A second year mathematics degree

Yu Coughlin

Contents

Real Analysis and Topology

Lectured by Someone
Typed by Yu Coughlin
Season Year

Introduction

The following are complementary reading for the course.

- G. Grimmett and D. J. A. Welsh, Probability: An Introduction, 1986
- J. K. Blitzstein and J. Hwang, Introduction to Probability, 2019
- D. F. Anderson et al, Introduction to Probability, 2018
- S. M. Ross, Introduction to Pro ability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

Notation. Unbracketed superscripts are used to label the components of vectors, with unbracketed subscripts labellin different vectors.

Lecture 1
Monday
30/10/2023

1 Euclidean spaces

Definition 1.0.1 ($\mathbb{R}^n$)**.** The set $\mathbb{R}^n = \{(x^1, x^2, \ldots, x^n) : x^i \in \mathbb{R},\ \forall i \in [1,n]\}$ will be considered with the operations to make it a real vector space.

1.1 Euclidean norm

Definition 1.1.1 (Inner product)**.** We will have the **inner product** on $\mathbb{R}^n$ by $\langle \cdot, \cdot \rangle : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ satisfying:

$$\langle x, y \rangle := \sum_{i=1}^{n} x^i y^i,$$

with the **Euclidean norm** given by,

$$||\cdot|| : \mathbb{R}^n \to [0, \infty) \text{ with } ||x|| = \sqrt{\langle x, x \rangle}.$$

Proposition 1.1.2 (Properties of the Euclidean norm)**.** The Euclidean norm satisfies the following properties:

(N1) for all $x \in \mathbb{R}^n$, $||x|| \geq 0$ achieving equality iff $x = 0$,

(N2) for all $x \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$, $||\lambda x|| = |\lambda| \cdot ||x||$,

(N3) for all $x, y \in \mathbb{R}^n$: $||x + y|| \leq ||x|| + ||y||$,

Theorem 1.1.3 (Cauchy-Swartz innequality)**.** For all $x, y \in \mathbb{R}^n$, $|\langle x, y \rangle| \leq ||x|| \cdot ||y||$.

Theorem 1.1.4 (Reverse triangle innequality)**.** For all $x, y \in \mathbb{R}^n$, $\big|\, ||x|| - ||y|| \,\big| \leq ||x - y||$.

Proposition 1.1.5. For $x = (x^1, x^2, \ldots, x^n) \in \mathbb{R}^n$,

$$\max_{k \in [1,n]} \left|x^k\right| \leq ||x|| \leq \sqrt{n} \max_{k \in [1,n]} \left|x^k\right|.$$

Proof. Exercise □

1.2 Convergence in $\mathbb{R}^n$

Definition 1.2.1 (Open ball)**.** In $\mathbb{R}^n$ we define the **open ball** around $x \in \mathbb{R}^n$ of size $r \in \mathbb{R}$ as

$$B_r(x) := \{y \in \mathbb{R}^n : ||x - y|| < r\}.$$

This will be analoguous the the notion of open intervals used throughout analysis 1.

Definition 1.2.2 (Sequence in $\mathbb{R}^n$)**.** A **sequence** in $\mathbb{R}^n$ is an ordered list $x_0, x_1, \ldots, x_i \ldots$ with $x_i \in \mathbb{R}^n$ for all $i \in \mathbb{N}$, written $(x_i)_{i=0}^{\infty}$

Definition 1.2.3 (Convergence in $\mathbb{R}^n$)**.** We say a sequence in $\mathbb{R}^n$, $(x_i)_{i=0}^{\infty}$ **converges to** $x \in \mathbb{R}^n$ iff

$$\forall \epsilon > 0\ \exists N \in \mathbb{N} \text{ such that, } \forall n \geq N,\ ||x_i - x|| < \epsilon$$

and we write $x_i \to x$ as $i \to \infty$ or $\lim_{i \to \infty} x_i = x$.

Lemma 1.2.4. The sequence of vectors in $\mathbb{R}^n$, $(x_i)_{i=0}^{\infty}$, converges to some $x = (x^1, x^2, \ldots, x^n) \in \mathbb{R}^n$ iff each componenet of x_i converges to the corresponding component in x:

$$\forall k \in [1,n]\ \lim_{i \to \infty} x_i^k = x^k.$$

Proof. ($\implies$) Given $\lim_{i \to \infty} x_i^k = x^k$ for all $k \in [1,n]$ we have that for all $\epsilon > 0$, $\left|x_i^k - x^k\right| < \frac{\epsilon}{\sqrt{n}}$ for all $i \geq N_k$ for each $k \in [1,n]$ respectively. We take $N = \max_{k \in [1,n]} N_k$ and now have:

$$\max_{k \in [1,n]} \left|x_i^k - x^k\right| < \frac{\epsilon}{\sqrt{n}} \implies ||x_i - x|| \leq \sqrt{n} \max_{k \in [1,n]} \left|x_i^k - x^k\right| < \epsilon.$$

($\impliedby$) Similarly, given $\lim_{i \to \infty} x_i = x \implies ||x_i - x|| < \epsilon$ for all $\epsilon > 0$:

$$\left|x_i^k - x^k\right| \leq \max_{k \in [1,n]} \left|x_i^k - x^k\right| \leq ||x_i - x|| < \epsilon,$$

therefore $\lim_{i \to \infty} x_i^k = x^k$ for all $k \in [1,n]$. □

2 Continuity and limits of functions

2.1 Open sets

Definition 2.1.1 (Open set in $\mathbb{R}^n$)**.** A subset $U \subseteq \mathbb{R}^n$ is **open** in $\mathbb{R}^n$ iff:

$$\forall x \in U,\ \exists r > 0 \text{ such that } B_r(x) \subseteq U.$$

2.2 Continuity

Definition 2.2.1 (Continuity)**.** Let $A \subseteq \mathbb{R}^n$ the we have $f : A \to \mathbb{R}^m$ **continuous at** some $p \in A$ iff

$$\forall \epsilon > 0,\ \exists \delta > 0 \text{ such that } \forall x \in A \text{ with } ||x - p|| < \delta,\ ||f(x) - f(p)|| < \epsilon.$$

If f is continuous at all $p \in A$ we say f is **continuous on** A.

Theorem 2.2.2. Let $A \subseteq \mathbb{R}^n$ and $B \subseteq \mathbb{R}^m$ with $f : A \to B$ continuous at $p \in A$. Suppose $g : B \to \mathbb{R}^l$ is continuous as $f(p)$, then $g \circ f : A \to \mathbb{R}^l$ is cotninuous at p.

Proof. Given any $\epsilon > 0$ have $||x-p|| < \delta_f \circ \delta_g(\epsilon) \implies ||f(x)-f(p)|| < \delta_g(\epsilon) \implies ||g \circ f(x) - g \circ f(p)|| < \epsilon$. □

3 Derivative of maps of Euclidean spaces

3.1 Total derivatives

Definition 3.1.1 (Total derivate)**.** Given open $\Omega \subset \mathbb{R}^n$, the function $f : \Omega \to \mathbb{R}^m$ is **differentiable as** $p \in \Omega$ iff there is a linear linear map $\Lambda : \mathbb{R}^n \to \mathbb{R}^m$ satisfying:

$$\lim_{x \to p} \frac{||f(x) - f(p) - \Lambda(x - p)||}{||x - p||} = 0.$$

Have $Df(p) := \Lambda$ be the **total derivative** of f at p.

Remark 3.1.2. Given $f : (a, b) \to \mathbb{R}$ differentiable at $p \in (a, b)$, we have

$$\lim_{x \to p} \frac{||f(x) - f(p) - \Lambda(x - p)||}{||x - p||} = \lim_{x \to p} \frac{|f(x) - f(p) - \lambda \cdot (x - p)|}{|x - p|} = \lim_{x \to p} \left| \frac{f(x) - f(p)}{x - p} - \lambda \right| = 0$$
$$\implies \lim_{x \to p} \left| \frac{f(x) - f(p)}{x - p} \right| = \lambda, \text{ which satisfies the normal definition for a derivative.}$$

Theorem 3.1.3 (Uniqueness of total derivatve)**.** If the total derivative of a function $f : \Omega \subseteq \mathbb{R}^n \to \mathbb{R}^m$ exists, then it is unique.

Proof. □

Theorem 3.1.4 (Chain rule)**.** Let $\Omega \subset \mathbb{R}^n$, $\Omega' \subset \mathbb{R}^m$ be open and have $g : \Omega \to \Omega'$, $f : \Omega' \to \mathbb{R}^l$ differentiable at $p, g(p)$ respectively and let $h := f \circ g$, $Dh(p) = Df(g(p)) \circ Dg(p)$.

Proof. □

3.2 Directional and partial derivatives

Definition 3.2.1 (Direction derivative)**.** Suppose $\Omega \subseteq \mathbb{R}^n$ is open with $f : \Omega \to \mathbb{R}^m$ differentiable at $p \in \Omega$. For all $v \in \mathbb{R}^n$ the **directional derivative** of f at p in the direction of v is:

$$\frac{\partial f}{\partial v}(p) := \lim_{t \to 0} \frac{f(p + tv) - f(p)}{t} = Df(p)[v].$$

With the partial derivatives of f given by:

$$D_i f(p) := \frac{\partial f}{\partial e_i}(p), \text{ for all } i \in [1, n].$$

Remark 3.2.2. If the total derivative of a function exists, then so do all of its directional derivatives.

Theorem 3.2.3. If $\Omega \subset \mathbb{R}^n$ is open with $f : \Omega \to \mathbb{R}$ with all partial derivatives existing for all $x \in \Omega$. If the map $x \mapsto D_i f(x)$ is continuous at $p \in \Omega$ for all partial derivatives, then f is differentiable at p.

Proof. □

3.3 Higher order derivatives

Definition 3.3.1 (Second order partial derivatives)**.** Let $\Omega \subset \mathbb{R}^n$ be open with differentiable $f : \Omega \to \mathbb{R}$ written as $(f^1, f^2, \ldots, f^n)^{\mathrm{T}}$, the ik**th second partial derivative** at p is

$$D_k D_i f^j(p) := \lim_{t \to 0} \frac{D_i f^j(p + te_k) - D_i f^j(p)}{t}.$$

This can naturally be extended to nth order partial derivatives.

Theorem 3.3.2. Given open $\Omega \subseteq \mathbb{R}^n$ and $f : \Omega \to \mathbb{R}^m$ differentiable on Ω, consider the map:

$$\begin{array}{cccll} Df & : & \Omega & \longrightarrow & \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m) \cong M_{n\times m}(\mathbb{R}) \cong \mathbb{R}^{m\times n} \\ & & p & \longmapsto & Df(p) \end{array},$$

which we can now show to be continuous or differentiable at $p \in \Omega$, when differentiable we can take $DDf(p) \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$. The componenents of the corresponding matrix are give by:

$$[DDf(p)[h]]_{ij} = \sum_{k=1}^{n} D_k D_i f^j(p) h^k.$$

Proof. □

Remark 3.3.3. The condition of a function being k times differentiable at a point p can is often difficult to establish, instead the continuous existence of all $k - th$ partial derivatives in a neighbourhood of p is a prefereable question which implies the former statement.

Theorem 3.3.4 (Schwartz's theorem)**.** Suppose $\Omega \subseteq \mathbb{R}^n$ is open and $f : \Omega \to \mathbb{R}^m$ is differentiable on Ω with $D_i D_j f(p), D_j D_i f(p)$ both exist continuous only Ω; then we have

$$D_i D_j f(p) = D_j D_i f(p) \text{ for all } p \in \Omega.$$

Proof. □

Notation 3.3.5. We need the following necessary notation around an n-vector of non-negative integers, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in (\mathbb{Z}_{>0})^n$ for some $n \in \mathbb{Z}_{>0}$, to easily express Taylor's theorem in multiple dimensions:

1. $|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n$,
2. $D^\alpha f = (D_1)^{\alpha_1} (D_2)^{\alpha_2} \cdots (D_n)^{\alpha_n}$,
3. for some vector $h = (h^1, h^2, \ldots, h^n) \in \mathbb{R}^n$, $h^\alpha = ((h^1)^{\alpha_1}, (h^2)^{\alpha_2}, \ldots, (h^n)^{\alpha_n})$,
4. $\alpha! = \alpha_1! \alpha_2! \cdots \alpha_n!$.

Theorem 3.3.6 (Taylor's theorem)**.** Given $p \in \mathbb{R}^n$ with $f : B_r(p) \to \mathbb{R}$, for some $r > 0$, k-times continuous differentiable on $B_r(p)$ and some $||h|| < r$; we have:

$$f(p + h) = \sum_{|\alpha| \le k-1} \frac{h^\alpha}{\alpha!} D^\alpha f(p) + R_k(p, h).$$

Where the remainder term, $R_k(p, h)$ is given by:

$$R_k(p, h) = \sum_{|\alpha| = k} \frac{h^\alpha}{\alpha!} D^\alpha f(x).$$

Proof. □

4 Inverse and implicit function theorems

4.1 Inverse function theorem

Theorem 4.1.1 (Inverse function theorem)**.** Have $f : \mathbb{R}^n \to \mathbb{R}^n$ continuous differentiable on $\Omega \subseteq \mathbb{R}^n$ and $Df(p)$ be invertible for a $p \in \Omega$. There exists open sets $U \in \Omega$ and $V \in \mathbb{R}^n$ such that $f : U \to V$ is a bijection. Furthermore, $f^{-1} : V \to U$ is continuous differentiable on V with:

$$Df^{-1}(y) = \left[Df(f^{-1}(y))\right]^{-1}.$$

Lemma 4.1.2. Have $B_r(p) \subset \mathbb{R}^n$ with $f : B_r(p) \to \mathbb{R}^n$ contoniously differntiable. If there exists some $M \in \mathbb{R}_{>0}$ with $|D_j f^i(x)| < M$ for all $x \in B_r(p)$ then

$$||f(x) - f(y)|| \leq nM||x - y||, \text{ for all } x, y \in B_r(p).$$

Proof. □

Lemma 4.1.3.

Lemma 4.1.4.

Lemma 4.1.5.

Proof of Theorem 4.1.1(Inverse function theorem). □

4.2 Implicit function theorem

Theorem 4.2.1 (Implicit function theorem)**.** Given $\Omega \subseteq \mathbb{R}^n$ and $\Omega' \subseteq \mathbb{R}^m$ both open with $f : \Omega \times \Omega' \to \mathbb{R}^m$ continuous differentiable on $\Omega \times \Omega'$. If there is some $p \in \Omega \times \Omega'$ with $f(p) = 0$ and $D_{n+j} f^i(p)$ invertible for $1 \leq i, j \leq m$. Then, there are open sets $A \in \Omega$ and $B \in \Omega'$ containg a and b respectively such that for all $x \in A$ ther is a unique and differentiable $g(x) \in B$ with $f(x, g(x)) = 0$.

Proof. □

5 Metric spaces

5.1 Introduction

Definition 5.1.1 (Metric)**.** A **metric** on some arbitrary set X is a function:

$$d : X \times X \to \mathbb{R}$$

that satisfies the following properties for all $x, y, z \in X$:

(M1) $d(x, y) \geq 0$ with $d(x, y) = 0$ iff $x = y$ (positibity),

(M2) $d(x, y) = d(y, x)$ (symmetry),

(M3) $d(x, y) \leq d(x, z) + d(z, y)$ (triangle innequality).

Definition 5.1.2 (Metric space)**.** A **metric space** is a pair consisting of a set and a metric on said set, often denoted $M = (X, d)$. The elements of X are called **points** and for any two points of M, x, y, their **distance (with respect to** d**)** is $d(x, y)$.

Examples 5.1.3. The following are common examples of metric spaces:

1. have $X = \mathbb{R}$ and $d_1 : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by $d_1(x, y) := |x - y|$,
2. have $X = \mathbb{R}^n$ and have $d(x, y) := \sqrt{\sum_{i=1}^{n} (x^i - y^i)^2}$,
3. for an arbitary non-empty set X we have $d_{\text{disc}} : X \times X \to \mathbb{R}$ by $d_{\text{disc}}(x, y) := 0$ iff $x = y$ and 1 otherwise (discrete metric),

4. have X be the set of bounded real sequences, then we can have $d_\infty : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ given by $d_\infty(x, y) := \sup_{k \geq 1} |x^k - y^k|$,
5. let X be the set of continuous real functions on $[a, b]$ with $d(f, g) := \int_{t=a}^{b} |f(t) - g(t)| \, \mathrm{d}t$.

Definition 5.1.4 (Induced metric)**.** Given the metric space (X, d) and some $Y \subset X$, we have $d_Y : Y \times Y \to \mathbb{R}$ with $d_Y(x, y) = d(x, y)$ for all $x, y \in Y$ as the **induced metric** on Y. (Y, d_Y) is a **metric subspace** of (X, d).

5.2 Normed vector spaces

Definition 5.2.1 (Normed vector spaces)**.** Given a real-vector space V, a function $|| \cdots || : V \to \mathbb{R}$ is a **norm** on V iff the following hold for all $u, v \in V$:

(N1) $||v|| \geq 0$ with $||v|| = 0$ iff $v = 0_V$,

(N2) for all $\lambda \in \mathbb{R}$, $||\lambda v|| = |\lambda| \cdot ||v||$,

(N3) $||u + v|| \leq ||u|| + ||v||$.

A vector space together with a norm is a **normed vector space**.

Lemma 5.2.2. If $(V, || \cdot ||)$ is a normed vector space, $d_{||\cdot||} : V \times V \to \mathbb{R}$ with $d_{||\cdot||}(u, v) = ||u - v||$ is a metric on V.

Proof. □

5.3 Open and closed sets

Definition 5.3.1 (ϵ-ball)**.** Given a point x in the metric space (X, d) and a real $\epsilon > 0$, the **ball** of radius ϵ centred at x is the set,

$$B_\epsilon(x) := \{y \in X : d(x, y) < \epsilon\},$$

which is sometimes referred to as a neighbourhood of x.

Definition 5.3.2 (Open sets)**.** Given metric space (X, d) a set $U \subseteq X$ is **open** in (X, d) iff, for all $\mathrm{u} \in U$ there exists some $\delta > 0$ such that $B_\delta(u) \subseteq U$.

Proposition 5.3.3. Have $\mathcal{X} = (X, d)$ a metric space, the follow hold true:

1. $\emptyset$ and $\mathcal{X}$ are open in $\mathcal{X}$,
2. for all $x \in \mathcal{X}$ and $\epsilon > 0$, $B_\epsilon(x)$ is open in $\mathcal{X}$,
3. the union of (up to uncountably many) open sets in $\mathcal{X}$ are open in $\mathcal{X}$,
4. the intersection of finitely many open sets in $\mathcal{X}$ is open in $\mathcal{X}$.

Proof. □

Definition 5.3.4 (Topological equivalence)**.** Two metrics d, d' on X are **topologically equivalent** iff $U \subseteq X$ is open in (X, d) iff it is also open in (X, d').

Definition 5.3.5 (Closed sets)**.** Given the metric space (X, d) with $U \subseteq X$, U is **closed** iff $X \setminus U$ is open.

Proposition 5.3.6. A set $U \subseteq X$ with (X, d) a metric spacpe is closed iff, every convergenct sequence in V has a limit in V.

Proof. □

Proposition 5.3.7. The intersection of (up to ocuntable many) closed sets in a metric space is closed; the union of finitely many sets in a metric space is closed.

Proof. □

5.4 Separable space

Definition 5.4.1 (Interior, isolated, limits and boundary points)**.** We will have (X, d) be a metric space with $V \subseteq X$ and $x \in X$:

- x is an **interor point** of V if there is some $\delta > 0$ with $B_\delta(x) \subseteq V$,
- x is an **isolated point** of V if there is some $\delta > 0$ such that $V \cap B_\delta(x) = \{x\}$,
- x is a **limit point** of V if for all $\delta > 0$, we have $(B_\delta(x) \cap V) \setminus \{x\} \neq \emptyset$,
- x is a **boundary point** of V if it is a limit point, under the previous definition, and $B_\delta(x) \setminus V \neq \emptyset$.

Remark 5.4.2. Interior and isolated points are necessarily in V, but limit points and boundary points need not be elements of V.

Definition 5.4.3 (Interior, closure and boundary)**.** Once again, we will have (X, d) a metric space with $V \subseteq X$:

- the **interior** of V is the set of all $v \in V$ with v an interior point of V, denoted V°,
- the **closure** of V is the union of V with the set of limit points of V, denoted $\overline{V}$,
- the **boundary** of V is the set of boundary points of V, denoted ∂V.

Proposition 5.4.4. $\partial V = \overline{V} \setminus V^\circ$.

Proof. □

Definition 5.4.5 (Dense set)**.** Have (X, d) a metric space, $V \subseteq X$ is **dense** in (X, d) iff $\overline{V} = X$.

Definition 5.4.6 (Separable space)**.** We say the metric space (X, d) is **separable** if there is a countable, dense set in X.

6 Continuous maps in metric spaces

6.1 Convergence

Definition 6.1.1 (Convergence in metric spaces)**.** Let $(x_n)_{n\geq 1}$ be a sequence in the metric space (X, d). We say $(x_n)_{n\geq 1}$ **converges** in (X, d) iff:

$$\exists x \in X \text{ such that, } \forall \epsilon > 0,\ \exists N \in \mathbb{Z}_{>0} \text{ with } d(x_n, x) < \epsilon \text{ for all } n \geq N.$$

And we say $(x_n)_{x\geq 1}$ converges to x in (X, d), or any other equivalent phrasing from analysis.

Definition 6.1.2 (Cauchy sequences)**.** A sequence $(x_n)_{n\geq 1}$ is **Cauchy** in (X, d) iff

$$\forall \epsilon > 0,\ \exists N \in \mathbb{Z}_{>0} \text{ such that } \forall n, m \geq N,\ d(x_n, x_m) < \epsilon.$$

Lemma 6.1.3 (Uniqueness of limits)**.** If the sequence $(x_n)_{n\geq 1}$ converges to some x in the metric space (X, d) then this limit is unique.

Proof. □

Theorem 6.1.4. Given two topologically equivalent metrics d, d' on X, the sequence $(x_n)_{n\geq 1}$ converges in (X, d) iff it also converges in (X, d').

Proof. □

6.2 Continuity of maps

Definition 6.2.1 (Continuous map)**.** Given the metric spaces $(X, d_X), (Y, d_Y)$ and $f : X \to Y$:

1. f is **continuous at** $x \in X$ iff for all $x' \in X$:
$$\forall \epsilon > 0, \exists \delta > 0 \text{ such that } d_X(x, x') < \delta \implies d_X(f(x), f(x')) < \epsilon,$$
2. f is **continuous on** $U \subseteq X$ if f is continuous at every $u \in U$,
3. f is **uniformly continuous** on $U \subseteq X$ is f is continuous on U and $\delta = \delta(\epsilon)$ does not depend on x.

Theorem 6.2.2. Let $(X, d_X), (Y, d_Y)$ be metric spaces, a function $f : X \to Y$ is continuous iff the pre-image of any open $U \subseteq Y$ is open in X.

Proof. □

Proposition 6.2.3. If, similarly, $(X, d_X), (Y, d_Y)$ are metric spaces with $f : X \to Y$, the following are equivalent:

1. f is continuous at $x \in X$,
2. if a sequence $(x_n)_{n\geq 1}$ converges to $x \in X$ then $(f(x_n))_{n\geq 1}$ converges to $f(x) \in Y$.

Proof. □

6.3 Metric homeomorphisms

Definition 6.3.1 (Homeomorphism)**.** Have $(X, d_X), (Y, d_Y)$ be metric spaces, a mapping $f : X \to Y$ is a **homeomorphism** if it is a bijection with f, f^{-1} both continuous. Metric spaces with homeomorphisms between then are **homeomorphic**.

Definition 6.3.2 (Lipschitz)**.** Given metric spaces $(X, d_X), (Y, d_Y)$ and $f : X \to Y$ we say:

1. f is **Lipschitz** if there is some $M > 0$ with:
$$d_Y(f(x_1), f(x_2)) \leq M \cdot d_X(x_1, x_2) \text{ for all } x_1, x_2 \in X,$$
2. f is **bi-Lipschitz** if there is some $M_1, M_2 > 0$ with:
$$M_1 \cdot d_X(x_1, x_2) \leq d_Y(f(x_1), f(x_2)) \leq M_2 \cdot d_X(x_1, x_2) \text{ for all } x_1, x_2 \in X,$$
3. f is **isometric** if,
$$d_Y(f(x_1), f(x_2)) = d_X(x_1, x_2) \text{ for all } x_1, x_2 \in X.$$

Remark 6.3.3. An isometry between metric spaces is a bi-Lipschitz map with two unit constants.

7 Topological spaces

7.1 Topologies and their spaces

Definition 7.1.1 (Topology)**.** Given a non-emtpy set X, we say τ, a collection of subsets of X, is a **topology** on X if it satisfies the following conditions:

(T1) $\emptyset, X \subseteq \tau$,

(T2) if $X_i \in \tau$ for all i in a indexing set $\mathcal{I}$, $\bigcup_{i \in \mathcal{I}} X_i \in \tau$,

(T3) if $X_1, X_2, \ldots, X_n \in \tau$, $\bigcap_{i=1}^{m} X_i \in \tau$.

The pair (X, τ) is called a **topological space** with elements of X called **points** and elements of τ called open sets. If $x \in X$ and $x \in U \in \tau$, U is a neighbourhood of x.

Examples 7.1.2. These are some common examples of topological spaces:

1. for any set X have $\tau = \{\emptyset, X\}$, the trivial topology on X,

2. instead have τ be the collection of subsets of X, the discrete topology on X,
3. if (X, d) is a metric space, $\tau := \{U \subseteq X : U \text{ is open in } (X, d)\}$ the metric topology on X,
4. for a non-empty set X, $\tau = \{\emptyset, V, X\}$ for some non-empty $V \subset X$,
5. if $X = \{a, b\}$ and $\tau = \{\emptyset, \{a, b\}, \{b\}\}$ is the smallest toplogical space that is neither trivial nor discrete (called the Sierpinski topology).

Definition 7.1.3 (Metrisability)**.** A topological space (X, τ) is **metrisable** iff it is the topology induced by some metric.

Definition 7.1.4 (Coarser and finer topologies)**.** Given two topologies τ_1, τ_2 both on X, we say τ_1 is **coarser** than τ_2, and equivalently τ_2 is **finer** than τ_1, iff $\tau_2 \subseteq \tau_1$.

7.2 Bases

Definition 7.2.1 (Basis)**.** Given a topological space (X, τ) we call a subfamily $B \subseteq \tau$ a **basis** for τ iff every open set in τ is the union of open sets in B.

7.3 Closed sets

Definition 7.3.1 (Closed sets)**.** Given a topological space (X, τ), we say $V \subseteq X$ is **closed** iff $X \setminus V$ is open.

Proposition 7.3.2. Closed sets in any given topological space (X, τ) satisfy the followoing:

(C1) $X, \emptyset$ are closed,

(C2) if C_1, C_2 are closed, $C_1 \cup C_2$ is closed,

(C3) the (up to uncountable) intersection of closed sets is closed.

Proof. □

Definition 7.3.3 (Closure)**.** Given an open set U in the topological space (X, τ) the **closure** of U in (X_τ) is given by:

$$\overline{U} := \bigcap_{\substack{V \subseteq X \\ V \,\text{closed}, A \subseteq V}} V.$$

Definition 7.3.4 (Point of closure)**.** Given the topological space $\mathcal{X}$ with $A \subseteq \mathcal{X}$, $x \in \mathcal{X}$ is a **point of closure** of A iff every open set U with $x \in U$ has $U \cap A = \emptyset$.

Proposition 7.3.5. $\overline{A} = \{x \in X : x \text{ is a point of closure for} A\}$.

Proof. □

7.4 Convergence and Hausdorff property

Definition 7.4.1 (Convergence)**.** For a sequences $(x_n)_{n\geq 1}$ in a topological space (X, τ) we say $(x_n)_{n\geq 1}$ **converges** (in (X, τ)) to $x \in X$ iff

$$\forall T \in \tau \text{ with } x \in T,\ \exists N \in \mathbb{Z}_{>0} \text{ such that } \forall n \geq N,\ x_n \in T.$$

Definition 7.4.2 (Hausdorff)**.** A topological space (X, τ) is **Hausdorff** iff for all $x, y \in X$ with $x \neq y$ there are open sets U, V containing x, y respectively with $U \cap V = \emptyset$. With U and V **separating** x and y.

Theorem 7.4.3. Limits of convergent sequences in Hausdorff spaces are unique.

Proof. □

Definition 7.4.4 (Regular spaces)**.** A topological space (X, τ) is **regular** iff for every closed subset $C \subseteq X$ with point $p \notin C$ there are open sets $U, V \in \tau$ such that $p \in U$, $C \subseteq V$ and $U \cap V = \emptyset$.

7.5 Continuous maps

Definition 7.5.1 (Continuous map)**.** Given two topological spaces $(X, \tau_X), (Y, \tau_Y)$ the map $f : X \to Y$ is **continuous** iff $f^{-1}(U) \in \tau_X$ for all $U \in \tau_Y$.

Definition 7.5.2 (Continuity at points)**.** The map $f : X \to Y$, with $(X, \tau_X), (Y, \tau_Y)$ topological spaces, is **continuous at** $x \in X$ iff $f^{-1}(U) \in \tau_X$ for all $U \in \tau_Y$ with $f(x) \in U$.

Definition 7.5.3 (Homeomorphism)**.** A **homeomorphism** between topolgical spaces is a bijection map, f, where both f and f^{-1} are continuous. Spaces with homeomorphisms between them are **topologically equivalent**.

7.6 Subspaces

Definition 7.6.1 (Subspace)**.** If (X, τ) is a topological space and $A \subseteq X$, the **subspace topology** on A is $\tau_A = \{A \cap U : U \in \tau\}$, (A, τ_A) is a topological space called the **supspace** of (X, τ).

Proof of topological space. □

Proposition 7.6.2 (Universal property)**.** Given topological spaces $(X, \tau_X), (Y, \tau_Y)$ with $A \subseteq X$ with its supspace topology and $g : Y \to A$, g is continuous iff $i \circ g$ is continuous, where i is the inclusion map,

$$\begin{tikzcd} & X \\ Y \arrow[ur, "i \circ g"] \arrow[r, "g"'] & A \arrow[u, hook, "i"'] \end{tikzcd} .$$

Proof. □

Theorem 7.6.3. Given the topological space (X, τ) and $A \subseteq X$, the subspace topology is the only topology such that for all (Y, τ_Y), $g : Y \to A$ is continuous iff $(i \circ g)$ is continuous.

Proof. □

Lemma 7.6.4. If B is a basis for the topological space (X, τ) and $A \subseteq X$, $B_A := \{U \cap A : U \in B\}$ is a basis for τ_A.

Proof. □

Proposition 7.6.5. For a metric space (X, d) with $A \subseteq X$, the two canonical topologies on A, τ_{d_A} and T_A are equal.

Proof. □

8 Connectedness

8.1 Definition

Definition 8.1.1 (Disconnected sets)**.** Let

Chapter 1

Groups and Rings

Lectured by Someone
Typed by Yu Coughlin
Autumn 2024

Introduction

The following are complementary reading for the course.

- G. Grimmett and D. J. A. Welsh, Probability: An Introduction, 1986
- J. K. Blitzstein and J. Hwang, Introduction to Probability, 2019
- D. F. Anderson et al, Introduction to Probability, 2018
- S. M. Ross, Introduction to Pro ability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

1 Quotient groups

1.1 Group homomorphisms

Definition 1.1.1 (Group isomorphism)**.** Given groups G, H, a function $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism. If there exists an isomorphism between groups, G is **isomorphic** to H written $G \cong H$.

Definition 1.1.2 (Group automorphism)**.** Given G a group, an isomorphism $f : G \xrightarrow{\sim} G$ is a **group automorphism**.

Theorem 1.1.3. $\operatorname{Aut} G$ (the set of automorphisms of a group G) is a group under function composition.

Proof. By examining the defintion of $\operatorname{Aut} G$, taking $e = \mathrm{id}$ and showing association elementwise. □

Theorem 1.1.4. Given groups G, H, if $f : G \xrightarrow{\sim} H$ then $f^{-1} : H \xrightarrow{\sim} G$.

Proof. $f^{-1}(f(g_1))f^{-1}(f(g_2)) = g_1g_2 = f^{-1}(f(g_1g_2)) = f^{-1}(f(g_1)g(g_2))$ is sufficient as f is surjective. □

1.2 Normal subgroups

Definition 1.2.1 (Normal subgroup)**.** A sugroup N of G is **normal**, written $N \trianglelefteq G$, if it satisfies any of these equal properties:

(N1) N is the kernel of some group homomorphism ϕ,

(N2) N is stable under conjugations ($\forall n \in N$ and $g \in G$, $gng^{-1} \in N$),

(N3) for all $g \in G$ $gN = Ng$.

Proof of equivalence. (N1 $\implies$ N2): $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_H$.

(N2 $\implies$ N3): $gng^{-1} \in N \implies gn \in Ng$ by g^{-1} so $gN \subseteq Ng$, similarly for $Ng \subseteq gN$ with g^{-1} replacing g.

(N3 $\implies$ N2): The set of left and right cosets of G by N are isomorphic with N as the kernel. □

1.3 Quotient groups

Definition 1.3.1 (Quotient groups)**.** Let $N \trianglelefteq G$, the **quotient group** of G modulo N, written G/N, is the group with elements as left cosets of N in G with $(g_1N) \cdot (g_2N) = (g_1g_2N)$.

Proof. One can easily check this satisfies all of the group axioms. □

Remark 1.3.2. By Lagrange's theorem $|G/N| = |G|/|N|$.

Definition 1.3.3 (Simple group)**.** A group G is **simple** if it has no normal subgroups except $\{e_G\}$ and G.

1.4 Isomorphism theorems

Theorem 1.4.1 (First isomorphism theorem)**.** If $f : G \to H$ is a group homomorphism, $G/\ker f \cong \operatorname{im} f$.

Proof. Have $\phi : G/\ker f \to \operatorname{im} f$ with $\phi : g\ker f \mapsto f(g)$.

well defined: if $g\ker f = h\ker f$, $gh^{-1}\ker f = \ker f \implies f(g) = f(gh^{-1}h) = f(gh^{-1})f(h) = f(h)$.

homomorphism: $\phi((g\ker f)(h\ker f)) = \phi(gh\ker f) = f(gh) = f(g)f(h) = \phi(g\ker f)\phi(h\ker f)$.

surjective: any $h = f(g) \in \operatorname{im} f$ is clearly $\phi(g\ker f)$ for any $g \in G$.

injective: if $\phi(g\ker f) = e_H$, $f(g) = e_H \implies g \in \ker f$ so $\ker f = \{\ker\phi\} = \{e_{G/\ker\phi}\}$. By a lemma from *Linear algebra and groups*, we now have ϕ injective. □

Theorem 1.4.2 (Universal property of quotients)**.** Let $N \trianglelefteq G$ and $f : G \to H$ be a group homomorphism such that $N \subseteq \ker f$. There exists a *unique* homomorphism $\tilde{f} : G/N \to H$ such that the diagram

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "f"] & \\ G/N \arrow[r, dashed, "\tilde{f}"'] & H \end{tikzcd}$$

commutes, (here $\pi : G \to G/N$ is the projection map with $\pi : g \to gN$).

Proof. The proof is essentially that of Theorem 1.4.1 with $H = \operatorname{im} f$. □

Lemma 1.4.3. If $N \trianglelefteq G$ and $N \leq H \leq G$ then $N \trianglelefteq H$.

Proof. $gN = Ng$ for all $g \in G$ so also for all $g \in H$. □

Theorem 1.4.4 (Second isomorphism theorem)**.** Let $K, L \trianglelefteq G$ with $K \leq L$, $G/L \cong (G/K)/(L/K)$

Proof. Have $f : G/K \to G/L$, via same arguments in Theorem 1.4.1, f is a surjective group homomorphism, $gK \in \ker f \implies f(gK) = gL = L$ so $g \in L$ and $\ker f = L/K$. By Theorem 1.4.1, $(G/K)/(\ker f) = (G/K)/(L/K) \cong (G/L)$. □

Definition 1.4.5 (Frobenius product)**.** Given $A, B \subseteq G$ a group, the **(Frobenius) product** of A and B is

$$AB := \{ab \in G : a \in A, b \in B\}.$$

Lemma 1.4.6. Given $H, N \leq G$ a group, N is normal $\implies HN \leq G$ and N, H normal $\implies HN \trianglelefteq G$.

Proof.
1. HN is nonempty with $(h_1n_1)(h_2n_2) = (n_1n_3)(h_1h_2) \in NH$ for some $n_3 \in N$ and $(hn)^{-1} = n^{-1}h^{-1} \in Nh^{-1} = h^{-1}N \subseteq HN$.
2. $gHNg^{-1} = gHg^{-1} \cdot gNg^{-1} = HN$. □

Theorem 1.4.7 (Third isomorphism theorem)**.** If $H \leq G$ and $N \trianglelefteq G$, $H/(H \cap N) \cong (HN)/N$. This is ometimes called the *diamond theorem* due to the shape of the subgroup lattice it produces:

$$\begin{tikzcd} & G \arrow[d] & \\ & HN \arrow[dl] \arrow[dr] & \\ H \arrow[dr] & & N \arrow[dl] \\ & H \cap N \arrow[d] & \\ & \{e_G\} & \end{tikzcd}$$

where arrows point to subgroups.

Proof. Have $\phi : H \to G/N$ be the canonical map, $\ker \phi = H \cap N$ as $hN = N$ iff $h \in N$, $\operatorname{im} \phi = \{hN : h \in H\} = HN/N$, Theorem 1.4.1 on ϕ gives the result. □

Note 1.4.8. The naming of the group isomorphism theorems throughout literatue is very inconsistent.

1.5 Centres

Definition 1.5.1 (Inner automorphisms)**.** Given the group G the conjugations by elements of G form the group $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

Proof. Have $\phi : G \to \operatorname{Aut}(G)$ assigning to each element in $g \in G$ the conjugation map by G, $\operatorname{Inn}(G) = \operatorname{im}\phi \subset \operatorname{Aut}(G)$. □

Definition 1.5.2 (Centre of group)**.** Given the group G the elements of G that commute with all other elements form the **centre** of G, $Z(G) \trianglelefteq G$.

Proof of normality. Have $\phi : G \to \operatorname{Aut} G$ with $\phi : g \mapsto$ conjugation by g, $\ker\phi = Z(G)$. □

Proposition 1.5.3. If $G/Z(G)$ is cyclic, G is Abelian.

Proof. $G/Z(G) = \langle aZ(G)\rangle$ for some $a \in G$, for all $g \in G$ $gZ(G) = [aZ(G)]^m = a^m Z(G)$ for some $m \in \mathbb{N}$ therefore $a^{-m}g = z \in Z(G)$ so $g = a^m z$ and for all $g, h \in G$ we have $gh = a^n z_g a^m z_h = a^{n+m} z_g z_h = a^m z_h a^n z_g = hg$. □

1.6 Commutators

Definition 1.6.1 (Commutator)**.** For $a, b \in G$ a group, we have $[a, b] := aba^{-1}b^{-1}$ the **commutator** of a and b. $[G, G]$ is the smallest subgroup of G containing all commutators of elements of G, called the **commutator** of G.

Remark 1.6.2. A group G is Abelian iff $[G, G] = e_G$.

Theorem 1.6.3. Given G a group, $[G, G] \trianglelefteq G$ with its quotient in G Abelian.

Theorem 1.6.4. Let $N \trianglelefteq G$, G/N is Abelian iff $[G, G] \subseteq N$.

Theorem 1.6.5. Given a group G with $A, B \trianglelefteq G$, $A \cap B = \{e_G\}$ and $AB = G$; $A \times B \cong G$.

1.7 Torsion and p-primary subgroups

Definition 1.7.1 (Torsion subgroup)**.** Given an abelian group G, the set of elemnts of G with finite order form the **torsion subgroup** of G, denoted G_{tors}. When $G = G_{\text{tors}}$, we call G a **torsion Abelian group**.

Definition 1.7.2 (p-primary subgroups)**.** Given an abelian group G, the set of elements of g with order p (a prime) is the **p-primary subgroup** of G, written $G\{p\}$. When $G = G_G\{p\}$, we call G a **p-primary torsion Abelian group**.

Theorem 1.7.3. Let the prime factorisation of $n \in \mathbb{N}$ be $p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ with C_n the cyclic group of order n.

$$C_n \cong C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_m^{a_m}}.$$

Proof. □

1.8 Generators

Lemma 1.8.1. Given an indexing set $\mathcal{I}$, and a sequence of subgroups $(H_i)_{i\in\mathcal{I}} \leq H$, $\bigcap_{i\in\mathcal{I}} H_i \leq G$.

Definition 1.8.2 (Subgroup generated by a set)**.** Given $S \subseteq G$ a group,

$$\langle S\rangle := \left(\bigcap_{S\subseteq H\leq G} H\right) \leq G$$

is the **subgroup of G generated by S**. If $\langle S\rangle = G$ then we say S **generates** G and G is **finitely generated** is S is finite.

1.9 Classification of finitely generated Abelian groups

Definition 1.9.1 (Free Abelian group of rank n)**.** The **Free Abelian group of rank** n is the group $\mathbb{Z}^n$ under addition. The free abelian group of rank 0 is the trivial group.

Lemma 1.9.2. If $\mathbb{Z}^m \cong \mathbb{Z}^n$ then $n = m$, so the rank of a free abelian group is well defined.

Lemma 1.9.3. Any subgroup of $\mathbb{Z}^n$ is isomorphic to some $\mathbb{Z}^m$ for some $m \leq m$.

Theorem 1.9.4. Every finitely generated Abelian group is isomorphic to a product of finitely many cyclic groups.

Theorem 1.9.5. Every finitely generated Abelian group is isomorphic to a product of finitely many infinite cyclic groups and finitely many cyclic groups of prime order. The number of ininfite cyclic factors and the number of cclic factors of order p^r, where p is primse and $r \in \mathbb{N}$ is determined solely by the group.

Theorem 1.9.6. A finitely generated Abelian group, G, is not cyclic iff there exists a prime p such that $G \cong C_p \times C_p$.

2 Group actions

2.1 Actions

Definition 2.1.1 (Actions)**.** Given a group G and a set X, a **group action** is: a binary operation

$$\begin{aligned} \cdot \ : \ G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

with $e_G \cdot x = x$ for all $x \in X$ and $(g_1 g_2) \cdot x = g_1 \cdot (g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$; or, equivalently, a homomorphism $\rho : G \to \mathrm{Sym}(X)$.

Definition 2.1.2 (Faithful set)**.** An action of a group G on a set X is **faithful** if the map $\rho : G \to \mathrm{Sym}(X)$ is injective.

2.2 Orbit-stabiliser theorem

Definition 2.2.1 (Orbit)**.** Given a group G acting on a set X, the G**-orbit** of $x \in X$ is

$$G(x) := \{g \cdot x : g \in G\} \subseteq X.$$

Orbits partition X into X/G.

Definition 2.2.2 (Stabiliser)**.** Given a group G acting on a set X, the **stabiliser** of $x \in X$ is

$$\mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\} \subseteq G.$$

Stabilisers also partition G.

Remark 2.2.3 (Conjugacy classes)**.** When G acts on itself by conjugations, orbits of G are the **conjugacy classes**, x^G of G and the stabilisers of G are the centralisers of G.

Lemma 2.2.4. Given a group G acting on a set X, $\mathrm{Stab}_G(g \cdot x) = g\,\mathrm{Stab}_G(x) g^{-1}$

Theorem 2.2.5 (Orbit-stabiliser theorem)**.** Given a group G acting on a set X. For all $x \in X$, we have $\phi_x : G/\mathrm{Stab}(x) \xrightarrow{\sim} G(x)$ by $\phi_x : g\,\mathrm{Stab}(x) \mapsto g \cdot x$, giving $|G(x)| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|$.

Proof. asdfsd □

Corollary 2.2.6. $|X| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$.

Corollary 2.2.7 (Cayley's theorem)**.** Let G be a finite group of order n. Then $S_n \cong \mathrm{Sym}(G)$ contains a finite subgroup isomorphic to G.

Corollary 2.2.8 (Cauchy's theorem)**.** Let G be a finite group of order n and let p be a prime factor of n. Then G contains an element of order p.

Definition 2.2.9 (p-group)**.** A finite group G is a p**-group** is the order of G is a power of prime p.

Theorem 2.2.10. Let G be a p-group, $Z(G) \neq \{e_G\}$.

Proof. □

2.3 Jordan's theorem

Definition 2.3.1 (Transitive action). Given a group G acting on a set X, if X is a G-orbit then we say G acts **transitively** on X.

Definition 2.3.2 (Fixed points). Given a group G acting on a set X, an element $x \in X$ is a fixed point of $g \in G$ iff $g \cdot x = x$. We have $\mathrm{Fix}(g) \subseteq X$ the set of fixed points of $g \in G$ satisying:

$$\mathrm{Stab}(x) \xleftarrow[\pi_G]{} \{(x, g) \in X \times G;\ g \cdot x = x\} \xrightarrow[\pi_X]{} \mathrm{Fix}(g)\ .$$

Theorem 2.3.3 (Jordan's theorem). Let G act transitively on a finite set X, we have

$$\sum_{g \in G} |\,\mathrm{Fix}(g)| = |G|,$$

with there being some element $g \in G$ such that $\mathrm{Fix}(g) = \emptyset$.

Corollary 2.3.4 (Burnside's lemma). Given a group G acting on a finite set X:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

3 Rings

3.1 Rings

Definition 3.1.1 (Ring). A ring (with 1) is a set R with elements $0, 1$ and binary operations $+, \times$ such that

1. $(R, +)$ is an abelian group with identity 0,
2. $(R, \times)$ is a semigroup with 1 as the identity,
3. both left and right multiplication are distributive over addition.

Examples 3.1.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings with their normal operations. $\mathbb{R}[x]$ is the set of real-valued polynomials and is also a ring.

Definition 3.1.3 (Subring). A subset of a ring wich is itself a ring under the same operators with the same 1 is a **subring**.

Definition 3.1.4 (Commutative ring). A ring, R, is **commutative** iff $a + b = b + a$ for all $a, b \in \mathbb{R}$.

Definition 3.1.5 (Invertible). An element x of a ring R is invertible if there exists $y, z \in R$ with $yx = zx = 1$.

Definition 3.1.6 (Division ring). A ring R is called a **division ring** if $R\backslash\{0\}$ is a group under multiplication with identity 1.

Remark 3.1.7. A commutative division ring is a field.

Definition 3.1.8 (Integral domain). A commutative ring R is an integral domain iff $0 \neq 1$ and for all $a, b \in R$ $ab = 0 \implies a = 0$ or $b = 0$.

3.2 Ring homomorphisms

Definition 3.2.1 (Ring homomorphism). Let R, S be rings, a function $f : R \to S$ is a **ring homomorphism** iff it satisfies

1. $f : (R, +) \to (S, +)$ is a group homomorphism,
2. $f(xy) = f(x)f(y)$ for all $x, y \in R$,
3. $f(1_R) = 1_S$.

Lemma 3.2.2. Given the ring homomorphism $f : R \to S$ the kernel of f is a subgroup of $(R, +)$ which satisfies $xr, rx \in \ker f$ for all $x \in \ker f$ and $r \in R$.

3.3 Ideals

Definition 3.3.1 (Ideal)**.** For a ring R, a subset $I \subseteq R$ is a **left ideal**, denoted $I \trianglelefteq R$ iff

1. $(I, +)$ is a subgroups of $(R, +)$,
2. if $r \in R$ and $i \in I$, $ri \in R$.

Similarly, for **right ideals**. A subset I is a bi-ideal if it is both a left and right ideal.

Definition 3.3.2 (Quotient ring)**.** Given ring R with proper ideal $I \subset R$, The quotient abelian group R/I, with natural multiplication, forms the **quotient ring** of R by I.

Definition 3.3.3 (Principal ideal)**.** Given a commutative ring R and some $a \in R$, $aR := \{ax : x \in R\}$ is an ideal called a **principal ideal** with **generator** a.

Definition 3.3.4. A bijective ring homomorphism is a **ring isomorphism**, a ring homomorphism $f : R \to R$ is a **ring endomorphism**, an isomorphic ring endomorphism is **ring automorphism**.

Proposition 3.3.5. Given the ring homomorphism $f : R \to S$, $f(R) = \operatorname{im} R$ is a subring of S which is isomorphic to $R/\ker f$.

Proposition 3.3.6. A commutative ring is a field iff its only proper ideal is the trivial / zero ideal.

Proposition 3.3.7. Given $f : R \to S$ a ring homomorphism with J a left (or right or bi) ideal of S, $f^{-1}(J)$ is a left (respectively) ideal of R.

Definition 3.3.8 (Prime ideal)**.** Let R be a commutative ring, a proper ideal $I \subset R$ is a **prime ideal** iff $ab \in I$ for $a, b \in R \implies a \in I$ or $b \in I$.

Theorem 3.3.9. If $I \subset R$ is a prime ideal, R/I is an integral domain

Definition 3.3.10 (Maximal ideal)**.** A proper ideal I in a commutative rign R is **maximal** iff there are no other proper ideals J with $I \subset J$.

Theorem 3.3.11. I is a maximal ideal of R iff R/I is a field.

4 Integral domains

Throughout this section we will always have R be an integral domain.

4.1 Integral domains

Theorem 4.1.1. $ab = ac \implies b = c$ for all $a, b, c \in R$. (the cancellation law holds for all integral domains)

Proposition 4.1.2. For $a, b \in R$, $aR = bR$ iff $a = br$ for some $r \neq 0 \in R$.

Proof. □

Theorem 4.1.3. All fields are integral domains and all finite integral domains are fields.

Remark 4.1.4. The ring $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff it is a field $\iff$ n is prime.

Definition 4.1.5 (Unit)**.** $r \in R$ is a **unit** if there exists some $y \in R$ with $x \times y = 1_R$. We write $R^\times$ for the group of units in R under multiplication.

Definition 4.1.6 (Irreducible)**.** $r \in R \setminus R^\times$ is **irreducible** if it cannot be written as the product of two elements of $R \setminus R^\times$.

4.2 Charateristic

Lemma 4.2.1. For any ring S there is a uniqure ring homomorphism $f : \mathbb{Z} \to S$.

Proof. Have $f(0_R) = 0$, $f(1) \to 1_S$ and inductively have $f(n)$ be the sum of 1_S n times. □

Lemma 4.2.2. The kernel of the unique homomorphism $\mathbb{Z} \to R$ is either $\{0\}$ or $p\mathbb{Z}$ for some prime p.

Definition 4.2.3 (Charateristic)**.** The **characteristic** of R is the unique non-negative generator of the kernel of $\mathbb{Z} \to R$, denoted $\operatorname{char} R$.

4.3 Polynomial rings

Definition 4.3.1 (Polynomial ring)**.** $R[t]$ is, formally, the set of infinite sequences of elements of R with finitely many non-zero terms, but more helpfully: the set of polynomials in t with coefficients in R.

Definition 4.3.2 (Polynomial degree)**.** The **degree** of a polynomial, $r_0 + r_1 t + r_2 t^2 + \ldots + r_i t^i + \ldots \in R[t]$, is the unique maximum $i \in \mathbb{N}$ with $r_i \neq 0$ and 0 otherwise.

Lemma 4.3.3. Given $p(t), q(t) \in R$, $\deg(p(t)q(t)) = \deg(p(t)) + \deg(q(t))$, $R[t]$ is an integral domain and $R[t]^* = R^*$.

Theorem 4.3.4. If k is a field with $a(t), b(t) \in k[t]$ with $b(t) \neq 0$, there exists $q(t), r(t) \in k[t]$ such that $a(t) = q(t)b(t) = r(t)$ with $\deg(r(t)) < \deg(b(t))$ and $q(t), r(t)$ unique.

5 PIDs and UFDs

5.1 Euclidian domains

Definition 5.1.1 (Euclidian domain)**.** An integral domain R is a Euclidian domain if there exists some $\phi : R^* \to \mathbb{N}_0$ satsifying:

1. $\phi(ab) \leq \phi(a)$ for all $a, b \neq 0$,
2. for all $a, b \in R$ there exists $q, r \in R$ with $a = qb + r$ with $r = 0$ or $\phi(r) \leq \phi(b)$.

5.2 Principal ideal domains

Definition 5.2.1 (Principal integral domain)**.** An integral domain R is a **principal integral domain** iff every ideal of R is principal.

Theorem 5.2.2. R is a Euclidian domain $\implies$ R is a principal integral domain.

Proof. □

Corollary 5.2.3. F is a field $\implies$ $F[t]$ is a PID.

5.3 Unique factorisation domains

Definition 5.3.1 (Unique factorisation domain)**.** An integral domain R is a **unique factorisation domain** iff every element of $R \setminus R^\times$ can be written as the product of a single unit and finitely many irreducibles in R which is unique up to rearrangement.

Definition 5.3.2 (Division)**.** Given a, b in the integral domain R, we say a **divides** b, written $a|b$ iff $b = ra$ for some $r \in R$ and **properly divides** if $r \notin R^\times$.

Lemma 5.3.3. Given $p, a, b \in R$ a UFD, if p is irreducible then $p|ab \implies p|a$ or $p|b$.

Lemma 5.3.4. There is no infinite sequence of non-zero $r_1, r_2, \ldots \in R$ a UFD such that r_{n+1} properly divides r for all $n \geq 1$.

Theorem 5.3.5. The integral domain R is a UFD iff the properties in Lemma 5.3.3 and Lemma 5.3.4 hold.

Theorem 5.3.6. Every principal ideal domain is a unique factorisation domain.

6 Fields

6.1 Vector spaces

Throughout this section let k be a field.

Definition 6.1.1 (Vector space)**.** A k-vector space V is an abelian group with an action of k on the elements of V satisfying

1. $1_k v = v$ for all $v \in V$,
2. $(x + y)V = xv + yv$ for all $x, y \in k$ and $v \in V$,

3. $x(v+w) = xv + xw$ for all $x \in k$ and $v, w \in V$.

Proposition 6.1.2. If $\operatorname{ch} k = 0$ then k contains a unique subfield isomorphic to $\mathbb{Q}$. Otherwise, if $\operatorname{ch} k = p$ then k contains a unique subfield isomorphic to $\mathbb{F}_p$.

Theorem 6.1.3. Every finite field has p^n elements for some prime p and $n \in \mathbb{N}$.

6.2 Field extensions

Definition 6.2.1 (Field extension)**.** A **field extension** F of k is a k-vector space.

Proposition 6.2.2. All homomorphisms between fields and rings are injective.

Proof. The only possible maps between fields are field extensions, the only proper ideal of a field is the zero ideal. □

Definition 6.2.3 (Finite field extension)**.** An extension of the fields $k \subset K$ is **finite** iff K is a finite dimensional vector space over k with $\dim K$ the **degree** of the extension

Theorem 6.2.4. If $k \subset F \subset K$ are field extensions, K is a finite extension of k iff K is a finite extension of F and F is a finite extension of k. We then have $[K : k] = [K : F][F : k]$.

Remark 6.2.5. Degree 2 and 3 field extensions are called quadratics and cubics respectively.

6.3 Constructing fields

Lemma 6.3.1. Given R a PID with $a \neq 0 \in R$, aR is maximal iff a is irreducible.

Proof. □

Corollary 6.3.2. Given R a PID with reducible $a \in R$, R/aR is a field.

Theorem 6.3.3. A polynomial $f(t) \in k[t]$ of degree 2 or 3 is irreducible iff it has no root in k.

Definition 6.3.4 (Non-Square)**.** $a \in k$ is non-square if there is no element $b \in k$ with $b^2 = a$.

Lemma 6.3.5. Let p be an odd prime. The field $\mathbb{F}_p$ contins $(p-1)/2$ non-squares. For all non-square $a \in \mathbb{F}_p$, $t^2 - a$ is irreducible in $\mathbb{F}_p[t]$.

Theorem 6.3.6. For all $p(t) \in k[t]$, there exists a finite field extension $k \subset K$ such that:

$$p(t) = c\prod_{i=1}^{n}(t - a_i),$$

for some $c \in k^\times$ and $a_i \in K$ for all $i \in [1, n]$.

6.4 Existence of finite fields

Theorem 6.4.1. Let k have characteristic $p \neq 0$, for all $x, y \in k$ and $m \in \mathbb{Z}^{\geq 0}$,

$$(x+y)^{p^m} = x^{p^m} + y^{p^m}.$$

Definition 6.4.2 (Derivative)**.** Let $p(t) = a_0 + a_1 t + \ldots + a_n t^n \in k[t]$, the **derivative** of $p(t)$ is

$$p'(t) := a_1 + 2a_2 t + \ldots + n a_n t^{n-1}.$$

Lemma 6.4.3. Let $p(t) = (x - a_1)(x - a_2)\ldots(x - a_n) \in k[t]$, $a_i \neq a_j$ for all $i \neq j$ iff $p(t)$ and $p'(t)$ have no common roots.

Theorem 6.4.4. For all prime p and natural n, there exists a field with p^n elements.

Chapter 2

Lebesgue Measure and Integration

Lectured by Someone
Typed by Yu Coughlin
Season Year

Introduction

The following are complementary reading for the course.

- G. Grimmett and D. J. A. Welsh, Probability: An Introduction, 1986
- J. K. Blitzstein and J. Hwang, Introduction to Probability, 2019
- D. F. Anderson et al, Introduction to Probability, 2018
- S. M. Ross, Introduction to Pro ability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

Lecture 1
Monday
30/10/2023

1 Motivation

2 Measures

2.1 Algebras and σ-algebras

2.2 Measures

2.3 Complete measure spaces

3 Constructing measures

3.1 Pre-measure

3.2 Outer measure

3.3 Restriction

3.4 Lebesgue measure

4 Measurable functions

4.1 Defintion

4.2 Properties

4.3 Continuity

5 Lebesgue integral

5.1 Construction

5.2 Properties

6 Convergence

6.1 Monotone convergence

6.2 Fatou's lemma

6.3 Lebesgue dominated convergence

6.4 Vitali's theorem

7 L^p spaces

7.1 Norms

7.2 L^p spaces

7.3 Normed vector spaces

7.4 Completeness

8 Product measures

8.1 Products of sets

8.2 σ-algebras on product sets

8.3 Product measures

9 Fubini's theorem

9.1 Motivations

9.2 Setup

9.3 Fubini's theorem

10 Differentiation

Chapter 3

Categories

Lectured by noone
Typed by Yu Coughlin
Season Year

Introduction

The following are complementary reading for the course.

- G. Grimmett and D. J. A. Welsh, Probability: An Introduction, 1986
- J. K. Blitzstein and J. Hwang, Introduction to Probability, 2019
- D. F. Anderson et al, Introduction to Probability, 2018
- S. M. Ross, Introduction to Pro ability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

1 Basic definitions

1.1 Categories

Definition 1.1.1 (Category)**.** A catgeory $\mathcal{C}$ contains the following data:

1. a *collection* of objects, $\mathrm{Ob}(\mathcal{C})$,
2. for every $x, y \in \mathrm{Ob}(\mathcal{C})$ a collection of morphisms $\mathrm{Hom}_{\mathcal{C}}(x, y)$ from x to y,
3. an identity morphism $\mathrm{id}_x \in \mathrm{Hom}_{\mathcal{C}}(x, x)$ for all $x \in \mathrm{Ob}(\mathcal{C})$,
4. a composition map of morphisms, $\circ : \mathrm{Hom}_{\mathcal{C}}(y, z) \times \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{C}}(x, z)$ for all $x, y, z \in \mathrm{Ob}(\mathcal{C})$.

Which satisfy the two axioms:

1. for all $f \in \mathrm{Hom}_{\mathcal{C}}(x, y)$ with $x, y \in \mathrm{Ob}(\mathcal{C})$ we have $f \circ \mathrm{id}_x = f = \mathrm{id}_y \circ f$,
2. for compatible morphisms f, g, h we have $f \circ (g \circ h) = (f \circ g) \circ h$.

We will use the shorthand $x \in \mathcal{C}$ for $x \in \mathrm{Ob}\,\mathcal{C}$, $\mathrm{Hom}(x, y)$ for $\mathrm{Hom}_{\mathcal{C}}(x, y)$ when $\mathcal{C}$ is obvious and $\mathrm{End}(x)$ for $\mathrm{Hom}(x, x)$.

Note 1.1.2. Note that in our definition the term *collection* is used instead of set, this is commonplace and necessary to prevent paradoxes when constructing the category of sets.

Examples 1.1.3. The following are all categories:

1. Set with sets as objects and functions as their morphisms,
2. Grp with groups as objects and their homomorphisms as morphisms,
3. Ab, Grp restricted to abelian groups,
4. for a field k, Vect_k with k-vector spaces as objects and linear transformations as morphisms,
5. Cat with categories as objects and soon to be defined **functors** as morphisms,
6. Top, Rng, Meas, Poset, Man with their objects and morphisms all defined similarly
7. Given a category $\mathcal{C}$, $\mathcal{C}^{op}$ wich has the same opjects as $\mathcal{C}$ but $\mathrm{Hom}_{\mathcal{C}^{op}}(x, y) = \mathrm{Hom}_{\mathcal{C}}(y, x)$ for all $x, y \in \mathcal{C}$,
8. Any set X with objects as elements in X and no morphisms except the identities
9. $(\mathbb{R}, \leq)$ with objects as $\mathbb{R}$ and a morphisms from x to y iff $x \leq y$ for all $x, y \in \mathbb{R}$.

Definition 1.1.4 (Isomorphism)**.** A morphism $f \in \mathrm{Hom}(x, y)$ is an **isomorphism** iff there is a morphism $f^{-1} \in \mathrm{Hom}(y, x)$ with $f \circ f^{-1} = \mathrm{id}_y$ and $f^{-1} \circ f = \mathrm{id}_x$.

1.2 Functors

Definition 1.2.1 ((Covariant) Functor)**.** Given categories $\mathcal{C}, \mathcal{D}$ a **(covariant) functor** $F : \mathcal{C} \to \mathcal{D}$ is the following data:

1. a map $\mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ (also denoted F),
2. for any two objects $x, y \in \mathcal{C}$ a map $\mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{D}}(F(x), F(y))$ (also also denoted F)

satisfying the properties:

1. for all $x \in \mathcal{C}$, $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$,
2. for all x, y, z with f, g in $\mathrm{Hom}_{\mathcal{C}}(y, z), \mathrm{Hom}_{\mathcal{C}}(x, y)$, $F(f \circ g) = F(f) \circ F(g)$.

Definition 1.2.2 (Contravariant functor)**.** A **contravariant functor** from $\mathcal{C}$ to $\mathcal{D}$ is a covariant functor from $\mathcal{C}^{op}$ to $\mathcal{D}$.

Definition 1.2.3 (Hom-functor)**.** The **hom-functor** for a given category $\mathcal{C}$ is $\mathrm{Hom}_{\mathcal{C}} : \mathcal{C}^{op} \times \mathcal{C} \to \mathsf{Set}$ sending a pair of elements $c, d \in \mathcal{C}$ to $\mathrm{Hom}_{\mathcal{C}}(c, d)$.

1.3 Natural transformations

Definition 1.3.1 (Natural transformation)**.** Given categories $\mathcal{C}, \mathcal{D}$ with functors $F, G : \mathcal{C} \to \mathcal{D}$, a **natural transformation** $\eta : F \to G$ consists of morphisms η_x for all $x \in \mathcal{C}$ such that the diagram,

$$\begin{tikzcd} F(x) \arrow[r, "F(f)"] \arrow[d, "\eta_x"] & F(y) \arrow[d, "\eta_y"] \\ G(x) \arrow[r, "G(f)"] & G(y) \end{tikzcd}$$

commutes for all $x, y \in \mathcal{C}$ and $f \in \mathrm{Hom}_{\mathcal{C}}(x, y)$.

Remark 1.3.2. By constructing the category of functors from $\mathcal{C}$ to $\mathcal{D}$, denoted $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$, morphisms are natural transformations. **Natural isomorphisms** are defined as isomorphisms in this category.

1.4 Equivalence of categories

Definition 1.4.1 (Equivalence)**.** Given categories $\mathcal{C}, \mathcal{D}$ an **equivalence of categories** is a pair of functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ with natural isomorphisms $FG \xrightarrow{\sim} \mathrm{id}_{\mathcal{D}}$ and $\mathrm{id}_{\mathcal{C}} \xrightarrow{\sim} GF$.

Definition 1.4.2 (Adjunction)**.** An **adjuction** between categories $\mathcal{C}, \mathcal{D}$ is a pair of functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that for all $x \in \mathcal{C}$ and $y \in \mathcal{D}$, there exists an $\eta_{x,y} : \mathrm{Hom}_{\mathcal{C}}(x, G(y)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(F(x), y)$ such that the diagram

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{D}}(F(x'), y) \arrow[r, "\circ F(f)"] & \mathrm{Hom}_{\mathcal{D}}(F(x), y) \arrow[r, "g\circ"] & \mathrm{Hom}_{\mathcal{D}}(F(x), y') \\ \mathrm{Hom}_{\mathcal{C}}(x', G(y)) \arrow[r, "\circ f"] \arrow[u, leftrightarrow, "\eta_{x',y}"] & \mathrm{Hom}_{\mathcal{C}}(x, G(y)) \arrow[r, "G(g)\circ"] \arrow[u, leftrightarrow, "\eta_{x,y}"] & \mathrm{Hom}_{\mathcal{C}}(x, G(y')) \arrow[u, leftrightarrow, "\eta_{x,y'}"] \end{tikzcd}$$

commutes for all $x, x' \in \mathcal{C}$; $y, y' \in \mathcal{D}$; $f : x \to x'$ and $g : y \to y'$.

Theorem 1.4.3. If F, G form an equivalence of the categories $\mathcal{C}, \mathcal{D}$ then F, G are an adjunction.

Examples 1.4.4 (Adjunctions in group theory)**.** Consider the **forgetful functor** $F : \mathrm{Ab} \to \mathrm{Grp}$ which simply forgets the Abelian property of a group. We also have the **abeliantisation functor** $(-)^{\mathrm{ab}} : \mathrm{Grp} \to \mathrm{Ab}$ which maps $G \mapsto G^{\mathrm{ab}} := G/[G, G]$. F and $(-)^{\mathrm{ab}}$ for an adjuction between Grp and Ab.

1.5 Representable functors

Definition 1.5.1 (Yoneda functor)**.** Given some x in a category $\mathcal{C}$, there is a functor $\mathrm{Hom}_{\mathcal{C}}(-, x) : \mathcal{C}^{op} \to \mathrm{Set}$ which satisfies the required properties to have the **Yoneda functor**:

$$Y : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set}).$$

Which sends an element $y \in \mathcal{C}$ to the functor from objects in $\mathcal{C}^{op}$ to the set of morphisms from these objects to y.

Lemma 1.5.2. The Yoneda functor and the hom-functor form an adjunction in Cat.

Definition 1.5.3 (Representable)**.** A functor $F \in \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$ is **representable** if $F \cong Y(c)$ for some $c \in \mathcal{C}$.

Example 1.5.4. Consider the functor $F : \mathrm{Set}^{(op)} \to \mathrm{Set}$ sending a set to its powerset. F is clearly isomorphic the functor $\mathrm{Hom}(-, \{0, 1\})$ from subsets to indicator functions on X. This is the image of the Yoneda functor so F is representable.

1.6 Yoneda lemma

Theorem 1.6.1 (Yoneda lemma)**.** Given some $x \in \mathcal{C}$ and $F \in \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$ we have

$$\mathrm{Hom}_{\mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})}(Y(x), F) \cong F(x).$$

Remark 1.6.2. This is a generalisation of Cayley's theorem which shows that we can study a group by instead studying the permutations of its underlying set.