Introduction to Algebra and Analysis

Qichen Huang

07/11/2020

In progress

Contents

Chapter 1

Basic Topology

1.1 Set

Notation.

- $\mathbb{N}_n = \{1, 2, \cdots, n\}$
- $A^n = \{(a_1, \cdots, a_n) : a_i \in A\}$

Definition 1 (Finite; Countable). Let A be a set.

- A is *finite* if $A \sim \mathbb{N}_n$ for some n.
- A is *countable* if $A \sim \mathbb{N}$ or A is finite.
- A is *infinite* if A is not finite.
- A is *uncountable* if A is not countable.
- $^*A$ is *infinite* if $\exists B \subset A,\ A \sim B$

Definition 2 (Cardinality). Sets A, B have the same *Cardinality* denoted $A \sim B$ if there is a bijection $f : A \to B$.

Remark. The relation $\sim$ defined in Definition 2 is equivalent.

Definition 3 (Sequence). *A sequence* $\{x_n\}$ *in* X is $f : \mathbb{N} \to X$, where:

- $x_n \in X$, $n \in \mathbb{N}$
- $f(n) = x_n$

Proposition 1. Every subset of a countable set is countable.
(No uncountable set can be subset of a countable set)

Proof. Let A be a countable set,
If $E \subset A$ is finite, then countable.
If $E \subset A$ is infinite, then we construct a sequence to obtain a 1-1 correspondence between J and E. □

Lemma 1.

- If $\exists f : \mathbb{N} \to S$ that is subjection, then S is countable.
- If $\exists g : S \to \mathbb{N}$ that is injection, then S is countable.

Proposition 2. Let $\{E_n : n \in \mathbb{N}\}$ be a countable collection of countable sets.
Then

$$\bigcup_{n=1}^{\infty} E_n$$

is countable.

Proposition 3. Let A be a countable set, then A^n is countable.

Corollary. The set of all rational numbers is countable.

Proposition 4. Let A be the set of all sequence $\{x_n\}$ in $\{0, 1\}$, then A is uncountable.

Corollary.

- $\mathcal{P}(\mathbb{N})$ is uncountable.
- $\mathbb{R}$ is uncountable.

1.2 Metric space

Definition 4 (Metric space; Points; Distance)**.** Let X be a set. X is a metric space if:
$\exists d : X \times X \to \mathbb{R}$ such that $\forall p, q \in X$:

- $d(p, q) > 0$ if $p \neq q$;
  $d(p, p) = 0$
- $d(p, q) = d(q, p)$
- $d(p, q) \leq d(p, r) + d(r, q)$, $\forall r \in X$

where p, q are called *points*, and d is called a *distence function.*

Remark. Every subset of a metric space is still a metric space.

Example. The distance function on $\mathbb{R}^k$ is defined by

$$d(x, y) = |x - y| \qquad (x, y \in \mathbb{R}^k)$$

Definition 5 (Segment; Interval; k-cell).

- *segment* $(a, b) := \{x : a < x < b\}$
- *interval* $[a, b] := \{x : a \leq x \leq b\}$
- Let $a_i < b_i$ for $i = 1, \cdots, k$. A *k-cell* is a set $\{(x_1, \cdots, x_k) \in \mathbb{R}^k : a_i \leq x_i \leq b_i\}$

Definition 6 (Ball). Let (X, d) be a metric space.
A *open ball centered at* $\mathbf{x} \in X$ *with radius* $r > 0$ is a set $\{\mathbf{y} \in X : d(\mathbf{y} - \mathbf{x}) < r\}$. A *closed ball* contains the open ball and the boundary where $d(\mathbf{y} - \mathbf{x}) = r$.

Definition 7 (Convex). A set $E \subseteq \mathbb{R}^k$ *convex* if

$$\lambda \mathbf{x} + (1 - \lambda)\mathbf{y} \in E$$

for all $\mathbf{x} \in E, \mathbf{y} \in E, 0 < \lambda < 1$.

Remark.

- Balls and k-cells are convex.

Geometrically, E is convex means for any two points in E, the line segment connects them is in E.

Definition 8. Let X be a metric space. Let $p, q \in X$, $E \subseteq X$.

- A *neighborhood* of a point p is an open ball centered at p with radius r.
- A point p is a *limit point* of the set E if every neighborhood of p contains a point $q \neq p$ such that $q \in E$.
- If $p \in E$ and p is not a limit point of E, then p is called an *isolated point of* E.
- E is *closed* if every limit point of E is a point of E.
- A point p is an *interior* point of E if there is a neighborhood N of p such that $N \subseteq E$.
- E is *open* if every point of E is an interior point of E.

- The *complement* of E (denoted by E^c) is $\{p \in X : p \notin E\}$.
- E is *perfect* if E is closed and if every point of E is a limit point of E.
- E is *bounded* if there is a real number b, and a point $q \in X$ such that $d(p,q) < b$ for all $p \in E$.
- E is *dense* in X if every point of X is a limit point of E, or a point of E, or both.

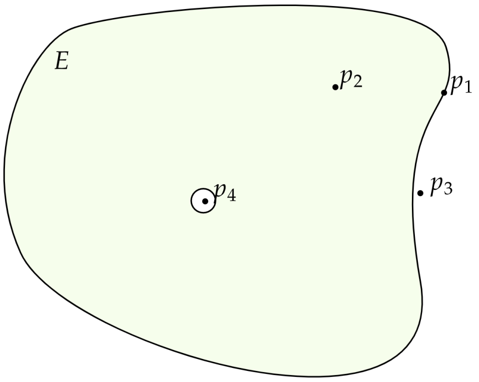

Figure 1.1: p_1, p_2 are limit points; p_3, p_4 are isolated points. Also, $p_1 \in E$ and p_1 is not interior point of E so E is not open. But E is closed.

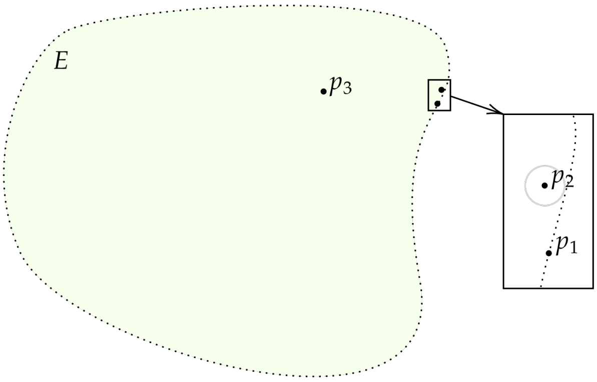

Figure 1.2: p_1 is a limit point but not in E; p_2 is an interior point; all three are limit points. E is open but not closed.

Example. Let the following be subsets of $\mathbb{R}^2$.

1. $\{z : z \in \mathbb{C}, |z| < 1\}$

2. $\{z : z \in \mathbb{C}, |z| \leq 1\}$

3. A finite set.

4. $\mathbb{Z}$

5. $\{\frac{1}{n} : n \in \mathbb{N}\}$

6. $\mathbb{C}$ or $\mathbb{R}^2$

7. The segment (a, b)

Example	**Closed**	**Open**	**Perfect**	**Bounded**
1	No	Yes	No	Yes
2	Yes	No	Yes	Yes
3	Yes	No	No	Yes
4	Yes	No	No	No
5	No	No	No	Yes
6	Yes	Yes	Yes	No
7	No	†	No	Yes

† Yes if $(a, b) \subset \mathbb{R}$, No if $(a, b) \subset \mathbb{R}^2$

Definition 9 (Relatively Open)**.** Let $E \subset Y \subset X$, where (X, d) is a metric space. Then E is *open relative to* Y if E is an open set of the metric space (Y, d).

Remark. The segment (a, b) is open relative to $\mathbb{R}$ but not $\mathbb{R}^2$.

Proposition 5.

1. Every neighborhood is an open set.

2. If p is a limit point of a set E, then every neighborhood of p contains infinitely many points of E.

   2.1. A finite point set has no limit points.

3. A set E is open if and only if its complement is closed.

Proof.

1. .

2. .

3. If E is open, assume $\exists x \in E^c$, such that x is a limit point of E^c and $x \notin E^c$.
   Then $x \in E$ and x is an interior point in E, implies there exists a neighborhood N of x, such that $N \subseteq E$, implies $N \nsubseteq E^c$, implies that x is not a limit point of E^c, which contradicts to the assumption. E^c is closed.

If E^c is closed, $\forall x \in E$, $x \notin E^c$, and x is not a limit point of E^c, implies there exists a neighbor N of x such that $N \not\subseteq E^c$, implies $N \subseteq E$. E is open.

□

Proposition 6.

1. For any collection $\{G_\alpha\}$ of open sets, $\bigcup_\alpha G_\alpha$ is open.
2. For any collection $\{F_\alpha\}$ of closed sets, $\bigcap_\alpha F_\alpha$ is closed.
3. For any finite collection $\{G_1, \cdots, G_n\}$ of open sets, $\bigcap_{i=1}^n G_i$ is open.
4. For any finite collection $\{F_1, \cdots, F_n\}$ of closed sets, $\bigcup_{i=1}^n F_i$ is closed.

Proof.

1. Trivial.
2. Follow from 1, apply De Morgen's Law and **Proposition 5**-3.
3. Trivial.
4. Follow from 3 as in 2.

□

Definition 10 (Closure)**.** Let X be a metric space.
Let $E \subset X$, and E' be the set of all limit points of E, then the *closure* of E is $\bar{E} = E \cup E'$.

Proposition 7. Let X be a metric space and $E \subset X$, then

1. $\bar{E}$ is closed.
2. $E = \bar{E} \Leftrightarrow E$ is closed.
3. $\bar{E} \subset F$ for every closed set $F \subset X$ such that $E \subset F$. ($\bar{E}$ is the smallest closed set containing E)

Proof.

1. Let $x \in \bar{E}^c = E^c \cap E'^c$. Since $x \notin E$ and is not a limit point of E, so there exists a neighbor N of x, such that $N \cap E = \varnothing$, implies $N \cap E' = \varnothing$ (check this one using contradiction), implies $N \subset E^c \cap E'^c$. $\bar{E}^c$ is open.
2. Trivial.
3. Let $F \subset X$ be closed and $E \subset F$, then $F' \subset F$. Since $E' \subset F'$, so $E' \subset F \Rightarrow \bar{E} = E \cup E' \subset F$.

□

Proposition 8. Let E be a nonempty subset of $\mathbb{R}$ bounded above.
Then $\sup(E) \in \bar{E}$, and (E is closed) $\Rightarrow$ ($\sup(E) \in E$)

Proposition 9. Let $E \subset Y \subset X$ where (X, d) is a metric space.
E is open relative to Y if and only if $\exists G,$ s.t. G is open relative to X and $E = G \cap Y$.

Proof. TODO □

1.2.1 Compactness in Metric Space

Definition 11 (Open cover)**.** Let X be a metric space.
An *open cover of* $E \subseteq X$ is $\{G_\alpha\}$, where G_α is an open subset of X, and $E \subseteq \bigcup_\alpha G_\alpha$.

Definition 12 (Compact)**.** Let X be a metric space, and K a subset of X.
K is *compact* if every open cover of K contains a finite subcover that covers K.

Proposition 10. Suppose $K \subseteq Y \subseteq X$. Then K is compact relative to Y if and only if K is compact relative to X.

Real Analysis

Contents

Chapter 1 Preliminary

Definition 1.1 (Isometry)

Let (X, d_X) and (Y, d_Y) be metric spaces. A map $f : X \to Y$ is called **isometry** if for any $a, b \in X$,

$$d_X(a, b) = d_Y(f(a), f(b)).$$

Definition 1.2 (Congruent)

Two subsets $E, F \subseteq \mathbb{R}^n$ are called **congruent** if there exists an isometry $f : \mathbb{R}^n \to \mathbb{R}^n$ s.t. $f(E) = F$.

Intuition E congruent to F if E can be transformed into F by translations, rotations, and reflections.

Definition 1.3 (Indexed family)

Let I and X be sets and f a function s.t.

$$\begin{aligned} f :&I \to X \\ &i \mapsto x_i = f(i) \end{aligned}$$

(note that we denoted the image of i under f by x_i). We then call the image of I under f a **family of elements in X indexed by I**.

Remark Similar definition goes to **indexed collection of nonempty sets**.

1.1 Topology

Proposition 1.1

1. Any open subset of $\mathbb{R}$ is a countable union of disjoint open intervals.
2. Any open interval is a countable union of closed intervals.

1.2 Sequence and series

Definition 1.4

If X is an arbitrary set and $f : X \to [0, \infty]$, we define

$$\sum_{x \in X} f(x) = \sup\{\sum_{x \in F} f(x) : F \subseteq X, |F| < \infty\}$$

Remark We define the sum to be the supremum of its finite partial sums so that it also works for uncountable set X.

Proposition 1.2

Given $f : X \to [0, \infty]$, let $A = \{x \in X : f(x) > 0\}$. If A is uncountable, then $\sum_{x \in X} f(x) = \infty$. If A is countably infinite, then $\sum_{x \in X} f(x) = \sum_1^\infty f(g(n))$ where $g : \mathbb{N} \to A$ is any bijection and the sum $\sum_1^\infty f(g(n))$ is an arbitrary infinite series.

Proof We can write $A = \bigcup_{n=1}^{\infty} A_n$, where $A_n = \{x \in X : f(x) > \frac{1}{n}\}$. If A is uncountable, then there exists A_k is uncountable, thus contains infinite many elements and $\sum_{x \in F} f(x) > |F|/n$ where $F \subset A_k$ is finite. As $|F| \to \infty$, $\sum_{x \in X} f(x) \to \infty$.

If A is countably infinite, then there exists a bijection $g : \mathbb{N} \to A$. For every finite subset F of A, we can always find a set $B_N = g(\{1, \cdots, N\})$ containing F with large enough N. Hence

$$\sum_{x \in F} f(x) \leq \sum_{1}^{N} f(g(n)) \leq \sum_{x \in X} f(x)$$

By taking the supremum over N, we have

$$\sum_{x \in F} f(x) \leq \sum_{1}^{\infty} f(g(n)) \leq \sum_{x \in X} f(x)$$

and then taking the supremum over F, we obtain the desired result.

Chapter 2 Measure Theory

2.1 Motivation

The motivation of measure theory is to measure the length, area, or volume of a region. Given a region $E \subseteq \mathbb{R}^n$, we would like to assign a non-negative number $\mu(E)$ to it. Intuitively, such function μ should satisfy the following:

1. For countable sequence of disjoint sets, $E_1, E_2, \cdots$ we have
$$\mu(E_1 \cup E_2 \cdots) = \mu(E_1) + \mu(E_2) + \cdots .$$
2. If E is congruent to F, then $\mu(E) = \mu(F)$.
3. $\mu(Q) = 1$, where Q is the unit cube
$$Q = \{x \in \mathbb{R}^n : 0 \le x_j < 1 \text{ for } j = 1, \cdots, n\}$$

But unfortunately, there conditions are mutually inconsistent. Consider the following example:

Example 2.1

Let $n = 1$. Define an equivalence relation by the Axiom of Choice, we can build a set N that contains one member of each equivalent class. Let $R = \mathbb{Q} \cap [0, 1)$ (set of all rationals in $[0, 1)$), and for each $r \in R$, let

$$N_r = \{x + r : x \in N \cap [0, 1 - r)\} \cup \{x + r - 1 : x \in N \cap [1 - r, 1)\},$$

Intuitively, we shifted the N to the right by r and then shifted the part sticks out beyond $[0, 1)$ one to the left.

We shall show that

Corollary 2.1

There is no such $\mu : \mathcal{P}(\mathbb{R}) \to [0, \infty]$ exists that satisfies the aforementioned three conditions. ♡

Proof We proof by contradiction. First show that $\{N_r\}$ partitions $[0, 1)$:

- For all $y \in N$, if $y \in [x]$, then $y \in N_r$ where $r = x - y$ or $r = x - y + 1$.
- Let $y \in [0, 1)$, if $y \in N_r \cap N_s$ $(r \neq s)$, then $y - r$ (or $y - r + 1$) and $y - s$ (or $y - s + 1$) would belong to two distinct equivalent classes, while their difference is a rational, so is a contradiction.

Suppose there exists a $\mu : \mathcal{P}(\mathbb{R}) \to [0, 1)$ satisfies the aforementioned three conditions, then by condition 1 and 2, we have $\mu(N) = \mu(N_s)$.

Also since R is countable, so by condition 1, we have $\mu([0, 1)) = \sum\limits_{r \in R} \mu(N_r) = |R|\mu(N_r)$, but $|R|\mu(N_r)$ is either 0 (if $\mu(N_r) = 0$) and ∞ (if $\mu(N_r) > 0$), which contradicts condition 3. ■

Remark

- Even weaken the condition 1 so that it only allows the additively holds for finite sequences it will still lead to contradiction when dimension $n \ge 3$. [1]
- Such contradiction also arises in probability theory, just consider $X \sim \text{Uniform}[0, 1]$, and for $E \subseteq X$, let $\mu(E) = \mathbb{P}(E)$.

[1] See Complementary 1

2.2 σ-algebras

Motivation Before measuring subsets, we first define the collection of subsets we want to give the measure to, that is, the collection of measurable sets. As we have seen it is not possible to give measure to the power set all the time.

Definition 2.1 (Semialgebras)

Let X be a nonempty set. A **semialgebra** of X is a nonempty collection $\mathcal{A}$ of subsets of X that is

1.

♣

Definition 2.2 (Algebra)

Let X be a nonempty set. An **algebra** of X is a nonempty collection $\mathcal{A}$ of subsets of X that is

1. closed under *finite unions*: If $E_1, \cdots, E_n \in \mathcal{A}$, then $E_1 \cup \cdots \cup E_n \in \mathcal{A}$,
2. and closed under complements: If $E \in \mathcal{A}$, then $E^c \in \mathcal{A}$.

♣

Definition 2.3 (σ-algebra)

A **σ-algebra** is an algebra that is closed under *countable unions*:
If $E_1, E_2, \cdots \in \mathcal{A}$, then $E_1 \cup E_2 \cup \cdots \in \mathcal{A}$.

♣

Corollary 2.2

1. Algebra (σ-algebra) is closed under finite (countable) intersections.
2. If $\mathcal{A}$ is an algebra, then $\varnothing \in \mathcal{A}$, and $X \in \mathcal{A}$.
3. If an algebra is closed under countable *disjoint* unions, then it is a σ-algebra.
4. Let $\mathcal{A}_i$ be a family of σ-algebra, then $\bigcap_i \mathcal{A}$ is also a σ-algebra.

♡

By Corollary 2.2.4, we can define the following

Definition 2.4

Let $\mathcal{E} \subseteq \mathcal{P}(X)$, and let $\sigma(\mathcal{E})$ be the intersection of all σ-algebra containing $\mathcal{E}$, then we call $\sigma(\mathcal{E})$ the σ-alegbra **generated** by $\mathcal{E}$, in another word, $\sigma(\mathcal{E})$ is the smallest σ-algebra containing $\mathcal{E}$.

♣

Lemma 2.1

If $\mathcal{E} \subseteq \sigma(\mathcal{F})$, then $\sigma(\mathcal{E}) \subseteq \sigma(\mathcal{F})$.

♡

Definition 2.5 (Borel σ-algebra)

Let X be a metric space, the σ-alegbra generated by the collection of all open sets (or, equivalently, by the collection of all closed sets) in X is called **Borel σ-algebra**, denoted by $\mathcal{B}_X$, and its members are called **Borel sets**.

♣

Proposition 2.1

$\mathcal{B}_{\mathbb{R}}$ is generated by each of the following:

1. the open intervals: $\mathcal{E}_1 = \{(a, b) : a < b\}$.
2. the clased intervals: $\mathcal{E}_2 = \{[a, b] : a < b\}$.
3. the half-open intervals: $\mathcal{E}_3 = \{(a, b] : a < b\}$ or $\mathcal{E}_4 = \{[a, b) : a < b\}$
4. the open rays: $\mathcal{E}_5 = \{(a, \infty) : a \in \mathbb{R}\}$ or $\mathcal{E}_6 = \{(-\infty, b) : a \in \mathbb{R}\}$.

5. the closed rays: $\mathcal{E}_7 = \{[a, \infty) : a \in \mathbb{R}\}$ or $\mathcal{E}_8 = \{(-\infty, a] : a \in \mathbb{R}\}$.

Proof Idea To prove this proposition, we apply Proposition 1.1 and Lemma 2.1. Note that half intervals can be build by the intersection of a ray and the complement of another ray.

2.3 Product σ-algebra

Given a collection of nonempty set $\{X_\alpha\}$ and their σ-algebra $\mathcal{M}_\alpha$, we want to obtain a σ-algebra of the Cartesian product space $X_1 \times \cdots$, so we define:

Definition 2.6 (product σ-algebra)

Let $\{X_\alpha\}_{\alpha \in A}$ be an indexed collection of nonempty sets, $X = \Pi_{\alpha \in A} X_\alpha$ the Cartesian product space, and $\pi_\alpha : X \to X_\alpha$ the coordinate maps. If $\mathcal{M}_\alpha$ is a σ-algebra on X_α for each α, the **product σ-algebra** on X is the σ-algebra generated by:

$$\{\pi_\alpha^{-1}(E_\alpha) : E_\alpha \in \mathcal{M}_\alpha, \alpha \in A\}$$

we denote this σ-algebra by $\bigotimes_{\alpha \in A} \mathcal{M}_\alpha$.

Proposition 2.2

If the index set A is countable, then $\bigotimes_{\alpha \in A} \mathcal{M}_\alpha$ is the σ-algebra generated by

$$\{\Pi_{\alpha \in A} E_\alpha : E_\alpha \in \mathcal{M}_\alpha\}$$

Proposition 2.3

Proposition 2.4

Corollary 2.3

2.4 Measures

Definition 2.7 (Measure)

Let X be a set equipped with a σ-algebra $\mathcal{M}$, we call $(X, \mathcal{M})$ **measurable space**, and $\mathcal{M}$ a collection of **measurable sets**. A **measure** on $(X, \mathcal{M})$ is a function $\mu : \mathcal{M} \to [0, \infty]$ such that

1. $\mu(\varnothing) = 0$,
2. (**countable additivity**) if $\{E_j\}_1^\infty$ is a sequence of disjoint sets in $\mathcal{M}$, then $\mu(\bigcup_1^\infty E_j) = \sum_1^\infty \mu(E_j)$.

We call $(X, \mathcal{M}, \mu)$ the measure space.

Also, for μ satisfies **finite additively** instead of countable additively we call it **finite additive measure**.

Theorem 2.1

1. (**Monotonicity**) If $E, F \in \mathcal{M}$ and $E \subseteq F$, then $\mu(E) \leq \mu(F)$.
2. (**Subadditivity**) If $\{E_j\}_1^\infty \subseteq \mathcal{M}$, then $\mu(\bigcup_1^\infty E_j) \leq \sum_1^\infty \mu(E_j)$.
3. (**Continuity from below**) If $\{E_j\}_1^\infty \subseteq \mathcal{M}$ and $E_1 \subseteq E_2 \subseteq \cdots$, then $\mu(\bigcup_1^\infty E_j) = \lim_{j\to\infty} \mu(E_j)$.
4. (**Continuity from above**) If $\{E_j\}_1^\infty \subseteq \mathcal{M}$, $E_1 \supseteq E_2 \supseteq \cdots$, and $\mu(E_1) < \infty$, then $\mu(\bigcap_1^\infty E_j) = \lim_{j\to\infty} \mu(E_j)$.

♡

Proof skip for now

Definition 2.8

Let $(X, \mathcal{M}, \mu)$ be a measure space,

- If $\mu(X) < \infty$, μ is called **finite**.
- If $E = \bigcup_1^\infty E_j$ where $E_j \in \mathcal{M}$ and $\mu(E_j) < \infty$ for all j, the set E is said to be σ-**finite** for μ, and if $E = X$ we call μ to be σ-**finite**.
- If for each $E \in \mathcal{M}$ with $\mu(E) = \infty$ there exists $F \in \mathcal{M}$ with $F \subset E$ and $0 < \mu(F) < \infty$, μ is called **semifinite**.

♣

Intuition If the measure of X is finite then μ called finite; if X is the union of countable subsets with finite measure then μ called σ-finite.

Example 2.2 Consider $(X, \mathcal{M}, \mu)$:

- X is any nonempty set,
- $\mathcal{M} = \mathcal{P}(X)$,
- $\mu(E) = \sum_{x\in E} f(x)$, where f any function from X to $[0, \infty]$

then

1. μ is semifinite iff $f(x) < \infty$ for every $x \in X$,
2. μ is σ-finite iff μ is semifinite and $\{x \in X : f(x) > 0\}$ is countable.

Explaination

1. If $f(x) = \infty$ for some $x \in X$, then $\mu(\{x\}) = \infty$ and no subset of $\{x\}$ has finite nonzero measure. On the other hand, if $f(x) < \infty$ for every $x \in X$, then for each $E \in \mathcal{M}$ with $\mu(E) = \infty$, there always exists a finite subset of E with finite measure,
2. If μ is σ-finite, then for every $x \in X$, $x \in E_j$ for some j (use Definite 2.7), since $\mu(E_j) < \infty$, so $f(x) = \mu(\{x\}) < \mu(E_j) < \infty$. Assume that $\{x \in X : f(x) > 0\}$ is uncountable, then some E_k is uncountable thus by Proposition 1.2, $\mu(E_k) = \infty$ $\lightning$. On the other hand, if μ is semifinite and $S = \{x \in X : f(x) > 0\}$ is countable, then exists a bijection h from $\mathbb{N}$ to S and let $E = \bigcup_1^\infty E_j$ where each E_j contains exact one element with positive measure: $h(j)$, then $\mu(E_j) < \infty$ since all other elements in E_j are either 0 or negative.

Definition 2.9

Given $(X, \mathcal{M}, \mu)$ defined in Example 2.2,

- if $f(x) = 1$ for all x, μ is called **counting measure**,
- if for some $x_0 \in X$, f is defined by $f(x_0) = 1$ and $f(x) = 0$ $(x \neq x_0)$, μ is called the **point mass**.

♣

Definition 2.10 (Complete measure)

Let $(X, \mathcal{M}, \mu)$ be a measure space, a set $E \in \mathcal{M}$ such that $\mu(E) = 0$ is called a **null set**.
μ is called **complete** if its domain, $\mathcal{M}$, contains all the subsets of null sets. ♣

We defined complete measure because it is natural for a subset of null set to have measure 0.

Theorem 2.2

Suppose that $(X, \mathcal{M}, \mu)$ is a measure space. Let

$$\mathcal{N} = \{N \in \mathcal{M} : \mu(N) = 0\}$$

and

$$\overline{M} = \{E \cup F : E \in \mathcal{M} \text{ and } F \subseteq N \text{ for some } N \in \mathcal{N}\}.$$

Then $\overline{M}$ is a σ-algebra, and there is a unique extension $\overline{\mu}$ of μ to a complete measure on $\overline{M}$. ♡

Proof Idea set $\overline{\mu}(E \cup F) = \mu(E)$.

2.5 Outer Measures

Motivation Recall we approximate the area of a region using outer rectangles in calculus, now we develop an abstract way of describing it.

Definition 2.11 (Outer Measure)

An **Outer Measure** on a nonempty set X is a function $\mu^* : \mathcal{P}(X) \to [0, \infty]$ that satisfies:

1. $\mu^*(\varnothing) = 0$,
2. (Monotonicity) $\mu^*(A) \leq \mu^*(B)$ if $A \subseteq B$,
3. (Subadditivity) $\mu^*(\bigcup_1^\infty A_j) \leq \sum_1^\infty \mu^*(A_j)$.

♣

To give an outer measure on any subset, we define a collection of subsets $\mathcal{E}$ that is easy to measure. For example to measure the area of any regions in $\mathbb{R}^2$, we could define $\mathcal{E}$ to be rectangles on $\mathbb{R}^2$, and use countably many rectangles that covers the region to approximate the area, the area will be the infimum of all possible approximations.

Proposition 2.5

Let $\mathcal{E} \subseteq \mathcal{P}(X)$ be such that $\varnothing \in \mathcal{E}$, $X \in \mathcal{E}$, and $\rho : \mathcal{E} \to [0, \infty]$ be such that $\rho(\varnothing) = 0$. For any $A \subseteq X$, define

$$\mu^*(A) = \inf\{\sum_{j=1}^\infty \rho(E_j) : E_j \in \mathcal{E} \text{ and } A \subseteq \bigcup_{j=1}^\infty E_j\}$$

Then μ^* is an outer measure. ♠

Proof skip for now.

To obtain a complete measure from an outer measure we need to restrict the collection a bit, and it turns out to be that if we restrict $\mathcal{P}(X)$ to μ^*-measurable sets as defined follow, μ^* becomes a complete measure.

Definition 2.12 (μ^*-measurable)

If μ^* is an outer measure on X, a set $A \subseteq X$ is called μ^***-measurable** if

$$\mu^*(E) = \mu^*(E \cap A) + \mu^*(E \cap A^c) \text{ for all } E \subseteq X$$

Theorem 2.3 (Caratheodory Extension Theorem)

If μ^* is an outer measure on X, the collection $\mathcal{M}$ of μ^*-measurable sets is a σ-algebra, and the restriction of μ^* to $\mathcal{M}$ is a complete measure.

Now we can extend measures from algebra to σ-algebra .

Definition 2.13 (Premeasure)

If $\mathcal{A} \subseteq \mathcal{P}(X)$ is an algebra, a function $\mu_0 : \mathcal{A} \to [0, \infty]$ is called **premeasure** if

1. $\mu_0(\varnothing) = 0$,
2. if $\{A_j\}_1^\infty$ is a sequence of disjoint sets in $\mathcal{A}$ such that $\bigcup_1^\infty A_j \in \mathcal{A}$, then $\mu_0(\bigcup_1^\infty A_j) = \sum_1^\infty \mu_0(A_j)$.

2.6 Borel Measures

Motivation Now we want to measure the subsets of $\mathbb{R}$ based on the idea that the measure of an interval is its length.

Complementary 1: The Axiom of Choice

Axiom 2.1 (The Axiom of Choice [AC])

For any collection X of nonempty sets, there exists a choice function $f : X \to \bigcup X$, such that for every $A \in X$, $f(A) \in A$.

Intuition AC tells us that for any given collection of non-empty sets, we can pick one element from each set and form a new set.

Corollary 2.4 (Zorn's lemma)

Suppose a partially ordered set P has the property that every chain in P has an upper bound in P. Then the set P contains at least one maximal element.

Proof Idea Assume the contrary, we can build a very long chain that has no upper bound in P.

Banach–Tarski paradox

Corollary 2.5 (strong form of the Banach–Tarski paradox)

Given any two bounded subsets A and B of a Euclidean space in at least three dimensions, both of which have a nonempty interior, there are partitions of A and B into a finite number of disjoint subsets, $A = A_1 \cup \cdots \cup A_k$, $B = B_1 \cup \cdots \cup B_k$ (for some integer k), such that for each (integer) i between 1 and k, the sets A_i and B_i are congruent.

Algebra

Contents

Chapter 1

Group Theory

Notation.

- $\mathbf{1}$ denote the identity element distinguish from 1.
- Denote u^{-1} the inverse of u.
- $a \cdot b$ can be written as ab for short.
- If r is finite, we write $r < \infty$.

1.0 Overview

1.1 Monoid

Definition 1 (Monoid). A *monoid* is a triple $(M, \cdot, \mathbf{1})$ in which

1. M is non-empty set,
2. $\cdot$ is an associate binary operation in M,
3. $\mathbf{1} \in M$, such that $\forall a \in M, \mathbf{1} \cdot a = a = a \cdot \mathbf{1}$.

Remark. $\mathbf{1}$ is unique.

Definition 2 (Monad; Semigroup).

- Dropping associativity of p from a monoid results a *monad*.
- Dropping identity element from a monoid results a *semigroup*.

Definition 3 (Submonoid). Let M be a monoid.
A subset N is *submonoid* of M if

- $\mathbf{1} \in N$,
- $\forall n_1, n_2 \in N$, $n_1 \cdot n_2 \in N$.

Remark.

- A submonoid is a monoid.
- A submonoid of a submonoid of M is a submonoid of M.

Example. Let $M(S)$ be a set of all transformation of S, $\cdot$ be the function composition, $\mathbf{1}$ be the identity transformation, then $(M(S), \cdot, \mathbf{1})$ is a monoid.

Definition 4 (Monoid of transformation). Let S be a set, and $M(S)$ be the set of transformation of S, then a submonoid of $M(S)$ is called a *monoid of transformation (of S)*.

Definition 5 (Order of monoid). The *order of a monoid* is its cardinality, denoted by $|M|$.

Remark. The order of the monoid of transformation of $S = \{1, 2, \cdots, n\}$ is n^n.

Definition 6 (Finite). A monoid is *finite* if it has finite order.

1.2 Group

Definition 7 (Invertible)**.** An element u of a monoid M is said to be *invertible* if there exists $v \in M$ such that $uv = \mathbf{1} = vu$.
Such v is called the *inverse* of u.

Remark. Let M be a monoid. $\forall u \in M$, if u is invertible, then its inverse is unique.

Definition 8 (Group; Subgroup)**.**

- A *group* G is a monoid all of whose elements are invertible.
- Let G be a group. A subset of G is a *subgroup of* G if it is a group.

Definition 9 (Group of units)**.** The set of invertible elements of the monoid M is called the *group of unites of* M, denoted by $U(M)$.

Definition 10 (Symmetric group)**.** Let S be a set.
The *symmetric group* of S is $U(M(S))$, the set of invertible transformation (bijection) of S.

Definition 11 (Permutation)**.** Let $S = \{1, 2, \cdots, n\}$, a *permutation* of S is an element of the symmetric group S_n of S.

Proposition 1. The order of S_n is $n!$.

Definition 12 (Group of transformations / Transformation group; Permutation group)**.**

- Let S be a set, and $G(S)$ be the symmetric group of S, then a subgroup of $G(S)$ is called a *group of transformations (of S)*.
- If S is finite, then we call the group of transformations of S the *permutation group (of S)*.

Definition 13 (Direct product)**.** Let $M_1, M_2, \cdots, M_n$ be given monoids. The *direct product* $M = M_1 \times M_2 \times \cdots \times M_n$ *of the monoids* M_i is defined as $\{(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n) : a_i, b_i \in M_i\}$.

Remark. The direct product of monoids is still a monoid.

1.3 Isomorphism

Definition 14 (Isomorphism). Two monoids $(M, \cdot, \mathbf{1})$ and $(M', *, \mathbf{1}')$ are said to be *isomorphic* (denoted by $M \cong M'$) if there exists a bijective map $\eta : M \to M'$ such that:

$$\eta(\mathbf{1}) = \mathbf{1}', \qquad \eta(x \cdot y) = \eta(x) * \eta(y), \qquad \forall x, y \in M$$

Proposition 2. Isomorphism is an equivalence relation on all monoids.

Theorem 1 (CAYLEY'S THEOREM FOR MONOIDS AND GROUPS).

1. Any monoid is isomorphic to a monoid of transformations.
2. Any group is isomorphic to a transformation group.

Proof. Idea: Let $(M, \cdot, 1)$, we could set up an isomorphism of $(M, \cdot, 1)$ with a monoid of transformations of the set M itself. □

Corollary. Any finite group of order n is isomorphic to a subgroup of the symmetric group S_n.

1.4 Associativity and Commutativity

Associativity

Let $\{a_i\}$ be a finite sequence of elements of a monoid M.

Lemma 1. Define $\prod_1^n a_i$ by $\prod_1^1 a_i = a_1$, $\prod_1^{r+1} a_i = (\prod_1^r a_j)a_{r+1}$. Then

$$\prod_1^n a_i \prod_1^m a_{n+j} = \prod_1^{n+m} a_k.$$

Remark. For a given product $a_1 a_2 \cdot a_n$, the parentheses does not affect the result.

Definition 15 (Power)**.**

- The *n-th power of a* is $a^n = a_1 a_2 \cdots a_n$ where all $a_i = a$.
- Define $a^0 = \mathbf{1}$.
- If a is invertible, then define $a^{-n} = a_1^{-1} a_2^{-1} \cdots a_n^{-1}$ where all $a_i^{-1} = a^{-1}$.

Remark.

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}, \qquad \forall m, n \in \mathbb{N}$$

If in addition a is invertible, then the above holds for all $m, n \in \mathbb{Z}$

Commutativity

Definition 16 (Commute)**.** Elements a, b of a monoid M said to *commute* if $a \cdot b = b \cdot a$.

Definition 17 (Commutative monoid; Abelian group)**.**

- A monoid is a *commutative monoid* if $\forall a, b \in M$, a, b commute.
- An *Abelian group* is a commutative group.

Definition 18 (Centralizer; Center)**.** Let M be a monoid.

- Let $a \in M$, the *centralizer of a*, $C_M(a)$ is $\{b \in M : a, b \text{ commute}\}$.
- Let $A \subseteq M$, the *centralizer of A*, $C_M(A) = \bigcap_{a \in A} C_M(a)$.
- $C_M(M)$ is the *center* of M.

Remark.

- The centralizer $C_M(a)$, $C_M(A)$ of a monoid M is a submonoid of M.
- The centralizer $C_G(a)$, $C_G(A)$ of a group G is a subgroup of G.

Proposition 3. Let $a_1, a_2, \cdots, a_n \in M$ such that $a_i a_j = a_j a_i$ for all i, j.
Then the product $a_1 a_2 \cdots a_n$ is invariant under all permutations. In particular, if $ab = ba$, then

$$(ab)^m = a^m b^m \qquad \forall m \in \mathbb{N} \cup \{0\}$$

If in addition a, b are invertible, then the above holds for $m \in \mathbb{Z}$.

1.5 Generator

We can approach the definition of generator in two ways. One is through a non-constructive way:

Definition 19 (Generator)**.** Let S be a subset of a monoid M (or a group G), and let $\{M_\alpha\}$ (or $\{G_\alpha\}$) be the set of all submonoids (or subgroup) of M (or G) which contain the set S. Then the *submonoid (or subgroup) generated by* S is

$$\langle S\rangle = \bigcap_\alpha M_\alpha \quad \left(\text{or} \quad \langle S\rangle = \bigcap_\alpha G_\alpha\right)$$

Another is through a constructive way:

Definition 20 (Generator)**.** Let S be a subset of a monoid M (or a group G), then the *submonoid (or subgroup) generated by* S is

$$\langle S\rangle = \{\mathbf{1}, \prod_{i=1}^{n} s_i : s_i \in S, n \in \mathbb{N}\}$$

$$\left(\text{or} \quad \langle S\rangle = \{\mathbf{1}, \prod_{i=1}^{n} s_i : s_i \in S \vee s_i^{-1} \in S, n \in \mathbb{N}\}\right)$$

In the case where $\langle S\rangle = M$ (or G), we say S a set of *generators* of M (or G).

Remark. $\langle S\rangle$ is a submonoid (or subgroup) of M.

The **Definition 20** tells us that the submonoid generated by S is the smallest submonoid of M that contains S.

Proposition 4. Given $S \subseteq M$. Obtain $\langle S\rangle$ from the **Definition 20**, $\langle S\rangle'$ from the **Definition 21**, $\langle S\rangle = \langle S\rangle'$.

1.6 Cyclic group

Definition 21 (Cyclic group; Order of element). Let G be a group and $a \in G$. The *cyclic group with generator* a is $\langle a \rangle$. The *order of* a, denoted by $o(a)$, is the order of $\langle a \rangle$.

Remark. Cyclic groups are Abelian.

Lemma 2.

1. A cyclic group of order infinite is isomorphic to $\mathbb{Z}$
2. A cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Theorem 2. Any two cyclic groups of the same order are isomorphic.

Theorem 3. Any subgroup of a cyclic group $\langle a \rangle$ is cyclic.

- If the order of $\langle a \rangle$ is infinite, then the order of its non-$\langle \mathbf{1} \rangle$ subgroup is also infinite, moreover, there exists a bijection from $\mathbb{N}$ to the set of subgroups of $\langle a \rangle$.
- If $\langle a \rangle$ is or order r, then the order of every subgroup of $\langle a \rangle$ is a divisor of r, and for every positive divisor q of r, $\langle a \rangle$ has one and only one subgroup of order q.

Corollary. Let $\langle a \rangle$ be a cyclic group of order $r < \infty$, and H is a subgroup of $\langle a \rangle$ of order $q|r$. Then $H = \{b \in \langle a \rangle : b^q = \mathbf{1}\}$.

Definition 22 (Exponent). Let G be a finite group. The *exponent*, $\exp(G)$, of G is the smallest positive integer e such that $\forall x \in G, x^e = \mathbf{1}$.

Lemma 3. Let g and h be elements of an Abelian group G having finite relatively prime orders m and n respectively (that is, $\gcd(m, n) = 1$). Then $o(gh) = mn$.

Lemma 4. Let G be an Abelian group with finite number of generators (or called *finitely generated abelian group*), $g \in G$ of maximal order. Then $\exp(G) = o(g)$.

Theorem 4. Let G be an finitely generated abelian group. Then G is cyclic if and only if $\exp(G) = |G|$.

1.7 Cycle and Alternating group

Definition 23 (r-cycle)**.** An r-*cycle*, is a permutation of γ of $\{1, 2, \cdots, n\}$ such that permutes a sequence of r elements $i_1, i_2, \cdots, i_r \in \{1, 2, \cdots, n\}$ cyclically in the sense that:

$$\gamma(i_1) = i_2, \quad \gamma(i_2) = i_3, \cdots, \gamma(r_{r-1}) = i_r, \quad \gamma(i_r) = i_1$$

and leaves order elements unchange.
We denote it as $(i_1 i_2 \cdots i_r)$, and the *length* of it is r.

Definition 24 (Disjoint)**.** Two cycles γ, γ' are said to be *disjoint* if their symbols contains no common letters.

Proposition 5. An r-cycle γ is of order r.

Proposition 6. Two disjoint cycles commute under function composition.

Proposition 7. Let α be a product of disjoint cycles, that is

$$\alpha = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots (l_1 l_2 \cdots l_u)$$

Let $m = \operatorname{lcm}(r, s, \cdots, u)$. Then m is the order of α.

Proposition 8. Every permutation of $\{1, 2, \cdots, n\}$ can be factored as a product of disjoint cycles. Apart from the commutation of these disjoint cycles, this factorization is unique.

Definition 25 (Transposition)**.** A 2-cycle is called a *transposition*.

Remark. An r-cycle, $(i_1 i_2 \cdots i_n) = (i_1 i_r) \cdots (i_1 i_3)(i_1 i_2)$, is a product of $r - 1$ transpositions.

Definition 26 (Sign of permutation)**.** Let σ be a permutation, and $C_1 \cdots C_r$ a product of disjoint cycles that factor σ. Let the length of C_i be l_i. Then the *sign* of σ is

$$\operatorname{sign}(\sigma) = (-1)^{(l_1 - 1) + (l_2 - 1) + \cdots + (l_r - 1)}$$

We say σ is even if $\operatorname{sign}(\sigma) = 1$ and odd if $\operatorname{sign}(\sigma) = -1$.

Lemma 5. Let (ab) be a transposition, and $(ac_1 \cdots c_h b d_1 \cdots d_k)$ be a $(h + k + 2)$-cycle. Then

$$(ab)(ac_1 \cdots c_h b d_1 \cdots d_k) = (b d_1 \cdots d_k)(a c_1 \cdots c_h)$$

and

$$(ab)(bd_1\cdots d_k)(ac_1\cdots c_h) = (ac_1\cdots c_h bd_1\cdots d_k)$$

Proposition 9. Let σ_1, σ_2 be permutations, then

$$\operatorname{sign}(\sigma_1\sigma_2) = \operatorname{sign}(\sigma_1)\operatorname{sign}(\sigma_2)$$

Corollary. If $\sigma \in S_n$ is a product of k transpositions, then $\operatorname{sign}(\sigma) = (-1)^k$

Proposition 10. Let σ be a permutation. Let $\tau_1\cdots\tau_k$ and $\tau_1'\cdots\tau_l'$ be two factorizations of σ for which $\tau_1,\cdots,\tau_k,\tau_1',\cdots,\tau_l'$ are transpositions. Then $l \equiv k \pmod 2$.

Corollary. Even permutations form a subgroup of S_n (symmetric group of $\{1,2,\cdots,n\}$). We call this subgroup the *alternating group of degree n* and is denoted by A_n.

Remark. $|A_n| = \frac{n!}{2}$

1.8 Lagrange's theorem

Let G be a group, $H \subseteq G$ be a subgroup, $g_1, g_2 \in G$. We define $g_1 \sim g_2$ if

$$\exists h \in H \text{ s.t. } g_2 = g_1 h$$

Remark. $\sim$ is an equivalence relation on G.

Definition 27 (Left coset)**.** Equivalence classes for $\sim$ are called *left cosets* of H in G. The *left coset containing* g is

$$gH = \{gh : h \in H\}$$

The set of left cosets of H in G is denoted by G/H.
The order of G/H is denoted by $[G : H]$, called the *index of* H *in* G.

Lemma 6. Every coset gH has $|H|$ elements.

Theorem 5 (LAGRANGE'S THEOREM)**.** Let G be a finite group, $H \subseteq G$ be a subgroup. Then

$$|G| = |H|\,[G : H] \tag{1.1}$$

in particular, $|H|$ divides $|G|$.

Corollary. Let G be a group, $g \in G$, take $H = \langle g \rangle$, then $|H|$ divides $|G|$.
If $|G|$ is prime, then $|H| = 1$ or $|G|$. If $|H| = |G|$, then $H = G$ and G is cyclic.

Corollary. G is finite, $g \in G$, then $g^{|G|} = 1$.

1.9 Normalizer

We want to define multiplication on coset, such that $g_1H \cdot g_2H$ is well-defined.

Definition 28 (Normal)**.** Let G be a group, and $H \subseteq G$ be a subgroup. Then H is *normal* if $\forall g \in G$, $gHg^{-1} = H$.

Proposition 11. If H is normal in G, then $\forall g \in G$, $gH = Hg$.

Proof. $\forall h \in H$, $ghg^{-1} = h_1 \in H \Leftrightarrow gh_1 = h_1g$ for some $h_1 \in H$, which implies $gH \subset Hg$. □

This lead to an equivalent definition of *normal*.

Definition 29 (Normal)**.** Let G be a group, and $H \subseteq G$ be a subgroup. Then H is *normal* if $\forall g \in G$, $gH = Hg$.

Note.

- $gH \subseteq G$ is a subset
- $gH \in G/H$ is an element

1.10 Group Action

1.10.1 Group Action

Definition 30 (Group Action)**.** Let G be a finite group and X be a finite set.
An *action of G on X* is a homomorphism:

$$\varphi : G \to \text{ group of permutation of } X$$

Definition 31 (Conjugation)**.** Let $X = G$, a conjugation of X by $g \in G$ is:

$$\varphi(g) : X \mapsto gXg^{-1}$$

Corollary. Conjugation is a group action.

Remark. Consider conjugation action φ,

1. $\text{kernel}(\varphi) = \{g \in G : \forall x \in X, gxg^{-1} = x\}$.
2. $\text{kernel}(\varphi) = Z(G)$
3. $\text{kernel}(\varphi) = G \Leftrightarrow G$ Abelian.

Observe. Once we have the definition of group action, we can ask two questions:

1. What other states in S are reachable from s? (orbits)
2. What are the group elements in G does not move s? (stabilizer)

1.10.2 Orbit

Definition 32. Consider G, X, φ
Define $x \sim y$ to be the relation satisfying:

1. $x, y \in X$
2. $\exists g \in G$ with $\varphi(g)x = y$

Intuition. $x \sim y$ iff there is a $g \in G$ that moves x to y, or there exists a permutation in the image $\varphi(G)$ containing a cycle $(\cdots xy \cdots)$.

Corollary. The above relation is an equivalent relation.

Proof. The symmetry and transitivity relies on the fact that φ is homomorphism.
Whole proof omitted. □

Definition 33 (orbit)**.** The orbit of $x \in X$ is $[x]$.

Remark. $X = \bigsqcup$ orbits.

Example. $X = G$, consider the action: $\varphi : x \mapsto gx$, the only one orbit is X itself, because $\forall x, y \in X$, let $g = yx^{-1}$, clearly $gx = y$.

Definition 34 (Transitive action)**.** Actions with only 1 orbit are called to be transitive.

Remark. Action $\varphi : x \mapsto gx$ is transitive.

Observe. Given a transitive action, we can get from any $x \in X$ to any $y \in X$.

Remark. Action $\varphi : x \mapsto gxg^{-1}$ is **not** transitive.

Example. Give G is Abelian, and the conjugation action φ,

$$x \sim y \Leftrightarrow \exists g \in G \text{ s.t. } gxg^{-1} = y \Leftrightarrow x = y$$

Therefore, the orbits are one element set.

Proposition 12. Consider conjugation action, if G is non-Abelian, then $x \sim y \Rightarrow o(x) = o(y)$.

Observe. Every orbit under conjugation action consist elements of the same order, which means that we can get at least one orbit for elements of the same order. (In general, the order of elements is not enough to specify orbits)

Definition 35 (Conjugacy class)**.** The orbit under conjugation action $[x] = \{gxg^{-1} : g \in G\}$ is the conjugacy class.

Example. Let $H \subseteq G$, $X = G$, and H acts on X by translation: $\varphi : x \mapsto hx$, then the right coset $Hx = \{hx : h \in H\}$ is an orbit of x. Intuitively, G breaks into orbits, and each coset is an orbit.

Example. Let $H < G$, $X = G/H$ (Quotient group), and G acts on X by $\varphi : xH \mapsto g(xH)$, this action is **transitive** because that $\forall xH, yH \in X$, let $g = yx^{-1}$, clearly $g(xH) = gxH = yH$.

1.10.3 Stabilizer

Definition 36 (Stabilizer)**.** Consider group action G on X, the *stabilizer of* $x \in X$ *under* G is

$$\operatorname{stab}_G(x) = \{g \in G : gx = x\}$$

Proposition 13. $\operatorname{stab}_G(x)$ is a subgroup of G.

Remark. Consider G acting on G by conjugation, $\operatorname{stab}_G(x) = \{g \in G : gxg^{-1} = x\} = C_G(x)$

Proposition 14. Consider G acts transitively on X, then $\exists g \in G$ s.t. $gx = y$, and $\forall x, y \in X$,

$$\operatorname{stab}_G(y) = g \cdot \operatorname{stab}_G(x) \cdot g^{-1}$$

1.10.4 Equivalent of group actions

Definition 37 (Equivalent of group actions)**.** Let $\varphi : G \to S_X$ ad $\phi : G \to S_Y$.
X is *equivalent* to Y as a set with action of G if there exists a bijection $f : X \to Y$ such that

$$\forall x \in X, f(\varphi(g)x) = \phi(g)(f(x))$$

Intuition.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi(g)"'] & Y \arrow[d, "\phi(g)"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

Theorem 6. If G acts on X transitively, then $\exists H < G$ such that X is **equivalent** to G/H as sets with action of G.

Proof. Construction of H from X: pick $x \in X$, let $H = \{g \in G : gx = x\}$, which by definition means $H = \operatorname{stab}_G(x)$. We want to prove X is equivalent to G/H:
Consider $f : gH \mapsto gx$ □

Intuition.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi(g)"'] & G/H \arrow[d, "\phi(g)"] \\ X \arrow[r, "f"] & G/H \end{tikzcd}$$

Corollary. $|X| = |G/H| = [G : H] \Rightarrow |X|\,\big|\,|G|$

Corollary. $|\operatorname{orbit}(x)| = [x] = |G/\operatorname{stab}_G(x)| = [G : \operatorname{stab}_G(x)]$

Corollary. Consider G acts on X, and the set of orbits under this action is $\{X_i\}$, then

$$|X| = \sum_i |X_i| = \sum_i |G/H_i|$$

Observe.

Proposition 15. Let G be a finite group, and $|G| = p^r$ where p is a prime and $r \geq 1$, then $Z(G) \neq \{1\}$.

Corollary. Suppose $|G| = p^2$, then G is Abelian.

Definition 38 (polynomial).

$$
\begin{aligned}
f(x) &= a_n x^n + \cdots + a_0 \\
f(x) &= \Pi(x - \alpha_i)
\end{aligned}
$$

(in $\mathbb{C}$)