Sets and groups

KYB

Thrn, it's a Fact

mathrnfact@gmail.com

January 13, 2021

Overview

Module Thoery
- Sets
- Groups

Sets

ZF+C

1. Axiom of Extensionalty
2. Axiom of Pairing
3. Axiom Schema of Separation
4. Axiom of Union
5. Axiom of Power Set
6. Axiom of Infinity
7. Axiom Schema of Replacement
8. Axiom of Regularity
9. Axiom of Choice

Russell's Paradox

$R = \{x : x \text{ is a set and } x \notin x\}$ is not a set.

Proof.

Since $\varnothing \notin \varnothing$, R is nonempty.

Suppose R is a set.

- If $R \in R$, by the property $x \notin x$ of R, $R \notin R$ (contradiction).
- If $R \notin R$, by the property $x \notin x$ of R, $R \in R$ (contradiction).

Hence R is not a set. $\square$

Under ZFC, we get

Definition

- $A \subset B$ iff $x \in A$ implies $x \in B$.
- $x \in A \cap B$ iff $x \in A$ and $x \in B$.
- $x \in A \cup B$ iff $x \in A$ or $x \in B$.
- $x \in A - B$ iff $x \in A$ but $x \notin B$.
- $x \in \bigcup_{A \in \mathcal{A}} A$ iff $x \in A$ for some $A \in \mathcal{A}$.
- $x \in \bigcap_{A \in \mathcal{A}} A$ iff $x \in A$ for all $A \in \mathcal{A}$.

Remark

For any set A,

- $A \cup \varnothing = A$,
- and $A \cap \varnothing = \varnothing$
- $\varnothing \subset A$

because there is no $x \in \varnothing$.

Definition (Ordered Pair)

Define $(a, b) = \{\{a\}, \{a, b\}\}$.
In general, $(a_1, \cdots, a_{n+1}) = ((a_1, \cdots, a_n), a_{n+1})$.

Remark

- $(a, a) = \{\{a\}\}$.
- $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

Definition (Power Set)

Let X be a set. The *power set* of X is the set of all subsets of X, denoted by $\mathcal{P}(X)$.

Definition (The Cartesian Product)

Let X and B be sets. The Cartesian product of X and Y is the set of all ordered pairs (x, y) where $x \in X$ $y \in Y$, denoted by $X \times Y$.
Define $X_1 \times \cdots \times X_{n+1} = (X_1 \times \cdots \times X_n) \times X_{n+1}$.
If $X_i = X$ for $i = 1, \cdots, n$, $X^n = X \times \cdots \times X$.

Remark

If $X = \varnothing$, $X \times Y = \varnothing$ because if not there is $(x, y) \in X \times Y$, i.e. $x \in X$ and $y \in Y$ but there is no such x.

Definition (Functions)

Let X and Y be sets. A function f is a subset of $X \times Y$ which satisfies

1. for all $x \in X$, there is $y \in Y$ such that $(x, y) \in f$,
2. if $(x_1, y), (x_2, y) \in f$, then $x_1 = x_2$.

If $(x, y) \in f$, write $f(x) = y$.

Remark

- If $X = \varnothing$, $X \times Y$ is always a function.
- If $Y = \varnothing$, there is no function from X to Y.

Definition (Equivalence Relation)

Let X and Y be sets.

- A (binary) relation R is a subset of $X \times Y$. If $(x, y) \in R$, write xRy.
- Suppose $X = Y$. If R satisfies
  1. (reflexive) for all $x \in X$, xRx,
  2. (symmetric) for all $x, y \in X$, xRy implies yRx,
  3. (transitive) for all $x, y, z \in X$, xRy and yRz implies xRz,

  R is called an equivalence relation.

Definition (Partition)

A partition $\mathcal{P}$ of a nonempty set X is a family of disjoint nonempty sets whose union is X, i.e.

1. for all $P \in \mathcal{P}$, $P \neq \varnothing$,
2. for $P_1, P_2 \in \mathcal{P}$, $P_1 \cap P_2 \neq \varnothing$ implies $P_1 = P_2$,
3. $\bigcup_{P \in \mathcal{P}} = X$.

Theorem

- *If $\mathcal{P}$ is a partition of a nonempty set X, there is a equivalence relation $\sim$ definded by $x \sim y$ iff there is $P \in \mathcal{P}$ such that $x, y \in P$.*
- *Conversely, if there is a equivalence relation $\sim$, there is a partition $\mathcal{P}$ consisting of a set $P_x = \{y \in X : y \sim x\}$ for each $x \in X$. In this case, write $\mathcal{P} = X/\sim$ (a quotient of X) and $P_x = [x]$ (a equivalence class of x).*

Definition ((Partial) Ordered Set)

A relation $<$ on a set X is called a partial ordering of X if

1. $a \not< a$ for any $a \in X$,
2. if $a < b$ and $b < c$, then $a < c$.

If there is one more condition

3. $a < b$ or $a = b$ or $a > b$ for all $a, b \in X$,

X is called an (linear, or totally) ordered set.

the Axiom of Choice

Observe

What is the meaning of 'choice' in math? If there is only language of sets, we must define 'choosing something from sets'.

Definition (Choice function)

Let I be an index set and let $\{A_\alpha : \alpha \in I\}$ be a collection of sets. A choice function is any function

$$f : I \to \bigcup_{\alpha \in I} A_\alpha$$

such that $f(\alpha) \in A_\alpha$ for each $\alpha \in I$.

So choosing something from sets means there is a choice function.

The Axiom of Choice

Let $\mathcal{A} = \{A_\alpha : \alpha \in I\}$ be a collection of nonempty sets A_α with index set I. Then there is a choice function on $\mathcal{A}$.

Fact

- If each A_α is singleton;
- If I is finite;
- If each A_α is a finite subset of $\mathbb{R}$,

there is a choice function.

The Well Ordering Principle

Every set can be well-ordered, i.e. every set has a ordering which satisfies every nonempty subset has the least elements in this order.

Zorn's Lemma

If A is a nonempty partially ordered set in which every chain has an upper bound, then A has a maximal element.

Remark

AoC, WOP, and Zorn's lemma are all equivalent, i.e.

AoC iff WOP iff Zorn's lemma

Application of Zorn's lemma

Every vector space V over a field F has a basis.

Proof

Recall that a basis is a subset of V which is (1) linearly independent and (2) spans V.
If $V = \{0\}$, we say $\{0\}$ is a basis.
Suppose $V \neq \{0\}$. Then for each nonzero vector v, $\{v\}$ is linearly independent. Let $\mathcal{V}$ be a family of all subsets of V which is linearly independent. Then $\mathcal{V}$ is nonempty. Give a partial order $\leq$ on $\mathcal{V}$ by

$$B_1 \leq B_2 \iff B_1 \subseteq B_2.$$

Let $\mathcal{C}$ be any chain of $\mathcal{V}$. (continue)

Proof

Claim) $\mathcal{C}$ has an upper bound in $\mathcal{V}$.
Let $C = \cup_{B \in \mathcal{C}} B$. Suppose

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$$

where $\alpha_i \in F$ and $v_i \in C$. Since $\mathcal{C}$ is a chain, we can choose $B \in \mathcal{C}$ such that $\{v_1, \cdots, v_n\} \subset B$. Since B is linearly independent, $\alpha_i = 0$ for all i, and so C is linearly independent ($C \in \mathcal{V}$). Moreover for all $B \in \mathcal{C}$, $B \subseteq C$, or $B \leq C$. Hence C is an upper bound of $\mathcal{C}$.

Now we can apply Zorn's lemma on $\mathcal{V}$ and let B be a maximal element of $\mathcal{V}$.
(continue)

Proof

Claim) B is a basis for V.
Since $B \in \mathcal{V}$, it suffices to show that $\operatorname{span} B = V$. Suppose not. Then there is $v \in V - \operatorname{span} B$. You can easily show that $B \cup \{v\}$ is linearly independent. So $B \lneq B \cup \{v\}$. But B is maximal under $\leq$ (contradiction). Hence $\operatorname{span} B = V$, B is a basis.

Groups

Definition

- A binary operation $\times$ on a set G is a function $\times : G \times G \to G$.
- $\times$ is associative if for all $a, b, c \in G$, $(a \times b) \times c = a \times (b \times c)$.
- For $a, b \in G$, we say a and b commute if $a \times b = b \times a$.
- If for all $a, b \in G$ a and b commute, $\times$ is commutative.

Definition (Groups)

Let G be a nonempty set with a binary operation $\times$. G is a group if

1. $\times$ is associative,
2. there is $e \in G$ such that for all $a \in G$, $a \times e = e \times a = a$,
3. for all $a \in G$, there is $b \in G$ such that $a \times b = b \times a = e$.

e is called a identity and b is called an inverse of a.

If $\times$ is commutative, G is called an abelian group.

Example

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(S_n, \circ)$, $\cdots$.

Remark

We describe groups in two ways, one is addition $(G, +)$, the other is multiplicatication $(G, \cdot)$.
In $(G, +)$, an identity is 0 and an inverse of a is $-a$.
In $(G, \cdot)$, an identity is 1 and an inverse of a is a^{-1}.

Proposition

Let $(G, \cdot)$ be a group.

1. The identity of G is unique
2. for each $a \in G$, the inverse of a is unique
3. $(a^{-1})^{-1} = a$
4. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Proposition

Let G be a group. The left and right cancellation laws hold in G, i.e.

1. $au = av \implies u = v$
2. $ub = vb \implies u = v$

Definition (Homomorphism)

Let G and H be groups and let $f : G \to H$ be a function. f is called a homomorphism if

$$f(xy) = f(x)f(y).$$

(f preserves a group structure)
If f is bijective, f is called an isomorphism.

Definition

- $\mathrm{Ker} f = \{x : f(x) = 1\}$
- $\mathrm{Im}\, f = \{f(x) : x \in G\}$.

Definition (Subgroups)

Let $(G, \cdot)$ be a group. A subset H of G is called a subgroup if

- if $a \in H$, then $a^{-1} \in H$
- if $a, b \in H$, then $ab \in H$

Denote $H \leq G$.

Proposition

Let G be a group. If a subset H of G satisfies

- $1 \in H$
- for all $x, y \in H$, $xy^{-1} \in H$,

then H is a subgroup of G.

Example

$\mathrm{Ker} f \leq G$ and $\mathrm{Im}\, f \leq H$.

Definition (Cyclic Groups)

A group H is cyclic if H can be generated by a single element, i.e. there is $x \in H$ such that $H = \{x^n : n \in \mathbb{Z}\}$. Denote $H = \langle x \rangle$

Example

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
2. For all $n \in \mathbb{Z}$, $n\mathbb{Z} = \langle n \rangle$.
3. For all $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$.

Theorem

Suppose G is a cyclic group.

1. *if G is infinite, $G \cong \mathbb{Z}$.*
2. *if G has only n elements, then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Definition

Let G be a group and H be a subset of G. For each $g \in G$, define

- $gH = \{gh : h \in H\}$, a left coset
- $Hg = \{hg : h \in H\}$, a right coset

If H is a subgroup of G, then the set of all left(resp. right) cosets forms a partition of G, i.e.

- '$x \sim y$ iff $xH = yH$' is an equivalence relation
- $gH = [g]$

Remark

Note that if H is a subgroup of G,

$$\begin{aligned} xH = yH &\iff xh_1 = yh_2 \text{ for some } h_1, h_2 \in H \\ &\iff y^{-1}x = h \text{ for some } h \in H \iff y^{-1}xH = H \end{aligned}$$

In general, $gH \neq Hg$.

Observe

Let H be a subgroup of G. We want to give a group structure on G/H (the set of all left (right) cosets). The natrul way is that

$$xH \cdot yH = (xy)H.$$

But to do this,

$$xHyH = xyH,$$

or for all $h_1, h_2 \in H$, $xh_1yh_2 = xyh$ for some $h \in H$ and vice versa. That means for all $h \in H$, there is $h' \in H$ such that

$$yhy^{-1} = h'.$$

Thus $yHy^{-1} = H$ for all $y \in G$, or $yH = Hy$.

Definition

Let G be a group and H be a subgroup of G. H is called a normal subgroup of G, denoted by $H \trianglelefteq G$, if

$$gHg^{-1} = H \text{ for all } g \in G.$$

Example

Let $f : G \to H$ be a homomorphism. Then $\mathrm{Ker} f \trianglelefteq G$.

Proposition

Let $N \leq G$. $N \trianglelefteq G$ iff N is a kernel of some homomorphism.

The First isomorphism Theorem

Let $f : G \to H$ be a homomorphism. Then there $G/\mathrm{Ker} f = \mathrm{Im}\, f$.

The End