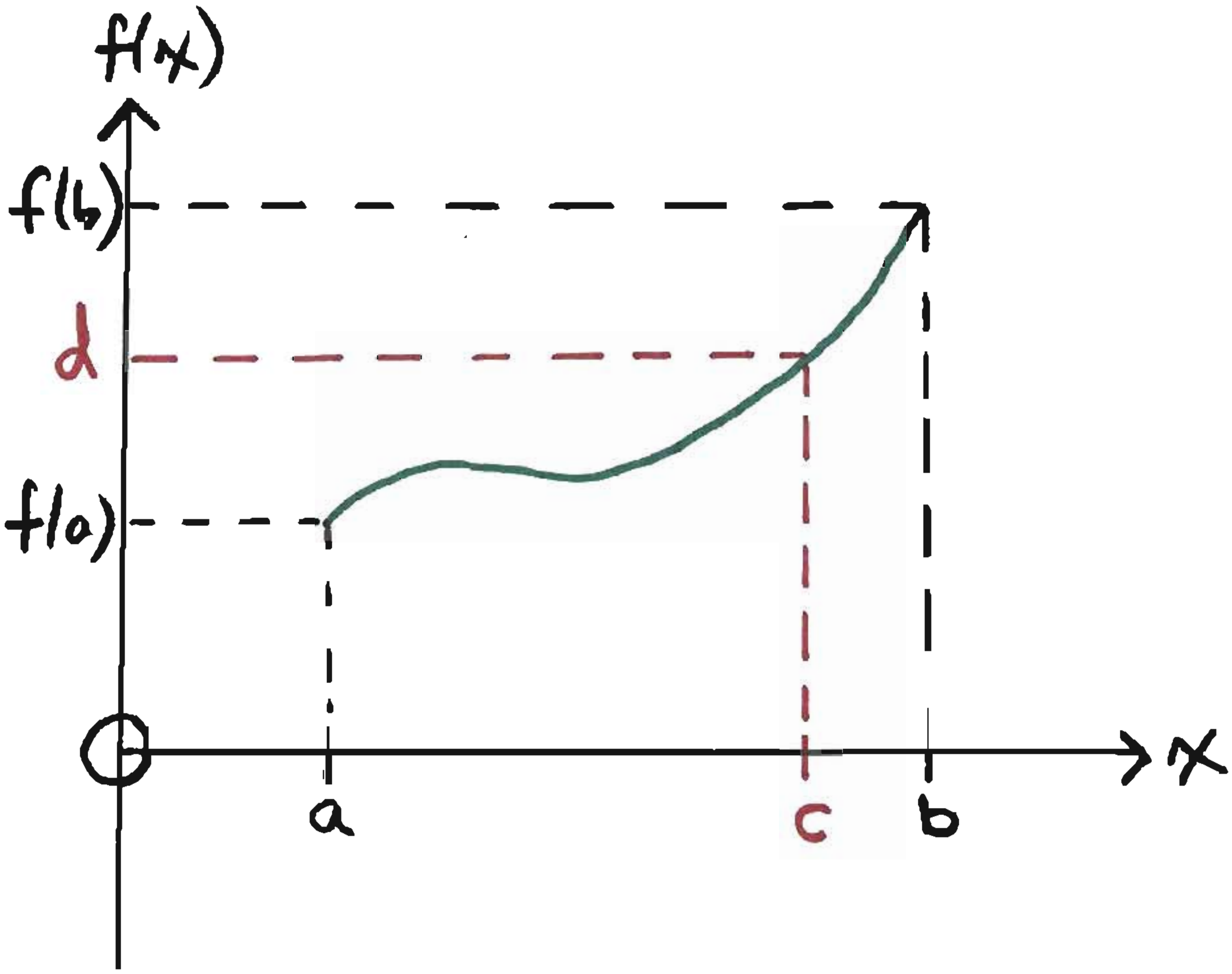
$a \in B$, so $B \neq \emptyset$; $B \subseteq [a,b]$, so B is bounded above. By the Supremum Property, $\sup B$ exists and is real so let $c = \sup B$. Since $a \in B$, $c \geq a$. $B \subseteq [a,b]$, so $c \leq b$. Therefore, $c \in [a,b]$.

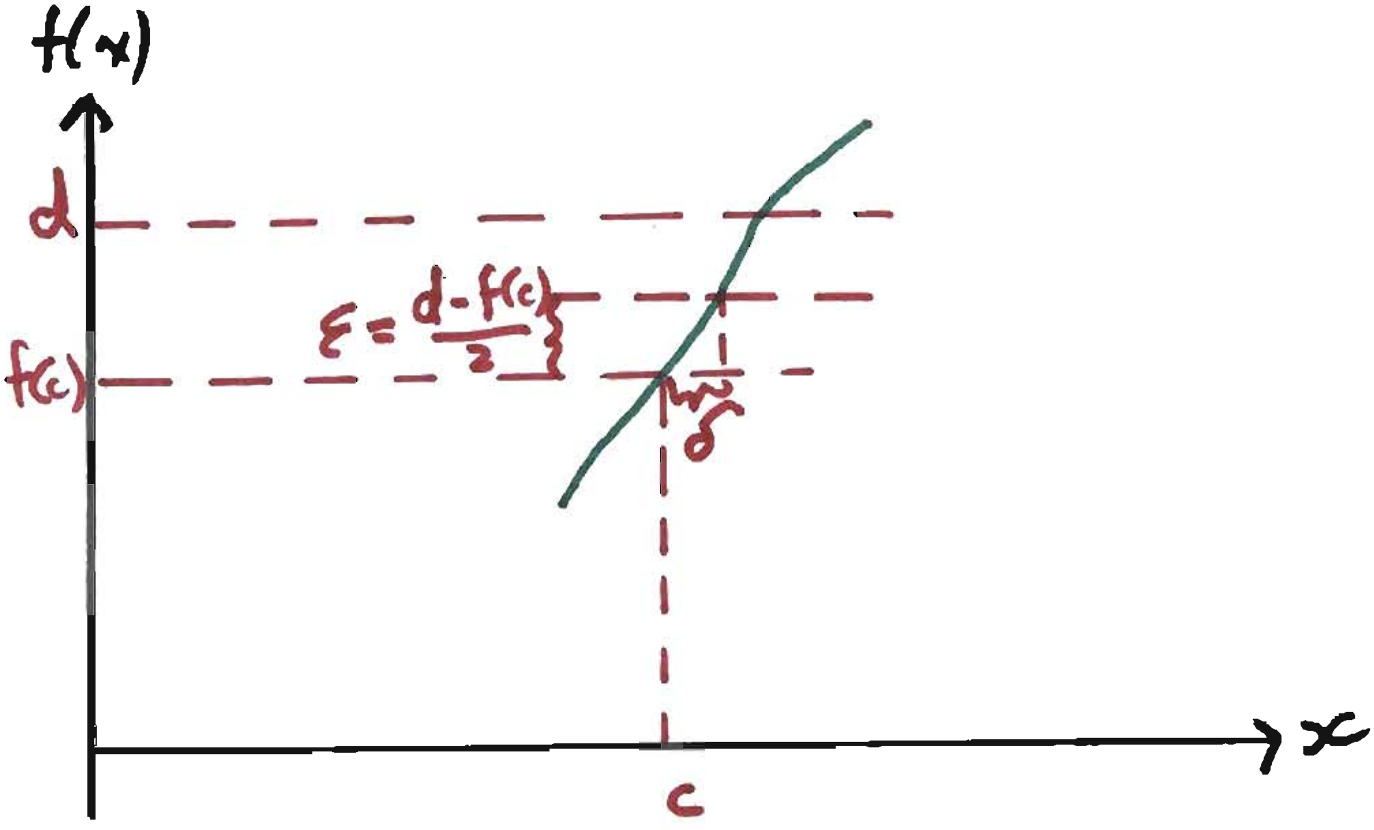
We claim that $f(c) = d$. If not, suppose $f(c) < d$. Then since $f(b) > d$, $c \neq b$, so $c < b$. Let $\varepsilon = \frac{d-f(c)}{2} > 0$. Since f is continuous at c, there exists $\delta > 0$ such that

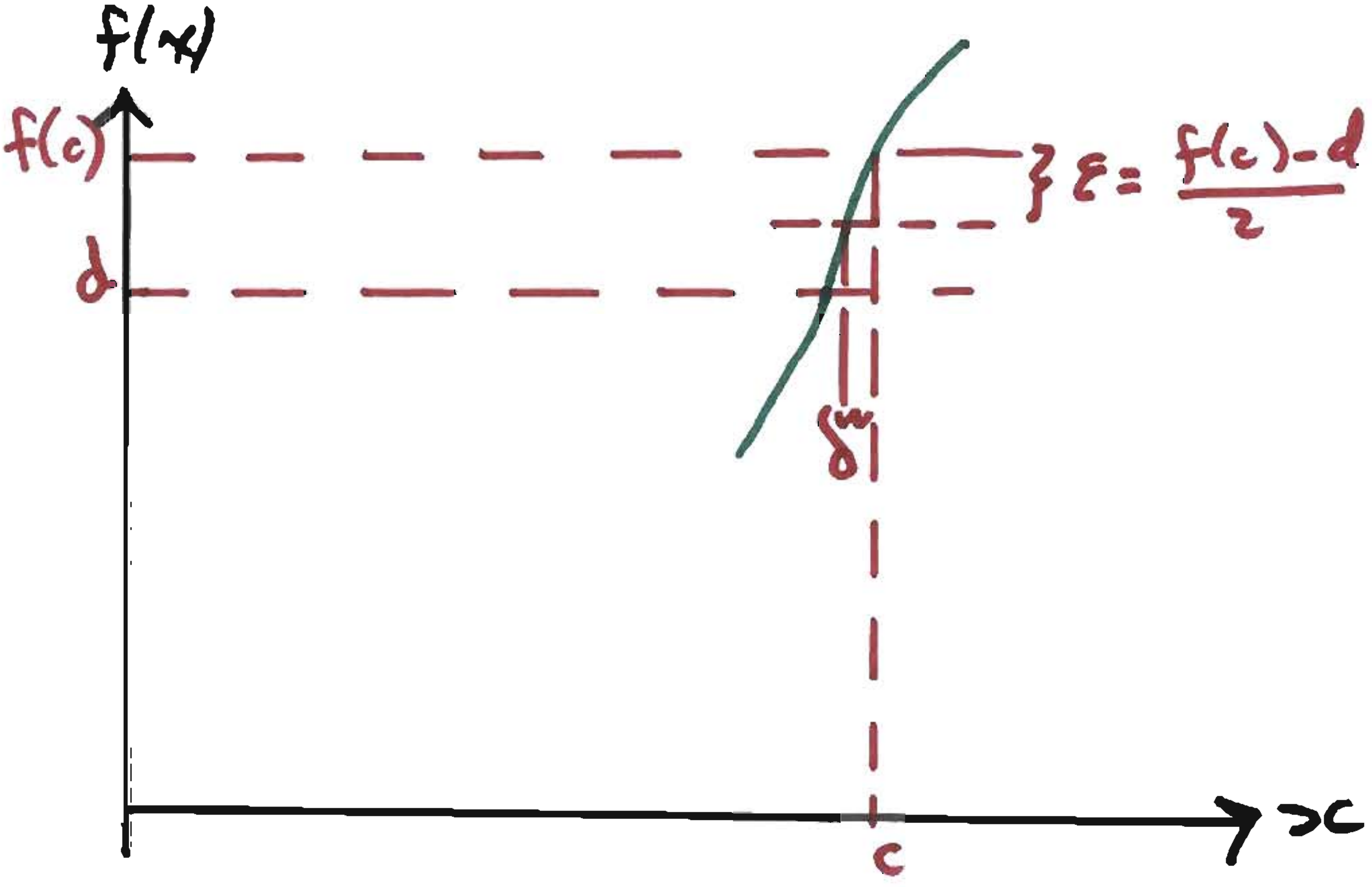
$$\begin{aligned} |x-c|<\delta \ \Rightarrow\ |f(x)-f(c)| &< \varepsilon \\ \Rightarrow\ f(x) &< f(c)+\varepsilon \\ &= f(c)+\tfrac{d-f(c)}{2} \\ &= \tfrac{f(c)+d}{2} \\ &< \tfrac{d+d}{2} \\ &= d \end{aligned}$$

so $(c, c+\delta) \subseteq B$, so $c \neq \sup B$, contradiction.

Suppose $f(c) > d$. Then since $f(a) < d$, $a \neq c$, so $c > a$. Let $\varepsilon = \frac{f(c)-d}{2} > 0$. Since f is continuous at


f(x)
f(b)
d
f(a)
O
a
c
b
x


f(x)
d
$\varepsilon = \frac{d - f(c)}{2}$
f(c)
δ
c
x


f(x)
f(c)
$\varepsilon = \frac{f(c) - d}{2}$
d
δ
c
x

c, there exists $\delta > 0$ such that

$$\begin{aligned}
|x-c| < \delta \;\Rightarrow\; |f(x) - f(c)| &< \varepsilon \\
\Rightarrow\; f(x) &> f(c) - \varepsilon \\
&= f(c) - \tfrac{f(c)-d}{2} \\
&= \tfrac{f(c)+d}{2} \\
&> \tfrac{d+d}{2} \\
&= d
\end{aligned}$$

so $(c-\delta, c+\delta) \cap B = \emptyset$. So either there exists $x \in B$ with $x \geq c + \delta$ (in which case c is not an upper bound for B) or $c - \delta$ is an upper bound for B (in which case c is not the least upper bound for B); in either case, $c \neq \sup B$, contradiction.

Since $f(c) \not< d$, $f(c) \not> d$, and the order is complete, $f(c) = d$. Since $f(a) < d$ and $f(b) > d$, $a \neq c \neq b$, so $c \in (a,b)$. ■

Corollary 7 *There exists $x \in \mathbf{R}$ such that $x^2 = 2$.*

Proof: Let $f(x) = x^2$, for $x \in [0,2]$. From Math 1A, f is continuous. $f(0) = 0 < 2$ and $f(2) = 4 > 2$, so by the Intermediate Value Theorem, there exists $c \in (0,2)$ such that $f(c) = 2$, i.e. $c^2 = 2$. ■

Read sections 1.6(c) (absolute values) and 1.7 (complex numbers) on your own.