Econ 204 2016

Lecture 2

Outline

1. Cardinality (cont.)
2. Algebraic Structures: Fields and Vector Spaces
3. Axioms for $\mathbb{R}$
4. Sup, Inf, and the Supremum Property
5. Intermediate Value Theorem
Cardinality (cont.)

**Notation:** Given a set $A$, $2^A$ is the set of all subsets of $A$. This is the “power set” of $A$, also denoted $P(A)$.

Important example of an uncountable set:

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

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>\ldots</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A_1 = \emptyset)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>\ldots</td>
</tr>
<tr>
<td>(A_2 = {1})</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>\ldots</td>
</tr>
<tr>
<td>(2^N) (A_3 = {1,2,3})</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>\ldots</td>
</tr>
<tr>
<td>(A_4 = \mathbb{N})</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>\ldots</td>
</tr>
<tr>
<td>(A_5 = 2\mathbb{N})</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>\ldots</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\ldots</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1$ = $\emptyset$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>$A_2$ = ${1}$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>$2^N$ $A_3$ = ${1,2,3}$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>$A_4$ = $\mathbb{N}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>...</td>
</tr>
<tr>
<td>$A_5$ = $2\mathbb{N}$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

The table shows the cardinality of each set $A_i$ for $i = 1, 2, 3, 4, 5$, along with the corresponding number of terms in each row following the pattern.
Let

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

Let \( A = \{ m \in \mathbb{N} : t_{mm} = 0 \} \).

\[ m \in A \iff t_{mm} = 0 \iff m \notin A_m \]

1 \( \in A \iff 1 \notin A_1 \text{ so } A \neq A_1 \)

2 \( \in A \iff 2 \notin A_2 \text{ so } A \neq A_2 \)

\[ \vdots \]

\[ m \in A \iff m \notin A_m \text{ so } A \neq A_m \]

Therefore, \( A \neq f(m) \) for any \( m \), so \( f \) is not onto, contradiction. \( \square \)
Some Additional Facts About Cardinality

Recall we let $|A|$ denote the cardinality of a set $A$.

- if $A$ is numerically equivalent to $\{1, \ldots, n\}$ for some $n \in \mathbb{N}$, then $|A| = n$.
- $A$ and $B$ are numerically equivalent if and only if $|A| = |B|$
- if $|A| = n$ and $A$ is a proper subset of $B$ (that is, $A \subseteq B$ and $A \neq B$) then $|A| < |B|$
• if $A$ is countable and $B$ is uncountable, then

$$n < |A| < |B| \quad \forall n \in \mathbb{N}$$

• if $A \subseteq B$ then $|A| \leq |B|$

• if $r : A \rightarrow B$ is 1-1, then $|A| \leq |B|$

• if $B$ is countable and $A \subseteq B$, then $A$ is at most countable, that is, $A$ is either empty, finite, or countable

• if $r : A \rightarrow B$ is 1-1 and $B$ is countable, then $A$ is at most countable
Algebraic Structures: Fields

**Definition 1.** A field $\mathcal{F} = (\mathcal{F}, +, \cdot)$ is a 3-tuple consisting of a set $\mathcal{F}$ and two binary operations $+ : \mathcal{F} \times \mathcal{F} \rightarrow \mathcal{F}$ such that

1. **Associativity of $+$:**
   \[ \forall \alpha, \beta, \gamma \in \mathcal{F}, \ (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \]

2. **Commutativity of $+$:**
   \[ \forall \alpha, \beta \in \mathcal{F}, \ \alpha + \beta = \beta + \alpha \]

3. **Existence of additive identity:**
   \[ \exists ! 0 \in \mathcal{F} \text{ s.t. } \forall \alpha \in \mathcal{F}, \ \alpha + 0 = 0 + \alpha = \alpha \]

"There exists a unique"
4. Existence of additive inverse:

\[ \forall \alpha \in F \ \exists! (-\alpha) \in F \ \text{s.t.} \ \alpha + (-\alpha) = (-\alpha) + \alpha = 0 \]

Define \( \alpha - \beta = \alpha + (-\beta) \)

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:

\[ \exists! 1 \in F \ \text{s.t.} \ 1 \neq 0 \ \text{and} \ \forall \alpha \in F, \ \alpha \cdot 1 = 1 \cdot \alpha = \alpha \]
$\alpha \cdot 0 = 0 \forall \alpha \in F$.

8. Existence of multiplicative inverse:

$$\forall \alpha \in F \text{ s.t. } \alpha \neq 0 \exists! \alpha^{-1} \in F \text{ s.t. } \alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$$

Define $\frac{\alpha}{\beta} = \alpha \beta^{-1}$. \hspace{1cm} (\beta \neq 0)

9. Distributivity of multiplication over addition:

$$\forall \alpha, \beta, \gamma \in F, \ \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$
Fields

Examples:

• **R** (real numbers \( \mathbb{R} \))
  - complex numbers

• **C** = \( \{x + iy : x, y \in \mathbb{R}\} \). \( i^2 = -1 \), so
  \[
  (x+iy)(w+iz) = xw + ixz + iwy + i^2yz = (xw - yz) + i(xz + wy)
  \]

• **Q**: \( Q \subset \mathbb{R}, Q \neq \mathbb{R} \). \( Q \) is closed under \( +, \cdot \), taking additive and multiplicative inverses; the field axioms are inherited from the field axioms on \( \mathbb{R} \), so \( Q \) is a field.
• \( \mathbb{N} \) is not a field: no additive identity.

• \( \mathbb{Z} \) is not a field; no multiplicative inverse for 2.

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

\[
\mathbb{Q}(\sqrt{2}) = \{q + r\sqrt{2} : q, r \in \mathbb{Q}\}
\]

For example,

\[
(q + r\sqrt{2})^{-1} = \frac{q}{q^2 - 2r^2} - \frac{r}{q^2 - 2r^2}\sqrt{2}
\]
• A finite field: $F_2 = (\{0, 1\}, +, \cdot)$ where

\[
\begin{align*}
0 + 0 &= 0 & 0 \cdot 0 &= 0 \\
0 + 1 &= 1 + 0 &= 1 & 0 \cdot 1 &= 1 \cdot 0 &= 0 \\
1 + 1 &= 0 & 1 \cdot 1 &= 1
\end{align*}
\]

(“Arithmetic mod 2”)

$1 = -1$
Vector Spaces

**Definition 2.** 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:**

\[ \exists ! 0 \in V \text{ s.t. } \forall x \in V, \ x + 0 = 0 + x = x \]

4. **Existence of vector additive inverse:**

\[ \forall x \in V \ \exists ! (-x) \in V \text{ s.t. } x + (-x) = (-x) + x = 0 \]

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 $\cdot$:

$$\forall \alpha, \beta \in F, x \in V \quad (\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$$

8. Multiplicative identity:

$$\forall x \in V \quad 1 \cdot x = x$$

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

"$V$ is a vector space over $F$"

"$V$ over $F$"
Vector Spaces

Examples:

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

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

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

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

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


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

   \[ \text{i.e. } (q, r) \text{ instead } q + r \sqrt{2} \]

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

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

7. $C([0, 1])$, the space of all continuous real-valued functions on $[0, 1]$, is a vector space over $\mathbb{R}$.

   - vector addition:
     \[
     (f + g)(t) = f(t) + g(t)
     \]

   define the function \( f + g \).
Note 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:
  \[(-f)(t) = -(f(t))\]
Axioms for \( \mathbb{R} \)

1. \( \mathbb{R} \) 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

\[
\forall \alpha, \beta \in \mathbb{R} \text{ either } \alpha \leq \beta \text{ or } \beta \leq \alpha
\]

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

\[
\forall \alpha, \beta, \gamma \in \mathbb{R} \left\{ \begin{array}{l}
\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma \\
\alpha \leq \beta, 0 \leq \gamma \Rightarrow \alpha \gamma \leq \beta \gamma
\end{array} \right.
\]

\( \alpha \geq \beta \) means \( \beta \leq \alpha \). \( \alpha < \beta \) means \( \alpha \leq \beta \) and \( \alpha \neq \beta \).
Completeness Axiom

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

$$\ell \leq h \ \forall \ell \in L, h \in H$$

Then

$$\exists \alpha \in \mathbb{R} \text{ s.t. } \ell \leq \alpha \leq h \ \forall \ell \in L, h \in H$$

The Completeness Axiom differentiates $\mathbb{R}$ from $\mathbb{Q}$: $\mathbb{Q}$ satisfies all the axioms for $\mathbb{R}$ except the Completeness Axiom.
Sups, Infs, and the Supremum Property

**Definition 3.** Suppose $X \subseteq \mathbb{R}$. We say $u$ is an upper bound for $X$ if
\[ x \leq u \quad \forall x \in X \]
and $\ell$ is a lower bound for $X$ if
\[ \ell \leq x \quad \forall x \in X \]

$X$ is bounded above if there is an upper bound for $X$, and bounded below if there is a lower bound for $X$. 
Definition 4. Suppose \( X \) is bounded above. The supremum of \( X \), written \( \sup X \), is the least upper bound for \( X \), i.e. \( \sup X \) satisfies

\[
\sup X \geq x \quad \forall x \in X \quad (\sup X \text{ is an upper bound})
\]

\[
\forall y < \sup X \exists x \in X \text{ s.t. } x > y \quad (\text{there is no smaller upper bound})
\]

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

\[
\inf X \leq x \quad \forall x \in X \quad (\inf X \text{ is a lower bound})
\]

\[
\forall y > \inf X \exists x \in X \text{ s.t. } x < y \quad (\text{there is no greater lower bound})
\]

If \( X \) is not bounded above, write \( \sup X = \infty \). If \( X \) is not bounded below, write \( \inf X = -\infty \). Convention: \( \sup \emptyset = -\infty \), \( \inf \emptyset = +\infty \).
The Supremum Property

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

**Note:** \( \sup X \) need not be an element of \( X \). For example, \( \sup(0, 1) = 1 \not\in (0, 1) \).
The Supremum Property

**Theorem 2** (Theorem 6.8, plus ...). *The Supremum Property and the Completeness Axiom are equivalent.*

**Proof.** Assume the Completeness Axiom. Let \( X \subseteq \mathbb{R} \) be a nonempty set that 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

\[
x \leq u \quad \forall x \in X, u \in U
\]

By the Completeness Axiom,

\[
\exists \alpha \in \mathbb{R} \text{ s.t. } x \leq \alpha \leq u \quad \forall x \in X, u \in U
\]

\( \alpha \) 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 \( \sup X = \alpha \in \mathbb{R} \). The case in which \( X \) is bounded below is similar. Thus, the Supremum Property holds.

Conversely, assume the Supremum Property. Suppose \( L, H \subseteq \mathbb{R}, L \neq \emptyset \neq H \), and

\[
\ell \leq h \ \forall \ell \in L, h \in H
\]

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, \( \alpha \) is an upper bound for \( L \), so

\[
\ell \leq \alpha \ \forall \ell \in L
\]

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

\[
\ell \leq \alpha \leq h \ \forall \ell \in L, h \in H
\]

so the Completeness Axiom holds. \qed
Archimedean Property

**Theorem 3** (Archimedean Property, Theorem 6.10 + ...).

\[ \forall x, y \in \mathbb{R}, y > 0 \ \exists n \in \mathbb{N} \ s.t. \ ny = (y + \cdots + y) > x \]

(\(n\ \text{times}\))

*Proof.* Exercise. This is a nice exercise in proof by contradiction, using the Supremum Property. \[\square\]
Intermediate Value Theorem

**Theorem 4** (Intermediate Value Theorem). *Suppose $f : [a, b] \to \mathbb{R}$ 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, $c \in [a, b]$. 

15
Claim: $f(c) = d$
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

\[
|x - c| < \delta \Rightarrow |f(x) - f(c)| < \varepsilon
\]

\[
\Rightarrow f(x) < f(c) + \varepsilon
\]

\[
= f(c) + \frac{d - f(c)}{2}
\]

\[
= \frac{f(c) + d}{2}
\]

\[
< \frac{d + d}{2}
\]

\[
= d
\]

so \( (c, c + \delta) \subseteq B \), so \( c \neq \sup B \), contradiction.
\[ f(c) < d \Rightarrow \exists \delta > 0 \text{ such that for } x \in (c-\delta, c+\delta), \ f(x) < d \Rightarrow c \neq \sup B \]
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 $c$, there exists $\delta > 0$ such that
\[ |x - c| < \delta \Rightarrow |f(x) - f(c)| < \varepsilon \]
\[ \Rightarrow f(x) > f(c) - \varepsilon \]
\[ = f(c) - \frac{f(c) - d}{2} \]
\[ = \frac{f(c) + d}{2} \]
\[ > \frac{d + d}{2} \]
\[ = d \]
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 1. There exists $x \in \mathbb{R}$ such that $x^2 = 2$.

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