Sets, Fields and Ordered Fields

Lec 2

Lec 3

Sets and Properties

Defn) A set is a collection of objects called elements

→ set with no elements is

$\emptyset$ → every property is vacuously true → you can't disprove that all elements are odd and even

→ $\emptyset \subset$ of any set

In sets we care about membership.
Ie. for set S either $x \in S$, $x \notin S$.

Note: Order & repeats don't matter

$X \subseteq Y$ p.t. $\forall x \in X$, $x \in Y$

To show equality of sets you must show 2-way containment. Ie

$X \subset Y$, $Y \subset X$, $X = Y$

Let X be a set & $A, B \subset X$

$$A \cap B = \{x \in X \mid x \in A \text{ and } x \in B\}$$

$$A \cup B = \{x \in X \mid x \in A \text{ or } x \in B\}$$

Defn

The cartesian product of 2 sets is defined as

$$A \times B := \{(a,b) \mid a \in A \text{ and } b \in B\}$$

Defn

$$(a,b) := \{\{a\},\{a,b\}\}$$

$\boxed{ex}$ $(a,b) = (c,d)$ iff $a = c$, $b = d$

Defn

A function is a subset of the cartesian product of its Domain & codomain. lets say $f : A \to B$

$f \subseteq A \times B$ s.t.

$\forall\, a \in A \quad \exists!\, b \in B$

s.t $(a,b) \in f$ so. $f(a) = b$

Bit of a sidetrack now. Functions and $\emptyset$ set.

If co-domain is $\emptyset$. The cartesian product is $\emptyset$. $\therefore \forall\, a \in A \nexists\, b \in B$ such that $(a,b) \in f$

So you can't have a function.

If domain is $\emptyset$. $A \times B = \emptyset$. But this time $\forall a \in A \exists b \in B$ such that $(a,b) \in f$ ✓

If $a = \emptyset$, $b \neq 0$. we still have a function

Defn A binary operation on set S is a function as follows.

$\star : S \times S \to S$

for $s_1, s_2 \in S$

$\star(s_1, s_2)$ is usually notated

$s_1 \star s_2$.

Eg! $\cap$ is a bin op on $P(X)$

$\cap : P(X)^2 \to P(X)$ $\quad A, B \in P(X)$

$A \cap B \in P(X)$

↳ even $\cup$ is a bin op

Important

$\mathrm{Fun}(X) := \{ f : X \to X \}$

↳ set of all functions from X to X

function composition is a binary op on $\mathrm{Fun}(X)$

$\circ : \mathrm{Fun}(X)^2 \to \mathrm{Fun}(X)$ $\quad f, g \in \mathrm{Fun}(X)$

$\circ(f, g) \to f \circ g$

$f \circ g : X \to X \;,\; x \mapsto f(g(x))$

Defn A bin op $\star$ on set S is commutative p.t

$\forall a, b \in S$, $a \star b = b \star a$

Eg $\cup$ on $P(X)$

$\cap$ on $P(X)$

$+$ on $\mathbb{Q}$

$\cdot$ on $\mathbb{Q}$

Non eg

$\to$ Taking complement of 2 sets on $P(X)$

$\to$ function composition.

Defn A bin op $\star$ on set S is associative p.t.

$\forall a, b, c \in S$ $\quad a \star (b \star c) = (a \star b) \star c$

Eg: $\cup$ on $P(X)$

$\cap$ on $P(X)$

Non-eg: complement on $P(X)$

Cool (Prove) : func composition is associative !! $\star$ Fun (X)

Defn for a set S and bin op $\star$. $e \in S$ is said to be the idenity pt $\forall\, s \in S$

$$e \star s = s \star e = s$$

$\hookrightarrow$ 2 assertions!!

Eg

bin-op	Set	e
$\cap$	$P(X)$	X
$\cup$	$P(X)$	$\emptyset$
$+$	$\mathbb{Q}$	0
$\cdot$	$\mathbb{Q}$	1
$-$	$\mathbb{Z}$	none
$\div$	$\mathbb{R} \setminus \{0\}$	none
$\circ$	$\mathrm{Fun}(X)$	Id_X

$Id_X : X \to X$
$x \mapsto x$
"Identity f"

Lemma

Let $\star$ be a bin op on set S.
If $\star$ has a identity e, then it is unique.
Let $e_1, e_2 \in S$ be $\star$ - identities.

$$e_1 = e_1 \star e_2 = e$$

Defn Let $*$ be a bin op on set S. $s \in S$, the element $s' \in S$ is the $*$-inv for s p.t.

$$s' * s = s * s' = e$$

→ 2 assertions

If s' is the inv of s, is s an inv of s'?

Eg

Set	bin op	e	inverse?
$\mathbb{N}$	$\cdot$	1	no
	$+$	no id	✗
$\mathbb{Z}$	$\cdot$	1	no – just 1 & 1
	$+$	0	yes
	$-$	no id	✗
$\mathbb{Q}$	$\cdot$	1	yes (except 0)
	$+$	0	yes
	$-$	no	✗
	$\div$	no	✗
$P(X)$	$\cup$	$\emptyset$	no – only $\emptyset$
	$\cap$	X	no, only X
$Fun(X)$	$\circ$	Id_X	???

Lemma

If $*$ is an associative bin op on set S, & if $s \in S$ has a $*$ inv s'. Then s' is the unique inv of s.

Suppose $s', s'' \in S$ are 2 inv of $s \in S$

Then

$$s' = s' \cdot e = s'(s \cdot s'') = (s' \cdot s) \cdot s'' = e \cdot s'' = s''$$

Defn/ A set F with commutative, associative binary operations $+$ and $\circ$ is called a field p.t.

① $\exists$ a $+$-identity called 0_F

② $\exists$ a $\circ$-identity called 1_F

③ $\forall f \in F$ $\exists$ a $+$-inv denoted $-f$

④ $\forall f \in F \setminus \{0\}$ $\exists$ a $\circ$ inv denoted f^{-1}

⑤ $\forall a, b, c \in F$ we have

$a \cdot (b + c) = ab + ac$ $\rightarrow$ distributive

⑥ $1_F \neq 0_F$

Question: Do we worry about $F = \emptyset$?

No since in a field $\exists\, 0_F, 1_F$

$0_F, 1_F \in \emptyset$

Eg: $\mathbb{Q}, +, \cdot$

$\mathbb{R}, +, \cdot$

$F = \{☺, ☹\}$

+	☺	☹
☺	☺	☹
☹	☹	☺

•	☺	☹
☺	☺	☺
☹	☺	☹

+ id is ☺, • id is ☹

Non eg

$\mathbb{Z}, +, \cdot$

$\mathbb{N}, +, \cdot$

Results about fields

F is a field with $\cdot, +, 0, 1$

$\forall a, b, c \in F$ we have

$a + b = c + b \implies a = c$

Proof

fix $a, b, c \in F$

SPS $a+b = c+d$

$a = a + 0 = a + (b + (-b)) = (a+b) - b$

$= (c+b) + -b = c + (b + (-b)) = c + 0$
$= c$

Lemma

for $r \in F$, we have $r \cdot 0 = 0$

$0 + r \cdot 0 = r \cdot 0 = r \cdot (0 + 0)$

$= r \cdot 0 + r \cdot 0$

$0 + r \cdot 0 = r \cdot 0 + r \cdot 0$

by previous lemma

$0 = r \cdot 0$

Lemma

$\forall a, b \in F$

$$(a \cdot b = 0) \iff \left(\begin{array}{c} a = 0 \\ \text{or} \\ b = 0 \end{array} \right)$$

proof

$\Leftarrow$ is done by previous lemma

$\Rightarrow$

fix $a, b \in F$

wlog $a \neq 0$. Since $a \neq 0$ $\exists a^{-1} \in F$

$$b = b \cdot 1 = b(a \cdot a^{-1}) = (b \cdot a) a^{-1}$$

$$0 \cdot a^{-1} = 0$$

Lemma

$\forall a, b \in F$

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

unique

proof fix $a, b \in F$

Note: $-(a \cdot b)$ is the additive inv of $a \cdot b$, so we need to show

$$a \cdot b + ((-a) \cdot b)) = 0$$

$$a \cdot b + (-a) \cdot b = b(a + (-a)) = b(0) = 0$$

$$\therefore -(a \cdot b) = (-a) \cdot b$$

Lemma

$\forall\ a, b \in F$

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

fix $a, b \in F$

$(-a)(-b) + \boxed{-(a\cdot b)} = 0$ + -inv

$-a \cdot -b + (-a)\cdot b$

$-a\,(b + (-b)) = -a\,(0) = 0$

$\therefore\ (-a)\cdot(-b) = ab$

Ordered Fields

Defn

A field F is said to have order structure iff $\exists\, P \subseteq F$ s.t.

① P is closed with respect to $+$ and $\cdot$.
That is for $a, b \in P$, $a+b \in P$, $a \cdot b \in P$

② Trichotomy $\forall\, a \in F$, Exactly 1 is true

1. $a \in P$
2. $a = 0$
3. $-a \in P$

Defn

A field F is said to be ordered if

$\exists\, P \subseteq F$ s.t. (F, P) has order structure.

Q: If F is an ordered field, can P be $\emptyset$.
No, $1 \neq 0$ so by trichotomy $1 \in P$ or $-1 \in P$

Eg 1 For $\mathbb{R}$ take $P := (0, \infty)$

Non Eg Smily face example

Remark: A field may have >1 order structure. (Look at HW1, Q3)