Lecture Notes on Point Set Topology and Algebraic Geometry[1]

Scribe: Liangzu Peng
Lecturer: Professor Manolis
School of Information Science and Technology
ShanghaiTech University
penglz@shanghaitech.edu.cn

June 16, 2018

[1]The material can be found at: http://www.liangzu.org/en/ag-notes.html.

Preface

This note developed based on the course Advanced Geometry by Professor Manolis at ShanghaiTech University is a first step towards Algebraic Geometry, a subject that is known to be elusive, abstract, and inaccessible. Manolis brings it to undergraduate life in a digestive and approachable way.

Disclaimer. While the lectures are made psychologically comfortable, which I definitely agree that is one of the most important factors forming a course, this note is not. There are English syntax errors, symbolic inconsistencies, and even wrong proofs in the note. The readers should be brave enough to find and attack them as exercises, although this note can be improved in many ways.

Motivation. The main motivation of writing notes for this course is as follows. While David A Cox et al. [3] introduce algebraic geometry at undergraduate level from a computational perspective and the target students of Math 145[1] by Ravi Vakil are from mathematical discipline, there is as far as I know no course or book that takes algebraic geometry to engineering students, in a proof-based manner. If a book is indeed desired, this course note is the very first step.

Story. But who will take it? There is always the same hesitation after each lecture that whether should I devote myself to developing this note. I have papers to read, code to write, girls to date with, and video games to play. It is always the case that I write after each lecture, with the aroma of coffee permeating in the windy afternoon or evening, tired yet happy. Mathematics is like an ocean, where the one diving deeply witnesses the beauty. I find a way of diving: hacking proofs, giving examples (not waiting for examples), and designing exercises. The note grows like that I am pouring the water into an apertured bucket. The more I wrote, the more errors I made. Will the constant dripping from the bucket hollow the stone? It was until the end of the course I did not realize the answer. Hesitation does not be turned into regret.

Content.

Part I: Point Set Topology. The topology part follows strictly from Mendelson [1], of which 80% are covered, including open set and closed set, continuity, compactness, connectedness, etc..

Part II: Algebraic Geometry. In the second part of the course, some fundamental theorems and results in algebraic geometry are considered. To develop them,

[1] http://math.stanford.edu/~vakil/17-145/

however, some just enough prerequisites in (commutative) algebra are introduced beforehand. This reverse engineering approach is used, not due to the habit of a mathematical hacker, for inevitable reasons. This is the first time to teach such a course in ShanghaiTech, before which no one knows what should be taught, and the target students major in engineering, who do not learn any topology or abstract algebra before. The main results developed in this part include Hibert's Nullstellensatz, Noether Normalization, and some dimension theory.

References

[1] Mendelson, B. (1990). *Introduction to topology*. Courier Corporation.

[2] Atiyah, M., & MacDonald, I. G. Introduction to Commutative Algebra.

[3] Cox, D. A., Little, J., & O'Shea, D. (2015). Ideals, varieties, and algorithms, 4th edn, Undergraduate Texts in Mathematics.

[4] Hartshorne, R. (1977). Algebraic geometry, volume 52 of Graduate Texts in Mathematics.

[5] Eisenbud, D. (2013). *Commutative Algebra: with a view toward algebraic geometry* (Vol. 150). Springer Science & Business Media.

[6] Judson, T. (2017). *Abstract algebra: theory and applications*. Stephen F. Austin State University.

[7] Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (Vol. 3). Hoboken: Wiley.

[8] Rudin, W. (1964). *Principles of mathematical analysis* (Vol. 3). New York: McGraw-hill.

[9] Abbott, S. (2015). *Understanding Analysis*. Springer.

[10] Pugh, C. C. (2015). *Real Mathematical Analysis*. Springer.

[11] Tao, T. (2016). *Analysis I* (Vol. 37). Springer.

[12] Tao, T. (2016). *Analysis II* (Vol. 38). Springer.

[13] Morris, S. A. (2018). *Topology without tears*. University of New England.

Contents

SI112: Advanced Geometry	Spring 2018
Lecture 01 — Feb. 27th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

1 Lecture 01

"*The materials invented 15 years ago are becoming important today, and will be more important after 15 years.*:)"

1.1 Overview of this lecture

1.1.1 What the course is about

This class is a path to *Algebraic Geometry*, where we have to learn *Topology* and *Ring Theory* as a prerequisite. If time permits, we will also introduce Convex *Geometry*, which is a foundation for convex optimization.

The goal of this class is to provide you a formal mathematical training, comprising mathematical intuition, principled thinking, and mathematical tools.

1.1.2 Where this class is applied.

(there may be typos since I do not understand the terminology.)

Topology is used in Data Science (e.g., Pattern Analysis via "Persistent Homology"), Electron Decives ("topological insulator"), Network/Graph Topologies, Molecular Biology (e.g., DNA and protein folding, Krot Theory).

Algebraic Geometry is used in Machine Learning (e.g., Data Clustering, Matrix Completion), Computer Vision (e.g., Structure from Motion, Multi-view Geometry), Robotics (e.g., Control and Planing, the motion space is algebraic), Biology (e.g. Phylogenetics)

1.1.3 Evaluation for the course

There will be no exams for the course, and the homework is occasional. As an alternative, we will have weekly tests, including 2 qustions which you need to solve/prove in 30 minutes.

The course proceeds as follows. 1) You take the class in the week i, 2) there will be a TA session in week $i+1$, where or when we will do again what we did in the week i, 3) you got a new lecture and the quiz in the week $i+2$.

1.1.4 A starting point for Mathematics

To begin mathematics, we have to use some langueges (e.g., we use Chinese to talk). We introduce *set* as a language, or as a primitive notion, to describe mathematics. You know what I mean by *set*, hopefully.

1.2 Math

We are ready to define *function*, as you might already know, it is merely a mapping from one set to another. Formally,

Definition 1.2.1 (function)**.** A function $f : X \to Y$ is a subset $\mathcal{F}$ of $X \times Y$, such that, for each $x \in X$, there is only one element $y \in Y$ satisfying $(x, y) \in \mathcal{F}$.

Usually we say that X is the *domain* of the function f, Y the *target domain* of the function f.

Definition 1.2.2 (image of a function)**.** The image of a function $f : X \to Y$ is defined as follows:

$$im(f) = \{y \in Y | \text{ there is } x \in X : y = f(x)\}. \tag{1.2.1}$$

Definition 1.2.3 (inverse image)**.** Let $f : X \to Y$ be a function and T a subset of Y, then

$$f^{-1}(T) = \{x \in X | f(x) \in T\} \tag{1.2.2}$$

is called inverse image of T. If T is a singleton set, i.e., $T = \{y\}$ where $y \in Y$. we call $f^{-1}(T) = f^{-1}(\{y\})$ the *fiber* over y.

Definition 1.2.4 (left-invertible and right-invertible)**.** The professor draws pictures to illustrate these two concepts. review the pictures or read the textbook for a reference.

Definition 1.2.5 (invertible function)**.** A function f is invertible if f is both left- and right-invertible.

Question 1.2.6. How to show that a function f is left (right) invertible?

Definition 1.2.7 (injectivity and surjectivity)**.** A function $f : X \to Y$ is called *injective* if whenever $f(x) = f(x')$ for $x, x' \in X$, then $x = x'$. That is, for each $y \in f(X)$ there is only one $x \in X$ such that $f(x) = y$.

A function $f : X \to Y$ is called *surjective* if $Y = f(X)$.

Proposition 1.2.8. *A function $f : X \to Y$ is injective if and only if it is left-invertible.*

proof skeleton. Just follow the definitions of injectivity and left-invertibility.

To show that $f : X \to Y$ is left-invertible, you have to find a function $g : Y \to X$ such that $g(f(x)) = x$ (the definition of left-invertibility).

To show that $f : X \to Y$ is injective, you have to prove that given $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$, it must be that $x_1 = x_2$ (the definition of injectivity). □

Exercise 1.2.9. Prove that a function $f : X \to Y$ is surjective if and only if it is right-invertible.

Definition 1.2.10 (Equivalence Relations)**.** A relation R of X is a subset of $X \times X$.

$$(x, y) \in R \iff xRy. \tag{1.2.3}$$

An equivalence relation should be reflexive (xRx), symmetric ($xRy \Rightarrow yRx$) and transitive ($xRy, yRz \Rightarrow xRz$).

Question 1.2.11. Can an equivalence relation even be an empty set?

Definition 1.2.12 (equivalence class)**.** Let R be equivalence relation on X, and $x \in X$, then we call $[x] = \{x' \in X | xRx'\}$ is the equivalence class of x.

Proposition 1.2.13. *Let X be a set and $x, y \in X$, then*

$$[x] \cap [y] \neq \emptyset \Rightarrow [x] = [y]. \tag{1.2.4}$$

Corollary 1.2.14. *Let X be a set and R a equivalence relation on X, then X is the disjoint union of all equivalence classes.*

proof skeleton. use the proposition above.

□

Example 1.2.15 (examples for understanding equivalence relations)**.** Let $\mathbb{R}$ be the set and $=$ the equivalence relation between real numbers. Then $[x] = \{x\}$.

The connected components in a graph can be viewed as a equivalence class.

Zorn's lemma is important but difficult to understand. Let's do it.

Let X be a set, and R be a partial order relation, in the sense that 1) xRx, 2) $xRy, yRx \Rightarrow x = y$, and 3) $xRy, yRz \Rightarrow xRz$.

Example 1.2.16 (examples for understanding partial order relation)**.** $\leq$ is a partial order relation on $\mathbb{R}$.

Axiom 1.2.17 (Axiom of Choice. v.1)**.** *Let $(X_i)_{i \in I}$ be a collection of non-empty sets. Then we can always choose one element from each set.*

Axiom 1.2.18 (Axiom of Choice. v.2)**.** *Let $(X_i)_{i\in I}$ be a collection of non-empty sets. Then there exists a choice function $f : I \to \cup_{i\in I} X_i$.*

Theorem 1.2.19 (Zorn's Lemma)**.** *Let $(X, \leq)$ be a partially ordered set. Suppose that every totally ordered subset Y of X has an upper bound (i.e., $\exists u \in X(u \geq y, \forall y)$). Then X has a maximal element (i.e. $\exists m \in X(x \geq m \Rightarrow x = m)$).*

Zorn's Lemma and Axiom of Choice is equivalent, the lemma itself is difficult to prove. We will not prove it here. Refer to Paul Halmos's *Naive Set Theory* if you want to understand the whole story.

Zorn's Lemma can be used to show that

- Every vector space has a basis (in Matrix Analysis course, next semester).
- The product of compact spaces is compact (in this class).
- Every ideal of a ring is contained in a maximal ideal (in this class).

1.3 Further Reading

Mendelson, chapter 1.

SI112: Advanced Geometry	Spring 2018
Lecture 02 — Mar. 1st, Thursday	
Prof. Manolis	*Scribe*: Liangzu

2 Lecture 02

"*Only if it is open!*"

— who said it

2.1 Overview of This Lecture

After introducing Zorn's lemma and Axiom of Choice (see lecture note 1), we dive straight into the world of continuity, where ϵ and δ live. Following Meldelson, the concept of *continuity* is defined, and refined, with increasing abstraction. That is, we shortly review the real-valued continuous functions, and then define continuity on metric space. As the concepts (e.g., open ball, neighborhood) defined, the theorems get refined and become more and more abstract. Thankfully, all definitions and theorems devoloped in this lecture can be visualized and you can therefore see the geometric intuition behind the complicated manipulation of ϵ and δ.

2.2 Proof of Things

Definition 2.2.1 (Metric Space)**.** Metric Space is a set X together with a function $d : X \times X \to \mathbb{R}$ satisfying 1) $d(x, y) = 0 \iff x = y$, 2) $d(x, y) = d(y, x), \forall x, y \in X$, and 3) $d(x, z) \leq d(x, y) + d(y, z)$.

Definition 2.2.2 (norm on $\mathbb{R}^n$)**.** norm on $\mathbb{R}^n$ is $||\cdot|| : \mathbb{R}^n \to \mathbb{R}$ satisfying 1) $||x|| = 0 \iff x = 0$, 2) $||\alpha x|| = |\alpha| \cdot ||x||, \forall \alpha \in \mathbb{R}$, and 3) $||x + y|| \leq ||x|| + ||y||$.

You may consider property (3) of both norm $||\cdot||$ and metric d to be triangular inequality.

Example 2.2.3 (examples of norm)**.** 1) ℓ_2 norm: $||x||_2 = (\Sigma_{i=1}^n x_i^2)^{\frac{1}{2}}$, 2) ℓ_1 norm: $||x||_1 = (\Sigma_{i=1}^n |x_i|$, and 3) ℓ_∞ norm: $||x||_\infty = \max_i |x_i|$. See also Vector Norm and Matrix Norm in wikipedia.

Proposition 2.2.4. *Let $||\cdot||$ be a norm on $\mathbb{R}^n$. Then $(\mathbb{R}, d)$ is a metric space where $d(x, y) = ||x - y||$.*

proof skeleton. proving this proposition will get you familiar with the definitions above. Try it. □

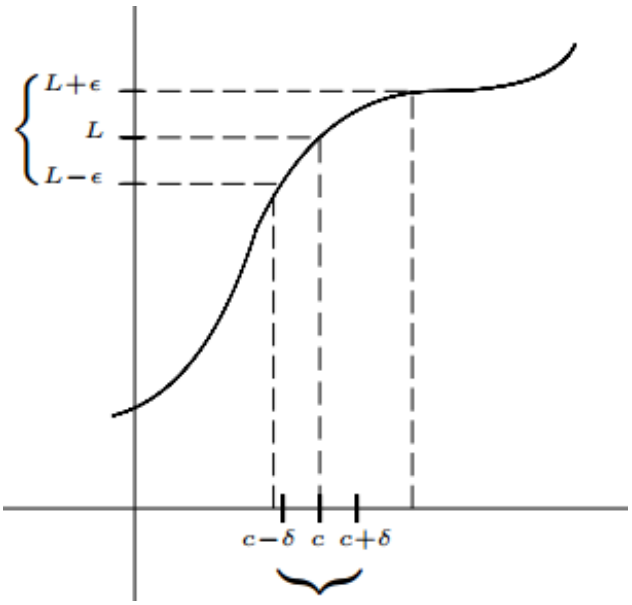

Figure 1: A function $f : \mathbb{R} \to \mathbb{R}$ is said to be *continuous* at a point $c \in \mathbb{R}$, if given $\epsilon > 0$, there is a $\delta > 0$, such that $|f(x) - f(c)| < \epsilon$ ($L = f(c)$ in the figure), whenever $|x - c| < \delta$. The function f is said to be *continuous* if it is continuous at each point of $\mathbb{R}$

.

Before learning the definition of continuity on metric space, you may want to review real-valued continuous functions which you've learned before.

Definition 2.2.5 (real-valued continuous function)**.** This is definition 3.1, chapter 2 in Medelson. See also figure 1.

Definition 2.2.6 (continuity on metric space, v.1)**.** Let (X, d) and (Y, d') be metric spaces. The function $f : X \to Y$ is said to be *continuous* at the point $\alpha \in X$, if for each $\epsilon > 0$, there exists $\delta_\epsilon > 0$ satisfying

$$d(x, \alpha) < \delta_\epsilon \Rightarrow d(f(x), f(\alpha)) < \epsilon. \tag{2.2.1}$$

Exercise 2.2.7. Try to find an error in the above definition (continuity on metric space, v.1).

Exercise 2.2.8. Try to compare two definitions above. Describe their differences in your mind.

Once we know the definition of continuity on metric space, we are ready to prove the continuity of some simple functions.

Theorem 2.2.9 (theorem 3.3, chapter 2 in Mendelson)**.** *Let (X, d) and (Y, d') be metric spaces. Let $f : X \to Y$ be a constant function, then f is continuous.*

proof skeleton. Let ϵ be given, try to find δ_ϵ satisfying the definition of continuity. □

Theorem 2.2.10 (theorem 3.4, chapter 2 in Medelson)**.** *Let (X, d) be a metric space. Then the identity function $i : X \to X$ is continuous.*

proof skeleton. Let ϵ be given, try to find δ_ϵ satisfying the definition of continuity. □

Theorem 2.2.11 (theorem 3.6, chapter 2 in Medelson)**.** *Let $(X, d), (Y, d'), (Z, d'')$ be metric spaces. Let $f : X \to Y$ be continuous at the point $a \in X$ and let $g : Y \to Z$ be continuous at the point $f(a) \in Y$. Then $gf : X \to Z$ is continuous at the point $a \in X$.*

proof skeleton. All you need is just patience. Step by step. Let ϵ be given, you have to find a $\delta > 0$ such that whenever $x \in X$ and $d(x, a) < \delta$, then $d''(g(f(x)), g(f(a))) < \epsilon$. □

Definition 2.2.12 (open ball, definition 4.1, chapter 2)**.** $B(a; \delta)$ is called an open ball, if it contains all the points $x \in X$ in X such that $d(a, x) < \delta$.

Exercise 2.2.13. $B(0.5; 0.5) = (0, 1)$ is an open ball on the metric space $\mathbb{R}$. Try to give a example of open ball on $\mathbb{R}^2$.

Lemma 2.2.14. *Let X, Y be sets, $f : X \to Y$ a function, and $S \subset X$, $T \subset Y$. Then we have $f(S) \subset T \iff S \subset f^{-1}(T)$.*

proof skeleton. Immediate! Just follow the definition. □

Theorem 2.2.15 (continuity on metric space, v.2, theorem 4.2/4.3, chapter 2)**.** *A function $f : (X, d) \to (Y, d')$ is continuous at a point $a \in X$ if and only if given $\epsilon > 0$ there is a $\delta > 0$ such that*

$$f(B(a; \delta)) \subset B(f(a); \epsilon)\,, \tag{2.2.2}$$

or

$$B(a; \delta) \subset f^{-1}(B(f(a); \epsilon))\,. \tag{2.2.3}$$

proof skeleton. If equation 2.2.2 is proved, the equation 2.2.3 is immediate because of the lemma above. Observe that the equation 2.2.2 is just the open ball version (v.2) of the definition of continuity. Try to translate the equation 2.2.1 into equation 2.2.2. □

Definition 2.2.16 (neighborhood, definition 4.4, chapter 2)**.** Let (X, d) be a metric space and $a \in X$. A subset N of X is called a *neighborhood* of a if there is a δ such that $B(a; \delta) \subset N$.

Lemma 2.2.17. *Let (X, d) be a metric space and $a \in X$. For each $\delta > 0$, the open ball $B(a; \delta)$ is a neighborhood of each of its points.*

proof skeleton. All is in figure 2. □

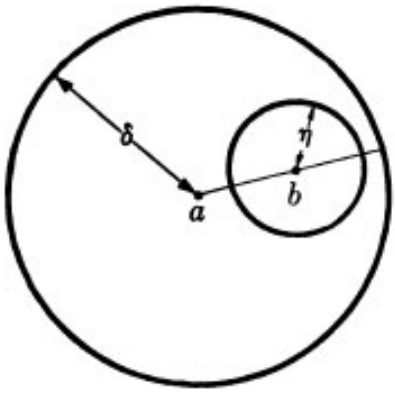

Figure 2: Choose arbitrarily a point $b \in X$, then you have to find a ball $B(b;\eta)$ contained in the ball $B(a;\delta)$

.

Exercise 2.2.18. Let the set S be a neighborhood of a point $a \in X$. Prove that the set containing S is also a neighborhood of a.

Theorem 2.2.19 (continuity on metric space, v.3, theorem 4.6, chapter 2)**.** *Let $f : (X, d) \to (Y, d')$. f is continuous at a point $a \in X$ if and only if for each neighborhood M of $f(a)$ there is a corresponding neighborhood N of a such that*

$$f(N) \subset M, \tag{2.2.4}$$

or equivalently,

$$N \subset f^{-1}(M). \tag{2.2.5}$$

Proof. Equation 2.2.4 implies equation 2.2.5. To prove the equation 2.2.4, you need to understand all of the previous definitions and theorems. You may use the continuity theorem in terms of open ball (v.2), so you need to think about what is the connection between an open ball and the neighborhood of a point. Also think pictorially. □

Theorem 2.2.20 (continuity on metric space, v.4, theorem 4.7, chapter 2)**.** *Let $f : (X, d) \to (Y, d')$. f is continuous at a point $a \in X$ if and only if for each neighborhood M of $f(a)$, $f^{-1}(M)$ is a neighborhood of a.*

proof skeleton. This is a homework problem. Notice that this theorem is quite similar to the previous one, with only one difference. We have two variables N and M as the neighborhoods of X and Y in continuity v.3, while only one variable M is used in continuity v.4 (we use $f^{-1}(M)$ to replace N). In this sense v.4 is terser, and easier to remember. □

2.3 Further Reading

Mendelson, chapter 2. Try to solve some problems at the end of chapter.
Bertrand Russell, *Logicomix*.

SI112: Advanced Geometry	Spring 2018
Lecture 03 — Mar. 6th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

3 Lecture 03

3.1 Overview of This Lecture

At the beginning of this lecture, we discussed the continuity in terms of neighborhoods (see lecture note 2). Then we introduced *limit* of a sequence in metric space (3.2.2), for which we reviewed limit of a sequence of real numbers (3.2.1). Of course, the concept of limit can also be described in the language of neighborhood (3.2.3). Once a new operation *limit* is defined, we want to see if this operation is consistent with the operations defined previously (e.g., Algebraic Limit Theorem). In this spirit, we arrive at theorem 3.2.4, which states the connection between continuous function and limit operation: continuous functions *preserve sequential convergence*.

3.2 Proof of Things

Definition 3.2.1 (limit of a sequence of real numbers.)**.** Let $a_1, a_2, \dots$ be a sequence of real numbers. A real number a is said to be the *limit* of the sequence $a_1, a_2, \dots$ if, given $\epsilon > 0$, there is a positive integer N such that, whenever $n > N$, $|a - a_n| < \epsilon$. In this event we shall also say that the sequence $a_1, a_2, \dots$ *converges* to a and write $\lim_n a_n = a$.

Definition 3.2.2 (limit of a sequence in a metric space)**.** Let (X, d) be a metric space. Let $a_1, a_2, \dots$ be a sequence of points of X. A point $a \in X$ is said to be *the limit of the sequence* $a_1, a_2, \dots$ if $\lim_n d(a, a_n) = 0$. Again in this event we shall say that the sequence $a_1, a_2, \dots$ *converges* to a and write $\lim_n a_n = a$.

Be careful. Try to understand $\lim_n d(a, a_n) = 0$.

Corollary 3.2.3. *Let (X, d) be a metric space and $a_1, a_2, \dots$ be a sequence of points of X. Then $\lim_n d(a, a_n) = 0$ for a point $a \in X$ if and only if for each neighborhood V of a there is an integer N such that $a_n \in V$ whenever $n > N$.*

proof skeleton. Immediate. From this corollary we can see that, if the limit of a sequence exists and N is big enough, the sequence will *eventually* fall into a neighborhood V of the limit a. Try to picture it on the real line. □

Theorem 3.2.4 (theorem 5.4, chapter 2)**.** *Let $(X, d), (Y, d')$ be metric spaces. A function $f : X \to Y$ is continuous at a point $a \in X$ if and only if, whenever $\lim_n a_n = a$ for a sequence $a_1, a_2, \dots$ of points of X, $\lim_n f(a_n) = f(a)$.*

proof skeleton. This theorem says that a continuous function *preserves sequential convergence*, i.e., a convergent sequence undergoing a function/transformation is still convergent, or, i.e., $\lim_n a_n = a \Rightarrow \lim_n f(a_n) = f(a) = f(\lim_n a_n)$.

On the one hand, suppose that f is continuous at a point $a = \lim_n a_n$, and there is a sequence $a_1, a_2, \dots$ of points of X (why we can suppose like this when proving this direction, what if there is no such sequences in X at all? *hint*: recall that how we prove $\emptyset \subset A$, where A is any set), we need to show $\lim_n f(a_n) = f(a)$. By Corollary 3.2.3, the sequence $a_1, a_2, \dots$ will eventually fall into any specified neighborhood of a, and of course, given that V is a neighborhood of $f(a)$, it will *eventually* fall into $f^{-1}(V)$, since $f^{-1}(V)$ is a neighborhood of a (why? by which theorem?). Hence the sequence $f(a_1), f(a_2), \dots$ will eventually fall into V (why?), which means $\lim_n f(a_n) = f(a)$ (why? by which theorem/corollary?).

On the other hand, suppose the function f preserves sequential convergence, where the sequence converges at a point a, you need to show f is continuous at a. It is proved in the lecture by proving that f is not sequential-convergence-preserving if f is not continuous. Following the lecture, you need to construct something like $(1, \frac{1}{2}, \dots, \frac{1}{n}, \dots)$, which is not convergent. □

Recall that a open ball is a neighborhood of each of its points (see lecture note 2, or pictures, or textbooks), we define *open set*, as an abstraction of open ball, to satisfy this important property.

Definition 3.2.5. A subset O of a metric space is said to be *open* if O is a neighborhood of each of its points.

Theorem 3.2.6 (theorem 6.2, chapter 2)**.** *A subset O of a metric space (X, d) is an open set if and only if it is a union of open balls.*

proof skeleton. Try it to get familiar with open set. □

Theorem 3.2.7 (theorem 6.3, chapter 2)**.** *Let $f : (X, d) \to (Y, d')$. Then f is continuous if and only if for each open set O of Y, the subset $f^{-1}(O)$ is an open subset of X.*

proof skeleton. To prove this theorem, you are invited to think about the connection between open set and neighborhood, just like previously we invite you to think about the relationship between open ball centered at a point a and neighborhood of the point a. □

Theorem 3.2.8 (theorem 6.4, chapter 2)**.** *Let (X, d) be a metric space. Then we have*

- *The empty set $\emptyset$ is open.*
- *X is open.*
- *If $O_1, O_2, \ldots, O_n$ is open, then $O_1 \cap \cdots \cap O_n$ is open.*
- *If for each $\alpha \in I$, O_α is an open set, then $\cup_{\alpha \in I} O_\alpha$ is open.*

proof skeleton. Immediate. □

3.3 Further Reading

2.5, 2.6 in Mendelson.

SI112: Advanced Geometry	Spring 2018
Lecture Note 4 — Mar. 8th, Thursday	
Prof.: Manolis	*Scribe*: Liangzu

SI112: Advanced Geometry	Spring 2018
Lecture 04 — Mar. 8th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

4 Lecture 04

"*We will have a quiz on Monday.*"

4.1 Overview of This Lecture

we discussed some examples of open ball, emphasizing that an open ball might not look like a ball at all (4.2.1). Keeping in the mind the notation of open set, an abstraction of open ball, it is natural to consider the complement of the open set, which we define as *closed set* (4.2.3). The definition of open set and closed set will lead to many important consequences, some of which (4.2.4, 4.2.9, 4.2.10) are explored in this lecture.

4.2 Proof of Things

Example 4.2.1. The "shape" of an open ball,

$$B(x,\epsilon) = \{y \in X | d(x,y) < \epsilon\},$$

where (X,d) is a metric space, depends on the metric d and the underlying space X. the name of open ball stems from $(\mathbb{R}^2, d)$ $(d(x,y) = ||x-y||_2)$, where an open ball looks like exactly a ball. However, it is not always the case.

If X itself doesn't contain a ball (e.g., $\mathbb{R}$), an open ball in X is of course doesn't look like a ball. Even if X contains balls (e.g., $X = \mathbb{R}^n$), an intentionally-designed metric d can make an open ball "not a ball" (e.g., discrete metric on any set X, $d(x,y) = ||x-y||_1$ on $\mathbb{R}^n$).

Exercise 4.2.2. Show that $d(A,B) = rank(A-B)$ is a metric on $\mathbb{R}^{m\times n}$.

Definition 4.2.3 (closed set, definition 6.5, chapter 2)**.** A subset F of a metric space is said to be *closed* if its complement, F^C, is open.

Definition 4.2.4 (limit point, definition 6.6, chapter 2)**.** Let A be a subset of a metric space X. A point $b \in X$ is called a *limit point* of A if every neighborhood of b contains a point of A different from b.

Exercise 4.2.5. Thinking of the intervals on the real line. Relates them to open set, closed set, and limit point. For example, given an interval $I = (0, 1)$, which is open. Then ask yourself, "is I open or closed? What's the limit points of I? Is 1.000000001 a limit point of I? How about 0.99999992317864?" Ask yourself the similar questions for the intervals $M = (0, 1], N = [0, 1]$.

Remark 4.2.6 (remark of limit point). The definition of *limit point* is somewhat weird. Here is my understanding.

1. First notice the term "every neighborhood". In the last lecture we've seen a description like this (see lecture note 3). We said that a convergent sequence $a_1, a_2, \dots$ with limit a will eventually falls into any specified neighborhood of a. In other words, for "every neighborhood" V_a of a, the sequence $a_1, a_2, \dots$ will eventually falls into V_a. That might be why we call it *limit point*.

2. Then we look at the entire definition. What does it mean that every neighborhood of b contains a point of A different from b. We are too lazy to care about *every neighborhood* of b. Can we have a neighborhood of b, which is, somewhat, *smallest*, contains a point of A different from b, and is included by all of other neighborhoods of b (we've known that if Q is a neighborhood of a and $Q \subset P$, then P is also a neighborhood of a)? In this way we may define *limit point* as "b is a limit point of A if the smallest neighborhood of b contains a point of A different from b". The answer is "No, we can not". Why?

Lemma 4.2.7. $A \cap B = \emptyset \iff A \subset B^C$.

proof skeleton. Immediate but seemingly irrelevant. Try to prove it both formally and graphically. □

Remark 4.2.8 (remark of the lemma 4.2.7). To prove the very first theorem 4.2.9 which relates closed set and limit point, we have no choice but use their definition. Closed set (B) is the complement of an open set (B^C). Open set (B^C) contains a neighborhood (A) of each of its points. Do you see it?

Theorem 4.2.9 (theorem 6.7, chapter 2)**.** *A subset F of X is closed if and only if F contains all limit points.*

proof skeleton. Try to prove it yourself by using the lemma 4.2.7. Do not read the proof in the book, which might make you cry. Read my proof below after some trials. In this proof

$N \in \mathcal{N}_a$ denotes that N is a neighborhood of a.

$$\begin{aligned} F \text{ is closed.} &\iff F^C \text{ is open.} \\ &\iff \forall a \in F^C, \exists N \in \mathcal{N}_a \text{ such that } a \in N \subset F^C. \\ &\iff \forall a \in F^C, \exists N \in \mathcal{N}_a \text{ such that } a \in N \text{ and } N \cap F = \emptyset. \qquad (4.2.1) \\ &\iff \forall a \in F^C, \ a \text{ is not a limit point of } F. \\ &\iff \text{all limit points of } F \text{ are contained in } F. \end{aligned}$$

□

Theorem 4.2.10 (theorem 6.8, chapter 2)**.** *In a metric space (X, d), a set $F \subset X$ is closed if and only if for each sequence $a_1, a_2, \ldots$ of points of F that converges to a point $a \in X$ we have $a \in F$.*

proof skeleton. When proving this theorem, you may invoke theorem 4.2.9, which is the first theorem we've proved about closed set and we do not want to go back to the its definition to prove other new theorems.

On the one hand, let F be closed. You may suppose there is a sequence $a_1, a_2, \cdots \in F$ and it converges to a (if there are no such sequences, you are done) and you have to prove $a \in F$. There are then two cases, the set $\{a_1, a_2, \ldots\}$ is finite, or it is an infinite set. Deal with them seperately.

On the other hand, you need to show F is closed if ..... what? □

4.3 Further Reading

2.5, 2.6 in Mendelson. Solve some problems in the book.

SI112: Advanced Geometry	Spring 2018
Lecture 05 — Mar. 13th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

5 Lecture 05

5.1 Overview of This Lecture

Closed set and limit point introduced in previous lecture are somewhat difficult to understand. It is hard to believe closed set, as a complement of open set, has many great properties, while the definition of limit point seems unmotivated. It is essential to introduce some theorems (5.2.1,5.2.3), as a concretion of open/closed set and limit point, to see what they truly are on the real line. In the end of this lecture we take a half-hour quiz containing 3 problems.

5.2 Proof of Things

Lemma 5.2.1 (lemma 5.6, chapter 2)**.** *Let b be the greatest lower bound of the non-empty subset A. Then, for each $\epsilon > 0$, there is an element $x \in A$ such that $x - b < \epsilon$.*

proof skeleton. Prove it by contradiction. □

Remark 5.2.2 (remark of lemma 5.2.1). Note that $S = [0, 1]$ ($S = (0, 1)$) is closed (open), 0 is the greatest lower bound of S, and it is also a limit point by definition. Also note that -0.0000001 is not a limit point of S. Is 0.7813 a limit point of S?

Corollary 5.2.3 (corollary 5.7, chapter 2)**.** *Let b be a greatest lower bound of the non-empty subset A of real numbers. Then there is a sequence $a_1, a_2, \ldots$ of real numbers such that $a_n \in A$ for each n and $\lim_n a_n = b$.*

proof skeleton. Prove it by using lemma 5.2.1 and by constructing something like $(1, \frac{1}{2}, \ldots, \frac{1}{n})$. □

Remark 5.2.4 (remark of corollary 5.2.3). Try to connect this corollary to the definition of limit point.

Definition 5.2.5 (definition 5.8, chapter 2)**.** Let (X, d) be a metric space. Let $a \in X$ and Let A be non-empty subset of X. The greatest lower bound of the set of numbers of the form $d(a, x)$ for $x \in A$ is called the *distance between a and A* and is denoted by $d(a, A)$.

Question 5.2.6. What's $d(a, A)$ for $A = [0, 1], a = 0.3$, for $A = [0, 1], a = -0.3$ and for $A = (0, 1), a = 0$?

Corollary 5.2.7 (corollary 5.9, chapter 2)**.** *Let (X, d) be a metric space, $a \in X$, and A a non-empty subset of X. Then there is a sequence $a_1, a_2, \ldots$ of points of A such that $\lim_n d(a, a_n) = d(a, A)$.*

proof skeleton. Use corollary 5.2.3 and definition 5.2.5. □

Exercise 5.2.8. Let (X, d) be a metric space, $A \subset X$. Prove or give a counterexample: for $a \in X$, $d(a, A) = 0$ if and only if $a \in A$ or a is a limit point of A.

Theorem 5.2.9 (theorem 6.9, chapter 2)**.** *A subset F of a metric space (X, d) is closed if and only if for each point $x \in X$, $d(x, F) = 0$ implies $x \in F$.*

proof skeleton. Recall that we've proved in the previous lecture that a set F is said to be closed if and only if F contains all its limit points. It is enough to show that F contains all its limit points if and only if for each point $x \in X$, $d(x, F) = 0$ implies $x \in F$, which follows from the exercise 5.2.8. □

Theorem 5.2.10 (theorem 6.10, chapter 2)**.** *Let $(X, d), (Y, d')$ be metric spaces. A function $f : X \to Y$ is continuous if and only if for each closed subset A of Y, the set $f^{-1}(A)$ is closed subset of X.*

proof skeleton. Immediate from open set characterization of continuity and $C(f^{-1}(A)) = f^{-1}(C(A))$. □

5.3 Further Reading

2.5, 2.6, 2.7 in Mendelson. Solve some problems in the book.

SI112: Advanced Geometry	Spring 2018
Lecture 06 — Mar. 15th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

6 Lecture 06

6.1 Overview of This Lecture

In previous lecture we introduced the notation of *topological equivalence* (6.2.1), and showed some examples (6.2.2, 6.2.3). Notice that *topological equivalence* relates two metric spaces, i.e., (X, d) and (Y, d'). It is natural to consider a special case, where $X = Y$. The corresponding theorems are 6.2.4, 6.2.6 and 6.2.8. However, does the concept, *topological equivalence*, even make sense? Theorem 6.2.12 gives a possible answer.

In the context of metric spaces, the various topological concepts such as continuity, neighborhood, and so on, may be characterized by means of open sets. Discarding the distance function and retaining the open sets of a metric space gives rise to a new mathematical object, called a *topological space* (6.2.14).

6.2 Proof of Things

Definition 6.2.1 (definition 7.6, chapter 2)**.** Two metric space (A, d_A) and (B, d_B) are said to be *topologically equivalent* or *homeomorphic* if there are inverse functions $f : A \to B$ and $g : B \to A$ such that f and g are continuous. In this event we say that the *topological equivalence is defined by* f *and* g.

Example 6.2.2 (homeomorphic spaces)**.** $X = \{0, 1\}, Y = \{0, 10\}$, $f : X \to Y$, $f(x) = 10x$, $g : Y \to X$, $g(y) = 0.1x$.

Example 6.2.3 (non-homeomorphic spaces)**.** (The explaination here for this example is from Real Mathematical Analysis) Consider the interval $[0, 2\pi) = \{x \in \mathbb{R} | 0 \leq x < 2\pi\}$ and define $f : [0, 2\pi) \to S^1$ to be the mapping $f(x) = (\cos x, \sin x)$, where S^1 is the unit circle in the plane, i.e., $S^1 = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$. The mapping f is a continuous bijection, but the inverse bijection is not continuous. For there is a sequence of points (z_n) on S^1 in the fourth quadrant that converges to $p = (1, 0)$ from below, and $f^{-1}(z_n)$ does not converge to $f^{-1}(p) = 0$. Rather it converges to 2π. Thus, f is a continuous bijection whose inverse bijection fails to be continuous. See figure 3.

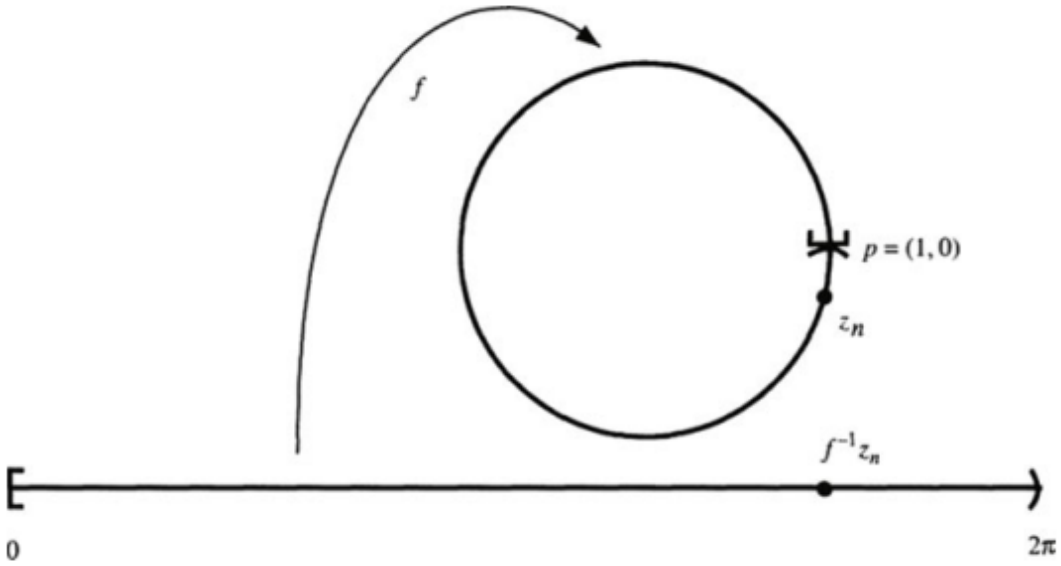

Figure 3: f wraps $[0, 2\pi)$ bijectively onto the circle.

Lemma 6.2.4 (lemma 7.8, chapter 2)**.** *Let (X, d) and (X, d') be two metric spaces. If there exists a number $K > 0$ such that for each $x, y \in X, d'(x, y) \leq Kd(x, y)$, then the identity mapping $i : (X, d) \to (X, d')$ is continuous.*

proof skeleton. Given $\epsilon > 0$, let $\delta = \frac{\epsilon}{K}$. □

Exercise 6.2.5 (homework exercise)**.** Find an example of X, d_1, d_2 such that i is not continuous.

Corollary 6.2.6 (corollary 7.9, chapter 2)**.** *Let (X, d) and (X, d') be two metric spaces. If there exist positive numbers K and K' such that for each $x, y \in X$, we have*

$$d'(x, y) \leq Kd(x, y) \leq K'Kd'(x, y)\,,$$

then the identity mappings define a topological equivalence between (X, d) and (X, d').

proof skeleton. Simply apply lemma 6.2.4 twice. □

Example 6.2.7. Isomorphism of categories.

Corollary 6.2.8. $(\mathbb{R}^n, ||\cdot||_2) \sim (\mathbb{R}^n, ||\cdot||_1) \sim (\mathbb{R}^n, ||\cdot||_\infty)$, *where* $||x||_2 = \sqrt{x_1^2 + \cdots + x_n^2}, ||x||_1 = |x_1| + \cdots + |x_n|, ||x||_\infty = \max_{i=1,\ldots,n} x_i$.

Proof. It is easy to see from the definition of the norm that

$$||x||_\infty \leq ||x||_2 \leq \sqrt{n}||x||_\infty$$

and

$$||x||_\infty \leq ||x||_1 \leq n||x||_\infty \,,$$

from which

$$||x||_2 \leq \sqrt{n}||x||_\infty \leq \sqrt{n}||x||_1 \leq \sqrt{n}n||x||_\infty \leq \sqrt{n}n||x||_2$$

immediately follows. We finished the proof. □

Lemma 6.2.9 (lemma for theorem 6.2.12)**.** *If a function $f : X \to Y$ is injective, then for each subset O of X, $f^{-1}(f(O)) = O$.*

true proof. Let O be a subset of X. Then for each $x \in O$, we have $f^{-1}(f(x)) = \{x\}$ since f is injective. It follows that $f^{-1}(f(O)) = O$. □

Lemma 6.2.10 (lemma for theorem 6.2.12)**.** *Let (X, d_1) and (X, d_2) be two metric spaces. Let $f : X \to Y$ and $g : Y \to X$ be inverse functions, i.e., $gf = id_X, fg = id_Y$. Then for each subset O of X, we have $f(O) = g^{-1}(O)$.*

true proof. Given a subset O of X, we have $g(f(O)) = O$ and hence $g^{-1}(g(f(O))) = g^{-1}(O)$. That is, $f(O) = g^{-1}(O)$. □

Lemma 6.2.11 (lemma for theorem 6.2.12)**.** *Let $f : X \to Y$ be a function and O be a subset of Y, then we have $f^{-1}(O^C) = (f^{-1}(O))^C$.*

true proof. For each $x \in X$, we have

$$\begin{aligned} x \in f^{-1}(O^C) &\iff f(x) \in O^C \\ &\iff f(x) \notin O \\ &\iff x \notin f^{-1}(O) \\ &\iff x \in (f^{-1}(O))^C, \end{aligned} \tag{6.2.1}$$

which implies that $f^{-1}(O^C) = (f^{-1}(O))^C$. □

Theorem 6.2.12 (theorem 7.10, chapter 2)**.** *Let (X, d_1) and (X, d_2) be two metric spaces. Let $f : X \to Y$ and $g : Y \to X$ be inverse functions, i.e., $gf = id_X, fg = id_Y$. Then the following four statements are equivalent:*

1. *f and g are continuous;*
2. *A subset O of X is open if and only if $f(O)$ is an open subset of Y.*
3. *A subset F of X is closed if and only if $f(F)$ is a closed subset of Y.*
4. *For each $a \in X$ and subset N of X, N is a neighborhood of a if and only if $f(N)$ is a neighborhood of $f(a)$.*

true proof. We will prove this theorem in detail. The lemmas above will be extensively used.

(1 $\Rightarrow$ 2) Assume that f and g are continuous. On the one hand, if $f(O)$ is an open subset of Y, then $O = f^{-1}(f(O))$ (lemma 6.2.9) is an open subset of X (f is continuous). On the other hand, if O is an open subset of X, then $f(O) = g^{-1}(O)$ (lemma 6.2.10) is open in Y (g is continuous), which completes the proof.

(2 $\Rightarrow$ 1) It is left to you as an exercise.

(2 $\Rightarrow$ 3) Suppose that (2) holds. On the one hand, if $f(F)$ is a closed subset of Y, which means $f(F)^C$ is open in Y, then, by lemma 6.2.10 and lemma 6.2.11,

$$f(F^C) = g^{-1}(F^C) = (g^{-1}(F))^C = (f(F))^C$$

is open in Y, which, by (2), means F^C is open in X and hence F is a closed subset of X. On the other hand, if F is closed in X, which means F^C is open in X and hence $f(F^C)$ is open in Y by (2). It follows that

$$(f(F))^C = (g^{-1}(F))^C = g^{-1}(F^C) = f(F^C)$$

is open in Y and hence $f(F)$ is a closed subset of Y, as desired.

(3 $\Rightarrow$ 2) Immediate from above proof. It is left to you as an exercise.

(3 $\iff$ 4) Unnecessarily verbose! We avoid this (Why can we skip it? Why is it unreasonable to prove this direction?).

(2 $\Rightarrow$ 4) Suppose that (2) holds. Then for each $a \in X$ and $N \subset X$, N is a neighborhood of a if and only if N contains an open set O containing a if and only if $f(N)$ contains an open set $O' = f(O)$ containing $f(a)$ (since $a \in O \subset N \iff f(a) \in f(O) \subset f(N)$) if and only if $f(N)$ is a neighborhood of $f(a)$.

(4 $\Rightarrow$ 1) Suppose that (4) holds. Then f is continuous, since for each $a \in X$ and each neighborhood $f(f^{-1}(U)) = U$ of $f(a)$, $f^{-1}(U)$ is a neighborhood of a. Similarly, g is continuous, since for each $b \in Y$ and each neighborhood V of $g(b)$, $g^{-1}(V) = f(V)$ is a neighborhood of $b = f(g(b))$.

□

Remark 6.2.13 (remark for theorem 6.2.12). The proof for theorem 6.2.12 we give here is too long! It turns out that there is a simpler and therefore more elegant one.

simpler proof. This proof is based on the following observation. When proving

$$(1) \iff (2)\,,$$

we observe that if (1) holds, then, by lemma 6.2.9, one direction of (2) is what we've already proved (which direction?)! Can you transfer another direction, by again applying some lemmas above, into something we've already done before? The same is true for (1) if (2) holds. Exactly the same is again true for (1) $\iff$ (3) and for (1) $\iff$ (4).

(1 $\iff$ 2) Obvious.

(1 $\iff$ 3) Obvious.

(1 $\iff$ 4) Obvious.

we finished the proof. □

Definition 6.2.14 (definition 2.1, chapter 3)**.** Let X be a non-empty set and $\mathcal{J}$ a collection of subsets of X such that:

1. $X \in \mathcal{J}$.
2. $\emptyset \in \mathcal{J}$.
3. if $O_1, O_2, \ldots, O_n \in \mathcal{J}$, then $O_1 \cap O_2 \cap \cdots \cap O_n \in \mathcal{J}$.
4. If $O_i \in \mathcal{J}$ for each $i \in I$, then $\cup_{i\in I} O_i \in \mathcal{J}$.

The pair of objects $(X, \mathcal{J})$ is called a *topological space*. The set X is called the *underlying set*. The collection $\mathcal{J}$ is called the *topology* on the set X, and the members of $\mathcal{J}$ are called *open* sets.

Remark 6.2.15 (remark of definition 6.2.14). This definition of topological space is in fact a theorem in metric space. Note that, here and in what follows, *open set* is nothing more than an element of the set $\mathcal{J}$. It is no longer (at least not now) a neighborhood of each of its points, and neighborhood is what we haven't defined yet. You have to forget the past to better start. We will eventually from this definition develop many theorems, which are what you've already been familiar with. Hence don't panic and stay tuned. Also note that our definition of topological space is in terms of open set. An alternative definition could be in terms of closed set. See the next example.

Example 6.2.16. Let $X = \mathbb{C}^n$. $Y \subset \mathbb{C}^n$ is defined to be closed if there exists $p_1, \ldots, p_l \in \mathcal{B}$, where $\mathcal{B} = \mathbb{C}[x_1, \ldots, x_n]$ is the ring of polynomial function on $\mathbb{C}^n$, such that

$$Y = \{z \in \mathbb{C}^n | p_1(z) = \cdots = p_l(z) = 0\} =: \mathbb{Z}(p_1, \ldots, p_l).$$

To show that the closed sets of $\mathbb{C}^n$ defined in this way give a topology on $\mathbb{C}^n$ (Zariski Topology), we need to show that

1. $\mathbb{C}^n$ is closed.
2. $\emptyset$ is closed.
3. The intersection of infinitely many Y_i is closed.
4. The union of finitely many Y_i is closed.

6.3 Further Reading

2.7, 3.1, 3.2 in Mendelson. Solve some problems in the book.

SI112: Advanced Geometry	Spring 2018
Lecture 07 — Mar. 20th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

7 Lecture 07

7.1 Overview of This Lecture

In the previous lecture we defined topological space $(X, \mathcal{J})$. To understand it, you may want to see some examples. Have a look at definition 2.1, followed by many EXAMPLES in chapter 3. See also the topology of R and Topological Space in wikipedia.

Note that open set is merely an element of the set $\mathcal{J}$, and neighborhood, closed set are something we haven't defined yet. And we will not. Instead, we invite you to define them in the exercises (7.2.1, 7.2.2, and 7.2.3).

We introduce many new concepts in this lecture. It is recommended to read the textbook or wikipedia to understand them.

7.2 Proof of Things

Exercise 7.2.1 (definition of closed set)**.** An element O of $\mathcal{J}$ is called an open set of X. So what's the corresponding closed set of X, in terms of O? Is your definition for closed set well-defined?

Exercise 7.2.2 (definition of neighborhood)**.** The definition of neighborhood in metric space (X, d) is as follows: A subset N of X is called a neighborhood of a if there is a δ such that $B(a; \delta) \subset N$. That is, the neighborhood of a contains an open ball of a. But in topological space, we do not have open ball any more. We have only open set, which is an abstraction of open ball. Now give your definition of neighborhood in topological space (definition 2.2, chapter 3). Again, is your definition for neighborhood well-defined?

Exercise 7.2.3 (neighborhood and open set)**.** Let $(X, \mathcal{J})$ be a topological space. Prove it: a subset O of X is open if and only if O is a neighborhood of each of its points. (This is corollary 2.3 in chapter 3, and is what you did before in metric space.)

Definition 7.2.4 (subspace topology, definition 6.1, chapter 3)**.** Let $(X, \mathcal{J})$ be topological space and $Y \subset X$. Then $(Y, \mathcal{J}|_Y)$, where $\mathcal{J}|_Y = \{U | U = Y \cap O, O \in \mathcal{J}\}$, is a subspace topology. An element $U \in \mathcal{J}|_Y$ is an open set in Y, or *relatively open* in Y.

Remark 7.2.5 (remark for definition 7.2.4). The main motivation to define *subspace topology* is as follows. Let $i : Y \to X$ be an inclusion map. We want to give Y a topology such that i is continuous.

Example 7.2.6 (example for definition 7.2.4)**.** Let $X = \mathbb{R}, Y = [0, 1)$ (with standard topology). Then $[0, 0.2)$, obviously not open in X, is open in $\mathcal{J}|_Y$.

Definition 7.2.7 (limit point)**.** Let $(X, \mathcal{J})$ be a topological space and $A \subset X$. We say $x \in X$ is a *limit point* of A if for each neighborhood N of x, we have $N/\{x\} \cap A \neq \emptyset$.

Remark 7.2.8 (remark for definition 7.2.7). As you should verify, this definition of limit point in topological space is exactly the same as in metric space, with only one difference (what's the difference?). Also note that Mendelson devoloped theorems for topological space, without defining limit point. Here we take a different approach, and we will finally arrive at the same place as Mendelson.

Definition 7.2.9 (closure of a set)**.** Let A be a subset of a topological space. A point x is said to be in the *closure* of A if $x \in A$ or x is a limit point of A. The closure of A is denoted by $\bar{A}$.

Corollary 7.2.10 (corollary for definition 7.2.9)**.** $A \subset \bar{A}$.

Exercise 7.2.11 (exercise for definition 7.2.9)**.** Compare the definition here to the one in Mendelson (definition 4.3, chapter 2). Are the two definitions equivalent? Prove it!

Lemma 7.2.12 (lemma 4.3, chapter 3)**.** *Given a subset A of a topological space and a closed set F containing A, $\bar{A} \subset F$.*

proof skeleton. Recall that $\bar{A}$ contains all the points of A and all the limit points of A. Given $A \subset F$ and to prove $\bar{A} \subset F$, it is enough to show that all limit points of A are in F, where F is closed. (We have done something similar, remember it? Theorem 6.7 in chapter 2, and also in the lecture note 4. Check it!) In short, for each $x \in F^C \subset A^C$, that F^C is open means that F^C is a neighborhood of x, from which, given $F^C \subset A^C \iff F^C \cap A = \emptyset$, it follows that x is not a limit point of A. That is, for each $x \in F^C$, x is not a limit point of A. That is, all limit points of A are contained in F. We finished the proof. □

Lemma 7.2.13 (lemma 4.4, chapter 3)**.** *Given a subset A of a topological space and a point $x \notin \bar{A}$, then $x \notin F$ for some closed set F containing A.*

proof skeleton. Lemma 7.2.12 gives you a closed set F containing A, while this lemma, in contrast, requires you to find a closed set F, which contains A. Think it: if $x \notin \bar{A}$, that is, $x \notin A$ and x is not a limit point of A, what will happen? This will lead you to the desired closed set F. □

Theorem 7.2.14 (theorem 4.5, chapter 3)**.** *Given a subset A of a topological space, $\bar{A} = \cap_{a\in I} F_a$ where $\{F_a\}_{a\in I}$ is the family of all closed sets containing A.*

proof skeleton. Immediate from lemma 7.2.12 and lemma 7.2.13, given that you understand the lemmas and know how to prove equality of two sets. □

Corollary 7.2.15 (corollary from theorem 7.2.14)**.** *$\bar{A}$ is closed.*

Theorem 7.2.16 (theorem 4.6, chapter 3)**.** *A is closed if and only if $A = \bar{A}$.*

proof skeleton. If $A = \bar{A}$, then A is closed since $\bar{A}$ is closed. If A is closed, then from lemma 7.2.12 and $A \subset \bar{A}$ we have $A = \bar{A}$. □

Definition 7.2.17 (Interior of A)**.** The interior of A, denoted by $int(A)$, is the largest open set contained in A.

Definition 7.2.18 (Boundary of A)**.** The boundary of A, denoted by ∂A, is defined as

$$\partial A = \bar{A} \cap (int(A))^C .$$

Remark 7.2.19. The concept of interior and boundary is heavily used in *Convex Geometry*, while closure oftentimes appears in the context of *Algebraic Geometry*.

Definition 7.2.20 (dense)**.** $A \subset X$, A is dense in X if $\bar{A} = X$.

Example 7.2.21. $\mathbb{Q}$ is dense in $\mathbb{R}$ since $\bar{\mathbb{Q}} = \mathbb{R}$.

Definition 7.2.22 (Hausdorff Space, definition 3.3, chapter 3)**.** A topological space $(X, \mathcal{J})$ is called a *Hausdorff space* or is said to satisfy the *Hausdorff axiom*, if for each pair a, b of distinct points of X, there are neighborhoods N and M of a and b respectively, such that $N \cap M = \emptyset$. *Hausdorff space* $(X, \mathcal{J})$ is also called *separable space*.

Example 7.2.23. $\mathbb{R}^n$ with standard topology is Hausdorff.

Example 7.2.24. R with Zariski topology is not seperable.

Definition 7.2.25 (Irreducible Space)**.** A topological space X is called *irreducible* if X is not the union of any two proper closed sets, i.e., there are no closed subsets $Y_1, Y_2 \subsetneq X$ such that $X = Y_1 \cup Y_2$.

Example 7.2.26. $\mathbb{R}$ is reducible.

Remark 7.2.27. If X is Hausdorff then X is reducible.

Theorem 7.2.28. *If X is irreducible, O is open in X, then O is irreducible and dense.*

Proof. You may want to prove it before the next lecture. □

7.3 Further Reading

3.1-3.6 in Mendelson.

SI112: Advanced Geometry	Spring 2018
Lecture 08 — Mar. 22th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

8 Lecture 08

8.1 Overview of This Lecture

We reviewed the definition of irreducible space (8.2.1) and from it we then developed some theorems (8.2.3, 8.2.4 and 8.2.6) absent in Mendelson, for which full proofs are given. We proceeded by introducing the product of topological spaces, discussing and exploring why it is defined as it is (8.2.10, 8.2.12). Finally we played a bit (?), which ends this lecture.

8.2 Proof of Things

Definition 8.2.1 (Irreducible Space)**.** If X is not the union of two proper closed sets, i.e., there are not $Y_1, Y_2 \subsetneq X$, which are closed, such that $X = Y_1 \cup Y_2$.

Example 8.2.2. Zariski Topology on $\mathbb{R}^2$ is irreducible. Y_1, Y_2 are curves and they can not cover the entire space.

Proposition 8.2.3. *Let A, B be a subset of a topological space X, then we have $\overline{A \cup B} = \overline{A} \cup \overline{B}$.*

Proof. For each $x \in X$, if $x \in A \cup B$, then we have $x \in \overline{A \cup B} \iff x \in \overline{A} \cup \overline{B}$ (as you can easily verify). Hence, to prove $\overline{A \cup B} = \overline{A} \cup \overline{B}$, it is enough to show that x is a limit point of $A \cup B$ if and only if x is a limit point of A or x is a limit point of B (why?). Let $N \in \mathcal{N}_x$ denotes that N is a neighborhood of x, we finished the proof since

$$\begin{aligned} x \text{ is a limit point of } A \cup B &\iff \forall N \in \mathcal{N}_x,\ N/\{x\} \cap (A \cup B) \neq \emptyset \\ &\iff \forall N \in \mathcal{N}_x,\ (N/\{x\} \cap A) \cup (N/\{x\} \cap B) \neq \emptyset \\ &\iff \forall N \in \mathcal{N}_x,\ N/\{x\} \cap A \neq \emptyset \text{ or } N/\{x\} \cap B \neq \emptyset \\ &\iff x \text{ is a limit point of } A \text{ or } x \text{ is a limit point of } B\ . \end{aligned} \tag{8.2.1}$$

□

Theorem 8.2.4. *Let X be an irreducible space, and $O \subsetneq X$ and O is open in X. Then O is irreducible and dense.*

Proof. We will first prove that O is dense and then O irreducible.

Saying that O is dense is equivalent to saying that $\overline{O} = X$. Observing that

$$X = O \cup O^C = \overline{O} \cup O^C \text{ (why?)},$$

where O^C and $\overline{O}$ closed subset of X and O^C is proper, $X = \overline{O}$, for $\overline{O} \subsetneq X$ contradicting the fact that X is irreducible.

Let F_1, F_2 be (relatively) closed in O and $O = F_1 \cup F_2$, we want to show that $O = F_1$ or $O = F_2$, from which it will follow that O is irreducible. By the definition of relative closeness, there are closed sets Z_1, Z_2 in X such that $F_1 = O \cap Z_1, F_2 = O \cap Z_2$. Then we have

$$\begin{aligned} O = (O \cap Z_1) \cup (O \cap Z_2) = O \cap (Z_1 \cup Z_2) &\Rightarrow O \subset Z_1 \cup Z_2 \\ &\Rightarrow \overline{O} \subset Z_1 \cup Z_2 \\ &\Rightarrow X = \overline{O} \subset Z_1 \cup Z_2 \subset X \\ &\Rightarrow X = Z_1 \cup Z_2 \,, \end{aligned} \tag{8.2.2}$$

which means, by irreducibility of X,

$$\begin{aligned} X = Z_1 \text{ or } X = Z_2 &\Rightarrow O \subset Z_1 \text{ or } O \subset Z_2 \\ &\Rightarrow F_1 = O \cap Z_1 = O \text{ or } F_2 = O \cap Z_2 = O \,. \end{aligned} \tag{8.2.3}$$

We finished the proof. □

Remark 8.2.5. Theorem 8.2.4 shows that, given an irreducible space X, A "smaller" set $O \subset X$ is also irreducible (and dense) if O is open. The next theorem (8.2.6), in contrast, shows that a "larger" set is irreducible if the smaller one promises to be irreducible.

Theorem 8.2.6. *If $Y \subset X$, where X is a topological space, and Y is irreducible, then $\overline{Y}$ is irreducible.*

Proof. Similar to proving the irreducibility in theorem 8.2.4, given that $Z_1 \cap \overline{Y}$ and $Z_2 \cap \overline{Y}$ are closed in $\overline{Y}$, where Z_1 and Z_2 are closed in X, and $\overline{Y} = (Z_1 \cap \overline{Y}) \cup (Z_2 \cap \overline{Y}) = (Z_1 \cup Z_2) \cap \overline{Y}$, we need to show that $\overline{Y} = (Z_1 \cap \overline{Y})$ or $\overline{Y} = (Z_2 \cap \overline{Y})$.

From $\overline{Y} = (Z_1 \cup Z_2) \cap \overline{Y}$ we have

$$\begin{aligned} \overline{Y} \subset Z_1 \cup Z_2 &\Rightarrow Y \subset Z_1 \cup Z_2 \\ &\Rightarrow Y = (Z_1 \cup Z_2) \cap Y = (Z_1 \cap Y) \cup (Z_2 \cap Y) \,, \end{aligned} \tag{8.2.4}$$

which, by irreducibility of Y, means that

$$\begin{aligned} Y = Z_1 \cap Y \text{ or } Y = Z_2 \cap Y &\iff Y \subset Z_1 \text{ or } Y \subset Z_2 \\ &\iff \overline{Y} \subset Z_1 \text{ or } \overline{Y} \subset Z_2 \\ &\iff \overline{Y} = Z_1 \cap \overline{Y} \text{ or } \overline{Y} = Z_2 \cap \overline{Y} \,. \end{aligned} \tag{8.2.5}$$

We finished the proof.

□

Example 8.2.7 (Zariski topology on $\mathbb{R}^2$)**.** Let $(0,0) = \mathbb{Z}(x^2+y^2) = \mathbb{Z}(x,y)$ (This is Punctured Plane).

Exercise 8.2.8 (Zariski topology on $\mathbb{R}^2$)**.** Let $Y = \mathbb{Z}(y-x^2)$. O is open in Y. How does it look like (check the pictures on the board, i.e., have a look at the board in the picture)?

Lemma 8.2.9 (lemma 3.7.1)**.** *Let $\mathcal{B}$ be a collection of subsets of a set X with the property that $\emptyset \in \mathcal{B}, X \in \mathcal{B}$, and finite intersection of elements of $\mathcal{B}$ is again in $\mathcal{B}$. Then the collection $\mathcal{J}$ of all subsets of X which are unions of elements of $\mathcal{B}$ is a topology.*

proof skeleton. Omitted. □

Exercise 8.2.10 (wrong definition for product of topological space)**.** Let $(X_1, \mathcal{J}_1), \ldots, (X_n, \mathcal{J}_n)$ be topological spaces, and let $X = \prod_{j=1}^n X_j$ and $\mathcal{J} = \prod_{j=1}^n \mathcal{J}_j$, i.e.,

$$X = \{(x_1, x_2, \ldots, x_n) | x_i \in X_i\}, J = \{(O_1, O_2, \ldots, O_n) | O_i \in \mathcal{J}_i\}.$$

Is $(X, \mathcal{J})$ a topological space? i.e.,

1. Is it that $\emptyset \in \mathcal{J}$? Yes, it is.
2. Is it that $X \in \mathcal{J}$? Yes, it is.
3. For each $O_1, \ldots, O_n \in \mathcal{J}$, is it that $O_1 \cap \cdots \cap O_n \in \mathcal{J}$? Yes it is. You need to prove something like
$$(O_1, O_2, \ldots, O_n) \cap (O_1', O_2', \ldots, O_n') = (O_1 \cap O_1', O_n \cap O_2', \ldots, O_n \cap O_n').$$
4. Is it that (fill the gap here)? No, it isn't. Review the picture on the board.

Remark 8.2.11 (remark for exercise 8.2.10). The first 3 clauses are easy to verify. the clause 4 is fundamentally the reason that (1) the union of two linear subspaces is not neccesarily a linear subspace and that (2) the union of two groups is not neccesarily a group.

Definition 8.2.12 (product of topological spaces, definition 3.7.2)**.** The topological space $(X, \mathcal{J})$, where $\mathcal{J}$ is the collection of subsets of X that are unions of sets of the form $O_1 \times O_2 \times \cdots \times O_n$, each O_i and open subset of X_i, is called *product* of the topological spaces $(X_i, \mathcal{J}_i), i = 1, 2, \ldots, n$.

Remark 8.2.13 (remark for 8.2.12). $(X, \mathcal{J})$ defined in this way is indeed a topology, as you should verify (*hint:* use lemma 8.2.9).

Definition 8.2.14 (neighborhood in product topology)**.** Let $(X, \mathcal{J})$ be a product of topological spaces. A set $N \subset X$ is said to be a neighborhood of a point $x \in X$, if there is an open set $O \in \mathcal{J}$ such that $a \in O \subset N$.

Exercise 8.2.15 (neighborhood in product topology, proposition 3.7.4)**.** Prove it: In a topological space $X = \prod_{j=1}^{n} X_j$, a subset N is a neighborhood of a point $a = (a_1, a_2, \ldots, a_n) \in N$ if and only if N contains a subset of the from $N_1 \times N_2 \times \cdots \times N_n$, where each N_i is a neighborhood of a_i.

Proposition 8.2.16. *The projection map.* $p_i : \prod_{j=1}^{n} X_j \to X_i$*, is continuous.*

Proof. Easy. For each open set $O \subset X_i$, what is the inverse image of O under p_i? i.e., what's $p_i^{-1}(O)$? □

Remark 8.2.17. Let's play a little bit. X_1, X_2 metric spaces. $(X_i, d_i) \to X_i, \mathcal{J}_i \to (X, \mathcal{J})$.

Zariski topology is not metrizable.

8.3 Further Reading

3.7 in Mendelson.

SI112: Advanced Geometry	Spring 2018
Lecture 09 — Mar. 27th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

9 Lecture 09

9.1 Overview of This Lecture

In this lecture we introduce an important concept: *compactness*. After introducing its definition (9.2.4), we devolops theorems, as usual, that relate compactness and other important topological concepts, e.g., compactness in relative topology (9.2.8), neighborhood (9.2.10), continuity (9.2.12) and closedness (9.2.15,9.2.17).

We will spend 2 lectures on compactness (this and the next lecture).

9.2 Proof of Things

Definition 9.2.1 (covering, definition 5.2.1)**.** Let X be a set, B a subset of X, and $\{A_i\}_{i\in I}$ is called a *covering* of B or is said to *cover* B if $B \subset \cup_{i\in I} A_i$. If, in addition, the indexing set I is finite, $\{A_i\}_{i\in I}$ a *finite covering* of B.

Definition 9.2.2 (subcovering, definition 5.2.2)**.** Let X be a set and let $\{A_i\}_{i\in I}, \{B_k\}_{k\in J}$ be two coverings of a subset C of X. If for each $i \in I, A_i = B_k$ for some $k \in J$, then the covering $\{A_i\}_{i\in I}$ is called a *subcovering* of the covering $\{B_k\}_{k\in J}$. Note that this definition is not introduced in the lecture.

Exercise 9.2.3 (open covering, definition 5.2.3)**.** An *open covering* of a set B is a union of open set which covers B. Try to give it a rigorous definition. Or have a look at definition 5.2.3 in Mendelson.

Definition 9.2.4 (definition 5.2.4)**.** A topological space X is said to be *compact* if for each open covering $\{U_i\}_{i\in I}$ of X there is a finite subcovering $U_{i_1}, \ldots, U_{i_n}$.

Remark 9.2.5 (remark for definition 9.2.4). Compactness allows to study global properties by looking at a finite number of neighborhood. Well, the concept of compactness is somewhat elusive and unmotivated. Have a look at this paper if you are interested in.

Remark 9.2.6 (remark for definition 9.2.4). Given the definition of compactness, how to prove a given set, say X, is compact or not? To prove X is compact, you need to show that **for each** *open* covering of X, there is a *finite* subcovering. To prove that X is not compact,

in contrast, you need to give an counterexample, i.e., there exists a open covering of X such that there are no subcoverings.

Definition 9.2.7 (definition 5.2.5)**.** A subset C of a topological space X is said to be *compact*, if C is a compact topological space in the relative topology.

Exercise 9.2.8 (theorem 5.2.6)**.** Prove it: A subset C a topological space X is compact if and only if for each open covering $\{U_i\}_{i\in I}$, U_i open in X, there is a finite subcovering $U_{i_1}, U_{i_2}, \ldots, U_{i_n}$ of C.

Remark 9.2.9 (remark for exercise 9.2.8). This exercise is theorem 5.2.6 in Mendelson. We skipped it in this lecture. You can prove it by yourself. Use the definition of relative topology and compactness.

Theorem 9.2.10 (theorem 5.2.7)**.** *A topological space X is compact if and only if, whenever for each $x \in X$ a neighborhood N_x of x is given, there is a finite number of points $x_1, x_2, \ldots, x_n$ of X such that $X = \cup_{i=1}^n N_{x_i}$.*

Proof. On the one hand, suppose X is compact. For each $x \in X$ there is a neighborhood N_x of x (why?). Hence for each x, there is an open set U_x such that $x \in U_x \subset N_x$ and $\{U_x\}_{x\in X}$ is an open covering of X. Since X is compact there is a finte subcovering $U_{x_1}, U_{x_2}, \ldots, U_{x_n}$, i.e., $X = \cup_{i=1}^n U_{x_i}$. But $U_{x_i} \subset N_{x_i}$ for each i, hence $X = \cup_{i=1}^n N_{x_i}$.

On the other hand, suppose whenever for each $x \in X$ a neighborhood N_x of x is given, there is a finite number of points $x_1, x_2, \ldots, x_n$ of X such that $X = \cup_{i=1}^n N_{x_i}$. We want to show that X is compact. The below is a **wrong** proof.

For each $x \in X$ there is an open set O_x in X containing x (why?), which is a neighborhood N_x of x, then we have $X = \cup_{x\in X} O_x = \cup_{x\in X} N_x$. By our hypothesis, there are points $x_1, x_2, \ldots, x_n$ of X such that $X = \cup_{i=1}^n N_{x_i} = \cup_{i=1}^n O_{x_i}$. Hence X is compact.

Why is this proof wrong? The problem here is that we have to start with an **arbitrary** open covering $\{U_i\}_{i\in I}$ of X, then we need to show that there is a finite subcovering. Since $\{U_i\}_{i\in I}$ covers X, for each $x \in X$ we have $x \in U_i$ for some $i \in I$. Notice here that different x can be in the same U_i, i.e., it is possible that $x_1, x_2 \in X$ and $x_1 \in U_i, x_2 \in U_i$ for some $i \in I$. To rephrase, for each $x \in X$, there is an $i = i(x)$ such that $x \in U_i$, which is a neighborhood of x. Let $N_x = U_i$, then by our hypothesis, there are points $x_1, x_2, \ldots, x_n$ of X such that $N_{x_i} = U_{i(x_i)}, i = 1, 2, \ldots, n$ covers X, and hence X is compact. □

Theorem 9.2.11 (theorem 5.2.8)**.** *A topological space is compact if and only if whenever a family $\cap_{i\in I} A_i = \emptyset$ of closed sets is such that $\{A_i\}_{i\in I}$ then there is a finite subset of indices $\{i_1, i_2, \ldots, i_n\}$ such that $\cap_{k=1}^n A_{i_k} = \emptyset$.*

proof skeleton. Use the definition of compactness and "the complement of a closed set is open". □

Theorem 9.2.12 (theorem 5.2.9)**.** *Let $f : X \to Y$ be continuous and let A be a compact subset of X. Then $f(A)$ is a compact subset of Y.*

Proof. This theorem shows that continuous functions preserve compactness.

To show that $F(A)$ is a compact subset of Y, let's start with an arbitrary open covering $\{V_i\}_{i\in I}$ of $f(A)$, i.e., $f(A) \subset \cup_{i\in I} V_i$. Then we have $A \subset f^{-1}(f(A)) \subset \cup_{i\in I} f^{-1}(V)$, which means that $\{f^{-1}(V_i)\}_{i\in I}$ is a covering of A. In addition, since f is continuous and V_i is open for each $i \in I$, $\{f^{-1}(V_i)\}_{i\in I}$ is an open covering of A. Since A is compact, there is a finite subcovering $f^{-1}(V_{i_1}), f^{-1}(V_{i_2}), \ldots, f^{-1}(V_{i_n})$ of A, i.e., $A \subset \cup_{k=1}^{n} f^{-1}(V_{i_k})$.

Remember that we want to show that there is a finite covering of $f(A)$. By theorem 9.2.8, it is enough to show that $f(A) \subset \cup_{k=1}^{n} V_{i_k}$. Does $A \subset \cup_{k=1}^{n} f^{-1}(V_{i_k})$ imply $f(A) \subset \cup_{k=1}^{n} V_{i_k}$? prove it!

□

Corollary 9.2.13 (corollary 5.2.10)**.** *Let the topological spaces X and Y be homeomorphic, then X is compact if and only if Y is compact.*

Example 9.2.14. The open interval $(0, 1)$ is not compact. To show this, we need to construct a covering of $(0, 1)$ that does not have a finite subcovering. (*hint:* construct something like $\{1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots\}$.)

Theorem 9.2.15 (theorem 5.2.11)**.** *Let X be compact and A closed in X. Then A is compact.*

Proof. Let $\{V_i\}_{i\in I}$ be an open covering of the closed set A, i.e., $A \subset \cup_{i\in I} V_i$. Then

$$X = A \cup A^C = \cup_{i\in I} V_i \cup A^C .$$

Since X is compact, there is a subcovering $U_{i_1}, \ldots, U_{i_n}$, i.e., $X = \cup_{k=1}^{n} U_{i_k}$, where for each k, $U_{i_k} = V_i$ for some $i \in I$, or $U_{i_k} = A^C$. Is $U_{i_1}, \ldots, U_{i_n}$ a finite subcovering of A? Why? How can we finish the proof? □

Lemma 9.2.16 (lemma for theorem 9.2.17)**.** *In a topological space X, the intersection of a finite set of neighborhoods of a point x is a neighborhood of x.*

proof skeleton. Immediate. Apply the definition of neighborhood. □

Theorem 9.2.17 (theorem 5.2.12)**.** *Let X be a Hausdorff Space. If a subset F of X is compact, then F is closed.*

Proof. This is a theorem that requires us to prove again that some set F is closed. Review how we prove a set is closed in lecture 4.

So, to prove F is closed, it is enough to show that there are no limit points of F in F^C (why?). Hence we need to prove the following:

$$\forall z \in F^C, \text{ there is a neighborhood } N \text{ of } z \text{ such that } N \cap F = \emptyset. \tag{9.2.1}$$

Now let's consider the compact set F. For each $x \in F$, let V_x be an open set containing x, then we have $F = \cup_{x \in F} V_x$, then there is a subcovering $V_{x_1}, \ldots, V_{x_n}$, i.e., $F = \cup_{i=1}^n V_{x_i}$. Hence we need to prove

$$\begin{aligned} &\forall z \in F^C, \text{ there is a neighborhood } N \text{ of } z \text{ such that } N \cap (\cup_{i=1}^n V_{x_i}) = \emptyset \\ \iff &\forall z \in F^C, \text{ there is a neighborhood } N \text{ of } z \text{ such that } \cup_{i=1}^n (N \cap V_{x_i}) = \emptyset \\ \iff &\forall z \in F^C, \text{ there is a neighborhood } N \text{ of } z \text{ such that } N \cap V_{x_i} = \emptyset, \forall i = 1, \ldots, n. \end{aligned} \tag{9.2.2}$$

Let $z \in F^C$ be given. For each $i = 1, \ldots, n$, there exists a neighborhood N_{x_i} of z such that $V_{x_i} \cap N_{x_i} = \emptyset$ (why?). Let $N = \cap_{i=1}^n N_{x_i}$, then N is a neighborhood of z (by lemma 9.2.16), and $N \cap V_{x_i} = \emptyset, \forall i = 1, \ldots, n$. We finished the proof.

□

Definition 9.2.18 (bounded, definition 5.3.1)**.** A subset A of $\mathbb{R}^n$ is said to be *bounded* if there is a real number K such that for each $x = (x_1, x_2, \ldots, x_n) \in A, |x_i| \leq K, i = 1, \ldots, n$.

Lemma 9.2.19 (lemma 5.3.2)**.** *If A is a compact subset of $\mathbb{R}$ then A is closed and bounded.*

proof skeleton. It is easy to prove by theorem 9.2.17 that A is closed. To prove A is bounded, you need to construct an open covering of A, which will be reduced to a finite subcovering. Note that, based on your construction, the finite subcovering is basically a collection of open intervals. Now show that A is bounded. □

9.3 Further Reading

5.1-5.4 in Mendelson.

SI112: Advanced Geometry	Spring 2018
Lecture 10 — Mar. 29th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

10 Lecture 10

Q: "Why don't you use different colors"?
A: "It is not professional".

10.1 Overview of This Lecture

Lecture 10 is a continuation of our exploration on compactness. Some theorems of great relevance are introduced. However, some of the proofs are quite challenging and elusive.

10.2 Proof of Things

Lemma 10.2.1 (lemma 5.3.3)**.** *The closed interval* $[0,1]$ *is compact.*

Proof. I read many proofs for this problem (this, and that), but none of them are rigorous. What's wrong with them? (read them, they are good lessons.)

Let $\{U_i\}_{i\in I}$ be any open covering of $[0,1]$. The trick is to consider the set

$$A = \{x \in [0,1] : [0,\text{ x}] \text{ can be covered by finitely many of the } U_i\text{'s}\}.$$

Note that A is non-empty and bounded, and $0 \in A$. Then use the completeness property of $\mathbb{R}$ to take s be the least upper bound of A. Note also that $0 \leq s \leq 1$.

We first show that $0 < s$. Since $0 \in U_i$ for some $i \in I$ and U_i is open, U_i is a neighborhood of 0. It follows that there is an open set $(-\epsilon, \epsilon)$ such that $0 \in (-\epsilon, \epsilon) \subset U_i$, which implies $[0, \frac{\epsilon}{2}]$ can be covered by U_i. Hence $0 < \frac{\epsilon}{2} \leq s$, i.e., $0 < s$.

We then show that for each $0 \leq t < s$, $[0,t]$ can be covered by finitely many sets in A, i.e.,$t \in A$. Suppose for the sake of contradiction $t \notin A$. Then every point $x \in A$ has to satisfy $x < t$, for if $x \geq t$ and $x \in A$, then finitely many open sets covering $[0,x]$ can also cover $[0,t]$. It follows that t is an upper bound for A, but $t < s$, contradicting the choice of s. Consequently, we have $[0,s) \subset A$.

Finally we will show that $s = 1$, which will prove that $[0,1]$ is compact. Suppose for the sake of contradiction $s < 1$. There is $U_0 \in \{U_i\}_{i\in I}$ such that $s \in U_0$, which means that there is an open set $(s-\epsilon, s+\epsilon)$ such that $s \in (s-\epsilon, s+\epsilon) \subset U_0$. Note that $s - \epsilon \in A$, that is, $[0, s-\epsilon]$ can be covered by finitely many open sets, say $U_{i_1}, U_{i_2}, \ldots, U_{i_n}$. Then the open sets,

$U_{i_1}, U_{i_2}, \ldots, U_{i_n}$, together with the open set U_0, will cover $[0, s + \frac{\epsilon}{2}]$, i.e., $s + \frac{\epsilon}{2} \in A$, which contradicts the definition of s. □

Corollary 10.2.2 (corollary 5.3.4)**.** *Each closed interval $[a, b]$ is compact.*

Proof. Immediate. □

Theorem 10.2.3 (theorem 5.3.5)**.** *A subset A of the real line is compact if and only if A is closed and bounded.*

Proof. Let A be compact. Then by lemma 9.2.19 A is closed and bounded.

Let A be closed and bounded. Then there exists $K > 0$ such that $A \subset [-K, K]$ and A is closed in the compact set $[-K, K]$. By theorem 9.2.15, A is compact. □

Definition 10.2.4 (basis for a topological space, definition 3.7.3)**.** Let X be a topological space and $\{B_i\}_{i\in I}$ a collection of open sets in X. $\{B_i\}_{i\in I}$ is called a *basis for the open sets of X* if each open set in X is a union of members of $\{B_i\}_{i\in I}$.

Remark 10.2.5. In lecture 8, we defined product topology without explicitly defining *basis*. It is recommended to read 3.7 in Mendelson before proceeding. You should verify that the sets of the form $O_1 \times O_2$, O_1, O_2 open in the topological spaces X_1, X_2 respectively, are a basis for the open sets of the topological space $X_1 \times X_2$.

Example 10.2.6. In $\mathbb{R}$ with standard topology a base for the topology is the collection of all open intervals.

Definition 10.2.7 (dimension of topological space)**.** Let X be a topological space, the dimension, denoted by $\dim X$ is the supremum among all lengths of chains $X_1 \subsetneq X_2 \subsetneq \cdots \subsetneq X_i$ of closed and irreducible subsets of X.

Remark 10.2.8 (remark for definition 10.2.7). This definition is irrelevant, at least for now.

Lemma 10.2.9 (lemma 5.4.1)**.** *Let $\mathcal{B}$ be a basis for the open sets of a topological space Z. If, for each covering $\{\mathcal{B}_\beta\}_{\beta\in J}$ of Z by members of $\mathcal{B}$, there is a finite subcovering, then Z is compact.*

Proof. Let $\{\mathcal{O}_i\}_{i\in I}$ be an open covering of Z, we need to show that there is a finite subcovering. Since $\mathcal{B}$ is a basis for the topologocal space Z, for each $i \in I$, there exists $J_i \subset J$ such that $O_i = \cup_{\beta\in J_i}\mathcal{B}_\beta$ and that $\mathcal{B}_\beta \subset O_i$ for each $\beta \in J_i$. Hence $Z \subset \cup_{i\in I} O_i = \cup_{i\in I} \cup_{\beta\in J_i} \mathcal{B}_\beta$. By the supposition, $Z \subset \cup_{k=1}^n \mathcal{B}_{\beta_k}$, where $\mathcal{B}_{\beta_k}$ is a subset of O_{β_k} for some $O_{\beta_k} \in \{\mathcal{O}_i\}_{i\in I}$. Consequently, $Z \subset \cup_{k=1}^n \mathcal{O}_{\beta_k}$. We finished the proof. □

Theorem 10.2.10 (theorem 5.4.2)**.** *Let X and X' be compact topological spaces, then $X \times X'$ is compact.*

Proof. The common strategy for proving compactness possibly fails to prove this theorem, which should not stop you having a try. A complete but not compact proof is given here.

As mentioned above, the set $\{O \times O' : O \text{ is open in } X \text{ and } O' \text{ is open in } X'\}$ is a basis for the open sets of the topological space $X \times X'$. By lemma 10.2.9, it is enough to show that each covering of $X \times X'$ by sets of the form $O \times O'$, O is open in X, O' is open in X', has a finite subcovering.

Let $\{O_i \times O_i'\}_{i \in I}$ be such a covering. Then for each $x_0 \in X$, the open covering $\{O_i \times O_i'\}_{i \in I}$ is necessarily an open covering of the set $X'_{x_0} = \{x_0\} \times X' = \{(x_0, x') : x' \in X'\}$. But X'_{x_0} is homeomorphic to X' and hence compact. There is therefore a finite subset I_{x_0} of I such that $\{O_i \times O_i'\}_{i \in I_{x_0}}$ covers X'_{x_0}.

Without loss of generality, we may assume that $x_0 \in O_j$ for each $j \in I_{x_0}$, for otherwise we may delete $O_j \times O_j'$ and still cover X'_{x_0} (why still cover X'_{x_0} after deleting?).

The set $O^*_{x_0} = \cap_{i \in I_{x_0}} O_i$ is a finite intersection of open sets containing x_0 and is therefore an open set containing x_0. Now we **claim** that $\{O_i \times O_i'\}_{i \in I_{x_0}}$ is an open covering of $O^*_{x_0} \times X'$. For each $(x, x') \in O^*_{x_0} \times X'$, we have that $x \in O^*_{x_0} = \cap_{i \in I_{x_0}} O_i$ and $x' \in X'$, which means that $x \in O_i$ for each $i \in I_{x_0}$ and $x' \in O_j'$ for some $j \in I_{x_0}$. Hence $(x, x') \in O_j \times O_j'$ for some $j \in I_{x_0}$.

Notice that $\{O^*_x\}_{x \in X}$ is an open covering of the compact space X, hence there is a finite subcovering $O^*_{x_1}, O^*_{x_2}, \ldots, O^*_{x_n}$ of X. Let us set $I^* = I_{x_1} \cup I_{x_2} \cup \cdots \cup I_{x_n}$ and show that the finite family $\{O_i \times O_i'\}_{i \in I^*}$ is a covering of $X \times X'$, from which it will follow that $X \times X'$ is compact. Suppose $(x, x') \in X \times X'$. Since $\{O_i\}_{i \in I^*}$ covers X, $x \in O^*_{x_i}$ and $(x, x') \in O^*_{x_i} \times X'$ for some x_i. By our previous **claim**, $(x, x') \in O_j \times O_j'$ for some $j \in I_{x_i}$, which certainly implies that $(x, x') \in O_i \times O_i'$ for some $i \in I^*$. We have thus established that $\{O_i \times O_i'\}_{i \in I^*}$ is a finite covering of $X \times X'$ and that therefore $X \times X'$ is compact. □

Corollary 10.2.11 (corollary 5.4.3)**.** *Let $X_1, X_2, \ldots, X_n$ be compact topological spaces. Then $\prod_{i=1}^n X_i$ is also compact.*

Corollary 10.2.12. *$[0, 1]^n$ is compact.*

Theorem 10.2.13. *$A \subset \mathbb{R}^n$ is compact if and only if A is closed and bounded.*

Theorem 10.2.14. *$f : X \to \mathbb{R}$, f is continuous and X is compact. Then there exists $x_1, x_2 \in X$ such that $\inf_{x \in X} f(x) = f(x_1), \sup_{x \in X} f(x) = f(x_2)$.*

Proof. $f(X)$ is compact (why?), and thus $f(X)$ is closed and bounded. Because $f(X)$ is bounded, $l = \inf_{x \in X} f(x)$ and $u = \sup_{x \in X} f(x)$ exist ($\mathbb{R}$ is complete). Then l and u are limit points of $f(X)$ (by which theorem?). That $f(X)$ is closed means that $l, u \in f(X)$. □

10.3 Further Reading

5.1-5.4 in Mendelson.

SI112: Advanced Geometry	Spring 2018
Lecture 11 — Apr. 3rd, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

11 Lecture 11

11.1 Overview of This Lecture

11.2 Proof of Things

Definition 11.2.1 (connected, definition 4.2.1)**.** A topological space X is said to be connected if the only two subsets of X that are simultaneously open and closed are X itself and the empty set $\emptyset$. A topological space which is not connected is said to be disconnected.

Example 11.2.2. Discrete topology is not connected, since every point is open and closed. $[0,1] \cup [2,3]$ on the real line is not connected.

Lemma 11.2.3 (lemma 4.2.3)**.** *Let A be a subspace of a topological space X. Then A is disconnected if and only if there exist two open subsets P and Q of X such that*

$$A \subset P \cup Q, P \cap Q \subset A^C, \text{ and } P \cap A \neq \emptyset, Q \cap A \neq \emptyset.$$

Proof. On the one hand, suppose that A is disconnected. Then there is a subset P' of A, different from $\emptyset$ and from A, such that P' is both relatively open and relatively closed in A. This means that P'^C is also different from $\emptyset$ and from A and relatively open. Let P, Q be such that $P' = P \cap A, P'^C = Q \cap A$, where P and Q are open subsets of X. We therefore have that $A = P' \cup P'^C \subset P \cup Q$, for $P' \subset P$ and $P'^C \subset Q$, and also $P \cap Q \cap A = (P \cap A) \cap (Q \cap A) = P' \cap P'^C = \emptyset$ so that $P \cap Q \subset A^C$. Finally, $P' = P \cap A$ and $P'^C = Q \cap A$ are non-empty.

On the other hand, given open sets P and Q satisfying the stated conditions, set $P' = P \cap A$ and $Q' = Q \cap A$. Then $A = A \cap (P \cup Q) = (A \cap P) \cup (A \cap Q) = P' \cup Q'$ and $P' \cap Q' = (A \cap P) \cap (A \cap Q) = \emptyset$. Thus $P' = Q'^C$, and P' is both relatively open and relatively closed in A. Since $P' \neq \emptyset$ and $P' \neq A$, A is disconnected. □

Theorem 11.2.4 (theorem 4.2.5)**.** *Let X and Y be topological spaces, and le $f : X \to Y$ be continuous. If X is connected, then $f(X)$ is connected.*

Proof. Suppose $f(X)$ is disconnected. Use 11.2.3, and after some steps we can derive that X is not connected, a contradiction. Hence $f(X)$ is connected. □

Theorem 11.2.5 (lemma 4.2.8)**.** *Let $Y = \{0, 1\}$ with discrete topology be a topological space. A topological space X is connected if and only if the only continuous mappings $f : X \to Y$ are the constant mappings.*

Proof. Let $f : X \to Y$ be a continuous non-constant mapping. Then $P = f^{-1}(\{0\})$ and $f^{-1}(\{1\})$ are both non-empty (why?). Thus $P \neq \emptyset$ and $P \neq X$ (why?). $\{0\}$ and $\{1\}$ are open subsets of Y (why?) and f is continuous, therefore P and Q are open subsets of X. But $P = Q^C$ (why?), so P is both open and closed and consequently X is disconnected. Thus, if X is connected, the only continuous mappings $f : X \to Y$ are constant mappings.

Conversely, suppose X is disconnected. Then there are non-empty open subsets P, Q of X such that $P \cap Q = \emptyset$ and $P \cup Q = X$. Define a mapping $f : X \to Y$ as follows: If $x \in P$, set $f(x) = 0$; if $x \in Q$, set $f(x) = 1$. f is continuous, for there are four open subsets, $\emptyset, \{0\}, \{1\}$, and Y of Y and $f^{-1}(\emptyset) = \emptyset, f^{-1}(\{0\}) = P, f^{-1}(\{1\}) = Q$, and $f^{-1}(Y) = X$, so that the inverse image of an open set is open. □

Theorem 11.2.6 (theorem 4.2.9)**.** *Let X and Y be connected topological spaces. Then $X \times Y$ is connected.*

Proof. It is enough to show that the only continuous mappings $f : X \times Y \to \{0, 1\}$ are constant mappings. Suppose, on the contrary, that there is a continuous mapping $f : X \times Y \to \{0, 1\}$ that is not constant. Then there are points $(x_0, y_0), (x_1, y_1) \in X \times Y$ such that $f(x_0, y_0) = 0, (x_1, y_1) = 1$. If □

Theorem 11.2.7. *The product of connected spaces is connected.*

Theorem 11.2.8 (theorem 4.3.4)**.** *A subset A of the real line that contains at least two distinct points is connected if and only if it is an interval.*

Theorem 11.2.9 (Intermediate Value Theorem, theorem 4.4.1)**.** *$f : [a, b] \to \mathbb{R}$ continuous. $a \neq b$. v is any number between $f(a)$ and $f(b)$, i.e., $f(a) < v < f(b)$. then there is $x \in [a, b]$ such that $f(x) = v$.*

Proof. $[a, b]$ is connected. It follows that $f([a, b])$ is connected and hence is an interval, which means $v \in f([a, b])$. □

Theorem 11.2.10 (theorem 4.5.1)**.** *The component of a is the largest connected set that contains a.*

Lemma 11.2.11 (lemma 4.5.2)**.** *In a topological space X, let $b \in Cmp(a)$. Then $Cmp(b) = Cmp(a)$.*

Theorem 11.2.12 (corollary 4.5.3)**.** *In a topological space X, define a b if $b \in Cmp(a)$. Then is an equivalence relation.*

Theorem 11.2.13 (path connectedness, 4.6.2)**.**

homotopy equivalent.

Remark 11.2.14. disconnected, jump

define topology for graph.

11.3 Further Reading

5.1-5.4 in Mendelson.

SI112: Advanced Geometry	Spring 2018
Lecture TA Session — Apr. 9th, Monday	
Prof. Manolis	*Scribe*: Liangzu

12 TA Session

12.1 Overview of This Lecture

In this TA session we will introduce the definition of *monoid, group, ring*, and *field*. Examples will be given to facilitate your understanding. Notice that the definition of ring given here is slightly different from the one given by Prof. Manolis. What's the difference?

12.2 Proof of Things

Definition 12.2.1 (binary operation)**.** A *binary operation* or *law of composition* on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a * b$, or ab in G, called the composition of a and b.

Definition 12.2.2 (monoid)**.** Suppose that S is a set and $*$ is some binary operation $S \times S \to S$, then $(S, *)$ is a *monoid* if it satisfies the following axioms.

- The binary operation is *associative*. That is,

$$(a * b) * c = a * (b * c)$$

  for $a, b, c \in S$.

- There exists an element $e \in S$, called the *identity element*, such that for any element $a \in S$

$$e * a = a * e = a.$$

Example 12.2.3. $(\mathbb{N} \cup \{0\}, +)$ is a monoid.

Example 12.2.4. $(\{f : \mathbb{R}^n \to \mathbb{R}\}, \cdot)$, where $\cdot$ is such that $(f_1 \cdot f_2)(x) = f_1(x)f_2(x)$, is a monoid. What is the identity element of this monoid?

Definition 12.2.5 (group)**.** A *group* $(G, *)$ is a set G together with a law of composition $(a, b) \mapsto a * b$ that satisfies the following axioms.

- The law of composition is *associative*. That is,

$$(a * b) * c = a * (b * c)$$

for $a, b, c \in G$.

- There exists an element $e \in G$, called the *identity element*, such that for any element $a \in G$

$$e * a = a * e = a.$$

- For each element $a \in G$, there exists an *inverse element* in G, denoted by a^{-1}, such that

$$a * a^{-1} = a^{-1} * a = e.$$

Remark 12.2.6. A group G with the property that $a * b = b * a$ for all $a, b \in G$ is called *abelian* or *commutative*. Groups not satisfying this property are said to be *nonabelian* or *non-commutative*.

Example 12.2.7. $\emptyset$ is not a group.

Example 12.2.8. The integers $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ form a group under the operation of addition.

Example 12.2.9. $(\{f : \mathbb{R}^n \to \mathbb{R}\}, \cdot)$ is a monoid, but no a group. $(\{f : \mathbb{R}^n \to \mathbb{R}/\{0\}\}, \cdot)$ is a group.

Example 12.2.10. The set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ is a group under the binary operation of addition mod n. But if we let modular multiplication be the binary operation on $\mathbb{Z}_n$, then $\mathbb{Z}_n$ fails to be a group. The element 1 acts as a group identity since $1 \cdot k = k \cdot 1 = k$ for any $k \in \mathbb{Z}_n$. However, a multiplicative inverse for 0 does not exist since $0 \cdot k = k \cdot 0 = 0$ for every k in $\mathbb{Z}_n$.

Example 12.2.11. Let $\mathbb{M}_2(\mathbb{R})$ be the set of all 2×2 matrices and $GL_2(\mathbb{R})$ be the subset of $\mathbb{M}_2(\mathbb{R})$ consisting of invertible matrices. Then $\mathbb{M}_2(\mathbb{R})$ with matrix multiplication operation is a monoid, but not a group. $GL_2(\mathbb{R})$ is a nonabelian group (hence a monoid) under matrix multiplication, called the *general linear group*.

Exercise 12.2.12. Prove that the identity element in a group is unique.

Exercise 12.2.13. If g is any element in a group G, then the inverse of g, denoted by g^{-1}, is unique.

Exercise 12.2.14. Let G be a group. Prove that if $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Exercise 12.2.15. Let G be a group. Prove that for any $a \in G$, $(a^{-1})^{-1} = a$.

Exercise 12.2.16 (cancellation laws)**.** If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Definition 12.2.17 (subgroup)**.** Let $(G, *)$ be a group. A subset H of G is called a subgroup of G if H also forms a group under the operation $*$. More precisely, H is a subgroup of G if the restriction of $*$ to $H \times H$ is a group operation on H.

Remark 12.2.18. The subgroup $H = \{e\}$ of a group G is called the *trivial subgroup*. A subgroup that is proper subset of G is called a *proper subgroup*.

Example 12.2.19. The set $\mathbb{Z}a = \{n \in \mathbb{Z} : n = ka \text{ for some } k \text{ in } \mathbb{Z}\} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$ is a subgroup of $(\mathbb{Z}, +)$.

Example 12.2.20. It is important to realize that a subset H of a group G can be a group without being a subgroup of G. For H to be a subgroup of G it must inherit G's binary operation. The set of all 2×2 matrices $\mathbb{M}_2(\mathbb{R})$ forms a group under the operation of addition. The 2×2 general linear group $GL_2(\mathbb{R})$ is a subset of $\mathbb{M}_2(\mathbb{R})$ and is a group under matrix multiplication, but it is not a subgroup of $\mathbb{M}_2(\mathbb{R})$. If we add two invertible matrices, we do not necessarily obtain another invertible matrix. Observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

but the zero matrix is not in $GL_2(\mathbb{R})$.

Proposition 12.2.21 (identifying a subgroup, 1)**.** *A subset H of G is a subgroup if and only if it satisfies the following conditions.*

1. *The identity e of G is in H.*
2. *If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.*
3. *If $h \in H$ then $h^{-1} \in H$.*

Proof. omitted. □

Proposition 12.2.22 (identifying a subgroup, 2)**.** *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

Proof. omitted. □

Definition 12.2.23 (ring)**.** A nonempty set R is a *ring* if it has two closed binary operations, addition and multiplication, satisfying the following conditions.

1. $a + b = b + a$ for $a, b \in R$.

2. $(a + b) + c = a + (b + c)$ for $a, b, c \in R$.

3. There is an element 0 in R such that $a + 0 = a$ for all $a \in R$.

4. For every element $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0$.

5. $(ab)c = a(bc)$ for $a, b, c \in R$.

6. For $a, b, c \in R$,
$$a(b + c) = ab + ac, (a + b)c = ac + bc.$$

Remark 12.2.24. The conditions 1, 2, 3 and 4 in the above definition imply that $(R, +)$ is an abelian group; The last condition is a condition that relates addition operation and multiplication.

Remark 12.2.25. Notice that in the above definition, a ring R may not have multiplicative identity and multiplicative inverse.

If there is an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for each element $a \in R$, we say that R is a ring with *unity* or *identity*. And then the condition 5 means that R with identity is a monoid under multiplication operation.

A ring for which $ab = ba$ for all a, b in R is called a *commutative ring*.

Due to the absence of multiplicative inverses, for some nonzero and distinct elements a, b, c in a commutative ring, the equation $ab = ac \iff a(b - c) = 0$ may not imply $b = c \iff b - c = 0$. That is, the cancellation laws for multiplication operation might not hold. This motivates the following definitions.

Example 12.2.26. The continuous real-valued functions on an interval $[a, b]$ form a commutative ring.

Definition 12.2.27 (integral domain)**.** A commutative ring R with identity is called an *integral domain* if, for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

Definition 12.2.28 (unit)**.** A nonzero element a in a ring R with identity is called a *unit* if there exists a unique element a^{-1} such that $a^{-1}a = aa^{-1} = 1$. In other words, the unit is a nonzero element of R that has a unique multiplicative inverse.

Definition 12.2.29 (division ring)**.** A *division ring* is a ring R, with an identity, in which every nonzero element in R is a *unit*. That is, every nonzero element in a division ring has a unique multiplicative inverse.

Remark 12.2.30 (field). A commutative division ring is called a *field*. The relationship among rings, integral domains, division rings, and fields is shown in figure 4.

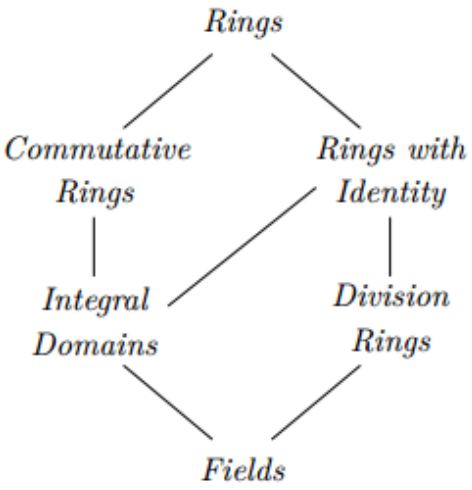

Figure 4: Types of rings

Example 12.2.31. $\mathbb{Z}$ is an integral domain, but not a field. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Example 12.2.32. We can define the product of two elements a and b in $\mathbb{Z}_n$ by $ab \pmod n$. For instance, in $\mathbb{Z}_{12}$, $5 \cdot 7 \equiv 11 \pmod{12}$. This product makes the abelian group $\mathbb{Z}_n$ into a ring. Certainly $\mathbb{Z}_n$ is a commutative ring; however, it may fail to be an integral domain. If we consider $3 \cdot 4 \equiv 0 \pmod{12}$ in $\mathbb{Z}_{12}$, it is easy to see that a product of two nonzero elements in the ring can be equal to zero.

Remark 12.2.33 (zero divisor). A nonzero element a in a ring R is called a *zero divisor* if there is a nonzero element b in R such that $ab = 0$. In the previous example, 3 and 4 are zero divisors in $\mathbb{Z}_{12}$.

Definition 12.2.34 (nilpotent)**.** An element x of a ring R is called *nilpotent* if there exists some positive integer n such that $x^n = 0$.

Example 12.2.35. The matrix $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ is nilpotent because $A^3 = 0$.

Proposition 12.2.36. *If x is nilpotent in a ring with identity, then $1 - x$ is a unit.*

Proof. That x is nilpotent means that there is a positive integer n such that $x^n = 0$, which implies $(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1 - x^n = 1$. Hence $1 - x$ is a unit. □

12.3 Further Reading

1. wikipedia for their definition.

2. Abstract Algebra: Theory and Applications

3. Abstract Algebra wikibook

SI112: Advanced Geometry	Spring 2018
Lecture 12-13 — Apr. 10th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

13 Lecture 13-14

13.1 Overview of This Lecture

Here and in what follows, unless explicitly stated otherwise, by *ring* we mean that it is a commutative ring with identity.

Since from now on I have no Mendelson to copy, some results of theorems/definitions, etc. that I am not sure are marked by p, denoting "personal", "Peng", or ":p".

To make things correct, $\mathbb{F}$ is assumed to be $\mathbb{R}$ or $\mathbb{C}$, which is not the case on the board.

13.2 Proof of Things

Definition 13.2.1 (vector space)**.** This definition might be An abelian group $(V, +)$ and an "action" of a field F on V, i.e., $F \times V \to V$ $((c, v) \mapsto cv)$.

Definition 13.2.2 (monomial)**.** A *monomial* in $x_1, x_2, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \alpha_2, \ldots, \alpha_n$ are nonnegative integers. The *total degree* of this monomial is the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Remark 13.2.3. Notice that $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ if and only if $\alpha_i = \beta_i$ for $i = 1, \ldots, n$.

Remark 13.2.4. We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be an n-tuple of nonnegative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

When $\alpha = (0, \cdots, 0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ denote the total degree of the monomial x^α. Then in what follows, we will use x^α to denote $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, and x to denote $(x_1, x_2, \ldots, x_n)$ unless otherwise specified.

Definition 13.2.5 (support)**.** Suppose that $f : X \to \mathbb{R}$ is a real-valued function whose domain is an arbitrary set X. The *support* of f, written $\mathrm{supp}(f)$, is the set of points in X where f is non zero

$$\mathrm{supp}(f) = \{x \in X : f(x) \neq 0)\}.$$

If $f(x) = 0$ for all but a finite number of points x in X, then f is said to have *finite support*.

Definition 13.2.6 (polynomial over a ring)**.** A *polynomial* f in a ring R is a finite linear combination (with coefficient in R) of monomials. We write a polynomial f in the form

$$f = \Sigma_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha, a_\alpha \in R\,,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. The set of all polynomials in x with coefficients in R is denoted $R[x]$.

Remark 13.2.7. $R[x]$ is a ring (verify it), typically referred as to a *polynomial ring*.

Definition 13.2.8 (polynomial function)**.** Given $p \in R[x]$, we can define a polynomial function $f_p : R^n \to R$ (i.e., $(r_1, \ldots, r_n = r) \mapsto \Sigma_{\alpha \in \mathbb{N}^n} a_\alpha r^\alpha$). The function f_p is also called *evaluation map*.

Remark 13.2.9 (polynomial and polynomial function). We will not distinguish between polynomials and polynomial functions. Read this, and that.

Lemma 13.2.10. *If $f \in \mathbb{F}[x]$ and $f(r) = 0$ for each $r \in \mathbb{F}^n$, then we have $f = 0$. ($\mathbb{F}$ is infinite).*

Proof. Suppose inductively that $n = 1$. Since $f(r) = 0$ for each $r \in \mathbb{F}^n$ and $\mathbb{F}$ is infinite, f is a polynomial that has infinitely many roots. But a nonzero polynomial in $\mathbb{F}$ of degree m has at most m distinct roots. Hence f must be zero polynomial, i.e., $f = 0$.

Now assume that the lemma is true for $n - 1$. Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $f(r) = 0$ for each $r \in \mathbb{F}^n$. By collecting the various powers of x_n, we can write f in the form

$$f(x) = f(x_1, x_2, \ldots, x_n) = \Sigma_{i=0}^{N} g_i(x_1, x_2, \ldots, x_{n-1}) x_n^i,$$

where N is the degree of the term x_n and $g_i \in \mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$.

If we fix $(a_1, a_2, \ldots, a_{n-1}) \in \mathbb{F}^{n-1}$, we get a polynomial $f(a_1, a_2, \ldots, a_{n-1}, x_n) \in \mathbb{F}[x_n]$. By the hypothesis on f, this vanishes for every $a_n \in \mathbb{F}[x_n]$. It follows from the case $n = 1$ that $f(a_1, a_2, \ldots, a_{n-1}, x_n)$ is a zero polynomial in $\mathbb{F}[x_n]$. That is, the coefficients of $f(a_1, a_2, \ldots, a_{n-1}, x_n)$ are zero. Hence $g_i(a_1, a_2, \ldots, a_{n-1}) = 0$ for all i. Since $(a_1, a_2, \ldots, a_{n-1})$ is arbitrarily chosen in $\mathbb{F}^{n-1}$, the inductive assumption then implies that each g_i is the zero polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$. This forces f to be the zero polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ and completes the proof of the lemma. □

Example 13.2.11 (p, geometric algebra)**.** Let $f(x_1, x_2) = x_1^2 + x_2^2 - 1 \in \mathbb{R}[x_1, x_2]$ be a polynomial. It is clear that the solution of $f(x_1, x_2) = 0$, when "plotted", is a unit circle on the plane, where the unit circle is merely a set of points in $\mathbb{R}^2$. In this way we can study the

property of the solution through geometry. More generally, let $I \subset \mathbb{F}[x]$, where $\mathbb{F}$ is a field, be a set of polynomials. Then we define a set $Z(I)$, called "Zero Set", in the following way.

$$Z(I) = \{v \in \mathbb{F}^n : f(v) = 0, \forall f \in I\}. \tag{13.2.1}$$

It can be seen that $Z(I)$ is merely a set of points in $\mathbb{F}^n$. In this way we can study the zero solution of the polynomials in the set I from $Z(I)$. The connection between I and $Z(I)$ remains to be discussed.

Example 13.2.12 (p, algebraic geometry)**. Conversely**, given a set of points $V \subset \mathbb{F}^n$ as a geometric object. Can we study it in an algebraic way, for example, by studying the solution of a specific set of polynomials? Let's start from the simplest example. Now we have a set V containing only one point $(0,0) \in \mathbb{R}^2$ (hence $V \subset \mathbb{R}^2$). Is there any polynomial $f(x_1, x_2) \in \mathbb{R}[x_1, x_2]$ satisfying $f(0,0) = 0$? there are obviously many of them. Indeed, all polynomials whose constant term is 0 satisfy $f(0,0) = 0$. The qualified polynomials will form a set, say $I_{\{(0,0)\}}$. You may want to understand the property of $(0,0)$ by studying $I_V = I_{\{(0,0)\}}$, but I will not. This example is too trivial to be interesting. More generally, let $V \subset \mathbb{F}^n$ be a set of points. Then we define a set I_V as follows:

$$I_V = \{f \in \mathbb{F}[x] : f(v) = 0, \forall v \in V\}. \tag{13.2.2}$$

In this way we can study the geometric object V by study the property of I_V, which is an algebraic object. However, the connection between V and I_V remains to be discussed. The set I_V and the connection between V and I_V might be a recurring theme of this course.

Definition 13.2.13 (ideal)**.** A subset $I \subset R$, where R is a ring, is an ideal if it satisfies

- $0 \in I$.
- If $f, g \in I$, then $f + g \in I$ (i.e., closed under addition).
- If $f \in I$ and $h \in R$, then $hj \in I$.

Exercise 13.2.14. Prove that I_V defined as in (13.2.2) is an ideal. Indeed, I_V is called *vanishing ideal*.

Definition 13.2.15. Let R be a ring and $r_1, r_2, \ldots, r_n \in R$. Then we set

$$\langle r_1, r_2, \ldots, r_n \rangle = \{\Sigma_{i=1}^n h_i r_i : h_1, h_2, \ldots, h_n \in R\}.$$

Exercise 13.2.16 (ideal generated by some elements)**.** A crucial observation is that $\langle r_1, r_2, \ldots, r_n \rangle$ is an ideal of R (prove it). We will call $\langle r_1, r_2, \ldots, r_n \rangle$ the *ideal generated by* $r_1, r_2, \ldots, r_n$.

Definition 13.2.17 (ideal generated by a subset)**.** An ideal I in a ring R is said to be generated by a subset T of the ring R if for each $\alpha \in I$, there is $s \in \mathbb{N}^+$ such that $\alpha = r_1 t_1 + \cdots + r_s t_s$ for some $t_1, \ldots, t_s \in T, r_1, \ldots, r_s \in R$.

Definition 13.2.18 (p, linear form)**.** $f_c \in \mathbb{F}[x]$ is called a *linear form with coefficient* $c \in \mathbb{F}^n$ if

$$f_c(x) = c^T x = c_1 x_1 + \cdots + c_n x_n$$

for some $c \in \mathbb{F}^n$.

Remark 13.2.19 (p). If $f_c(x) = c^T x$, or f_c, is a linear form and the coefficient c is irrelevant, we use $f(x)$, or f, instead of $f_c(x)$ to the denote linear form $c^T x$ for convenience.

Lemma 13.2.20. $(\mathbb{F}[x])_1$*, the set of linear forms of* $\mathbb{F}[x]$*, is a vector space over* $\mathbb{F}$*.*

Proof. Let $\alpha_1, \alpha_2 \in \mathbb{F}$ and let $f_{c_1}, f_{c_2} \in (\mathbb{F}[x])_1$. Then

$$\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x) = \alpha_1 c_1^T x + \alpha_2 c_2^T x = (\alpha_1 c_1 + \alpha_2 c_2)^T x = f_{\alpha_1 c_1 + \alpha_2 c_2}(x) \in (\mathbb{F}[x])_1.$$

This proves that $(\mathbb{F}[x])_1$ is a vector space. □

Lemma 13.2.21. $c_1, c_2, \ldots, c_s \in \mathbb{F}^n$ *is linearly independent if and only if* $f_{c_1}, f_{c_2}, \ldots, f_{c_s} \in (\mathbb{F}[x])_1$ *is linearly independent.*

Proof. Suppose $f_{c_1}, f_{c_2}, \ldots, f_{c_s}$ is linearly independent, and let $\alpha_1 c_1 + \cdots + \alpha_s c_s = 0$ for some $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{F}$. Then for each $r \in \mathbb{F}^n$,

$$\alpha_1 f_{c_1}(r) + \cdots + \alpha_s f_{c_s}(r) = \alpha_1 c_1^T r + \cdots + \alpha_s c_s^T r = (\alpha_1 c_1 + \cdots + \alpha_s c_s)^T r = 0\,,$$

which implies that $\alpha_i = 0$ for $i = 1, \ldots, s$ and thus that $f_{c_1}, f_{c_2}, \ldots, f_{c_s}$ is linearly independent.

On the other hand, suppose $c_1, c_2, \ldots, c_s$ is linearly independent, and let

$$\alpha_1 f_{c_1}(r) + \cdots + \alpha_s f_{c_s}(r) = \alpha_1 c_1^T r + \cdots + \alpha_s c_s^T r = 0\,,$$

for each $r \in \mathbb{F}^n$ and $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{F}$. Then we have

$$\alpha_1 f_{c_1}(e_i) + \cdots + \alpha_s f_{c_s}(e_i) = \alpha_1 c_1^T e_i + \cdots + \alpha_s c_s^T e_i = 0, \text{ for } i = 1, \ldots, n\,,$$

where $e_1, e_2, \ldots, e_n$ is the standard basis for $\mathbb{F}^n$. These n equations imply that

$$\alpha_1 c_1 + \cdots + \alpha_s c_s = 0\,.$$

□

Proposition 13.2.22. $(\mathbb{F}[x])_1$ *is a* n*-dimensional vector space over* $\mathbb{F}$*.*

Proof. We have proved that $(\mathbb{F}[x])_1$ is a vector space in lemma 13.2.20. It remains to be shown that the dimension of $(\mathbb{F}[x])_1$ is n. It suffices to show that $c_1, c_2, \ldots, c_s \in \mathbb{F}^n$ is linearly independent if and only if $f_{c_1}, f_{c_2}, \ldots, f_{c_s} \in (\mathbb{F}[x])_1$ is linearly independent (why? think about their dimensions), which has been proved in lemma 13.2.21. □

Definition 13.2.23 (p, vanishing at a point)**.** Let $f : X \to Y$ be a function and $x \in X$ be a point. f is said to vanish at the point x if $f(x) = 0$.

Definition 13.2.24 (p, vanishing on a set)**.** Let $f : X \to Y$ be a function and I be a subset of X. f is said to vanish on the set I if f vanishes at every point of the set X, i.e., $f(x) = 0$ for each $x \in X$.

Next, we will establish some simple facts. Proving them requires basis linear algebra, which you are supposed to be familiar with.

Fact 13.2.25 (p)**.** *If* $f_1, f_2, \ldots, f_s \in \mathbb{F}[x]$ *vanish at a point* $x \in \mathbb{F}^n$*, then their linear combination*

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_s f_s,$$

where $\alpha_i \in \mathbb{F}$ *for* $i = 1, 2, \ldots, s$*, also vanishes at the point* x*.*

Fact 13.2.26 (p)**.** *If a linear form* $f \in (\mathbb{F}[x])_1$ *vanishes on a set* $S \subset \mathbb{F}^n$*, then* f *also vanishes on the set*

$$span(S) = \{\Sigma_{i \in I} k_i s_i : k_i \in \mathbb{F}, s_i \in S\}.$$

Fact 13.2.27 (p)**.** *If* $f_1, f_2, \ldots, f_s \in (\mathbb{F}[x])_1$ *vanish on a set* $S \subset \mathbb{F}^n$*, then their linear combination*

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_s f_s,$$

where $\alpha_i \in \mathbb{F}$ *for* $i = 1, 2, \ldots, s$*, vanishes on the set* $span(S) = \{\Sigma_{i \in I} k_i s_i : k_i \in \mathbb{F}, s_i \in S\}$ *(and of course* S*).*

Definition 13.2.28. Let V be a d-dimensional linear subspace of $\mathbb{F}^n$. $(I_V)_1$ be the set of linear forms that vanish on V. That is, $(I_V)_1 = \{f \in I_V : f \text{ is a linear form}\}$.

Proposition 13.2.29. $(I_V)_1$ *is a vector space over* $\mathbb{F}$*.*

Proof. Let $\alpha_1, \alpha_2 \in \mathbb{F}$ and $f_{c_1}, f_{c_2} \in (I_V)_1$. Then $\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x) = f_{\alpha_1 c_1 + \alpha_2 c_2}(x)$. It is obvious that $f_{\alpha_1 c_1 + \alpha_2 c_2}$ is a linear form and $\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x)$ vanishes on V, hence $\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x) \in (I_V)_1$. □

Remark 13.2.30. Let V be a d-dimensional linear subspace of $\mathbb{F}^n$. We've proved that $(\mathbb{F}[x])_1$ and $(I_V)_1$ is vector space. Hence $(I_V)_1$ is a subspace of $(\mathbb{F}[x])_1$. It is then natural to ask what is the dimension of the subspace $(I_V)_1$. It turns out that $\dim(I_V)_1 = n - d$, as proved in the following theorem.

Theorem 13.2.31. *Let V be a d-dimensional linear subspace of $\mathbb{F}^n$, where $\mathbb{F}$ is an infinite field. Then $(I_V)_1$ is an $\mathbb{F}$-subspace of $(\mathbb{F}[x])_1$ of dimension $n-d$, and I_V is the ideal generated by $(I_V)_1$. Hence, if $f_{b_1}, \ldots, f_{b_{n-d}}$ is a basis for $(I_v)_1$ then $I_v = \langle f_{b_1}, \ldots, f_{b_{n-d}} \rangle$.*

Proof. It is trivial when $V = \mathbb{F}^n$.

Assume V is a proper subset of $\mathbb{F}^n$. Let $v_1, v_2, \ldots, v_d \in \mathbb{F}^n$ be an orthonormal basis for V and $u_{d+1}, u_{d+2}, \ldots, u_n \in \mathbb{F}^n$ an orthogonal basis for $V^\perp$, where $V^\perp$ is the orthogonal complement of V. Hence v's and u's form an orthonormal basis for $\mathbb{F}^n$, say

$$B = [v_1, v_2, \ldots, v_d, u_{d+1}, u_{d+2}, \ldots, u_n], \tag{13.2.3}$$

and we have $B^T B = I$.

We've proved that $(I_V)_1$ is a vector space. Hence $(I_V)_1$ is a subspace of $\mathbb{F}^n$. It remains to be shown that 1. the dimension of $(I_V)_1$ is $n - d$, and that 2. I_V is the ideal generated by $(I_V)_1$.

1. To prove $\dim(I_V)_1 = n - d$, It is enough to do the following: (a) find $n - d$ linearly independent linear forms in $(I_V)_1$, which implies that $\dim(I_V)_1 \geq n-d$; (b) Prove that for arbitrary $n - d + 1$ linear forms in $(I_V)_1$, they are linearly dependent.

   (a) By the definition of orthogonal complement, we have

   $$u_{d+i}^T v_j = 0, \forall i = 1, \ldots, n-d, \forall j = 1, \ldots, d. \tag{13.2.4}$$

   It is obvious from (13.2.4) that the linear forms $f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n}$ vanish on the set $\{v_1, v_2, \ldots, v_d\}$. By the fact 13.2.26, $f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n}$ vanish on the set $span(\{v_1, v_2, \ldots, v_d\}) = V$. Hence we have

   $$f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n} \in (I_V)_1.$$

   In addition, that A is invertible means that $u_{d+1}, u_{d+2}, \ldots, u_n$ is linearly independent, which further implies, by lemma 13.2.21, that $f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n}$ is linearly independent.

   (b) Let $f_{c_d}, f_{c_{d+1}}, \ldots, f_{c_n} \in (I_V)_1$, where $c_i \in \mathbb{F}^n$ for $i = d, \ldots, n$. Suppose for the sake of contradiction that $f_{c_d}, f_{c_{d+1}}, \ldots, f_{c_n}$ is linearly independent. Then by lemma

13.2.21, $c_d, c_{d+1}, \ldots, c_n$ is linearly independent. But $f_{c_d}, f_{c_{d+1}}, \ldots, f_{c_n} \in (I_V)_1$ and thus they vanish on $V = span(\{v_1, v_2, \ldots, v_d\})$, which means that

$$c_d, c_{d+1}, \ldots, c_n \in V^\perp,$$

contradicting the fact that $\dim V^\perp = n - \dim V = n - d$.

2. We know from the proof above that the linear forms $f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n}$ is a basis for $(I_V)_1$. To prove I_V is the ideal generated by $(I_V)_1$, it suffices to show, according to definition 13.2.17, that (a) $\langle f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n} \rangle \subset I_V$ and that (b) for each $p \in I_V$, we have

$$p = b_{d+1} f_{u_{d+1}} + b_{d+2} f_{u_{d+2}} + \cdots + b_n f_{u_n}\,, \tag{13.2.5}$$

for some $b_{d+1}, b_{d+2}, \ldots b_n \in \mathbb{F}[x]$.

   (a) Note that We can not use fact 13.2.25 or fact 13.2.27 to prove it (why?).
   Let $f_a \in \langle f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n} \rangle$. Hence there exists $p_{d+1}, \ldots, p_n \in \mathbb{F}[x]$ such that

$$f_a = p_{d+1} f_{u_{d+1}} + p_{d+2} f_{u_{d+2}} + \cdots + p_n f_{u_n}.$$

   It follows that for any $x \in V$, we have

$$f_a(x) = p_{d+1}(x) f_{u_{d+1}}(x) + p_{d+2}(x) f_{u_{d+2}}(x) + \cdots + p_n(x) f_{u_n}(x) = 0,$$

   which means that $f_a \in I_V$. Hence $\langle f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n} \rangle \subset I_V$.

   (b) Let $p \in I_V$. Then for each $x \in \mathbb{F}^n$, there exists a $q \in \mathbb{F}[x]$ such that $q(B^T x) = p(x)$, where B is defined in (13.2.3) (why does such a $q \in \mathbb{F}[x]$ exist?). Then

$$p(x) = q(B^T x) = q(v_1^T x, \ldots, v_d^T x, u_{d+1}^T x, \ldots, u_n^T x).$$

   As in 13.2.10, we can split $q(v_1^T x, \ldots, v_d^T x, u_{d+1}^T x, \ldots, u_n^T x)$ into two parts, one containing the terms including $u_{d+1}^T x, \ldots, u_n^T x$, which can be represented as

$$\Sigma_{i=1}^{n-d} (u_{d+i}^T x) q_i(x), \text{ where } q_i \in \mathbb{F}[x] \text{ for } i = 1, \ldots, n-d\,,$$

   and the other not containing them, which can be represented as

$$q'(v_1^T x, \ldots, v_d^T x)\,.$$

   Hence

$$p(x) = \Sigma_{i=1}^{n-d} (u_{d+i}^T x) q_i(x) + q'(v_1^T x, \ldots, v_d^T x)\,,$$

   where $q_i \in \mathbb{F}[x]$ for $i = 1, \ldots, n-d$. If suffices to show that $q' = 0$, by which we will have $p = \Sigma_{i=1}^{n-d} q_i f_{u_{d+i}}$ and we can set $b_{d+i} = q_i$ for $i = 1, \ldots, n-d$ to obtain (13.2.5), completing the proof.

We will use the hypothesis $p \in I_V$ to prove $q' = 0$. For each $r \in V$, we have $p(r) = 0$. Since $\Sigma_{i=1}^{n-d} q_i f_{u_{d+i}}$ vanishes on V, $(\Sigma_{i=1}^{n-d} q_i f_{u_{d+i}})(r) = 0$. This implies $q'(v_1^T r, \ldots, v_d^T r) = 0$. Recall that $v_1, v_2, \ldots, v_d$ is a basis for V, there exist unique $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{F}$ such that $r = \Sigma_{i=1}^{d} \alpha_i v_i$. Hence $q'(\alpha_1, \alpha_2, \ldots, \alpha_d) = 0$. This holds for each $r \in V$, but this is not, though close to, what we want.

We desire to prove that for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathbb{F}^d$, $q'(\alpha) = 0$. But for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathbb{F}^d$, there exists a unique $r \in V$ such that $r = \Sigma_{i=1}^{d} \alpha_i v_i$. $p(r) = 0$ implying $p'(\alpha) = 0$, by lemma 13.2.10, $p' = 0$. We finished the proof.

□

Remark 13.2.32 (subspaces and ideals). A subspace V of $\mathbb{F}^n$ and its ideal I_V are connected deeply. They both have to be closed under addition and multiplication, except that, for V, we multiply by scalars, whereas for an ideal, we multiply by polynomials. Further, notice that the ideal generated by polynomials $f_1, f_2, \ldots, f_s$ is similar to the span of vectors $v_1, v_2, \ldots, v_s$.

Exercise 13.2.33. Describe the connection between $(I_V)_1$ and orthogonal complement.

Definition 13.2.34 (p, projective variety)**.** $X \subset \mathbb{F}^n$ is called a *projective variety*, if for each $x \in X$, $span(\{x, 0\}) \subset X$.

Remark 13.2.35. Let $X \subset \mathbb{F}^n$ be a projective variety and $I_X \subset \mathbb{F}[x]$ vanish on X. Then for each $x \in X$, $\lambda \in \mathbb{F}$, and $f \in I_X$, we have $f(\lambda x) = f(x) = 0$.

Proposition 13.2.36. *$\mathbb{F}[x]$ is a $\mathbb{Z}^+$-graded ring. That is, $\mathbb{F}[x]$ can be written as the direct sum of $(\mathbb{F}[x])_i, i \in \mathbb{N}$, i.e., $\mathbb{F}[x] = \oplus_{i \in \mathbb{N}} (\mathbb{F}[x])_i$, where $(\mathbb{F}[x])_i$ is the set of all homogeneous polynomials of degree i, and is a vector space over $\mathbb{F}$ of dimension $\binom{i+n-1}{n-1}$.*

Proof. ..... □

Example 13.2.37. The basis of $(\mathbb{F}[x])_2$, where $\mathbb{F}[x] = \mathbb{F}[x_1, x_2, x_3]$, is $x_1^2, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2$. Its dimension is 6.

Question 13.2.38. I_X is an $\mathbb{F}$-subspace of $\mathbb{F}[x]$. Can we write I_X as a direct sum of $(I_X)_i, i \in \mathbb{N}$, i.e., $I_X = \oplus_{i \in \mathbb{N}} (I_X)_i$? (This is true if X is a projective variety).

13.3 Further Reading

1. for review linear algebra, read relevant chapters on this book and that book.
2. formal polynomials: 1, 2.
3. chapter 1 of this book: Ideals, Varieties, and Algorithms, very excellent.
4. not-so-useful notes here

SI112: Advanced Geometry	Spring 2018
Lecture 14-15 — Apr. 17th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

14 Lecture 14-15

14.1 Overview of This Lecture

The proof that I_V is generated by $(I_V)_1$ is in the previous lecture note. To make things correct, $\mathbb{F}$ is assumed to be $\mathbb{R}$ or $\mathbb{C}$, which is not the case on the board.

14.2 Proof of Things

Proposition 14.2.1. *Let V be a d-dimensional linear subspace of $\mathbb{F}^n$ and $I_V \in \mathbb{F}[x]$ the set of polynomials vanishing on V. Then we have $V = Z(I_V)$, where*

$$Z(I_V) = \{v \in \mathbb{F}^n : f(v) = 0, \forall f \in I_V\}.$$

Proof. Suppose $v \in V$, then $f(v) = 0$ for each $f \in I_V$, which means $v \in Z(I_V)$. Hence $V \subset Z(I_V)$.

On the other hand, let $v \in Z(I_V)$. Then we have $f(v) = 0$ for any $f \in I_V$. Specifically, let $u_{d+1}, \dots, u_n$ be a basis for $V^\perp$, then for the linear forms $f_{u_{d+1}}, \dots, f_{u_n} \in I_V$, we have

$$f_{u_{d+i}}(v) = u_{d+i}^T v = 0 \text{ for } i = 1, \dots, n-d,$$

implying that $v \in V$. Hence $Z(I_V) \subset V$. □

Definition 14.2.2 (addition of ideals)**.** Let R be a ring and $I_1, I_2 \subset R$ be ideals. We define addition operation of ideals as follows:

$$I_1 + I_2 = \{r \in R : r = r_1 + r_2 \text{ for some } r_1 \in I_1, r_2 \in I_2\}.$$

Remark 14.2.3. An observation is that $I_1 + I_2$ is an ideal, as you should verify.

Proposition 14.2.4. *Let I_1, I_2 be ideals of a ring. Then $I_1 \cap I_2$ is an ideal.*

Proof. Immediate. □

Proposition 14.2.5 (p)**.** *Let $I_1, I_2 \subset F[x]$ be ideals. Then $\langle I_1 \cup I_2 \rangle = I_1 + I_2$.*

Proof. Immediate. □

Proposition 14.2.6. *Let $I_1, I_2 \subset F[x]$ be ideals. Then $Z(I_1 \cup I_2) = Z(\langle I_1 \cup I_2 \rangle) = Z(I_1 + I_2)$.*

Proof. Immediate. □

Let R be a ring and $I_1, I_2 \subset R$ be ideals. The set

$$\{r \in R : r = r_1 r_2, \text{ where } r_1 \in I_1, r_2 \in I_2\}$$

is not neccesarily an ideal of R. This motivates definition 14.2.7.

Definition 14.2.7 (product of ideals)**.** Let R be a ring and $I_1, I_2 \subset R$ be ideals. We define product of ideals as follows:

$$I_1 I_2 = \{r \in R : \exists l \in \mathbb{N}^+ \text{ such that } r = \Sigma_{i=1}^{l} r_i^1 r_i^2, \text{ where } r_i^1 \in I_1, r_i^2 \in I_2 \text{ for } i = 1, \ldots, l\}.$$

Remark 14.2.8. $I_1 I_2$ is an ideal, as you should verify.

Proposition 14.2.9. *Let I_1, I_2 be ideals of a ring R. Then $I_1 I_2 \subset I_1 \cap I_2$.*

Proof. Immediate. □

Proposition 14.2.10. *Let I_1, I_2 be ideals of the ring $\mathbb{F}[x]$. Then $Z(I_1) \cup Z(I_2) = Z(I_1 I_2)$.*

Proof. For each $f \in I_1 I_2$, $f = \Sigma_{i=1}^{s} h_i g_i$ for some $h_1, \ldots, h_s \in I_1, g_1 \ldots, g_s \in I_2$. Then it is easy to see that f vanishes on $Z(I_1) \cup Z(I_2)$. Hence

$$I_1 I_2 \subset I_{Z(I_1) \cup Z(I_2)} \Rightarrow Z(I_1) \cup Z(I_2) \subset Z(I_1 I_2).$$

On the other hand, let $v \in Z(I_1 I_2)$. Suppose for the sake of contradiction that $v \notin Z(I_1) \cup Z(I_2)$, then there exist some $h \in I_1$ and $g \in I_2$ such that $h(v) \neq 0$ and $g(v) \neq 0$, which means that $hg(v) \neq 0$ ($\mathbb{F}$ is an integral domain). But $hg \in I_1 I_2$, contradicting to the fact $v \in Z(I_1 I_2)$. Hence $v \in Z(I_1) \cup Z(I_2)$. □

It can be easily verified that if an element r is in an ideal, then for each $n \in \mathbb{N}^+$ we have that r^n is in the same ideal. Conversely, we define a new set, called the radical of an ideal, as follows.

Definition 14.2.11 (radical of an ideal)**.** Let I be an ideal of a ring R. Then the set

$$\sqrt{I} = \text{rad}(I) = \{r \in R : \exists n \in \mathbb{N}^+ \text{ such that } r^n \in I\}$$

is called *the radical of the ideal I*.

Exercise 14.2.12. Let I be an ideal of a ring and $\sqrt{I}$ the radical of I. Show that $I \subset \sqrt{I}$.

Definition 14.2.13 (Zariski Topology)**.** We define $Y \subset \mathbb{F}^n$ to be a closed set if there is an ideal I of $\mathbb{F}[x]$ such that $Y = Z(I)$. These closed sets form a topology (indeed, this is called *Zariski Topology*).

Remark 14.2.14. To show that the closed sets defined in definition 14.2.13 form a topology, we need to show that

1. $\emptyset$ is closed.
2. $\mathbb{F}^n$ is closed.
3. Any union of finitely many closed sets are closed.
4. Any intersection of closed sets are closed.

The terms 1, 2, 3 are easily verified (for the term 3, you need to realize that if Y_1, Y_2 are closed, then there exist ideals I_1, I_2 such that $Y_1 \cup Y_2 = Z(I_1 I_2)$). To verify the term 4, you may want to check the proof by Ziyu in the piazza.

The definitions of *zero divisor* and *integral domain*, already given in lecture 12 (TA Session), are repeated here for your convenience.

Definition 14.2.15 (zero divisor)**.** A nonzero element a in a ring R is called a *zero divisor* if there is a nonzero element b in R such that $ab = 0$.

Definition 14.2.16 (integral domain)**.** A commutative ring R with identity is called an *integral domain* if, for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

Example 14.2.17 (The product of nonzero elements would be zero)**.**

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Example 14.2.18. $\mathbb{F}[x]$ is an integral domain. then $pq = 0 \Rightarrow p = 0$ or $q = 0$. Also check this page.

Proposition 14.2.19. *Let $X_1, X_2 \subset \mathbb{F}^n$. Then $I_{X_1 \cup X_2} = I_{X_1} \cap I_{X_2}$.*

Proof. Immediate. □

Definition 14.2.20 (prime ideal)**.** Let I be an ideal of the ring R. I is called *prime ideal* if $ab \in I$ where $a, b \in R$, then $a \in I$ or $b \in I$.

Example 14.2.21. The ring R itself is an ideal in R and is prime.

Example 14.2.22 (p)**.** The set $P = \{0, 2, 4, 6, 8, 10\}$ is an ideal in $\mathbb{Z}_{12} = \{0, 1, \dots, 11\}$. This ideal is prime.

Example 14.2.23 (p)**.** The set $4\mathbb{Z}$ of integers that are multiple of 4, i.e.,

$$4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\},$$

is an ideal in $\mathbb{Z}$. This ideal is not prime. However, $2\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Furthermore, $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ if and only if p is a prime number.

Theorem 14.2.24. *Let V be d-dimensional linear subspace of $\mathbb{F}^n$. Then I_V is a prime ideal.*

Proof. If $V = \mathbb{F}^n$, i.e., $d = n$, then $I_V = I_{\mathbb{F}^n} = \{0\}$, where $0 \in \mathbb{F}[x]$ denotes the zero polynomial in $\mathbb{F}[x]$. For any $g, h \in \mathbb{F}[x]$ such that

$$gh \in I_V \iff gh = 0\,,$$

we have, by example 14.2.18,

$$g = 0 \text{ or } h = 0 \iff g \in I_V \text{ or } h \in I_V\,.$$

This means that I_V is a prime ideal.

Now we begin to consider the case that V is a proper subset of $\mathbb{F}^n$, i.e., $d < n$. Let $v_1, v_2, \dots, v_d \in \mathbb{F}^n$ be an orthonormal basis for V and $u_{d+1}, u_{d+2}, \dots, u_n \in \mathbb{F}^n$ an orthogonal basis for $V^\perp$, where $V^\perp$ is the orthogonal complement of V. Hence v's and u's form an orthonormal basis for $\mathbb{F}^n$, say

$$B = [v_1, v_2, \dots, v_d, u_{d+1}, u_{d+2}, \dots, u_n]\,, \tag{14.2.1}$$

and we have $B^T B = I$. Also let $B_V = [v_1, v_2, \dots, v_d] \in \mathbb{F}^{n\times d}, B_{V^\perp} = [u_{d+1}, u_{d+2}, \dots, u_n] \in \mathbb{F}^{n\times(n-d)}$.

For any $g, h \in \mathbb{F}[x]$ such that $gh \in I_V$, there exist $p, q \in \mathbb{F}[x]$ such that for each $r \in \mathbb{F}^n$, we have $p(B^T r) = g(r), q(B^T r) = h(r)$. Hence

$$\begin{aligned} gh(r) &= g(r)h(r) \\ &= p(B^T r)q(B^T r) \\ &= p(v_1^T r, \dots, v_d^T r, u_{d+1}^T r, \dots, u_n^T r)q(v_1^T r, \dots, v_d^T r, u_{d+1}^T r, \dots, u_n^T r) \\ &= (p'(v_1^T r, \dots, v_d^T r) + \Sigma_{i=1}^{n-d}(u_{d+i}^T r)p_i(r))(q'(v_1^T r, \dots, v_d^T r) + \Sigma_{i=1}^{n-d}(u_{d+i}^T r)q_i(r))\,, \end{aligned} \tag{14.2.2}$$

where $p', q' \in \mathbb{F}[x_1, x_2, \dots, x_d]$ and $p_i, q_i \in \mathbb{F}[x]$ for $i = 1, 2, \dots n-d$. Since gh vanishes on V, we have that $p'(v_1^T w, \dots, v_d^T w)q'(v_1^T w, \dots, v_d^T w) = 0$ for each $w \in V$.

For any $\alpha \in \mathbb{F}^d$, let $z = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_d v_d \in V$. Then we have

$$\begin{aligned} p'(\alpha)q'(\alpha) &= p'(\alpha_1, \ldots, \alpha_d)q'(\alpha_1, \ldots, \alpha_d) \\ &= p'(v_1^T z, \ldots, v_d^T z)q'(v_1^T z, \ldots, v_d^T z) \\ &= 0. \end{aligned} \tag{14.2.3}$$

This means $p'q' = 0$, and thus by example 14.2.18, we have

$$\begin{aligned} & p' = 0 \text{ or } q' = 0 \\ \Rightarrow & g(r) = \Sigma_{i=1}^{n-d}(u_{d+i}^T r)p_i(r) \text{ or } h(r) = \Sigma_{i=1}^{n-d}(u_{d+i}^T r)q_i(r) \text{ for any } r \in \mathbb{F}^n \\ \Rightarrow & g \in I_V \text{ or } h \in I_V. \end{aligned} \tag{14.2.4}$$

This proves that I_V is a prime ideal. □

Proposition 14.2.25. *Let I_1, I_2 be ideals in $\mathbb{F}[x]$ and $I_1 \subset I_2$. Then we have $Z(I_2) \subset Z_(I_1)$.*

Proof. Immediate. □

We discussed problem 3 in the quiz, its geometry, and its applications in data clustering. Have a look at this paper for further information.

Theorem 14.2.26. *Let $X \subset \mathbb{F}^n$ and $I_X \subset \mathbb{F}[x]$ the vanishing ideal on X. Then $Z(I_X) = \overline{X}$, where $\overline{X}$ is the closure of X.*

Proof. Obviously $\overline{X} \subset Z(I_X)$ since $X \subset Z(I_X)$ and $Z(I_X)$ is closed. Let $\overline{X} = Z(J)$, where $J \in \mathbb{F}[x]$ is an ideal. Hence $J \subset I_{\overline{X}}$. Then we have

$$X \subset \overline{X} \Rightarrow J \subset I_{\overline{X}} \subset I_X \Rightarrow Z(I_X) \subset Z(J) \Rightarrow Z(I_X) \subset \overline{X}.$$

□

Review the final picture for a preview of the next week (radical, Hilbert Basis Theorem, Hilbert's Nullstellensatz, etc.)

14.3 Further Reading

SI112: Advanced Geometry	Spring 2018
Lecture 16-18 — May 3rd, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

15 Lecture 16-18

Consistency is the last refuge of the unimaginative.

—— Oscar Wilde

15.1 Overview of This Lecture

It turns out to be a brave thoughtlessness to refer to x^α as (multi-variable) monomials, as I used to do. It is painful to type $\underline{x}$ (the underline) in LaTeX, you know, very similar to the reason why Unix pioneers use the string *cp(mv)* instead of *copy(move)* to denote the command copy(move). Brave again, the symbol x from now on will be used to denote simply a single variable.

The goal of these three lectures is to prove Hilbert Basis Theorem, as described below.

Theorem 15.1.1 (Hilbert Basis Theorem)**.** *If every ideal of a ring R is finitely generated, then so is every ideal of $R[x]$.*

Corollary 15.1.2. *If every ideal of a ring R is finitely generated, then so is every ideal of $R[x_1, x_2, \ldots, x_n]$.*

15.2 Proof of Things

Definition 15.2.1 (module M over a ring R)**.** Let R be a ring. An *R-module* (or *module over R*) M consists of an abelian group $(M, +)$ and multiplication operation, denoted by juxtaposition, $R \times M \to M$ such that for all $r, s \in R$ and $u, v \in M$

- $r(u + v) = ru + rv$
- $(r + s)u = ru + su$
- $(rs)u = r(su)$
- $1u = u$

The ring R is called the *base ring* of M.

Definition 15.2.2 (submodule)**.** A *submodule* of an R-module M is a nonempty subset S of M that is an R-module in its own right, under the operations obtained by restricting the operations of M to S.

Proposition 15.2.3. *A nonempty subset S of an R-module M is a submodule if and only if it is closed under the taking of linear combinations, that is,*

$$r, s, \in R, u, v \in S \Rightarrow ru + sv \in S.$$

Proof. Left as an exercise. □

Proposition 15.2.4. *If S and T are submodules of a module M, then $S \cap T$ and $S + T$ are also submodules.*

Proof. Left as an exercise. □

Example 15.2.5. Vector space V over a field $\mathbb{F}$ is a module over $\mathbb{F}$.

Example 15.2.6. If R is a ring, then the sets $\mathbb{F}^n$, R^n are R-modules.

Example 15.2.7. The ring R is an R-module. Furthermore, every ideal of a ring R is a module, and thus a submodule of R. Finally and similarly, $R[x]$ is an R-module and every ideal of $R[x]$ is a submodule. You are invited to verify the converse: is every submodule of R or $R[x]$ an ideal?

Definition 15.2.8 (finitely generated ideal)**.** Let I be an ideal of the ring R. We said that I is *finitely generated* if there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in I$ such that for each $\alpha \in I$, there exist $r_1, r_2, \ldots, r_n \in R$ satisfying

$$\alpha = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n.$$

The set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is called *generating set* of I. We may also write for convenience like this: $I = R\alpha_1 + R\alpha_2 + \cdots + R\alpha_n$, where the symbol Rx is defined as $Rx = \{x' : x' = rx \text{ for some } r \in R\}$.

Definition 15.2.9 (finitely generated module)**.** An R-module M is finitely generated if there exists $\alpha_1, \alpha_2, \ldots, \alpha_n \in M$ such that for each $\alpha \in M$, there exist $r_1, r_2, \ldots, r_n \in R$ satisfying

$$\alpha = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n.$$

Remark 15.2.10. Notice in Definition 15.2.8 and Definition 15.2.9 that an ideal is a subset of a ring, while the module M is over a ring.

Definition 15.2.11 (morphism of R-modules)**.** Let M and M be R-modules. Then the function $f : M \to N$ is called a *morphism* from M to N if

- $f(x + y) = f(x) + f(y)$ for all $x, y \in M$
- $f(\alpha x) = \alpha f(x)$ for all $\alpha \in R, x \in M$

In addition, we define the set

$$\mathrm{Ker}(f) = \{x \in M : f(x) = 0\}$$

as the *kernel* of f and the set

$$\mathrm{Im}(f) = \{y \in N : y = f(x) \text{ for some } x \in M\}$$

the *image* of f.

Proposition 15.2.12. *Let $f : M \to N$ be a morphism of R-modules. Then the kernel $\mathrm{Ker}(f)$ and image $\mathrm{Im}(f)$ of f are submodules of M and N, respectively.*

Proof. Let $x_1, x_2 \in \mathrm{Ker}(f), r_1, r_2 \in R$. Then

- $f(r_1x_1 + r_2x_2) = r_1f(x_1) + r_2f(x_2) = 0$, which implies $r_1x_1 + r_2x_2 \in \mathrm{Ker}\, f$.
- $f(r_1x_1) \in \mathrm{Im}(f)$.

□

Exercise 15.2.13. Let $f : M \to N$ be a morphism of R-modules. Show that $f(0) = 0$.

Proposition 15.2.14. *Let $f : M \to N$ be a morphism of R-modules. Then f is injective if and only if $\mathrm{Ker}(f) = \{0\}$.*

Proof.

- Suppose f is injective and let $x \in \mathrm{Ker}(f)$. Then $f(x) = 0 = f(0)$. This implies $x = 0$.
- Suppose $\mathrm{Ker}(f) = \{0\}$ and let $x_1, x_2 \in M$ be such that $f(x_1) = f(x_2)$. Then

$$f(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in \mathrm{Ker}(f) \Rightarrow x_1 - x_2 = 0.$$

□

Definition 15.2.15 (exact sequence)**.** A sequence

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} M_n,$$

where f_i's are morphisms and M_i are modules, is called *exact* if the image of each morphism is equal to the kernel of the next, i.e., $\mathrm{Im}(f_k) = \mathrm{Ker}(f_{k+1})$ for $k = 0, 1, \ldots, n - 1$.

Exercise 15.2.16. Let $\{0\} \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to \{0\}$ be an exact sequence. Show that f is injective and g is surjective.

Example 15.2.17. Let R be a ring and $S = \{0\} \to R \xrightarrow{f} R^n \xrightarrow{g} R^{n-1} \to \{0\}$ a sequence. Then S is exact for the function $f : \alpha \mapsto (0_1, \ldots, 0_{n-1}, \alpha)$ and the function $g : (\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$, where $a_i \in R$ for $i = 1, \ldots, n$.

You may want to review the definitions of partially ordered set and maximal element. Check lecture 1 or wikipedia.

Proposition 15.2.18 (6.1\AM)**.** *Let Σ be a partially ordered set and $\leq$ the partial order relation on Σ. The following conditions on Σ are equivalent.*

1. *Every increasing sequence $x_1 \leq x_2 \leq \cdots$ in Σ is stationary, i.e., there exists a number n such that $x_n = x_{n+1} = \ldots$.*

2. *Every nonempty subset of Σ has a maximal element.*

Proof.

1. ($1 \Rightarrow 2$) Let S is a nonempty subset of Σ. Suppose for the sake of contradiction that S has no maximal element. Then there is an element a_1 in S though a_1 is not maximal. Hence there is an element $a_2 \in S$ such that $a_1 < a_2$. But a_2 can not be a maximal element. Inductively we can construct a non-terminating strictly increasing sequence in S. This is a contradiction.

2. ($2 \Rightarrow 1$) Let $x_1 \leq x_2 \leq \cdots$ be an increasing sequence in Σ. The sequence forms a set, say S. Let x_n be a maximal element of S. Then we have $x_n = x_{n+1} = \ldots$, i.e., this sequence is stationary.

□

Remark 15.2.19. If Σ is the set of submodules of a module M, ordered by set inclusion $\subset$, then the condition (1) is called *ascending chain condition* (a.c.c or ACC for short). A module M satisfying either of these equivalent conditions is said to be *Noetherian* (after Emmy Noether).

Definition 15.2.20 (Noetherian)**.** Let M be an R-module. R is *Noetherian* if it satisfies the ACC on the set of its submodules.

Exercise 15.2.21. Prove that if a module is Noetherian, then all of its submodules are Noetherian.

Proposition 15.2.22 (6.2\AM)**.** *M is Noetherian R-module if and only if every submodule of M is finitely generated.*

Proof.

- Suppose that M is a Neotherian R-module. Let N be a submodule of M. We need to prove that N is finitely generated. Let Σ be the set of all finitely generated submodules of N. Then we know that Σ is not empty ($\{0\} \in \Sigma$) and there therefore exists some maximal element N_0 of Σ (why?). If $N = N_0$ we are done. Otherwise let $y \in N \backslash N_0$, then $N_0 + Ry$ properly contains N_0. But the set $N_0 + Ry$ properly containing N_0 is finitely generated, implying $N_0 + Ry \in \Sigma$, which contradicts the maximality of N_0.

- Suppose that every submodule of M is finitely generated. Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules of M. Then $N = \cup_{i=1}^{\infty} M_i$ is a submodule of M (why?). Hence N is finitely generated, i.e., there exist some $x_1, x_2, \ldots, x_n \in N$ such that $N = Rx_1 + Rx_2 + \cdots Rx_n$. Now suppose $x_i \in M_{k_i}$ for $i = 1, \ldots, n$ and let $k = \max_{i=1,\ldots,n}\{k_i\}$. Then $x_1, x_2, \ldots, x_n \in M_k$. Then we have

  $$N = Rx_1 + Rx_2 + \cdots + Rx_n \subset M_k \subset N,$$

  which means $M_k = N$. Hence $N = M_k = M_{k+1} = \ldots$, that is, the ascending chain

  $$M_1 \subset M_2 \subset \cdots$$

  is stable.

□

Hilbert Basis Theorem (Theorem 15.1.1) then can be equivalently stated as follows.

Theorem 15.2.23. *If R is a Noetherian ring, then $R[x]$ is a Noetherian ring.*

Corollary 15.2.24. *If R is a Noetherian ring, then $R[x_1, x_2, \ldots, x_n]$ is a Noetherian ring.*

Exercise 15.2.25 (p)**.** Let $f : M' \to M$ be a morphism of R-modules and S', S submodules of M', M respectively. Prove that $f(S'), f^{-1}(S)$ are submodules of M, M' respectively.

Lemma 15.2.26 (p)**.** *Let $f : M' \to M$ be an injective function and let S_1, S_2 be subset of M such that $f^{-1}(S_1) = f^{-1}(S_2)$. Then $S_1 \cap \mathrm{Im}(f) = S_2 \cap \mathrm{Im}(f)$.*

Proof. It is enough to show $S_1 \cap \mathrm{Im}(f) \subset S_2 \cap \mathrm{Im}(f)$. Another direction can be proved directly by symmetry. Let $y \in S_1 \cap \mathrm{Im}(f)$. Specifically $y \in \mathrm{Im}(f)$. Hence there exists a unique $x \in M'$ such that $x = f^{-1}(y) \iff f(x) = y$. This implies

$$x \in f^{-1}(S_1) = f^{-1}(S_2) \Rightarrow y = f(x) \in S_2.$$

□

Remark 15.2.27. Lemma 15.2.26 can be proved pictorially.

Remark 15.2.28. After Exercise15.2.25 and Lemma 15.2.26, we are able to prove the following proposition. Note that I pointed to a wrong way in piazza for this proposition. The mistake I made is that I manipulated submodules as pure sets. As a remainder, when we say that a module is Neotherian, we are saying that it is the set of its submodules that satisfy ascending chain condition.

Proposition 15.2.29 (6.3\AM)**.** *Let* $\{0\} \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to \{0\}$ *be an exact sequence. Then* M *is Neotherian if and only if* M' *and* M'' *are Neotherian.*

Proof.

- $\Rightarrow$) Suppose M is Neotherian. We need to prove M' (resp. M'') is Neotherian. Let $N_1 \subset N_2 \subset \cdots$ be an ascending chain of the submodules of M' (resp. M''). Then by Exercise 15.2.25,

  $$f(N_1) \subset f(N_2) \subset \cdots \text{ (resp. } g^{-1}(N_1) \subset g^{-1}(N_2) \subset \cdots)$$

  is an ascending chain of the submodules of M. This implies that there is some $n \in \mathbb{N}^+$ such that

  $$f(N_n) = f(N_{n+i}) \text{ (resp. } g^{-1}(N_n) = g^{-1}(N_{n+i}))$$

  for $i \in \mathbb{N}$ and thus $N_n = N_{n+i}$ for $i \in \mathbb{N}$ (by injectivity of f or surjectivity of g). Hence M' (resp. M'') is Neotherian.

- $\Leftarrow$) Suppose M' and M'' are Neotherian. We need to prove M are Neotherian. Let $S_1 \subset S_2 \subset \cdots$ be an ascending chain of the submodules of M. Then by Exercise 15.2.25,

  $$f^{-1}(S_1) \subset f^{-1}(S_2) \subset \cdots \text{ and } g(S_1) \subset g(S_2) \subset \cdots$$

  are ascending chains of the submodules of M' and M'' respectively, which implies that there are some n' and n'' such that

  $$f^{-1}(S_{n'}) = f^{-1}(S_{n'+i}) \text{ and } g(S_{n''}) = g(S_{n''+j})$$

  for $i, j \in \mathbb{N}$. Let $n = \max\{n', n''\}$. It is enough to show that $S_n = S_{n+k}$ for $k \in \mathbb{N}$. But $S_n \subset S_{n+k}$, it suffices to show that for each $a_{n+k} \in S_{n+k}$, we have $a_{n+k} \in S_k$.

  Let $a_{n+k} \in S_{n+k}$. That $g(S_{n+k}) = g(S_n)$ implies that there exists some $b_n \in S_n \subset S_{n+k}$ such that

  $$g(a_{n+k}) = g(b_n) \Rightarrow g(a_{n+k} - b_n) = 0 \Rightarrow a_{n+k} - b_n \in \mathrm{Ker}(g) = \mathrm{Im}(f).$$

But $a_{n+k} - b_n \in S_{n+k}$, hence by Lemma 15.2.26,

$$a_{n+k} - b_n \in S_{n+k} \cap \mathrm{Im}(f) = S_n \cap \mathrm{Im}(f) \Rightarrow a_{n+k} - b_n \in S_n.$$

Now we can conclude $a_{n+k} \in S_n$ since $b_n \in S_n$.

□

Lemma 15.2.30. *Let R be a Neotherian ring. Then R^n is Neotherian for each $n \in \mathbb{N}^+$.*

proof skeleton. Recall Example 15.2.17, Proposition 15.2.29 and use induction on n. □

Proposition 15.2.31 (6.5\AM)**.** *Let R be a Neotherian ring and M finitely generated R-module. Then M is Neotherian.*

proof skeleton. There exist some $x_1, x_2, \ldots, x_n \in M$ such that $M = Rx_1 + Rx_2 + \cdots + Rx_n$. By Lemma 15.2.30 and Proposition 15.2.29, it is enough to find a morphism $f : R^n \to M$ with f surjective. □

Now we are ready to prove the theorem.

Theorem 15.2.32 (7.5\AM, Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is a Noetherian ring.*

Proof. It is enough to prove that every ideal $\overline{I}$ of $R[x]$ is finitely generated. Let

$$I = \{a \in R : \ a \text{ is the leading coefficient of } f \text{ for some } f \in \overline{I}\}.$$

Then I is an ideal since

- $0 \in I$,
- If $\alpha \in I$ and $r \in R$, then $r\alpha \in I$, and
- If $\alpha_1, \alpha_2 \in I$, then $\alpha_1 + \alpha_2 \in I$ (If $\alpha_1, \alpha_2 \in I$ then there exist $f_1, f_2 \in \overline{I}$ such that $f_1 = \alpha_1 x^{m_1} + \cdots$ and $f_2 = \alpha_2 x^{m_2} + \cdots$. Suppose without loss of generality that $m_1 \geq m_2$ and consider $f_1 + x^{m_1 - m_2} f_2$).

Since R is Neotherian and I is a submodule of R, by Proposition 15.2.22, I is finitely generated, i.e.,

$$I = R\alpha_1 + R\alpha_2 + \cdots R\alpha_n$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in I$. Then there exist $f_1, f_2, \ldots, f_n \in \overline{I}$ such that

$$f_i = \alpha_i x^{m_i} + \cdots \text{ for } i = 1, 2, \ldots, n.$$

Let $d_{\max} = \max\{m_1, m_2, \ldots, m_n\}$ and Let $\overline{\overline{I}}$ be the ideal generated by $f_1, f_2, \ldots, f_n$. Then $\overline{\overline{I}} \subset \overline{I}$. Let $f = \alpha x^m + \cdots \in \overline{I}$. Then $\alpha \in I$ and thus there exist $r_1, r_2, \ldots, r_n \in R$ such that

$$\alpha = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n = \Sigma_{i=1}^n r_i\alpha_i.$$

Noticing that $\Sigma_{i=1}^n r_i f_i x^{m-m_i} \in \overline{\overline{I}} \subset \overline{I}$, the polynomial $f - \Sigma_{i=1}^n r_i f_i x^{m-m_i}$ is in $\overline{I}$ and its degree is less than m. Proceeding in this way, we can go on subtracting elements of $\overline{\overline{I}}$ from f until we obtain a polynomial $g \in \overline{I}$ of degree less than $d_{\max}$ (can we obtain a polynomial of degree less than $d_{\min} = \min\{m_1, m_2, \ldots, m_n\}$?). That is, $f = h + g$, where $h \in \overline{\overline{I}}$ and $g \in \overline{I}$ is a polynomial of degree less than $d_{\max}$.

Let M be the R-module (finitely) generated by $1, x, x^2, \cdots, x^{d_{\max}}$. Then $g \in M \cap \overline{I}$ and

$$\overline{I} = \overline{\overline{I}} + M \cap \overline{I}.$$

We know from Proposition 15.2.31 that M is Neotherian. Hence $M \cap \overline{I}$ as a submodule of M (by Proposition 15.2.4) is finitely generated by Proposition 15.2.22. Let $M \cap \overline{I}$ be (finitely) generated by $g_1, g_2, \ldots, g_k$, then $\overline{I}$ is (finitely) generated by $f_1, f_2, \ldots, f_n$ and $g_1, g_2, \ldots, g_k$. □

Corollary 15.2.33. *If every ideal of a ring R is finitely generated, then so is every ideal of $R[x_1, x_2, \ldots, x_n]$.*

Proof. It holds for the case $n = 1$ because of Theorem 15.2.32. Suppose inductively that it holds for the case $n - 1$, i.e., $R[x_1, x_2, \ldots, x_{n-1}]$ is Neotherian. Then (you may want to review the multiplication of two ideals)

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}]R[x_n]$$

is a polynomial ring $R[x_n]$ over the Neotherian ring $R[x_1, x_2, \ldots, x_{n-1}]$. Again by Theorem 15.2.32, $R[x_1, x_2, \ldots, x_n]$ is Neotherian. That is, the case n holds. □

Corollary 15.2.34. *$\mathbb{F}[x]$ is Neotherian for any field $\mathbb{F}$.*

The topics for the next lecture are *quotient spaces* and *localization*.

15.3 Further Reading

- AM: http://www.saheleriyaziyat.net/images/k1zut2e5peefixbx6kty.pdf.
- Chapter 2 of this book: Ideals, Varieties, and Algorithms.

SI112: Advanced Geometry	Spring 2018
Lecture 19 — May 5th, Difficult Day	
Prof. Manolis	*Scribe*: Liangzu

16 Lecture 19

16.1 Overview of This Lecture

quotient space, quotients of vector space.

16.2 Proof of Things

Definition 16.2.1 (quotients of vector spaces)**.** Let V be a vector space over a field $\mathbb{F}$ and U a subspace of V. Define a relation $\sim$ as follows:

$$x, y \in V, x \sim y \iff x - y \in U.$$

Exercise 16.2.2. Show that the relation defined in is an equivalence relation.

Definition 16.2.3. The set V/U to be the set of equivalences of V under $\sim$, i.e.,

$$V/U = \{y \in V : x \sim y\}.$$

reminder: $[x]_\sim = \{y \in V : x \sim y\}$.

Proposition 16.2.4. $[x]_\sim = \{x + u : u \in U\}$.

16.3 Further Reading

SI112: Advanced Geometry	Spring 2018
Lecture 20-21 — May 10th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

17 Lecture 20-21

17.1 Overview of This Lecture

The goal of this two lectures is to prove Hilbert's Nullstellensatz (and its consequences).

17.2 Proof of Things

Definition 17.2.1. A proper ideal I of a ring R is called *prime* if $ab \in I$ implies $a \in I$ or $b \in I$ for any elements $a, b \in R$.

Definition 17.2.2 (maximal ideal)**.** A proper ideal m of a ring R is called *maximal* if $m \subset I$ implies $m = I$ or $I = R$ for any ideal $I \subset R$.

Example 17.2.3. The zero ideal of some ring R is prime if and only if R is an integral domain. For a field $\mathbb{F}$ the zero ideal $0 \subset \mathbb{F}$ is prime and maximal at the same time.

Proposition 17.2.4. *Let R be a ring and $I \subset R$ an ideal. Then I is prime if and only if R/I is an integral domain.*

Proof. Let $a, b \in R$ (i.e., $\overline{a}, \overline{b} \in R/I$). Then

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

is equivalent to

$$\overline{a}\overline{b} = 0 \Rightarrow \overline{a} = 0 \text{ or } \overline{b} = 0.$$

□

Proposition 17.2.5. *Let R be a ring and m an ideal of R. Then m is a maximal ideal of the ring R if and only if R/m is a field.*

Proof.

- $\Rightarrow$) To prove that R/m is a field, we need to show that every nonzero element in R/m is invertible. Let $a + m \in R/m$ be a nonzero element in R/m. Then $Ra + m$ is an

ideal properly containing m (you should verify that $Ra + m$ is an ideal). This means $Ra + m = R$. Then there exists $r \in R, \mu \in m$ such that

$$ra+\mu = 1 \iff ra+\mu+m = 1+m \iff ra+m = 1+m \iff (r+m)(a+m) = 1+m.$$

This implies that $a + m$ is invertible.

- $\Leftarrow$) Since R/m is a field, it must contain at least two elements: $0 + m = m$ and $1 + m$. Hence, m is a proper ideal of R. Let I be an ideal properly containing m. We need to show that $I = R \iff 1 \in I$. Let $a \in I - M$. Since $a + m$ is a nonzero element in a field, there exists an element $b+m$ in R/M such that $ab+m = (a+m)(b+m) = 1+m$. Hence there exists an element $\mu \in m$ such that $ab + \mu = 1 \Rightarrow 1 \in I$.

□

The following corollary is a direct consequence of Proposition 17.2.4 and Proposition 17.2.5.

Corollary 17.2.6. *Let m be a maximal ideal of a ring. Then m is prime.*

Proposition 17.2.7. *The ring $\mathbb{C}[x_1, x_2, \ldots, x_n]$ contains a maximal ideal.*

Proof. $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is Noetherian. □

Proposition 17.2.8. *Let I be a proper ideal in $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then there exists a maximal ideal $m \subset \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $I \subset m$.*

Proof. $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is Noetherian. □

Theorem 17.2.9. *Let m be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then m is maximal if and only if $m = \langle x_1 - \alpha_1, \ldots, x_1 - \alpha_n \rangle$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$.*

Proof.

- $\Rightarrow$) Cor 7.10\ AM (difficult).
- $\Leftarrow$) It is enough to show that $\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{\langle x_1-\alpha_1,\ldots,x_n-\alpha_n\rangle}$ is a field. For $i = 1, 2, \ldots, n$, we have $[x_i] = [\alpha_i]$ since $x_i - \alpha_i \in \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$. Hence (before this "hence", ask yourself: what is the equivalence class of $p \in \mathbb{C}[x_1, x_2, \ldots, x_n]$?)

$$\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle} \cong \mathbb{C}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{C}$$

is a field.

□

Theorem 17.2.10 (Hilbert's Nullstellensatz, weak form)**.** *Let $T \neq \emptyset$ be a set of polynomials in $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then $Z(T) = \emptyset$, where $Z(T) = \{v \in \mathbb{C}^n : f(v) = 0, \forall f \in T\}$, if and only if the ideal I generated by T contains* 1.

Proof.

- $\Rightarrow$) Suppose $1 \notin I$. We will show that $Z(T) \neq \emptyset$. $1 \notin I$ implying $I \neq \mathbb{C}[x_1, x_2, \ldots, x_n]$, by Proposition 17.2.8 and Theorem 17.2.9, there exists a maximal ideal $m = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ in $\mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $I \subset m$. Hence $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in Z(T)$: Let $p(\underline{x}) = \Sigma c_{\underline{w}} \underline{x}^{\underline{w}} \in T \subset m$. Then

$$0 = [p(\underline{x})] = [\Sigma c_{\underline{w}} \underline{x}^{\underline{w}}] = \Sigma c_{\underline{w}} [\underline{x}]^{\underline{w}} = \Sigma c_{\underline{w}} [\underline{\alpha}]^{\underline{w}} = p(\underline{\alpha}).$$

- $\Leftarrow$) There exist $t_1, t_2, \ldots, t_l \in T, r_1, r_2, \ldots, r_l \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that

$$r_1 t_1 + r_2 t_2 + \cdots + r_l t_l = 1.$$

  Hence $Z(T) = \emptyset$, for otherwise let $v \in Z(T)$ then we have

$$0 = r_1(v) t_1(v) + r_2(v) t_2(v) + \cdots + r_l(v) t_l(v) = 1,$$

  a contradiction.

□

Definition 17.2.11. The spectrum of a ring R, denoted by $\mathrm{Spec}(R)$, is the set of all prime ideals in R.

Exercise 17.2.12. Let J be an ideal of a ring R, prove that the radical

$$\sqrt{J} = \{r \in R : r^l \in J \text{ for some } l \in \mathbb{N}^+\}$$

of J is an ideal of R.

Let R be a ring and let $f \in R$ be such that f is not nilpotent. Note that in general f is not invertible in R. What we want to do now is to construct a ring R_f and a homomorphism $\phi : R \to R_f$ such that $\phi(f)$ is invertible in R_f. Then we may want to have some manipulations on $\phi(f)$, and return back to R (e.g., via ϕ^{-1}). The construction process is called *localization*, described as below.

Let R be a ring and let $f \in R$ be such that f is not nilpotent. Define a set $T = \{1, f, f^2, \cdots\}$ and define a relation $\sim$ on $R \times T$ by

$$(r, t) \sim (r', t') \iff \text{there is some } t'' \in T \text{ such that } t''(rt' - r't) = 0.$$

The relation is an equivalence relation as you should verify.

Now consider the set $(R \times T)/\sim$ of all equivalence classes in $R \times T$ under the relation $\sim$ and write $\frac{r}{t}$ for the class of an element $(r,t) \in R \times T$, i.e., $(R \times T)/\sim = \{\frac{r}{t} : r \in R, t \in T\}$. The set $(R \times T)/\sim$ is a ring under the standard addition and multiplication of fractional arithmetic

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

You should first verify that these two operations are well-defined. Furthermore, it is easily checked that $\frac{0}{1}$ is the zero element and $\frac{1}{1}$ is the unit element. As a more handy notation, we will write R_f instead of $(R \times T)/\sim$.

The inclusion map $i : R \to R \times T$ maps $r \in R$ to $(r,1) \in R \times T$ and the canonical homomorphism $\pi : R \times T \to R_f$ maps $(r,t) \in R \times T$ to its equivalence class $\frac{r}{t} \in R_f$. This implies $\pi i(f)$ is invertible in R_f, as desired.

Definition 17.2.13 (localization of a ring by an element in the ring)**.** Let R be a ring and $f \in R$ be such that f is not nilpotent. Let $T = \{1, f, f^2, \cdots\}$ Then $R_f = (R \times T)/\sim$ is called the *localization* of R by f.

Theorem 17.2.14 (Hilbert's Nullstellensatz, strong form)**.** *Let J be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$ and let $Y = Z(J)$. Then $I_Y = \sqrt{J}$.*

Proof. Let $g \in \sqrt{J}$, i.e., there exists m such that $g^m \in J$. Then g^m vanishes on $Z(J)$, and thus g vanishes on $Z(J)$ ($\mathbb{C}[x_1, x_2, \ldots, x_n]$ is an integral domain). Hence $g \in I_{Z(J)}$. It remains to be shown that $I_{Z(J)} \subset \sqrt{J}$.

Suppose that the polynomial $f \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ vanishes on $Y = Z(J)$, i.e., $f \in I_{Z(J)}$. If f is nilpotent, i.e., $f^m = 0 \in \sqrt{J}$ for some $m \in \mathbb{N}^+$, we are done. Now suppose f is not nilpotent.

The set of polynomials $J \cup \{1 - x_{n+1}f\} \subset \mathbb{C}[x_1, x_2, \ldots, x_{n+1}]$ has no roots in $\mathbb{C}^{n+1}$ (for otherwise there is $v = (v_1, v_2, \ldots, v_{n+1}) \in \mathbb{C}^{n+1}$ such that $p(v) = 0$ for all $p \in J$ and $1 - v_{n+1}f(v) = 0$, implying $v \in Z(J) \iff f(v) = 0$, then $1 = 0$). Then by Theorem 17.2.10, 1 is in the ideal generated by $J \cup \{1 - x_{n+1}f\}$. Hence, (a little bit tricky) there exist

$$p_1, p_2, \ldots, p_s \in J,$$

$$h_1, h_2, \ldots, h_s \in \mathbb{C}[x_1, x_2, \ldots, x_n],$$

$$h'_1, h'_2, \ldots, h'_s \in \mathbb{C}[x_{n+1}],$$

and

$$h \in \mathbb{C}[x_1, x_2, \ldots, x_{n+1}]$$

such that

$$1 = p_1h_1h'_1 + p_2h_2h'_2 + \cdots + p_sh_sh'_s + h(1 - x_{n+1}f).$$

Let $p_i' = p_i h_i \in J$ for $i = 1, 2, \cdots, s$, then we have

$$1 = p_1' h_1' + p_2' h_2' + \cdots + p_s' h_s' + h(1 - x_{n+1} f).$$

Now let

$$\phi : \mathbb{C}[x_{n+1}] \to (\mathbb{C}[x_{n+1}])_f = \{\frac{g}{f^l} : g \in \mathbb{C}[x_{n+1}], l \in \mathbb{N}\}$$

be a ring homomorphism that maps $q(x_{n+1}) \in \mathbb{C}[x_{n+1}]$ to $q(\frac{1}{f}) \in (\mathbb{C}[x_{n+1}])_f$. For example, ϕ maps $q(x_{n+1}) = x_{n+1}^2 + x_{n+1}$ to $q(\frac{1}{f}) = \frac{1}{f^2} + \frac{1}{f}$. Noticing that $\phi(1) = \frac{1}{1}, \phi(x_{n+1}) = \frac{1}{f}$ and $\phi(h_i'(x_{n+1})) = h_i'(\frac{1}{f})$ for $i = 1, 2, \cdots, s$, we have

$$\frac{1}{1} = p_1'(x_1, x_2, \ldots, x_n) h_1'(\frac{1}{f}) + \cdots + p_s'(x_1, x_2, \ldots, x_n) h_s'(\frac{1}{f}). \tag{17.2.1}$$

Let d be the maximal degree of h_i's. Multiplying Eq. 17.2.1 by f^d we obtain

$$\frac{f^d}{1} = p_1'(x_1, x_2, \ldots, x_n)(h_1'(\frac{1}{f}) f^d) + \cdots + p_s'(x_1, x_2, \ldots, x_n)(h_s'(\frac{1}{f}) f^d).$$

Notice that for $i = 1, 2, \cdots, s$, $h_i'(\frac{1}{f}) f^d$ is of the form $\frac{g_i f^{k_i}}{1}$ where $g_i \in \mathbb{C}[x_{n+1}]$ and $0 \leq k_i \leq d, k_i \in \mathbb{N}$. There is a homomorphism $\psi : (\mathbb{C}[x_{n+1}])_f \to \mathbb{C}[x_{n+1}]$ that maps $\frac{g_i f^{k_i}}{1}$ to $g_i f^{k_i}$. Then

$$f^d = p_1'(x_1, x_2, \ldots, x_n) g_1 f^{k_1} + \cdots + p_s'(x_1, x_2, \ldots, x_n) g_s f^{k_s},$$

which means that $f^d \in J$ and hence $f \in \sqrt{J}$. □

Proposition 17.2.15. *Let J be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then $Z(J) = Z(\sqrt{J})$.*

Proof. We have $Z(\sqrt{J}) \subset Z(J)$ since $J \subset \sqrt{J}$. Now let $v \in Z(J)$. For each $p \in \sqrt{J}$, there is some $m \in \mathbb{N}^+$ such that $p^m \in J$, then $p^m(v) = 0 \iff (p(v))^m = 0$. Hence $p(v) = 0$ for $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is an integral domain. □

Theorem 17.2.16. *There is a one-to-one correspondence between closed sets of $\mathbb{C}^n$ and radical ideals of $\mathbb{C}[x_1, x_2, \ldots, x_n]$.*

Proof. Let Y be closed, i.e., $Y = Z(J)$ for some J being an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then

$$Y \mapsto I_Y = \sqrt{J} \mapsto Z(\sqrt{J}) = Z(J) = Y.$$

□

Remark 17.2.17. Let X be any set of $\mathbb{C}^n$. Then

$$X \mapsto I_X \mapsto Z(I_X) = \overline{X} \mapsto \sqrt{I_X} = I_{\overline{X}}.$$

Theorem 17.2.18 (Hartshorne\Prp I.1.5, p5)**.** *Let Y be a closed set $\iff$ $Y = Z(J)$ $\iff$ Y algebraic variety. Then Y can be uniquely written as $Y = Y_1 \cup \cdots \cup Y_s$, where Y_i's are irreducible closed sets.*

Proof. □

Lemma 17.2.19. *Let R be a ring and P a prime ideal. Let $J_1, J_2, \ldots, J_s$ be ideals of R. If $J_1 \cap \cdots \cap J_s \subset P$, then $J_i \subset P$ for some i.*

Proof. Suppose $J_i \not\subset P$ for any $i = 1, 2, \cdots, s$. Then for any $i = 1, 2, \cdots, s$, there is some $\alpha_i \subset J_i$ such that $\alpha_i \notin P$. Let $\alpha = \alpha_1\alpha_2 \cdots \alpha_s$. Then $\alpha \notin P$ since P is prime. But $\alpha \in J_1 \cap \cdots \cap J_s \subset P$ since J_i's are ideals of R. This is a contradiction. □

Definition 17.2.20 (Irreducible Space)**.** A topological space X is called *irreducible* if X is not the union of any two proper closed sets, i.e., there are no closed subsets $Y_1, Y_2 \subsetneq X$ such that $X = Y_1 \cup Y_2$.

Theorem 17.2.21. *Let Y be a closed set of $\mathbb{C}^n$. Then Y is irreducible if and only if I_Y is prime.*

Proof.

- $\Rightarrow$) Let $f, g \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ such that $fg \in I_Y$. Then we have

$$\langle fg \rangle \subset I_Y \Rightarrow Y = \overline{Y} = Z(I_Y) \subset Z(\langle fg \rangle) = Z(fg) = Z(f) \cup Z(g),$$

  which implies $Y = (Z(f) \cap Y) \cup (Z(g) \cap Y)$. Since Y is irreducible and $Z(f) \subset Y, Z(g) \subset Y$ are closed, either $Y = Z(f) \cap Y$ or $Y = Z(g) \cap Y$. Without loss of generality let $Y = Z(f) \cap Y$, then we have

$$Y \subset Z(f) \Rightarrow \langle f \rangle \subset \sqrt{\langle f \rangle} = I_{Z(\langle f \rangle)} = I_{Z(f)} \subset I_Y.$$

  Hence I_Y is prime.

- $\Leftarrow$) Suppose $Y = Y_1 \cup Y_2$ where Y_1, Y_2 are closed subsets of Y. Then we have

$$I_Y = I_{Y_1 \cup Y_2} = I_{Y_1} \cap I_{Y_2} \Rightarrow I_Y \subset I_{Y_1}, I_Y \subset I_{Y_2}. \tag{17.2.2}$$

  By Lemma 17.2.19, we have either $I_{Y_1} \subset I_Y$ or $I_{Y_2} \subset I_Y$ and hence either

$$I_{Y_1} = I_Y \iff Y_1 = Z(I_{Y_1}) = Z(I_Y) = Y$$

  or

$$I_{Y_2} = I_Y \iff Y_2 = Z(I_{Y_2}) = Z(I_Y) = Y.$$

  Consequently Y is irreducible.

□

17.3 Further Reading

- Chapter 1, Algebraic Geometry and Commutative Algebra: https://www.springer.com/la/book/9781447148289
- Chapter 16, Abstract Algebra: Theory and Applications

SI112: Advanced Geometry	Spring 2018
Lecture 22 — May 15th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

18 Lecture 22

18.1 Overview of This Lecture

It takes us almost the whole lecture (i.e., lecture 22) to prove irreducible decomposition theorem.

18.2 Proof of Things

Lemma 18.2.1. *Let Σ be the set of all closed set in $\mathbb{F}^n$ and G a subset of Σ. Then G contains a minimal element.*

Proof. Let $G' = \{I_Y : Y \in G\}$. Then G' is a set of (vanishing) ideals, where the ideals are in the Noetherian ring $\mathbb{F}[x_1, x_2, \dots, x_n]$, which means that there is a maximal element I_{Y^*} in G'. We will show that Y^* is a minimal element in G. Let $Y \subset Y^* \in G$. Then

$$I_{Y^*} \subset I_Y \in G' \Rightarrow I_{Y^*} = I_Y \Rightarrow Y^* = \overline{Y^*} = Z(I_{Y^*}) = Z(I_Y) = \overline{Y} = Y.$$

This proves that Y^* is minimal in G. □

Theorem 18.2.2 (irreducible decomposition theorem, Hartshorne\Prp I.1.5, p5)**.** *Let Y be a nonempty closed set of $\mathbb{F}^n$ ($\mathbb{F}^n$ is an infinite field). Then Y can be uniquely written as $Y = Y_1 \cup \cdots \cup Y_n$, where Y_i's are irreducible closed sets and $Y_i \not\subset Y_j$ for $i \neq j$.*

Proof. We first prove the existence and then the uniqueness. For uniqueness part a wrong proof is additionally given.

- **Existence.** Let G be the set of nonempty closed subsets of $\mathbb{F}^n$ that can not be written as a finite union of irreducible closed subsets. It is enough to show $G = \emptyset$, from which we will know that every closed subsets of $\mathbb{F}^n$ can be decomposed. Then there are three immediate observations to understand the structure of G.

  1. There is a minimal element Y^* in G by Lemma 18.2.1.
  2. every nonempty closed set Y in G is not irreducible, for otherwise $Y = Y$ is a unique irreducible decomposition.

3. every nonempty closed set X, which is not in G, can be (uniquely) written as a finite union of irreducible closed subsets $X_1 \cup X_2 \cup \cdots \cup X_n$.

Then, specifically, the set Y^* as a minimal element in G is not irreducible, i.e., $Y^* = Y \cup Y'$ for some Y, Y' being nonempty proper closed subsets of Y^*. Hence $Y, Y' \notin G$ by the minimality of Y^*. Observation 3. tells us that there exist some $Y_1, Y_2, \ldots, Y_n, Y_1', Y_2', \ldots, Y_m'$ such that $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_n$ and $Y' = Y_1' \cup Y_2' \cup \cdots \cup Y_m'$. This implies

$$Y^* = Y_1 \cup Y_2 \cup \cdots \cup Y_n \cup Y_1' \cup Y_2' \cup \cdots \cup Y_m',$$

contradicting to the construction of G. Hence $G = \emptyset$.

We conclude that every closed set Y in $\mathbb{F}^n$ can be written as a union $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_n$ of irreducible subsets. By throwing away a few if necessary, we may assume $Y_i \not\subset Y_j$ for $i \neq j$.

- **Uniqueness.** Now suppose $Y = Y_1' \cup Y_2' \cup \cdots \cup Y_m'$ is another such representation and $n \leq m$. Then we have

$$Y_1 \subset Y = Y_1' \cup Y_2' \cup \cdots \cup Y_m' \Rightarrow Y_1 = \cup_{i=1}^m (Y_1 \cap Y_i').$$

But Y_1 is irreducible, hence

$$Y_1 = Y_1 \cap Y_j' \iff Y_1 \subset Y_j'$$

for some $j \in \{1, 2, \ldots, m\}$, say without loss of generality $j = 1$. Similarly we have $Y_1' \subset Y_i$ for some $i \in \{1, 2, \ldots, n\}$. Hence $Y_1 (\subset Y_1') \subset Y_i$. But $Y_i \not\subset Y_j$ for $i \neq j$. This implies $i = 1$. Then $Y_1 = Y_1'$. Going deeper, we can do the similar for Y_2 to obtain $Y_2 = Y_2'$. Indeed,

$$Y_2 \subset Y = Y_1' \cup Y_2' \cup \cdots \cup Y_m' \Rightarrow Y_2 = \cup_{i=1}^m (Y_2 \cap Y_i'),$$

which, by irreducibility of Y_2, means

$$Y_2 = Y_2 \cap Y_j' \iff Y_2 \subset Y_j'$$

for some $j \in \{2, 3 \ldots, m\}$ (j can not be 1, for otherwise $Y_2 \subset Y_1' = Y_1$), say $j = 2$. Then similarly we have $Y_2' \subset Y_i$ for some $i \in \{2, 3, \ldots, n\}$, which means $i = 2$ and thus $Y_2 = Y_2'$. Continuing in this way we have $Y_i = Y_i'$ for $i = 1, 2, \ldots n$. Then we have $n = m$ for a similar reason (Consider Y_{n+1}' if $n < m$).

□

SI112: Advanced Geometry	Spring 2018
Lecture 23 — May 17th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

19 Lecture 23

Section 8.1 and 8.2 in the book Ideals, Varieties, and Algorithms give rich examples for projective spaces and varieties, though a little bit wordy.

19.1 Further Reading

- Section 8.1, 8.2 in this book: Ideals, Varieties, and Algorithms.

SI112: Advanced Geometry	Spring 2018
Lecture 24 — May 15th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

20 Lecture 24

20.1 Overview of This Lecture

20.2 Proof of Things

Definition 20.2.1. The spectrum of a ring R, denoted by $\mathrm{Spec}(R)$, is the set of all prime ideals in R. That is

$$\mathrm{Spec}(R) = \{I \subset R : \ I \text{ is prime ideal of } A\}.$$

Proposition 20.2.2 (contraction of an ideal)**.** *Let $f : A \to B$ be a ring homomorphism and $I \subset B$ an ideal. Then the inverse image $f^{-1}(I)$ is an ideal of A, called the contraction of I to A.*

Proof. Firstly, $0 \in f^{-1}(I)$ since $f(0) \in I$. Let $a, b \in f^{-1}(I) \Rightarrow f(a), f(b) \in I$ and $c \in A$. Then

$$f(a+b) = f(a) + f(b) \in I \Rightarrow a + b \in f^{-1}(I)$$

and

$$f(ac) = f(a)f(c) \in I \Rightarrow ac \in f^{-1}(I).$$

□

Proposition 20.2.3. *Let $f : A \to B$ be a ring homomorphism and $P \subset B$ a prime ideal. Then $f^{-1}(P)$ is a prime ideal of A.*

Proof. Let $a, b \in A$ be such that $ab \in f^{-1}(P) \Rightarrow f(ab) = f(a)f(b) \in P$. Then we have either $f(a) \in P \iff a \in f^{-1}(P)$ or $f(b) \in P \iff b \in f^{-1}(P)$, which implies $f^{-1}(P)$ is prime. □

Remark 20.2.4 (remark for Propsitions 20.2.2 and 20.2.3). If $A \subset B$ and $f : A \to B$ is the inclusion mapping. Then for a prime ideal P in B, $f^{-1}(P) = P \cap A$ is prime.

Proposition 20.2.5. *Let $f : A \to B$ be a surjective ring homomorphism and $Q \subset A$ a prime ideal containing* $\mathrm{Ker}(f)$*. Then $f(Q)$ is a prime ideal of B.*

Proof. It is easy to verify that $f(Q)$ is an ideal. Let $y_1, y_2 \in B$ be such that $y_1 y_2 \in f(Q)$. Then since f is surjective, there exist $x_1, x_2 \in A$ and $x \in Q$ such that $f(x_1) = y_1, f(x_2) = y_2$ and $f(x) = y_1 y_2$. Hence

$$f(x_1 x_2 - x) = 0 \Rightarrow x_1 x_2 - x \in \mathrm{Ker}(f) \Rightarrow x_1 x_2 - x \in Q \Rightarrow x_1 x_2 \in Q.$$

This implies either x_1 or x_2 is in Q and thus either $y_1 = f(x_1)$ or $y_2 = f(x_2)$ is in $f(Q)$. □

Corollary 20.2.6. *Let A be a ring and J an ideal of A. Then for each $P \in \mathrm{Spec}(A)$ such that $P \supset J$, $\pi(P)$ is prime, where $\pi : A \to A/J$ is the canonical homomorphism.*

Proposition 20.2.7. *Let A be a ring and J an ideal of A. Then if P_1, P_2 are ideals of A such that $J \subsetneq P_1 \subsetneq P_2$, $\pi(J) \subsetneq \pi(P_1) \subsetneq \pi(P_2)$, where $\pi : A \to A/J$ is the canonical homomorphism.*

Proof. It is obvious that $\pi(J) \subsetneq \pi(P_1)$ and $\pi(P_1) \subset \pi(P_2)$. Suppose for the sake of contradiction that $\pi(P_1) = \pi(P_2)$. Let $p_2 \in P_2 \backslash P_1$, then there is $p_1 \in P_1, j \in J$ such that $p_2 - p_1 = j \iff p_2 = j + p_1$, which implies $p_2 \in P_1$ since $j \in J \subset P_1$ and P_1 is an ideal, a contradiction. □

Proposition 20.2.8. *Let A be a ring and J an ideal of A. Then*

$$\mathrm{Spec}(A/J) = \{\pi(P) : \ P \in \mathrm{Spec}(A) \text{ and } J \subset P\},$$

where $\pi : A \to A/J$ is the canonical projection that maps $a \in A$ to $a + J \in A/J$.

Proof. Let $Q \in \mathrm{Spec}(A/J)$ and let $P = \pi^{-1}(Q)$. Then by Proposition 20.2.3, $P \in \mathrm{Spec}(A)$. We have $\pi(P) = \pi(\pi^{-1}(Q)) = Q$ since π is surjective. $[0] \in Q$ since Q is an ideal. Hence $\pi^{-1}([0]) \subset \pi^{-1}(Q) \Rightarrow J \subset P$. □

Remark 20.2.9. Let $\pi : A \to A/J$ be the canonical homomorphism. Then from the discussions above, we can see that there is a one-to-one correspondence between the prime ideals containing J in A and the prime ideals in A/J. Moreover, since if $Q_1 \subsetneq Q_2$ are two ideals in A/J, then $\pi^{-1}(Q_1) \subsetneq \pi^{-1}(Q_2)$, and Proposition 20.2.7, their "order" are preserved.

Definition 20.2.10. Let A be a ring and J an ideal of A. Then the dimension of A/J, called *Krull dimension* is the supremum of the lengths of all chains $Q_l \supsetneq Q_{l-1} \supsetneq \cdots \supsetneq Q_0$ of prime ideals $Q_l, Q_{l-1}, \ldots, Q_0 \in \mathrm{Spec}(A/J)$.

Remark 20.2.11. By Corollary 20.2.6 and Proposition 20.2.7, a chain $P_l \supsetneq P_{l-1} \supsetneq \cdots \supsetneq P_0 = P$ of prime ideals properly containing an ideal P gives rise to a chain $\pi(P_l) \supsetneq \pi(P_{l-1}) \supsetneq \cdots \supsetneq \pi(P_0) = \pi(P) = \{[0]\}$. Moreover, if A is an integral domain, then $\{[0]\}$ is prime in A/P. Hence these two chains are of the same length.

Definition 20.2.12. Let $Y \subset \mathbb{C}^n$ be an irreducible closed set. We define $\dim Y$ to be the supremum among all lengths l of chains $Y_l \subsetneq Y_{l-1} \subsetneq \cdots \subsetneq Y_1 \subsetneq Y_0 = Y$ of closed and irreducible subsets $Y_1, \ldots, Y_l$ contained in Y.

Remark 20.2.13. Chains $\cdots \subsetneq Y_l \cdots \subsetneq Y_1 \subsetneq Y_0$ of infinite length can not exist because this would imply infinite ascending chains of prime ideals that are not stable.

Remark 20.2.14. Note that if $Y_l \subsetneq Y_{l-1} \subsetneq \cdots \subsetneq Y_1 \subsetneq Y_0 = Y$, where Y_i's are irreducible and closed and thus I_{Y_i}'s are prime ideals, then we have

$$\begin{aligned}
&Y_l \subsetneq Y_{l-1} \subsetneq \cdots \subsetneq Y_1 \subsetneq Y_0 = Y \\
\Rightarrow &I_{Y_l} \supsetneq I_{Y_{l-1}} \supsetneq \cdots \supsetneq I_{Y_1} \supsetneq I_{Y_0} = I_Y \\
\Rightarrow &Z(I_{Y_l}) \subsetneq Z(I_{Y_{-1}}) \subsetneq \cdots \subsetneq Z(I_{Y_1}) \subsetneq Z(I_{Y_0}) = Z(I_Y) \\
\Rightarrow &\overline{Y_l} \subsetneq \overline{Y_{l-1}} \subsetneq \cdots \subsetneq \overline{Y_1} \subsetneq \overline{Y_0} = \overline{Y} \\
\Rightarrow &Y_l \subsetneq Y_{l-1} \subsetneq \cdots \subsetneq Y_1 \subsetneq Y_0 = Y.
\end{aligned}$$

By Proposition 20.2.3, a chain whose ideals are in $\mathrm{Spec}(\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{I_Y})$ gives rise to a chain with the same length whose ideals are in $\mathrm{Spec}(I_Y)$, which implies $\dim Y \geq \dim(\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{I_Y})$. By Remark 20.2.11, on the other hand, a chain whose ideals are in $\mathrm{Spec}(I_Y)$ gives rise to a chain with the same length whose ideals are in $\mathrm{Spec}(\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{I_Y})$, which implies $\dim Y \leq \dim(\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{I_Y})$.

Definition 20.2.15. Let Y be a closed set of $\mathbb{C}^n$. We define $\dim Y$ to be the maximum dimension $\max_{i=1,2,\ldots,s} Y_i$, where $Y_1, \ldots, Y_s$ are the unique irreducible components of Y.

Proposition 20.2.16. *Let Y be a closed set in $\mathbb{C}^n$ and $Y_1, Y_2, \ldots, Y_s$ the unique irreducible components of Y. Then*

$$\dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{I_Y}) = \max_{i=1,2,\ldots,s} \dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{I_{Y_i}}).$$

Proof. A chain of prime ideals containing I_{Y_i} can contain I_Y since $I_Y \subset I_{Y_i}$ for $i = 1, 2, \ldots, s$. Hence

$$\dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{I_Y}) \leq \max_{i=1,2,\ldots,s} \dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{I_{Y_i}}).$$

On the other hand, let $P \in \mathrm{Spec}(\mathbb{C}[x_1, x_2, \ldots, x_n])$ such that $I_Y = I_{Y_1} \cap I_{Y_2} \cap \cdots \cap I_{Y_s} \subset P$. Then we have $I_{Y_j} \subset P$ for some j, which implies

$$\dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{I_Y}) \geq \max_{i=1,2,\ldots,s} \dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{I_{Y_i}})$$

(we can replace I_Y by I_{Y_j} in a chain where every prime ideal contains I_Y). □

Proposition 20.2.17. *Let J be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then*

$$\sqrt{J} = \cap_{\substack{P \in \mathrm{Spec}(\mathbb{C}[x_1,x_2,\ldots,x_n]) \\ P \supset J}} P.$$

Moreover, there are finitely many factors in this intersection.

Proof. Let $Y_1, Y_2, \ldots, Y_s$ be the unique irreducible decomposition of $Z(J)$. Then we have

$$\begin{aligned} Z(J) &= Y_1 \cup Y_2 \cup \cdots \cup Y_s \\ \Rightarrow \sqrt{J} &= I_{Z(J)} = I_{Y_1} \cap I_{Y_2} \cap \cdots \cap I_{Y_s}. \end{aligned}$$

□

Proposition 20.2.18. *Let J be an ideal of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Then*

$$\dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{J}) = \dim(\frac{\mathbb{C}[x_1, x_2, \ldots, x_n]}{\sqrt{J}}).$$

Proof. $\dim(\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{J}) \geq \dim(\frac{\mathbb{C}[x_1,x_2,\ldots,x_n]}{\sqrt{J}})$ since $J \subset \sqrt{J}$. On the other hand, let $P \in \mathrm{Spec}(\mathbb{C}[x_1, x_2, \ldots, x_n])$ such that $P \supset J$. It is enough to show that $P \supset \sqrt{J}$. For $r \in \sqrt{J}$, we have $r^k \in J \subset P \Rightarrow r \in P$. □

The aim is to achieve three goals in the next few lectures:

- prove that $\dim \mathbb{F}[x_1, x_2, \ldots, x_n] = n$,
- Noether Normalization, and
- Hilbert Functions.

Definition 20.2.19 (integral)**.** Let B be a ring and A a subring of B. An element $b \in B$ is called *integral* over A if

$$b^n + \alpha_{n-1} b^{n-1} + \cdots + \alpha_1 b + \alpha_0 = 0$$

for some $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in A$.

Proposition 20.2.20 (AM\2.4)**.** *Let M be a finitely generated A-module, let I be an ideal of A, and let f be an A-module endomorphism of M such that $f(M) \subset IM = \{\alpha_1 w_1 + \cdots + \alpha_n w_n : n \in \mathbb{N}, \alpha_i \in I, w_i \in M\}$. Then f satisfies an equation of the form*

$$f^n + \alpha_1 f^{n-1} + \cdots + a_n = 0,$$

where α_i's are in I.

Proof. Please read the pictures or the book for the proof. □

Definition 20.2.21 (faithful module)**.** Let A be a ring and M an A-module. Then M is called *faithful* if there is no nonzero element α in A such that $\alpha M = 0$.

Proposition 20.2.22 (5.1\AM)**.** *Let B be a ring, let A be a subring of B, and let $b \in B$. Then the following are equivalent.*

1. *b is integral over A.*
2. *$A[b]$ is a finitely generated A-module.*
3. *$A[b]$ is contained in a ring C such that C is a finitely generated A-module.*
4. *there is a faithful $A[b]$-module M which is finitely generated over A.*

Proof.

- $1 \Rightarrow 2)$. Since b is integral over A, we have

$$b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0 = 0 \iff b^n = -(\alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0)$$

  for some $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in A$, which implies $A[b]$ is (finitely) generated by $1, b, \ldots, b^{n-1}$.

- $2 \Rightarrow 3)$. Take $C = A[b]$.

- $3 \Rightarrow 4)$. Take $M = C$, which is a $A[b]$-module since $A = A[1] \subset A[b] \subset C$. Then M is faithful because if there is $p(b) \in A[b]$ such that $p(b)M = p(b) = C = 0$, then $p(1) \cdot 1 = 0$.

- $4 \Rightarrow 1)$. Let $f : M \to M$ be an endomorphism of multiplying b, i.e., $f(m) = bm$ for each $m \in M$. Then $f(M) = bM \subset AM$. By Proposition 20.2.20, we have

$$(b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0)M = 0.$$

  Since M is faithful, $b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0 = 0$. This implies b is integral over A.

□

SI112: Advanced Geometry	Spring 2018
Lecture 26 — May 24th, Thursday	
Prof. Manolis	*Scribe*: Liangzu

21 Lecture 26

21.1 Overview of This Lecture

The goal of lecture 26 is to prove Theorem 21.2.13.

21.2 Proof of Things

Proposition 21.2.1. *Let P be a prime ideal of a ring R, then $S = R\backslash P$ is a multiplicatively closed set (i.e., $s_1 s_2 \in S$ for each $s_1, s_2 \in S$), and $0 \notin S$.*

Proof. Left as an exercise. □

Proposition 21.2.2. *Let R be a ring and P, Q prime ideals of R. Let $\phi : R \to R_P$ be a ring homomorphism that maps $r \in R$ to $\frac{r}{1} \in R_P$. If $Q \cap (R\backslash P) \neq \emptyset$, then $\phi(Q)R_P$ is not a prime ideal.*

Proof. Since $Q \cap (R\backslash P) \neq \emptyset$, let $q \in Q \cap (R\backslash P)$. Then $\frac{q}{1} \in \phi(Q), \frac{1}{q} \in R_P$ and thus $\frac{1}{1} \in \phi(Q)R_P$, which implies that $\phi(Q)R_P$ is not prime. □

For the sake of simplicity, we will use QR_P to denote $\phi(Q)R_P$ in what follows.

Proposition 21.2.3. *Let R be a ring and P, Q prime ideals of R with $Q \cap (R\backslash P) = \emptyset$. Then Q is a prime ideal of R if and only if QR_P is a prime ideal of R_P.*

Proof. Note that QR_P is properly contained by R_P since $1 \notin QR_P$ ($1 \notin Q$ and $Q \cap (R\backslash P) = \emptyset$), and that the set QR_P is of the form

$$\{\frac{q}{t} : \ q \in Q \text{ and } t \in R\backslash P\}.$$

Then

- $\Rightarrow$). Let $\frac{q_1}{t_1}, \frac{q_2}{t_2} \in R_P$ be such that $\frac{q_1 q_2}{t_1 t_2} \in QR_P$, then we have $q_1 q_2 \in Q$ since $t_1 t_2 \in R\backslash P$, which means that either $q_1 \in Q$ or $q_2 \in Q$. Hence we have either $\frac{q_1}{t_1} \in QR_P$ or $\frac{q_2}{t_2} \in QR_P$.

- $\Leftarrow$). Let $q_1, q_2 \in R$ be such that $q_1 q_2 \in Q$ and let $t_1, t_2 \in R \backslash P$. Then we have $\frac{q_1}{t_1}, \frac{q_2}{t_2} \in R_P$ and $\frac{q_1 q_2}{t_1 t_2} \in QR_P$. This implies either $\frac{q_1}{t_1} \in QR_P$ or $\frac{q_2}{t_2} \in QR_P$. Hence we have either $q_1 \in Q$ or $q_2 \in Q$. There is a much quicker way: $\phi^{-1}(QR_P) = Q$ is prime by Proposition 20.2.3.

□

Remark 21.2.4 (remark for Proposition 21.2.3). The occurrence of QR_P is weird. It is because $\phi(Q)$ is in general not an ideal, but $\phi(Q)R_P$ always is.

Proposition 21.2.5. *Let P be a prime ideal of a ring R and $S = R - P$, then the ring $R_P = S^{-1}R$ contains only one maximal ideal equal to PR_P.*

Proof. The elements $\frac{p}{s}$ with $p \in P$ form an ideal $m = PR_P$ in R_P. If $\frac{b}{t} \notin m$, then $b \notin P$, hence $b \in S$ and therefore, noticing $t \in S$, $\frac{b}{t}$ is a unit in R_P ($\frac{b}{t} \cdot \frac{t}{b} = 1$). It follows that if I is an ideal in R_P and $I \not\subset m$, then I contains a unit, say $\frac{b}{t}$, which implies I contains $1 = \frac{b}{t} \cdot \frac{t}{b} = 1$ and hence $I = R_P$. Thus m is the only maximal ideal in R_P. □

Definition 21.2.6. Let $\phi : A \to B$ be an injective ring homomorphism, an element $b \in B$ is called *integral over A via ϕ* if

$$b^n + \phi(\alpha_{n-1})b^{n-1} + \cdots + \phi(\alpha_1)b + \phi(\alpha_0) = 0$$

for some $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in A$. Moreover, we say that B is integral over A if for each $b \in B$, b is integral over A.

Corollary 21.2.7 (5.2\AM)**.** *Let $b_1, b_2, \ldots, b_n \in B$ be such that they are integral over A. Then the ring $A[b_1, b_2, \ldots, b_n]$ is a finitely generated A-module.*

Proof. The case $n = 1$ is part of Proposition 20.2.22. Suppose inductively it holds for the case $n - 1$, i.e., the ring $A_{n-1} = A[b_1, b_2, \ldots, b_{n-1}]$ is a finitely generated A-module. Since $A \subset A_{n-1}$ and b_n is integral over A, b_n is integral over A_{n-1}. Therefore $A[b_1, b_2, \ldots, b_n] = A_{n-1}[b_n]$ is a finitely generated A_{n-1}-module by the case $n = 1$. Then we have

$$A[b_1, b_2, \ldots, b_n] = A_{n-1} + A_{n-1}b_n + A_{n-1}b_n^2 + \cdots A_{n-1}b_n^m,$$

where

$$A_{n-1} = Ap_1(b_1, b_2, \ldots, b_{n-1}) + Ap_2(b_1, b_2, \ldots, b_{n-1}) + \cdots + Ap_k(b_1, b_2, \ldots, b_{n-1})$$

for some

$$p_1(b_1, b_2, \ldots, b_{n-1}), p_2(b_1, b_2, \ldots, b_{n-1}), \ldots, p_k(b_1, b_2, \ldots, b_{n-1}) \in A_{n-1},$$

which implies that $A[b_1, b_2, \ldots, b_n]$ is finitely generated. □

Proposition 21.2.8 (5.6\AM)**.** *Let $A \subset B$ be rings, B integral over A (via the inclusion mapping).*

1. *If Q is an prime ideal of B and $P = A \cap Q$, then B/Q is integral over A/P.*
2. *If S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof.

1. Let $b \in B$. Then there exists $\alpha_0, \ldots, \alpha_{n-1} \in A$ such that

$$b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0 = 0.$$

Let $\pi_P : A \to A/P, \pi_Q : B \to B/Q$ be the canonical homomorphisms, let $i : A \to B$ be the inclusion mapping. Then by First Isomorphism Theorem, there exists an injective ring homomorphism $i^* : A/P \to B/Q$ such that $\pi_Q i = i^* \pi_P$ (have a look at the diagram in the pictures). Then we have

$$\begin{aligned} &\pi_Q(b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0) = 0 \\ \Rightarrow &[b]^n + [\alpha_{n-1}][b]^{n-1} + \cdots + [\alpha_1][b] + [\alpha_0] = 0. \end{aligned}$$

Noticing that $[a_i] \in i^*(A/P)$ for $i = 0, 1, \ldots, n-1$ and i^* is injective, B/Q is integral over A/P via i^*.

2. First note that $S^{-1}A \subset S^{-1}B$. Let $b \in B, s \in S$ (hence $\frac{b}{s} \in S^{-1}B$). Then there exists $\alpha_0, \ldots, \alpha_{n-1} \in A$ such that

$$b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0 = 0.$$

Let $\phi : B \to S^{-1}B$ be a ring homomorphism that maps $x \in B$ to $\frac{x}{1} \in S^{-1}B$. Then we have

$$\begin{aligned} &\phi(b^n + \alpha_{n-1}b^{n-1} + \cdots + \alpha_1 b + \alpha_0) = 0 \\ \iff &\frac{b^n}{1} + \frac{\alpha_{n-1}}{1}\frac{b^{n-1}}{1} + \cdots + \frac{\alpha_1}{1}\frac{b}{1} + \frac{\alpha_0}{1} = 0 \\ \iff &(\frac{b}{s})^n + \frac{\alpha_{n-1}}{s}(\frac{b}{s})^{n-1} + \cdots + \frac{\alpha_1}{s^{n-1}}(\frac{b}{s}) + \frac{\alpha_0}{s^n} = 0. \end{aligned}$$

Noticing that $\frac{a_k}{s^{n-k}} \in S^{-1}A$ for $k = 1, 2, \ldots, n-1$, $S^{-1}B$ is integral over $S^{-1}A$ (via the inclusion mapping).

□

Proposition 21.2.9 (5.7\AM)**.** *Let $A \subset B$ be integral domains, B integral over A (via the inclusion mapping). Then A is a field if and only if B is a field.*

Proof.

1. $\Rightarrow$). Let $y \in B$ and $y \neq 0$. There exists $\alpha_0, \ldots, \alpha_{n-1} \in A$ such that

$$y^n + \alpha_{n-1}y^{n-1} + \cdots + \alpha_1 y + \alpha_0 = 0.$$

Without loss of generality suppose that n is minimal. If $\alpha_0 = 0$, then $y(y^{n-1} + \alpha_{n-1}y^{n-2} + \cdots + \alpha_1) = 0$, which implies $y^{n-1} + \alpha_{n-1}y^{n-2} + \cdots + \alpha_1 = 0$, contradicting to the minimality of n. Hence $\alpha_0 \neq 0$. Since A is a field, $a_0^{-1} \in A \subset B$. Then

$$y[-a_0^{-1}(y^{n-1} + \alpha_{n-1}y^{n-2} + \cdots + \alpha_1)] = 1.$$

Hence $y^{-1} = -a_0^{-1}(y^{n-1} + \alpha_{n-1}y^{n-2} + \cdots + \alpha_1) \in B$.

2. $\Leftarrow$). Let $x \in A \subset B$ and $x \neq 0$. Then $x^{-1} \in B$. There exists $\beta_0, \ldots, \beta_{n-1} \in A$ such that

$$(x^{-1})^m + \beta_{n-1}(x^{-1})^{m-1} + \cdots + \beta_1(x^{-1}) + \beta_0 = 0.$$

Hence

$$x^{-1} = -(\beta_{m-1} + \cdots + \beta_1 x^{m-2} + \beta_0 x^{m-1}) \in A.$$

□

Corollary 21.2.10 (5.8\AM)**.** *Let $A \subset B$ be rings, B integral over A (via the inclusion mapping). If Q is an prime ideal of B and $P = A \cap Q$, then Q is a maximal if and only if P is maximal.*

Proof. Since P and Q are prime, A/P and B/Q are integral domains. By Proposition 21.2.8, B/Q is integral over A/P. Then by Proposition 21.2.9, Q is maximal if and only if B/Q is a field if and only if A/P is a field if and only if P is maximal. □

Proposition 21.2.11 (5.9\AM)**.** *Let $A \subset B$ be rings, B integral over A (via the inclusion mapping). If $Q, Q' \in \mathrm{Spec}(B)$ such that $Q' \subset Q$ and $Q' \cap A = Q \cap A = P \in \mathrm{Spec}(A)$. Then $Q' = Q$.*

Proof. Note that by Proposition 21.2.3, $QB_P, Q'B_P \in \mathrm{Spec}(B_P)$, and that $P \subset Q$, $PA_P \subset A_P$ and $A_P \subset B_P$, we have

$$PA_P \subset QB_P \cap A_P \subsetneq A_P$$

(if $QB_P \cap A_P = A_P \iff A_P \subset QB_P$, then $1 \in QB_P \iff QB_P = B_P$, contradicting that QB_P is prime). Similarly

$$PA_P \subset Q'B_P \cap A_P \subsetneq A_P.$$

But by Proposition 21.2.5, PA_P is the unique maximal ideal of A_P, hence

$$QB_P \cap A_P = Q'B_P \cap A_P = PA_P.$$

Hence, by Proposition 21.2.8, B_P is integral over A_P, and by Corollary 21.2.10 and Proposition 21.2.5, $QB_P = Q'B_P$. Let $\phi : B \to B_P$ be a ring homomorphism that maps $x \in B$ to $\frac{x}{1} \in B_P$. Then we have

$$Q = \phi^{-1}(QB_P) = \phi^{-1}(Q'B_P) = Q',$$

as desired. □

Theorem 21.2.12 ("lying over", 5.10\AM)**.** *Let $A \subset B$ be rings, B integral over A (via the inclusion mapping). Then for each $P \in \operatorname{Spec}(A)$, there exists $Q \in \operatorname{Spec}(B)$ such that $Q \cap A = P$.*

Proof. Firstly, by Proposition 21.2.8, B_P is integral over A_P. Let $\phi_A : A \to A_P, \phi_B : B \to B_P$ be ring homomorphisms that maps $a \in A$ and $b \in B$ to $\frac{a}{1} \in A_P$ and $\frac{b}{1} \in B_P$ respectively. Assume (without loss of generality) that B_P is not the zero ring, let Q' be a maximal ideal of B_P. Then by Corollary 21.2.10, $Q' \cap A_P$ is maximal and hence $Q' \cap A_P = PA_P$. By commutativity of the diagram (review the picture), $P = \phi_A^{-1}(PA_P) = \phi_A^{-1}(Q' \cap A_P) = \phi_B^{-1}(Q') \cap A$. Let $Q = \phi_B^{-1}(Q')$, finishing the proof. □

Theorem 21.2.13. *Let $A \subset B$ be rings, B integral over A (via the inclusion mapping). Then* $\dim A = \dim B$.

Proof.

- Let $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ be a chain of prime ideals of B. Then $Q_0 \cap A \subset Q_1 \cap A \subset \cdots \subset Q_n \cap A$ is a chain of prime ideals of A. If $Q_i \cap A = Q_{i+1} \cap A$ for some i, then we have $Q_i = Q_{i+1}$ by Proposition 21.2.11, contradicting to the construction of the chain. Hence $\dim A \geq \dim B$.

- On the other hand, let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m$ be a chain of prime ideals of A. By Theorem 21.2.12 there exists $Q_0 \in \operatorname{Spec}(B)$ such that $P_0 = A \cap Q_0$. Let $\pi_A : A \to A/P_0, \pi_B : B \to B/Q_0$ be canonical homomorphisms. By Proposition 21.2.8, B/Q_0 is integral over A/P_0 via an injective homomorphism i^* (see the diagram). By again Theorem 21.2.12, there is $\overline{Q_1} \in \operatorname{Spec}(B/Q_0)$ such that $(i^*)^{-1}(\overline{Q_1}) = \pi_A(P_1)$. At the same time we have $Q_0 \subset Q_1$ by letting $Q_1 = \pi_B^{-1}(\overline{Q_1}) \in \operatorname{Spec}(B)$. Suppose $Q_0 = Q_1$, then by the injectivity of i^*,

$$\pi_A(P_1) = (i^*)^{-1}(\overline{Q_1}) = (i^*)^{-1}(\overline{0}) = \overline{0},$$

which is impossible since $P_0 \subsetneq P_1 \Rightarrow \pi_A(P_1) \neq \overline{0}$. Hence $Q_0 \subsetneq Q_1$. Proceeding in a similar way we can construct a chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$ of prime ideals of B, showing that $\dim A \leq \dim B$.

□