

A second year mathematics degree

Yu Coughlin

Contents

1	Real Analysis and Topology	1
L1 1	Euclidean spaces	2
	1.1 Euclidean norm	2
	1.2 Convergence in \mathbb{R}^n	4
2	Continuity and limits of functions	4
	2.1 Open sets	4
	2.2 Continuity	4
3	Derivative of maps of Euclidean spaces	4
	3.1 Total derivatives	4
	3.2 Directional and partial derivatives	4
	3.3 Higher order derivatives	4
4	Inverse and implicit function theorems	4
	4.1 Inverse function theorem	4
	4.2 Implicit function theorem	4
5	Metric spaces	4
	5.1 Introduction	4
	5.2 Normed vector spaces	4
	5.3 Sets in metric spaces	4
	5.4 Continuous maps of metric spaces	4
6	Topological spaces	4
	6.1 Topologies and their spaces	4
	6.2 Convergence and Hausdorff property	4
	6.3 Closed sets	4
	6.4 Continuous maps	4
7	Connectedness	4
	7.1 Definition	4
	7.2 Continuous maps	4
	7.3 Path connected sets	4
8	Compactness	4
	8.1 Covers	4
	8.2 Sequential compactness	4
	8.3 Continuous maps	4
	8.4 Arzelá-Ascoli theorem	4
9	Completeness	4
	9.1 Banach spaces	4
	9.2 Fixed point theorem	4
2	Groups and Rings	5
1	Quotient groups	6
	1.1 Group homomorphisms	6
	1.2 Normal subgroups	6
	1.3 Quotient groups	6
	1.4 Isomorphism theorems	6
	1.5 Centres	8
	1.6 Commutators	8
	1.7 Torsion and p -primary subgroups	8
	1.8 Generators	8
	1.9 Classification of finitely generated Abelian groups	9

2	Group actions	9
2.1	Actions	9
2.2	Orbit-stabiliser theorem	9
2.3	Jordan's theorem	10
3	Rings	10
3.1	Rings	10
3.2	Ring homomorphisms	10
3.3	Ideals	11
4	Integral domains	11
4.1	Integral domains	11
4.2	Charateristic	11
4.3	Polynomial rings	12
5	PIDs and UFDs	12
5.1	Euclidian domains	12
5.2	Principal ideal domains	12
5.3	Unique factorisation domains	12
6	Fields	12
6.1	Vector spaces	12
6.2	Field extensions	13
6.3	Constructing fields	13
6.4	Existence of finite fields	13
3	Lebesgue Measure and Integration	14
L1 1	Motivation	17
2	Measures	17
2.1	Algebras and σ -algebras	17
2.2	Measures	17
2.3	Complete measure spaces	17
3	Constructing measures	17
3.1	Pre-measure	17
3.2	Outer measure	17
3.3	Restriction	17
3.4	Lebesgue measure	17
4	Measurable functions	17
4.1	Defintion	17
4.2	Properties	17
4.3	Continuity	17
5	Lebesgue integral	17
5.1	Construction	17
5.2	Properties	17
6	Convergence	17
6.1	Monotone convergence	17
6.2	Fatou's lemma	17
6.3	Lebesgue dominated convergence	17
6.4	Vitali's theorem	17
7	L^p spaces	17
7.1	Norms	17
7.2	L^p spaces	17
7.3	Normed vector spaces	17
7.4	Completeness	17
8	Product measures	17
8.1	Products of sets	17
8.2	σ -algebras on product sets	17
8.3	Product measures	17
9	Fubini's theorem	17
9.1	Motivations	17
9.2	Setup	17
9.3	Fubini's theorem	17
10	Differentiation	17

10.1	Hardy-Littlewood maximal function	17
10.2	Compact support spaces	17
10.3	Lebesgue's differentiation theorem	17
11	Decomposition	17
11.1	Signed measures	17
11.2	Hahn decomposition theorem	17
11.3	Mutually singular measures	17
11.4	Jordan decomposition theorem	17
11.5	Lebesgue decomposition theorem	17
11.6	Radon-Nikodym theorem	17
4	Categories	18
1	Basic definitions	19
1.1	Categories	19
1.2	Functors	19
1.3	Natural transformations	20
1.4	Equivalence of categories	20

Chapter 1

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 Probability Models, 2014
- G. Grimmett and D. Stirzaker, Probability and Random Processes, 2001
- G. Grimmett and D. Stirzaker, One Thousand Exercises in Probability, 2009

1 Euclidean spaces

1.1 Euclidean norm

ya

1.2 Convergence in \mathbb{R}^n

2 Continuity and limits of functions

2.1 Open sets

2.2 Continuity

3 Derivative of maps of Euclidean spaces

3.1 Total derivatives

3.2 Directional and partial derivatives

3.3 Higher order derivatives

4 Inverse and implicit function theorems

4.1 Inverse function theorem

4.2 Implicit function theorem

5 Metric spaces

5.1 Introduction

5.2 Normed vector spaces

5.3 Sets in metric spaces

5.4 Continuous maps of metric spaces

6 Topological spaces

6.1 Topologies and their spaces

6.2 Convergence and Hausdorff property

6.3 Closed sets

6.4 Continuous maps

7 Connectedness

7.1 Definition

7.2 Continuous maps

7.3 Path connected sets

8 Compactness

8.1 Covers

8.2 Sequential compactness

8.3 Continuous maps

8.4 Arzelá-Ascoli theorem

9 Completeness

9.1 Banach spaces

9.2 Fixed point theorem

Chapter 2

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 Probability 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 $f : G \rightarrow H$ 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. $\text{Aut } G$ (the set of automorphisms of a group G) is a group under function composition.

Proof. By examining the definition of $\text{Aut } G$, taking $e = \text{id}$ and showing association elementwise. \square

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. \square

1.2 Normal subgroups

Definition 1.2.1 (Normal subgroup). A subgroup 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. \square

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. \square

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 $f : G \rightarrow H$ is a group homomorphism, $G/\ker f \cong \text{im } f$.

Proof. Have $\phi : G/\ker f \rightarrow \text{im } f$ 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 $h = f(g) \in \text{im } f$ 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. \square

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

$$\begin{array}{ccc} G & & \\ \pi \downarrow & \searrow f & \\ G/N & \xrightarrow{\tilde{f}} & H \end{array}$$

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

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

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 $f : G/K \rightarrow G/L$, 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

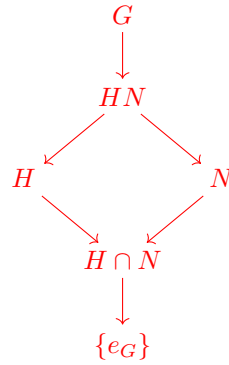
$$AB := \{ab \in G : a \in A, b \in B\}.$$

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:



where arrows point to subgroups.

Proof. Have $\phi : H \rightarrow G/N$ be the canonical map, $\ker \phi = H \cap N$ as $hN = N$ iff $h \in N$, $\text{im } \phi = \{hN : h \in H\} = HN/N$, 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 $\text{Inn } G \trianglelefteq \text{Aut } G$.

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

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 $\phi : G \rightarrow \text{Aut } G$ with $\phi : g \mapsto \text{conjugation by } g$, $\ker \phi = Z(G)$. \square

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 $gh = a^n z_g a^m z_h = a^{n+m} z_g z_h = a^m z_h a^n z_g = hg$. \square

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 elements 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 $G = G\{p\}$, 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 .

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

Proof. \square

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** if 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 $m \leq n$.

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 infinite cyclic factors and the number of cyclic factors of order p^r , where p is prime 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 $\rho : G \rightarrow \text{Sym}(X)$.

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

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

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 , $\text{Stab}_G(g \cdot x) = g \text{Stab}_G(x) g^{-1}$

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

Proof. asdfs □

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

Corollary 2.2.7 (Cayley's theorem). Let G be a finite group of order n . Then S_n 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** if 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 $\text{Fix}(g) \subseteq X$ the set of fixed points of $g \in G$ satisfying:

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

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

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

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

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

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

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 which 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 $a, b \in R$.

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 $R \setminus \{0\}$ 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 $f : R \rightarrow S$ is a **ring homomorphism** iff it satisfies

1. $f : (R, +) \rightarrow (S, +)$ 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 $f : R \rightarrow S$ the kernel of f is a subgroup of $(R, +)$ which satisfies $rx, rx \in \ker f$ 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 $i \in I$, $ri \in I$.

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 $f : R \rightarrow R$ is a **ring endomorphism**, an isomorphic ring endomorphism is **ring automorphism**.

Proposition 3.3.5. Given the ring homomorphism $f : R \rightarrow S$, $f(R) = \text{im } R$ 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 $f : R \rightarrow S$ 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 ring 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 Characteristic

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

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

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

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

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, $r_0 + r_1t + r_2t^2 + \dots + r_it^i + \dots \in R[t]$, 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 $\phi : R^* \rightarrow \mathbb{N}_0$ satisfying:

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 $\phi(r) < \phi(b)$.

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 $r_1, r_2, \dots \in R$ a UFD such that r_{n+1} properly divides r_n 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. $1_kv = v$ 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 $\text{ch } k = 0$ then k contains a unique subfield isomorphic to \mathbb{Q} . Otherwise, if $\text{ch } k = p$ 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. \square

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. \square

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 contains $(p-1)/2$ 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 $p(t) = a_0 + a_1 t + \dots + a_n t^n \in k[t]$, the **derivative** of $p(t)$ is

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

Lemma 6.4.3. Let $p(t) = (x - a_1)(x - a_2) \dots (x - a_n) \in k[t]$, $a_i \neq a_j$ 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 3

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 Probability 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 Definition

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 4

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 Probability 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 category \mathcal{C} contains the following data:

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

Which satisfy the two axioms:

1. for all $f \in \text{Hom}_{\mathcal{C}}(x, y)$ with $x, y \in \text{Ob}(\mathcal{C})$ we have $f \circ \text{id}_x = f = \text{id}_y \circ f$,
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 $x \in \text{Ob} \mathcal{C}$, $\text{Hom}(x, y)$ for $\text{Hom}_{\mathcal{C}}(x, y)$ when \mathcal{C} is obvious and $\text{End}(x)$ for $\text{Hom}(x, x)$.

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} which has the same objects as \mathcal{C} but $\text{Hom}_{\mathcal{C}^{op}}(x, y) = \text{Hom}_{\mathcal{C}}(y, x)$ 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 $f \in \text{Hom}(x, y)$ is an **isomorphism** iff there is a morphism $f^{-1} \in \text{Hom}(y, x)$ with $f \circ f^{-1} = \text{id}_y$ and $f^{-1} \circ f = \text{id}_x$.

1.2 Functors

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

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

satisfying the properties:

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

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 (Full). A functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is **full** if the map

1.3 Natural transformations

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

$$\begin{array}{ccc} F(x) & \xrightarrow{F(f)} & F(y) \\ \downarrow \eta_x & & \downarrow \eta_y \\ G(x) & \xrightarrow{G(f)} & G(y) \end{array}$$

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

Remark 1.3.2. By constructing the category of functors from \mathcal{C} to \mathcal{D} , denoted $\text{Fun}(\mathcal{C}, \mathcal{D})$, 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 $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ with natural isomorphisms $FG \xrightarrow{\sim} \text{id}_{\mathcal{D}}$ and $\text{id}_{\mathcal{C}} \xrightarrow{\sim} GF$.

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

$$\begin{array}{ccccc} \text{Hom}_{\mathcal{D}}(F(x'), y) & \xrightarrow{\circ F(f)} & \text{Hom}_{\mathcal{D}}(F(x), y) & \xrightarrow{g \circ} & \text{Hom}_{\mathcal{D}}(F(x), y') \\ \updownarrow \eta_{x',y} & & \updownarrow \eta_{x,y} & & \updownarrow \eta_{x,y'} \\ \text{Hom}_{\mathcal{C}}(x', G(y)) & \xrightarrow{\circ f} & \text{Hom}_{\mathcal{C}}(x, G(y)) & \xrightarrow{G(g) \circ} & \text{Hom}_{\mathcal{C}}(x, G(y')) \end{array}$$

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

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