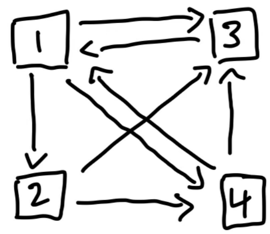
MATH 4310 Lecture Notes (Dylan Tom)

Introduction & Fields



Question: How do we determine the page order for a mini "google"?

1. (Simple Approach) Determine the importance by the number of back links (we expect page 3 should be the top*)
2. (Weighted Approach) Back links from "important" pages should weigh more. Let the "score" of a page be the sum of the scores of its back links.
3. Prevent undue influence by one page linking to too many other pages. If page j contains n_j links, one of which is page k, then boost the score of page k by $\frac{x_j}{n_j}$ where x_j is the score of page j

In our example,

$$\begin{aligned} x_1 &= \frac{1}{1}x_3 + \frac{1}{2}x_4 \\ x_2 &= \frac{1}{3}x_1 \\ x_3 &= \frac{1}{3}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_4 \\ x_4 &= \frac{1}{3}x_1 + \frac{1}{2}x_2 \end{aligned}$$

Answer: $x_1 = \frac{12}{31} \quad x_2 = \frac{4}{31} \quad x_3 = \frac{9}{31} \quad x_4 = \frac{6}{31}$

*We have shown that page 1 should be ranked higher than 3, so our intuition wasn't correct.

Question: What are some properties of the set of real numbers with addition and multiplication?

1. There is a $0 \in S$ such that $0 + a = a$ for all $a \in S$
2. There is a $1 \in S$ such that $1 \cdot a = a$ for all $a \in S$
3. commutativity, associativity, distributivity
4. There exists a $(-a) \in S$ such that $a + (-a) = 0$ for all $a \in S$

5. There exists a $a^{-1} \in S$ such that $aa^{-1} = 1$ for all $a \in S$
6. $a - b = a + (-b)$ and $\frac{a}{b} = a \cdot b^{-1}$

Question: What sets have these properties?

$$\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p$$

Question: What sets do not satisfy these properties?

$$\mathbb{Z}, \mathbb{N}, \mathbb{M}_{2\times 2}$$

Definition. A **field**, $\mathbb{F}$, is a set on which addition $(+)$ and multiplication $(\cdot)$ are defined so that the following properties hold for all $a, b, c \in \mathbb{F}$.

1. $a + b = b + a \quad a \cdot b = b \cdot a$ (commutativity)
2. $(a + b) + c = a + (b + c) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity)
3. There exists *distinct* elements $0, 1$ such that $0 + a = a$ and $1 \cdot a = a$ (identity)
4. There exists $c, d \in \mathbb{F}$ such that $a + c = 0$ and $bd = 1$ where $d \neq 0$ (invertibility). Define $c = -a$ and $d = b^{-1}$ (see uniqueness below)
5. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributivity)

Example: Some fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F} = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, \mathbb{F}_2 = \{0, 1\}$

Example: Cancellation Laws

1. $a + b = a + c \Rightarrow b = c$

   Proof. Let's assume $a + b = a + c$. By (4), there is some x such that $x + a = 0$. Now $x + (a + b) = x + (a + c)$. By (2), $(x + a) + b = (x + a) + c \Rightarrow 0 + b = 0 + c$. By (3), $b = c$. □

2. $a \cdot b = a \cdot c$ and $a \neq 0 \Rightarrow b = c$

   Proof. Let's assume $a \cdot b = a \cdot c$ and $a \neq 0$. By (4), there is some x such that $ax = 1$. Now $x(ab) = x(ac)$. By (2), $(xa)b = (xa)c \Rightarrow 1b = 1c$. By (3), $b = c$. □

Example: Uniqueness of 0, 1, additive inverse, and multiplicative inverse

Proof. (multiplicative inverse) Given $b \neq 0$, let d and d' satisfy $b \cdot d = 1$ and $b \cdot d' = 1$. Then, $b \cdot d = b \cdot d'$. So, $d = d'$ (by cancellation). Similarly, for others. □

Example: Some more properties of fields

1. $a \cdot 0 = 0$

   Proof. $(a \cdot 0) + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0$ □

2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

   Proof. $[(-a) \cdot b] + [a \cdot b] = b \cdot (a + (-a)) = b \cdot 0 = 0$
   $[a \cdot (-b)] + [a \cdot b] = a \cdot (b + (-b)) = a \cdot 0 = 0$ □

3. $(-a) \cdot (-b) = a \cdot b$

   Proof. $(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b$ □

Properties of Relations:

1. Reflexive: $\forall a \in S$, $a \sim a$
2. Symmetric: $\forall a, b \in S$, if $a \sim b$, then $b \sim a$
3. Transitive: $\forall a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$

An equivalence relation satisfies all 3 of these properties

Example: Define $S = \{\text{all humans}\}$. $a \sim b$ if a and b share a parent. It is reflexive, symmetric, but not transitive.

Definition. The class of a is all elements related to a, denoted by $[a]$. There can be no intersection between two classes.

Example: Define $S = \mathbb{Z}$. $a \sim b$ if $a - b$ is even. This is an equivalence relation. We can partition $\mathbb{Z}$ into even and odd, $[0]$ and $[1]$. We call this $\mathbb{Z}_2 = \mathbb{F}_2$.

In general, fix $d \geq 1$. Define $a \sim b$ if $a - b$ is divisible by d. In $\mathbb{Z}_d$,

1. $[a] + [b] = [(a + b) \mod d]$
2. $[a] \cdot [b] = [(a \cdot b) \mod d]$

Question: When is $\mathbb{Z}_d$ a field? Only if d is prime.

Definition. Let $\mathbb{F}$ be a field. A vector (linear) space, V over $\mathbb{F}$ is a set with two operations, addition $(+) : V \times V \to V$ and scalar multiplication $(\cdot) : \mathbb{F} \times V \to V$. For all vectors, $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ and $a, b \in \mathbb{F}$.

- $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$
- $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$
- There is a 0 such that $0 + \mathbf{x} = \mathbf{x}$
- There is a $\mathbf{y}$ such that $\mathbf{x} + \mathbf{y} = 0$
- There is a 1 such that $1 \cdot \mathbf{x} = \mathbf{x}$
- $(ab)\mathbf{x} = a(b\mathbf{x})$
- $a \cdot (\mathbf{x} + \mathbf{y}) = (a \cdot \mathbf{x}) + (a \cdot \mathbf{y})$
- $(a + b)\mathbf{x} + a\mathbf{x} + b\mathbf{x}$