University of Warsaw
Faculty of Mathematics, Informatics and Mechanics

Kamil Braun
Student nr: 346840

Krzysztof Pszeniczny
Student nr: 347208

Introduction to persistent homology

Bachelor thesis
in MATHEMATICS

Thesis supervisor
dr Krzysztof Ziemiański

August 2018

Oświadczenie kierującego pracą

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Data Podpis kierującego pracą

Oświadczenie autora (autorów pracy)

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Data Podpis autora (autorów) pracy

Abstract

'Data has shape and the shape matters' is a buzzword phrase recently gaining popularity in the community of data scientists. Under it lies the idea that data can be analyzed using methods rooted in algebraic topology, and the resulting approach is known as TDA – topological data analysis. One of the central tools in TDA is persistent homology, which provides a way to systematically study homology groups of certain topological spaces assiociated to data sets, allowing the study of 'holes' in the data.

This thesis, written in the form of a book, intends to provide an elementary introduction to the basic definitions and theorems of persistent homology. It is aimed at the data analyst and the computer scientist, who presumably meet topology and abstract algebra for the first time, and assumes only basic knowledge of linear algebra; as a self-contained source, it introduces the necessary topological and algebraic concepts. It also describes in detail the basic algorithm for computing persistent homology of a filtered simplicial complex.

Keywords

Persistent homology, topological data analysis, simplicial complexes, finitely generated modules over PID

Subject Area (Socrates/Erasmus code)

11.1 Mathematics

Categories and Subject Descriptors

55U10 Simplicial sets and complexes; 55U15 Chain complexes; 68U05 Computational geometry; 13P25 Applications of commutative algebra; 13C05 Structure, classification theorems of modules and ideals; 54-01 Instructional exposition to general topology

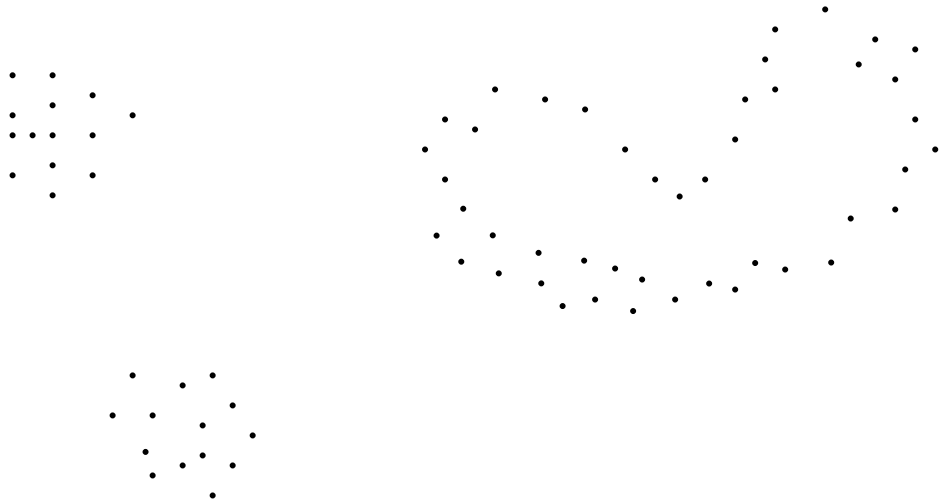
Thesis title in Polish

Wprowadzenie do homologii persystentnych

Contents

Introduction

Consider the following problem. We are given a finite set of points in $\mathbb{R}^2$ such as the one drawn below:

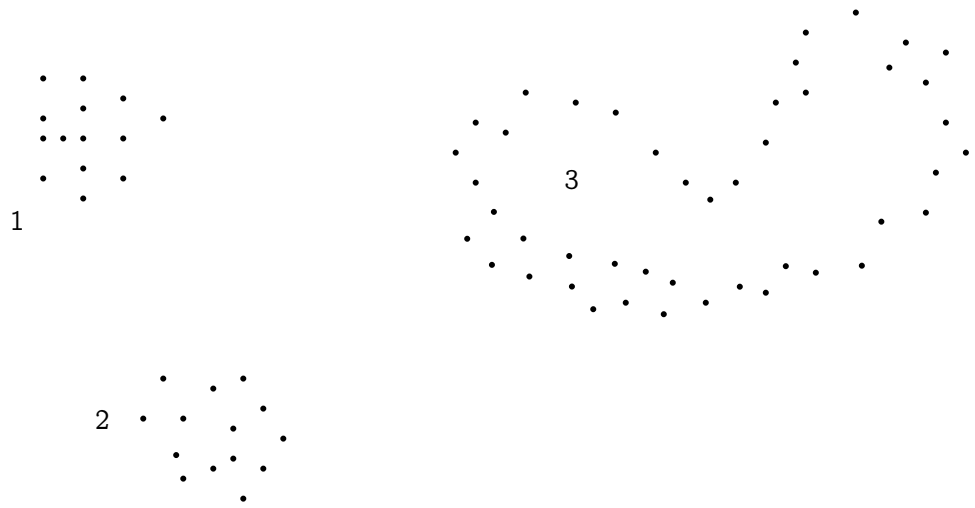


We assume that the set represents some data gathered in the real world and our goal is to analyze it. In this case the data is unlabeled; we know only the positions of data points in Euclidean space. Using only this knowledge we would like to give a summary of the data set – find any hidden patterns, explain its features. This is the *unsupervised* approach to data analysis.

Here the data set lies in two-dimensional space and does not have many points, so we can easily visualize it. By simply looking at the picture we are able to notice some features.

Our intuition tells us that points lying close to each other are somehow related. Obviously all of the points have something in common but presumably lower distances indicate stronger relationships. This hypothesis leads us to cluster analysis where we split the points into groups based on their spatial arrangement.

In our case, one could argue that the points naturally split into 3 groups:



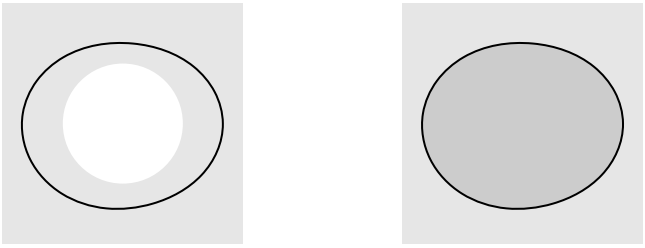
How to translate this vague idea into mathematics and then to a method of computation? One way to approach this problem is by choosing a parameter, a positive real number – call it ϵ – and then construct a set by placing an *Euclidean ball* of radius ϵ at the center of every point. This is what we get for a certain ϵ:

Perhaps the reader is familiar with the notion of a connected set and connected component of a subset of Euclidean space from mathematical analysis; in any case, it is intuitively clear that the above set has three connected components, in contrast to the original set which had one 'trivial' component for each point. The 'shape' of this new set is much more interesting. Now we can say that two points in the original data set lie in the same cluster if and only if they belong to the same connected component in the above set.

Let us analyze this new set a little bit further, because there is an interesting thing going on with the third component – there is a 'hole' in the middle. Again, how do we mathematically describe this phenomenon?

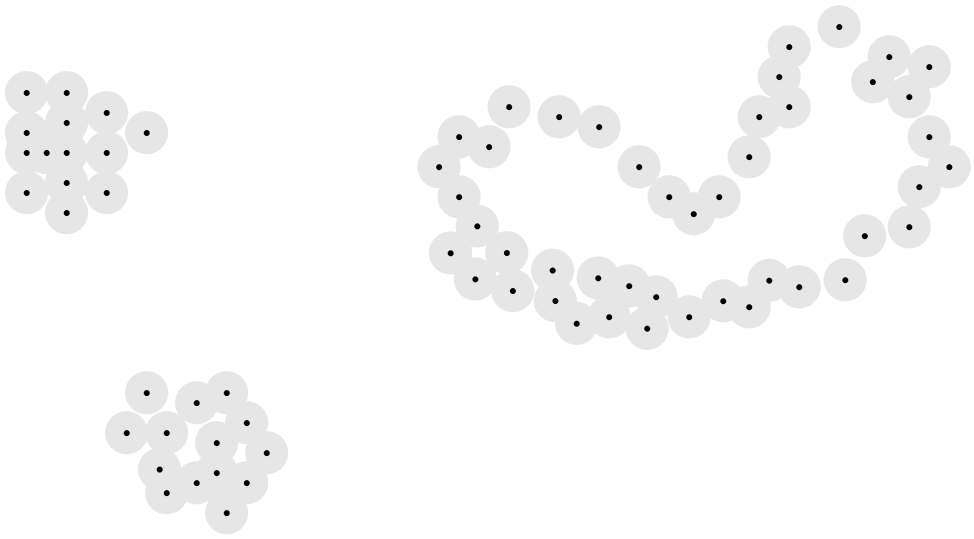
The required technical apparatus is a bit more complicated compared to the problem of defining connected components; we will develop all the necessary tools in upcoming chapters. For the current discussion we will use the following simplification: a subset X of Euclidean

space has a hole if it is possible to find a closed path contained in X which is not a boundary of some Y contained in X. The following example illustrates the idea:



The path drawn on the left is not a boundary of anything contained in the set in which the path lives; we call it *nonbounding*. On the right however, the path is a boundary of a subset which has been marked using a darker color; we call it *bounding*. It is of course necessary to formally define notions such as 'path' or 'boundary'. It is also not clear how different paths are related to each other and what happens if the set has two 'holes' – how do we distinguish between them? We will soon provide answers to these questions, relying on intuition for the time being.

Coming back to the set of our interest, we see that it has three components and a hole in one of them. However this was made possible due to a suitable choice of ϵ; by taking different ϵs we can obtain vastly different results. For example if ϵ is small enough then every point in the original set still has a component of its own and there are no holes. If ϵ is big enough, everything gets merged into a single convex blob. In these cases we don't really obtain any new information about the set – the interesting things happen 'in the middle', such as in the following examples:



Example A

Example B

In example A there are a lot of components with a lot of small holes. In example B there are just three components similarly to the case analyzed before, but this time one of the components has two holes in contrast to the previous situation where the third component had one hole. What does that mean?

To get a complete picture of the situation, we need to analyze a whole range of ϵs. Suppose we start with a very small ϵ so that every data point belongs to a separate component. As time passes, we let ϵ continuously grow, and we observe the components and closed paths that exist in our set. At certain points in time components merge and closed paths appear that are nonbounding. These paths eventually become bounding during the process. We can track their lifetimes – starting from the point of 'birth', ϵ_1, where a nonbounding path appears, to the point of its 'death', $\epsilon_2 > \epsilon_1$, where it becomes bounding. The length of the interval (ϵ_1, ϵ_2) indicates whether the detected hole is an actual feature of the data or if it's just noise.

For instance, in the case of our dataset, a lot of holes appear at the beginning of the process – some of them can be seen in example A. However they dissapear very quickly, which suggests that they 'don't matter'. At some point a nonbounding path is born that detects the hole observed by us at the beginning. This path remains nonbounding for a relatively long time, and similarly for paths that detect the two holes indicated in example B. The long lifetimes of these features suggest that they actually tell us something about the 'shape' of our data.

As for the components, we can also study how they merge and take note of the corresponding sequence of clusters. This leads to a clustering method known as *single-linkage clustering*.

Up to this point the sets we were dealing with were 'small' and lying in the two-dimensional Euclidean plane so we could easily visualize them. Perhaps it wouldn't be very beneficial to develop a formal theory of 'detecting holes' if the data can be simply looked on by a human expert, but the tools we will develop work for arbitrary number of dimensions. We will also be able to detect holes of 'higher dimensions'. As an example consider

the sphere. It can be proved that every closed path lying on the surface of the sphere is bounding – there are no 'one-dimensional holes'. On the other hand intuition tells us that the sphere 'is empty inside', and there is a way to formalize this idea.

In the discussion above we were looking at features such as components and 'holes'. The basic premise behind this book is that *data has shape*, and this shape can be studied using tools from the field of mathematics called *topology*, or more concretely, *algebraic topology*. Indeed, topology allows us to formalize the presented ideas; in chapter 1 we provide an elementary introduction to this field. Chapter 2 deals with *homology*, a tool from algebraic topology that allows the study of 'holes' in a single topological space. Finally in chapters 3 and 4 we describe a way to apply the methods of chapter 2 to a sequence of spaces that arise by considering different choices of ϵ.

Chapter 1

Topological spaces and simplicial complexes

The goal of this chapter is to introduce basic notions that allow us to study the 'shape' of data. A reader familiar with topological spaces can skip fragments of this chapter. To talk about shape we will talk about 'spaces' – sets of points with some additional structure attached to them. This strategy of taking a set and considering some additional structure is common in mathematics.

For example, in mathematical analysis, we study the real numbers. They consist of a set – the set of numbers itself, with elements such as 1, 3, π – together with the operations of addition, multiplication, taking the inverse, and the relation of order, satisfying certain axioms. As a set only, the real numbers are not at all interesting, and from the set-theoretical point of view there are a lot of sets which are 'the same' as real numbers, i.e. there exists a bijection between the real numbers and these sets. But then we 'augment' this set, so that we can do $1+2$, $5*3$, π^{-1}, ask questions such as $1<2$, etc. The entire field of mathematical analysis stands on few simple rules.

Continuing with the example of analysis, we can talk about Euclidean spaces. There we still have a set, which can be represented simply by the cartesian product $\mathbb{R}\times\cdots\times\mathbb{R}$, and addition, inherited directly from the real numbers (we add 'coordinate-wise'), but we cannot talk about multiplication, taking inverses, or order. However, there are a lot of other structures that we can put on $\mathbb{R}^n$ that make it interesting and worth studying, for example the notion of distance coming from the real numbers. Again, as a set they are not interesting at all, in fact they are 'the same' as real numbers (i.e. in bijection with the reals).

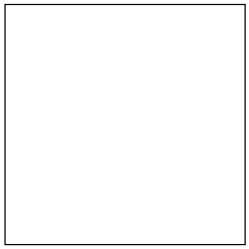
Groups are very important structures in algebra. Again, a group can be thought of as a set together with an operation, often called multiplication (or addition in the case of abelian groups) satisfying a few simple rules. For the definition of a group and a bunch of examples see Appendix A. Similarly, we can talk about rings, fields, modules, vector spaces, normed vector spaces, vector spaces together with a dot product, and so on. Some of these algebraic structures will play an important role later in the book.

For a moment let's fix the type of mathematical structure that we are working with. As an example, think of groups. In the world of considered structures, in this case groups, we can talk about two structures being 'the same'. In this case, two groups are 'the same' if one of them can be obtained from the other by 'renaming' the elements in a way that preserves the structure of the group, i.e. multiplication. The formal way to do this is the notion of a group

isomorphism, a bijection between groups $f : G \to H$ which is a homomorphism: $f(g * g') = f(g) * f(g')$. The bijection 'renames' the elements and the fact that it's a homomorphism allows the renaming to preserve group structure. For more details see Appendix A. This is what we do in general when talking about mathematical structures – we use 'structure-preserving bijections'. In case of rings, that would be ring isomorphisms. Vector spaces – linear isomorphisms, and so on.

What should be the notion of space, i.e. what structure should be put on a set of points to give it a sensible meaning of 'shape'? After that question is answered, another arises: what should be the correct way of saying that two objects of this type are 'the same'?

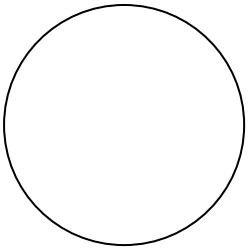
Example 1. Let's take a look at a few examples.



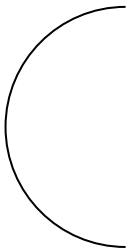
(a) $\{x \in \mathbb{R}^2 : \max(|x_1|, |x_2|) = 1\}$

(b) $[0, 1] \subseteq \mathbb{R}$

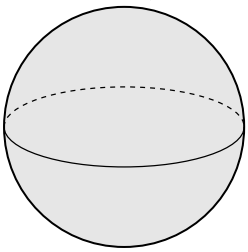
(c) $[0, 2] \subseteq \mathbb{R}$



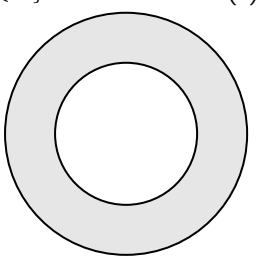
(d) $\{x \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}$



(e) $\{x \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1, x_1 \leqslant 0\}$



(f) $\{x \in \mathbb{R}^2 : x_1^2 + x_2^2 + x_3^2 = 1\}$



(g) $\{x \in \mathbb{R}^2 : \frac{1}{2} \leqslant x_1^2 + x_2^2 \leqslant 1\}$

All of them are subsets of Euclidean spaces, since these in a sense closely resemble the world we live in (at least locally; forget about general relativity for a moment). All of them are bijective – there is really no difference from the set-theoretic point of view.

You might've noticed that pictures b) and c) are the same. They are in fact pictures of different spaces – one of them is the $[0,1]$ segment in $\mathbb{R}$ and the other the $[0,2]$ segment in $\mathbb{R}$. The picture is suggestive on purpose. The idea is that if two spaces can at least be drawn in the same way, they should be considered 'the same'. Shape should be independent of the chosen 'coordinates'. So, for example, if we draw an axis on paper representing the real numbers on which the natural numbers are equally spaced with the distance of 1 cm, and draw the $[0,2]$ segment on this axis, then scale the axis (but leave the drawn segment intact) by making the natural numbers spaced by 2 cm instead of 1 cm, the shape should not change. The same should apply if we considered it as a subset $[0,2] \times \{0\}$ of $\mathbb{R}^2$ and performed rotations, translations or scaling on the chosen coordinate system. The object is only viewed 'from different angles' but it's still the same object.

We can also argue that e) is the same as b) (and so as c)), since it is still as segment, just differently 'placed' in the Euclidean plane. Intuitively, 'continuous deformations' such as 'bending' or 'stretching' an object do not change the object. In a similar fashion a) and d) should be considered the same: the circle can be deformed into the rectangle. We wouldn't consider the circle d) to be the same as the segment b), since if we 'cut' the segment in a single point it splits into two segments, while performing a similar cut on a circle changes it into a single segment. However we should be careful with these kinds of arguments and before we proceed any further we should actually define what are the objects we're dealing with and what it means for two objects to be 'the same'. For example we will define the notion of *homeomorphism* in section 1.2 and of *homotopy equivalence* in section 1.5, and while d) and g) are not homeomorphic, they are homotopy equivalent.

1.1. Metric spaces

The key idea that allows us to think about shape is 'nearness' – when are two elements of a set lying 'close' to each other? When we think about 'nearness', we probably think about distance. Our first approach will be to consider metric spaces – sets augmented with the notion of distance.

Definition. Let X be a set. A **metric** on X is a function $d : X \times X \to [0, +\infty)$ (also called a distance function) satisfying the following axioms:

- For all x, y, $d(x,y) = 0 \iff x = y$,
- Symmetry: for all x, y, $d(x,y) = d(y,x)$,
- Triangle inequality: for all x, y, z, $d(x,z) \leqslant d(x,y) + d(y,z)$.

Definition. A **metric space** is a pair (X, d) where X is a set and d is a metric on X.

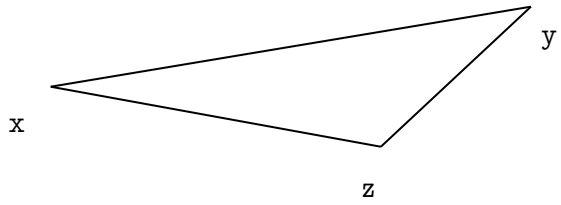
For a metric space (X, d) we will call the elements of X points and $d(x,y)$ for $x, y \in X$ the distance between x and y. We will usually simply write X for a metric space instead of (X, d).

Example 2. The Euclidean spaces $\mathbb{R}^n$ are examples of metric spaces. The usual Euclidean distance, $d(x,y) = \|x - y\| = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$, is a metric. The reader is encouraged to check the axioms on his own.

Example 3. In $\mathbb{R}^n$ a lot of different metrics can be considered. For example, the Manhattan distance is defined as $d(x,y) = \sum_{i-1}^{n}|x_i - y_i|$ and the maximum metric as $d(x,y) = \max_{i=1}^{n}|x_i - y_i|$.

Example 4. Any set can be trivially equipped with a metric. Simply define the distance between any two distinct points to be some constant positive number. For example, $d(x, y) = 1$ for $x \neq y$ and $d(x, x) = 0$. This is sometimes called a discrete, or trivial metric, and the space is called a discrete, or trivial metric space.

The definition of a metric should be clear. A distance between any two points is a non-negative number, which is zero if and only if these points are actually the same point. The distance between x and y is the same as between y and x. The route from x to y and then from y to z is never shorter than the direct route from x to z (intuitively; talking about 'routes' or 'paths' is not sensible in general).

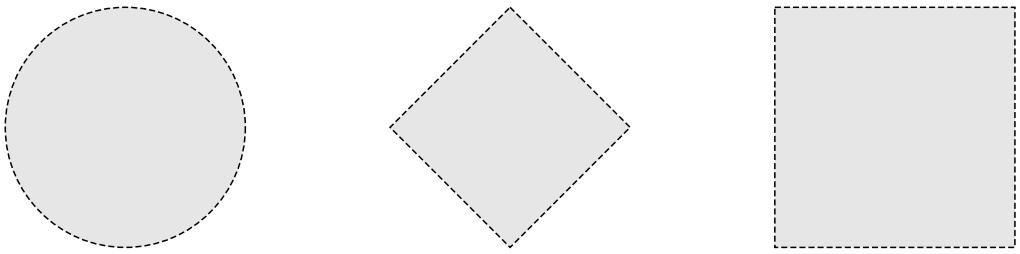


Triangle inequality in the Euclidean plane: $d(x, y) \leqslant d(x, z) + d(z, y)$.

Definition. Let X be a metric space and $x \in X$ a point. Let $r \in \mathbb{R}$, $r > 0$. An **open ball** in X of radius r and center x is the set $\{y \in X : d(y, x) < r\}$. We denote it by $B_X(x, r)$ or just $B(x, r)$ when it is clear which space X we consider.

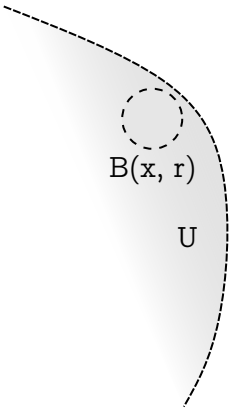
Example 5. Euclidean open balls in $\mathbb{R}$ are simply open intervals: $B(x, r) = (x - r, x + r)$.

Example 6. Open balls in $\mathbb{R}^n$ depend on the metric used. The picture below illustrates open balls obtained when using the Euclidean metric, the Manhattan metric, and the maximum metric.



Euclidean ball | Manhattan ball | Maximum ball

Definition. Let X be a metric space. A subset $U \subseteq X$ is called open in X if and only if for every $x \in U$ there exists some open ball in X centered at x and contained in U, i.e. there exists $r > 0$ such that $B(x, r) \subseteq U$.



U is an open set if at any point $x \in U$ a ball $B(x, r)$ fits inside U.

Example 7. $(0, 1] \subseteq \mathbb{R}$ is not open. Indeed, any open ball in $\mathbb{R}$ centered at 1 is not contained in $(0, 1]$. On the other hand, $(0, 1) \subseteq \mathbb{R}$ is open.

Intuitively, an open set in the Euclidean space is a set such that at any point in this set there is still room to move around in the set from that point. However, the intuition doesn't generalize very well to all metric spaces.

Example 8. In a discrete metric space X every set is open. Indeed, suppose that $d(x, y) = 1$ for all $x \neq y$. Then for any $U \subseteq X$ and $x \in U$, $B(x, \frac{1}{2}) = \{x\} \subseteq U$, hence U is open.

We should be careful when talking about open sets. The notion of openness depends on the considered metric space. If $U \subseteq X$ for some metric space (X, d), U might not be open in X, but U itself can be viewed as a metric space: the distance function is inherited from X, i.e. $d|_{U\times U}$ is a metric on U and $(U, d|_{U\times U})$ is a metric space. Any metric space is of course open in itself by definition: any open ball in a metric space is a subset of this space. In particular, if $U \subseteq X$, then U is open in U, even if U is not open in X.

Example 9. Let $X = \mathbb{R}$ and $U = (0, 1] \subseteq X$. Open balls in U centered at 1 are of the form $(1 - r, 1]$ for some $r > 0$ and are contained in U. However, as we have seen, open balls in X centered at 1 are of the form $(1 - r, 1 + r)$ and are never contained in U, hence U is not open in X.

Observation. Every open ball in a metric space X is open in X.

Proof. Let $x \in X$, $r > 0$. We will show that $B(x, r)$ is open. Let $y \in B(x, r)$. Then $B(y, s)$, where $s = r - d(x, y)$, is contained in $B(x, r)$. Indeed, for any $z \in B(y, s)$, $d(x, z) \leqslant d(x, y) + d(y, z) < d(x, y) + s = d(x, y) + r - d(x, y) = r$, hence $z \in B(x, r)$. □

Observation. A subset U of a metric space X is open if and only if it is a sum of open balls.

Proof. Suppose $U \subseteq X$ is open. Then for any $x \in U$ we have some $B(x, r_x) \subseteq U$, hence $U = \bigcup_x B(x, r_x)$.

On the other hand, if U is a sum of open balls, then for any $x \in U$ there is some $B(y, r) \subseteq U$ such that $x \in B(y, r)$, but $B(y, r)$ is open from the previous observation, hence we have $B(x, r') \subseteq B(y, r) \subseteq U$. Thus U is open. □

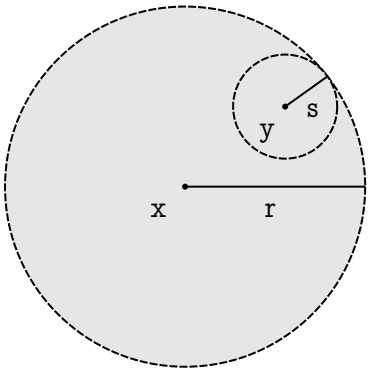
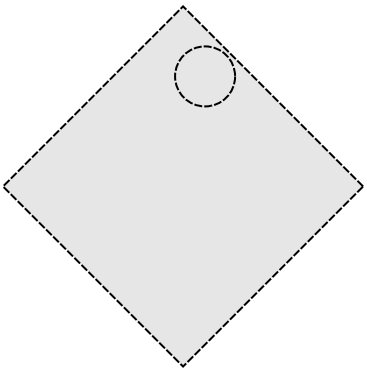


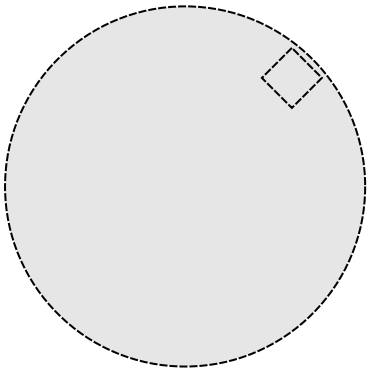
Illustration of the proof that an open ball is open.
For $y \in B(x, r)$ the ball $B(y, s)$ fits inside $B(x, r)$, where $s = r - d(x, y)$.

Definition. Let (X, d) be a metric space. The family of all open sets in X, denoted $\mathcal{T}(d)$, is called the topology of X (induced by the metric d).

Example 10. Let $X = \mathbb{R}^n$, d_1 be the Euclidean metric, and d_2 be the Manhattan metric. Then $\mathcal{T}(d_1) = \mathcal{T}(d_2)$, i.e. any open set in (X, d_1) is open in (X, d_2) and vice-versa. Indeed, since open sets are sums of open balls, it is enough to show that open balls in (X, d_1) are open in (X, d_2) and vice-versa. The following picture illustrates the proof, and the reader is encouraged to write out the details.



Manhattan balls are open in the Euclidean topology.



Euclidean balls are open in the manhattan topology.

To talk about open sets in a metric space (X, d) we will say "let U be open in X" or equivalently "let $U \in \mathcal{T}(d)$".

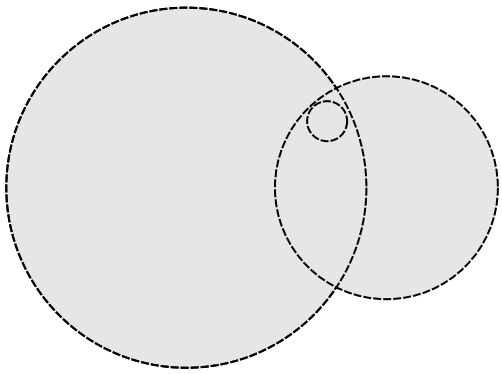
Theorem 1. *Let (X, d) be a metric space. The topology $\mathcal{T}(d)$ of X has the following properties:*

1. $\emptyset \in \mathcal{T}(d)$, $X \in \mathcal{T}(d)$.
2. *If $\mathcal{U} \subseteq \mathcal{T}(d)$ is a finite family of open sets, then $\bigcap \mathcal{U} \in \mathcal{T}(d)$.*
3. *If $\mathcal{U} \subseteq \mathcal{T}(d)$ is any family of open sets, than $\bigcup \mathcal{U} \in \mathcal{T}(d)$.*

Proof. The empty set is obviously open, and X is open as we've noted before, hence 1. Every open set is a sum of open balls, so any sum of open sets is a sum of open balls, hence is open, therefore 3. To prove 2, it is enough to show that the intersection of two open sets is open, and 2 will follow by induction.

Let U, V be open. Then $U = \bigcup_i B_i$, $V = \bigcup_j B'_j$ for some open balls B_i, B'_j, and $U \cap V = \bigcup_{i,j} B_i \cap B'_j$. By 3 it's enough to show that the intersection of two open balls is open.

Let $B(x, r)$, $B(y, s)$ be two open balls. Let $z \in B(x, r) \cap B(y, s)$. Since $B(x, r)$ is open, there is some t_1 such that $B(z, t_1) \subseteq B(x, r)$. Since $B(y, s)$ is open, there is some t_2 such that $B(z, t_2) \subseteq B(y, s)$. Take $t = min(t_1, t_2)$. Then $B(z, t) \subseteq B(x, r) \cap B(y, s)$. □



The intersection of two open balls is open.

Example 11. The intersection of an infinite family of open sets does not have to be open. Take the sets $B(0, 1/n) \subseteq \mathbb{R}^2$: $\bigcap_{n=1}^{\infty} B(0, 1/n) = \{0\}$, which is not open in $\mathbb{R}^2$.

Using open sets we can talk about interesting properties of metric spaces related to the idea of 'shape', for example connectedness.

Definition. A metric space X is **connected** if for any two open sets U, V such that $U \cup V = X$, $U \cap V \neq \emptyset$.

Intuitively a connected metric space cannot be 'separated' using two disjoint open sets.

Definition. A **connected component** of a metric space X is a maximal connected subset of X.

Example 12. Let $U = B(-1, 1) \cup B(1, 1) \subseteq R^2$. Then U is a metric space (using Euclidean distance again) which is disconnected. Indeed, $B(-1, 1)$ and $B(1, 1)$ are disjoint and open in U. They are, in fact, the connected components of U. Now, if we add the point $\{0\}$ to U, then the obtained metric space is connected. These claims should be intuitively clear. Unfortunately formal proofs, although elementary, are pretty technical and there is no point to give them here. If the reader wishes to learn how to prove such claims he should consult a topology book such as [5].

When are two metric spaces 'the same'? Recall that two mathematical structures should be the same if there is a bijection between them that preserves the structure. For metric spaces, the structure is the metric.

Definition. Let (X, d_X), (Y, d_Y) be metric spaces. An **isometry** is a function $f : X \to Y$ which is bijective and for any $x_1, x_2 \in X$, $d_Y(f(x_1), f(x_2)) = d_X(x_1, x_2)$.

Observe that if $f : X \to Y$ is an isometry then $f^{-1} : Y \to X$ is also an isometry.

Definition. Two metric spaces are **isometric** if there is an isometry between them.

Example 13. Any translation and rotation of the Euclidean plane is an isometry. In particular, the metric spaces $[0,1] \times \{0\}$ and $\{0\} \times [0,1]$ with the Euclidean metric are isometric – the isometry is given by $f(x,0) = (0,x)$.

The notion of isometry turns out to be too strong for our purposes. In particular, scaling objects in $\mathbb{R}^n$, which intuitively should not change their 'shape', as we've discussed before with the example of $[0,1]$ and $[0,2]$, is not an isometry.

Observation. $[0,1]$ and $[0,2]$ with the Euclidean metric are not isometric.

Proof. $d(0,2) = 2$, but there are no two points in $x, y \in [0,1]$ such that $d(x,y) = 2$. □

1.2. Topological spaces

We've seen before that connectedness, which is an interesting property related to shape, can be defined using open sets only, without referencing the metric directly. We've also seen that two different metrics in $\mathbb{R}^n$ can give the same topology. Can we 'forget' about the metric and consider open sets only? That is indeed the case. The idea of considering a set together with a structure of open sets gives rise to the field of mathematics called topology.

Which properties of open sets allow us to develop an interesting and fruitful theory? It turns out that the three simple properties listed in Theorem 1 are enough.

Definition. Let X be a set. A **topology** $\mathcal{T}$ on X is a family of subsets of X satisfying the following properties:

1. $\emptyset, X \in \mathcal{T}$.
2. For any finite family of subsets $\mathcal{U} \subseteq \mathcal{T}$, $\bigcap \mathcal{U} \in \mathcal{T}$.
3. For any family of subsets $\mathcal{U} \subseteq \mathcal{T}$, $\bigcup \mathcal{U} \in \mathcal{T}$.

Definition. A **topological space** is a pair $(X, \mathcal{T})$ where X is a set and $\mathcal{T}$ is a topology on X. The elements of X are called points and the elements of $\mathcal{T}$ are called open subsets of X.

Example 14. Let X be a set and $\mathcal{T}$ be the family of all subsets of X. Then $\mathcal{T}$ is called the discrete topology on X and $(X, \mathcal{T})$ is called a discrete topological space. This can also be obtained by taking $\mathcal{T}(d)$ where d is a discrete metric on X.

Example 15. Let X be a set and $\mathcal{T} = \{\emptyset, X\}$. $\mathcal{T}$ is called the indiscrete topology or trivial topology on X.

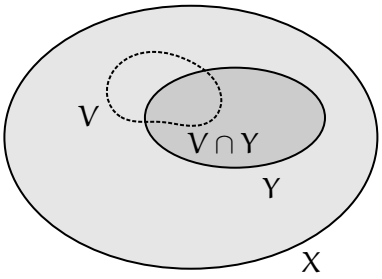
Example 16. Let (X, d) be a metric space. Then $(X, \mathcal{T}(d))$ is a topological space (theorem 1). In particular, the Euclidean distance on $\mathbb{R}^n$ gives rise to a topology, which is called the Euclidean topology.

Thus every metric space gives rise to a topological space. The converse is not true, i.e. there exist topological spaces $(X, \mathcal{T})$ such that there is no metric d on X such that $\mathcal{T}(d) = \mathcal{T}$. These spaces are called non-metrizable. Thus the theory of topological spaces is more general than the theory of metric spaces.

The definition of (dis)connected space and connected components generalizes instantly to any topological space.

From now on, when we use the word 'space', we mean 'topological space'. We will also simply use the notation X for a topological space, without mentioning the topology explicitly. To refer to open sets, we will simply say "open set in X".

Definition. Let $(X, \mathcal{T})$ be a space and Y a subset of X. The **induced topology** on Y (from X), denoted $\mathcal{T}|_Y$, is defined as follows: for $U \subseteq Y$, $U \in \mathcal{T}|_Y$ if and only if there exists some $V \in \mathcal{T}$ such that $V \cap Y = U$. Thus in the induced topology, open sets in Y are intersections of open sets in X with Y. $(Y, \mathcal{T}|_Y)$ is called a **subspace** of $(X, \mathcal{T})$. We will simply say that Y is a subspace of X.



Example 17. Let (X, d) be a metric space and Y a subset of X. Then $d|_{Y\times Y}$ is a metric on Y and $\mathcal{T}(d|_{Y\times Y}) = \mathcal{T}(d)|_Y$. In other words, the topology of a subspace of a metric space is the induced topology.

Proof. Let $U \in \mathcal{T}(d|_{Y\times Y})$. Then $U = \bigcup B_Y(y, r_y)$ for some open balls $B_Y(y, r_y)$ in Y. Let $V = \bigcup B_X(y, r_y)$, where we now use the points y and radii r_y to make open balls in the bigger space X. Since $B_Y(y, r_y) = B_X(y, r_y) \cap Y$, we have $U = V \cap Y$, hence $U \in \mathcal{T}(d)|_Y$.

On the other hand, let $U \in \mathcal{T}(d)|_Y$. Then we have some $V \in \mathcal{T}(d)$, $V \cap Y = U$. V is a sum of open balls in X. Intersecting these balls with Y, we represent U as a sum of open balls in Y. □

From now on, unless otherwise stated, any subset of $\mathbb{R}^n$ will be considered with the topology induced from the Euclidean topology.

Having the notion of topological space defined, we can also define when two spaces are 'the same'.

Definition. Let X, Y be topological spaces. A **homeomorphism** is a function $f : X \to Y$ which is bijective and for every $U \subseteq X$, U is open in X if and only if $f(U)$ is open in Y.

Definition. Topological spaces X, Y are **homeomorphic** if there exists a homeomorphism between them.

Example 18. Every isometry is a homeomorphism. More formally, if $f : X \to Y$ is an isometry between metric spaces (X, d_X) and (Y, d_Y), then it is a homeomorphism between topological spaces $(X, \mathcal{T}(d_X))$ and $(Y, \mathcal{T}(d_Y))$.

Proof. f is bijective by definition. We will show that images of open balls are open balls: then images of open sets, which are sums of open balls, will be sums of open balls, hence open. Since f^{-1} is also an isometry, the statement will follow.

But if $y \in B_X(x, r)$, i.e. $d_X(y, x) < r$, then $d(f(x), f(y) = d(y, x) < r$, i.e. $f(y) \in B_Y(f(x), r)$. Similarly if $y \notin B_X(x, r)$ then $f(y) \notin B_Y(f(x), r)$. Thus $f(B_X(x, r)) = B_Y(f(x), r)$. □

Example 19. Consider the sets in Example 1 as topological spaces, with the topology induced from $\mathbb{R}^n$. We can group the spaces according to whether they are homeomorphic or

not: $\{a, d\}, \{b, c, e\}, \{f\}, \{g\}$ (i.e. within every group the spaces are all homeomorphic to each other and they are not homeomorphic between groups). For example, a homeomorphism between b) and e) is given by $f(x) = (\cos(x\pi + \frac{\pi}{2}), \sin(x\pi + \frac{\pi}{2}))$. Similarly we can cut the circle d) into four parts such that two adjacent parts intersect in a single point, and on each part give a homeomorphism to an edge of the square a) using trigonometric functions so that the points of intersection get mapped to the vertices. A homeomorphism between b) and c) is obvious. On the other hand, proving that two spaces are not homeomorphic would require some ingenuity (for now, since we didn't develop the necessary tools).

Some examples of spaces being non-homeomorphic can be proven quickly after making some very simple observations. Let us prove that the open interval $(0, 1)$ is not homeomorphic to the half-closed interval $(0, 1]$. Intuitively, $(0, 1]$ has a one-sided 'boundary', the point 1, which can be removed without disconnecting the space. However, removing any point from $(0, 1)$ splits the space into two connected components.

Lemma 1. *Let X, Y be homeomorphic spaces. Then X is connected if and only if Y is connected.*

Proof. Let $f : X \to Y$ be a homeomorphism. Suppose that X is disconnected, i.e. we have U, V open in X, $U \cup V = X$, $U \cap V \neq \emptyset$. Then $f(U)$, $f(V)$ are open in Y, $f(U) \cup f(V) = Y$, and $f(U) \cap f(V) \neq \emptyset$. Thus Y is disconnected. In the other direction, observe that f^{-1} is also a homeomorphism, hence if Y is disconnected then X is disconnected by the same argument. □

Lemma 2. *Let X, Y be homeomorphic and $X' \subseteq X$ be a subspace of X. Let $f : X \to Y$ be a homeomorphism. Then X', $f(X')$ are also homeomorphic using $f|_{X'}$, where $f(X')$ is considered with the subspace topology from Y.*

Proof. Of course $f|_{X'}$ is a bijection between X' and $f(X')$. Let $U \subseteq X'$ be open, so we have $U = V \cap X'$ for some V open in X. Then $f(V)$ is open since f is homeo- and $f(U) = f(V) \cap f(X')$, hence $f(U)$ is open in $f(X')$. A similar argument shows that if U is open in $f(X')$ then $f^{-1}(U)$ is open in X'. □

Example 20. $(0, 1)$ and $(0, 1]$ are non-homeomorphic. Indeed, suppose that there is a homeomorphism $f : (0, 1] \to (0, 1)$. Then $f|_{(0,1)}$ is also a homeomorphism between $(0, 1)$ and $f((0, 1))$ by lemma 2. But $(0, 1)$ is connected, and $f((0, 1))$ is not connected (since after removing any point from $(0, 1)$ we obtain a disconnected space), which is a contradiction.

Example 21. In Example 1, spaces d) and b) are not homeomorphic. We proceed as above, observing that removing any point from the circle gives us a connected space, while there are points in the segment such that removing them gives us a disconnected space. Similarly d) and g) are not homeomorphic since removing two points from the circle gives a disconnected space (two disjoint segments), while the space obtained by removing any two points from the ring g) is still connected (that last statement is intuitively clear, but it would be quite tedious to prove it formally).

Lemmas 1 and 2 are examples of a more general rule: any property of a topological space which can be defined using only open sets (i.e. in the definition we do not use any additional structures that we might have on our space, for example a metric) is preserved under homeomorphisms. Connected components are mapped to connected components and so on.

1.3. Continuous maps

When dealing with mathematical structures, we usually define maps between those structures that are functions which 'preserve' or 'respect' the structure in some sense but do not necessarily identify two structures. Some examples of identifying maps are bijections of sets (when we only consider sets without additional structure), linear isomorphisms of vector spaces, isomorphisms of groups, or isometries of metric spaces. Examples of maps that respect structure but don't necessarily identify two structures are functions between sets, linear maps between vector spaces or homomorphisms between groups. What would be the corresponding notion for metric spaces or topological spaces?

In mathematical analysis we have the notion of continuous maps between $\mathbb{R}^n$ and $\mathbb{R}^m$ which use the properties of the real numbers. Let us recall the definition.

Definition. A function $f : \mathbb{R}^n \to \mathbb{R}^m$ is **continuous** if for every $x \in \mathbb{R}^n$ and $\epsilon > 0$ there exists $\delta > 0$ such that for every $y \in \mathbb{R}^n$, if $\|x - y\| < \delta$ then $\|f(x) - f(y)\| < \epsilon$.

As we can see, this definition uses only distances between points – $\|x - y\|$ – and not the fact that they lie in $\mathbb{R}^n$ (or $\mathbb{R}^m$ for $f(x), f(y)$). The definition instantly generalizes to metric spaces.

Definition. A function $f : X \to Y$ between metric spaces (X, d_X), (Y, d_Y) is **continuous** if for every $x \in X$ and $\epsilon > 0$ there exists $\delta > 0$ such that for every $y \in X$, if $d_X(x, y) < \delta$ then $d_Y(f(x), f(y)) < \epsilon$.

Let us restate the definition in terms of open balls. For a given x, instead of explicitly considering ys such that $d_X(x, y) < \delta$, we will instead use the open ball of radius δ and center x, and similarly open ball of radius ϵ and center $f(x)$ instead of $d_Y(f(x), f(y)) < \epsilon$. The equivalence of the definition below with the definition above should be obvious.

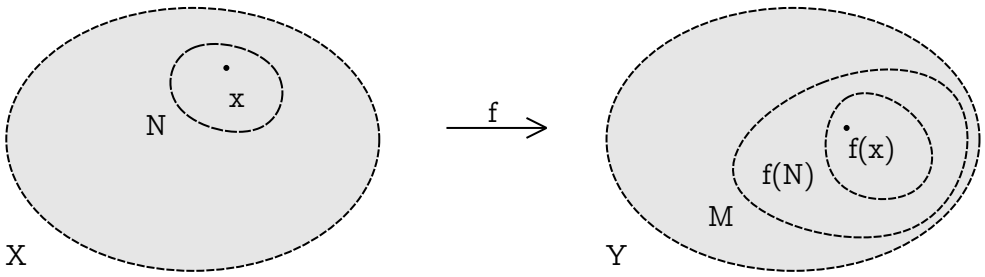
Definition. A function $f : X \to Y$ between metric spaces is **continuous** if for every $x \in X$ and $\epsilon > 0$ there exists $\delta > 0$ such that $f(B_X(x, \delta)) \subseteq B_Y(f(x), \epsilon))$.

Why restrict our attention to open balls? We can consider arbitrary open sets in X and Y that contain x and $f(x)$ respectively. To talk about open sets which contain a given point we usually use the notion of a neighbourhood.

Definition. Let X be a topological space and $x \in X$. $N \subseteq X$ is a **neighbourhood** of x if and only if there exists an open set U such that $x \in U$ and $U \subseteq N$. If a neighbourhood N of x is open, it is called an open neighbourhood of x.

The definition of continuity can be elegantly stated using neighbourhoods.

Lemma 3. *A function $f : X \to Y$ between metric spaces is continuous if and only if for every $x \in X$ and a neighbourhood M of $f(x)$ in Y there exists a neighbourhood N of x in X such that $f(N) \subseteq M$.*



Proof. Suppose $f : X \to Y$ is continuous. Let $x \in X$ and M be a neighbourhood of $f(x)$. Let $x \in V \subseteq M$, where V is open. Then there is some open ball $B_Y(f(x), \epsilon)$ contained in V. From continuity of f we have $B_X(x, \delta)$ such that $f(B_X(x, \delta)) \subseteq B_Y(f(x), \epsilon)$. Take $N = B(x, \delta)$. In the other direction, let $x \in X$ and $\epsilon > 0$. Since $B_Y(f(x), \epsilon)$ is a neighbourhood of $f(x)$ in Y, we have a neighbourhood N of x in X such that $f(N) \subseteq B_Y(f(x), \epsilon)$. Take U open such that $x \in U \subseteq N$. Then there is some open ball $B_X(x, \delta)$ contained in U and we have $f(B_X(x, \delta)) \subseteq B_Y(f(x), \epsilon)$. □

The equivalent condition stated above is stated in terms of neighbourhoods which are defined using open sets. Thus it instantly generalizes to topological spaces.

Definition. A function $f : X \to Y$ between topological spaces is **continuous** if and only if for every $x \in X$ and a neighbourhood M of $f(x)$ in Y there exists a neighbourhood N of x in X such that $f(N) \subseteq M$.

We will use the term 'continuous map' or simply 'map' for a continuous function. We will also use the notation $f : (X, \mathcal{T}_X) \to (Y, \mathcal{T}_Y)$ when we want to explicitly state which topologies we refer to when discussing continuity.

Lemma 4. *A function $f : X \to Y$ between topological spaces is continuous if and only if the preimage of every open set is open.*

Proof. Suppose f is continuous and let $V \subseteq Y$ be open. Let $x \in f^{-1}(V)$. V is a neighbourhood of $f(x)$, hence we have a neighbourhood N of x such that $f(N) \subseteq V$, i.e. $N \subseteq f^{-1}(V)$. Thus we have $x \in U_x \subseteq N \subseteq f^{-1}(V)$, where U_x is open. Since $f^{-1}(V) = \bigcup_x U_x$, $f^{-1}(V)$ is open. In the other direction, let $x \in X$ and M be a neighbourhood of $f(x)$, i.e. $f(x) \in V \subseteq M$ where V is open. Let $N = f^{-1}(V)$. Then N is an open neighbourhood of x and $f(N) \subseteq V \subseteq M$. □

Example 22. Any map from a discrete space to any other space is continuous, since the preimage of any set is always open.

Observe that a function is a homeomorphism if and only if it is a continuous bijection and its inverse is also continuous. However it is not enough to say that it is a continuous bijection.

Example 23. Let $X = \{x, y\}$ (two point space), $\mathcal{T}_1 = \{\emptyset, \{x, y\}\}$ (the trivial topology) and $\mathcal{T}_2 = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$ (the discrete topology). Then the identity function on the set X, considered as a map $f : (X, \mathcal{T}_2) \to (X, \mathcal{T}_1)$, is a continuous bijection, but not a homeomorphism, since $\{x\} \in \mathcal{T}_2$ but $f(\{x\}) \notin \mathcal{T}_1$.

Remark. The theory of topological spaces is vast, general and often very non-intuitive. We don't expect the reader to understand topological spaces for this book. Here we will consider only subspaces of $\mathbb{R}^n$ and soon we will restrict our attention to very simple types of spaces, simplicial complexes, which have a simple combinatorial description. We only discuss topological spaces for motivation, since our goal is to study shape, and topology gives us the necessary tools. The curious reader should open a topology book.

As explained in the introduction, we would like to study data which comes as a finite set of points in Euclidean space.

Definition. A point cloud is a finite subset of $\mathbb{R}^n$.

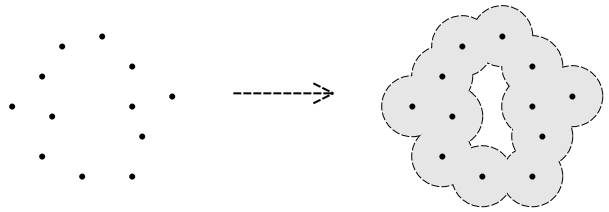
Observe that point clouds have discrete topology (i.e. the topology induced from $\mathbb{R}^n$ is discrete). To see that it is enough to show that every singleton $\{x\}$, where x is a point in the point cloud, is open, since then any subset, being a sum of singletons, will be open (in general, a topology is discrete iff every singleton is open). From the definition of induced topology, we need to show that every singleton is an intersection of an open set in $\mathbb{R}^n$ with the point cloud. Indeed, let x be any point and let d be the minimum of distances between x and other points in the cloud. Then the intersection of $B(x, d)$ with the point cloud is $\{x\}$.

This shows, for example, that point clouds are disconnected, and the connected components consist of single points. From the topological point of view point clouds on their own are not interesting, they have 'trivial' shape. But not all is lost: they are subsets of $\mathbb{R}^n$, and we can use the metric structure of $\mathbb{R}^n$ to study them.

Notation. Let $X \subseteq \mathbb{R}^n$ be a point cloud. Let $\epsilon > 0$. Then

$$X_\epsilon = \bigcup_{x \in X} B(x, \epsilon).$$

X_ϵ arises from X by 'thickening' the points in X by ϵ. Depending on the choice of ϵ, this can give us interesting topological spaces.



X $\qquad$ X_ϵ

Which space should we study though? In general there is no choice of 'the' ϵ. It will turn out later in the book that we can study an entire range of ϵs 'at once'. For now however we will focus on studying X_ϵ for a fixed choice of ϵ.

Topology offers tools to theoretically study topological spaces, although non-trivial topological spaces, which are often infinite sets, are in general not tractable for computations. There are some classes of topological spaces that can be finitely represented and operated on by a machine. Our space, X_ϵ, is such a space, since we can describe it using a finite set of points and a single number ϵ (at least approximately, using floating point arithmetic). This description, however, is not yet well suited to directly apply tools from computational topology which will be introduced later. Our goal for now will be to find a topological space with is in some sense similar to X_ϵ and has a description that is easy to deal with. The types of spaces that are well suited for computations are called simplicial complexes.

1.4. Simplicial complexes

We start with a definition, seemingly unrelated to topology.

Definition. Let S be a set. An **abstract simplicial complex** (ASC in short) Δ on S is a family of non-empty finite subsets of S, such that

1. For all $x \in S$, $\{x\} \in \Delta$.

2. If $\sigma \in \Delta$ and $X \subseteq \sigma$, then $X \in \Delta$.

S is the **set of vertices** of Δ. An element σ of Δ is a **simplex**. If a simplex consists of $n+1$ vertices, its **dimension** is n and the simplex is **n-dimensional**.

The ASC is **finite** if S is finite. The **dimension** of a finite ASC (in contrast to the dimension of a simplex) is the maximum of the dimensions of its simplices.

We will usually omit the set S and talk about Δ only, since S can be obtained by summing all the simplices of Δ. We will only deal with finite abstract simplicial complexes.

A finite ASC Δ with set of vertices S such that $S \in \Delta$ will also be called a simplex (of dimension n, where $n+1$ is the number of its vertices). It is the greatest (with respect to inclusion) ASC for a given set of vertices S.

Abstract simplicial complexes are purely combinatorial objects, but they can be presented as topological spaces.

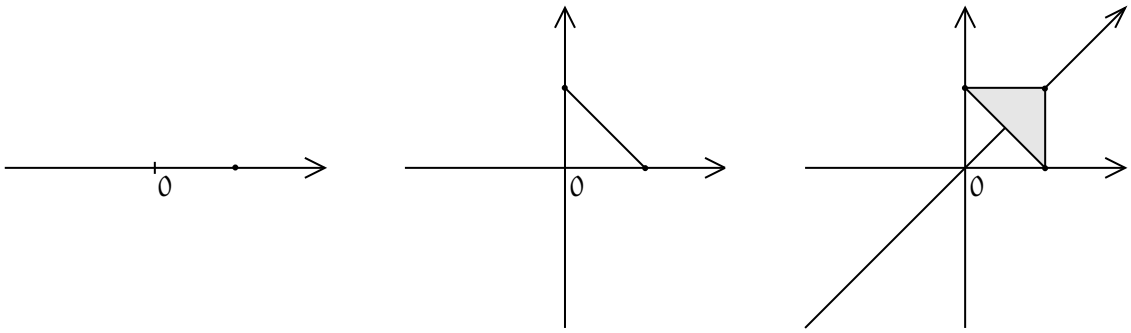
Definition. Let Δ be a finite ASC with n vertices. Take any bijection $\varphi : S \to \mathbb{R}^n$ between S and the set of standard vectors $\{e_1, \ldots, e_n\}$ in $\mathbb{R}^n$. For $\sigma \in \Delta$, let $|\sigma|$ be the convex hull of $\varphi(\sigma)$. Then

$$|\Delta| = \bigcup_{\sigma \in \Delta} |\sigma|.$$

is the **geometric realization** of the ASC Δ.

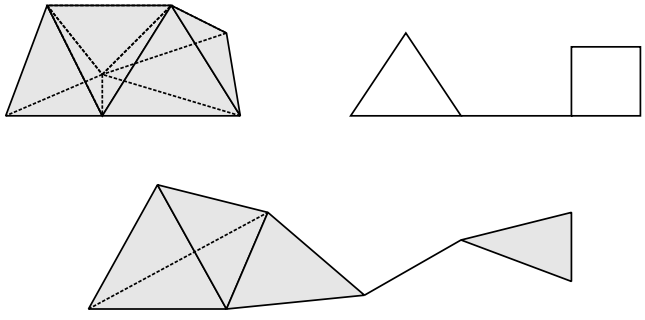
Strictly speaking, $|\Delta|$ depends on the bijection φ and the obtained spaces might be different, but they homeomorphic. Thus we will speak of 'the' geometric realization – fix any φ for a given ASC.

The following picture shows the geometric realizations of simplices of dimension 0 to 2.



Definition. A topological space is a **simplicial complex** if it is homeomorphic to the geometric realization of some ASC. Such a homeomorphism is a **triangulation** of the space.

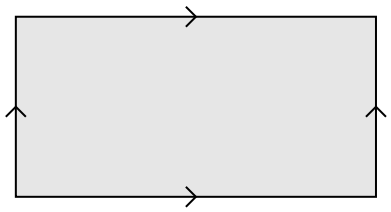
Simplicial complexes can be thought of as collections of simplices that can have common vertices. The following picture shows a bunch of examples of simplicial complexes.



A triangulation of a space can be thought of as splitting the space into simplices. The resulting collection of simplices must have the properties of an abstract simplicial complex: a set of vertices can determine at most one simplex, or equivalently, the intersection of two simplices is either empty or a single simplex. The following example illustrates that condition.

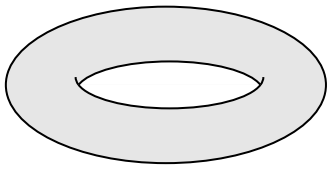
Example 24. Consider the torus.

We can triangulate the torus in the following way. First, imagine the torus as a rectangle in which opposite sides have been glued together:

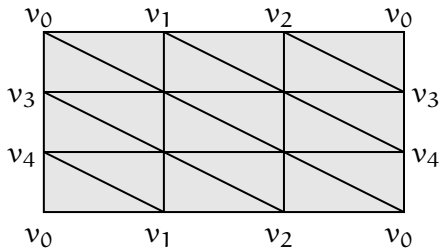


The arrows indicate the directions of gluing: the left edge is identified with the right edge so that the beginning of the left edge (bottom left corner) becomes the beginning of the right edge (bottom right corner) and similarly for the top and bottom edges. In effect all corners get identified. To see why this gives the torus, first identify the top and bottom edges to get a tube:

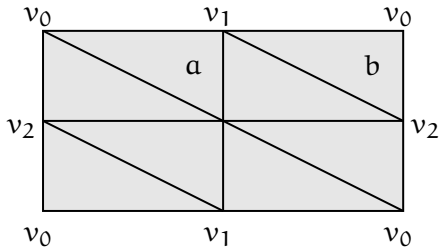
then it is easy to see how the tube needs to be deformed so that the left and right edges get glued together, giving the torus.



When viewing the torus as a rectangle with edges identified we can easily give it a triangulation:



We've named the vertices on the edges to see which vertices are identified. The reader can check that this gives an abstract simplicial complex. Each subset of vertices either doesn't determine a simplex or determines exactly one simplex. On the other hand we could try to 'triangulate' it differently:



This does not give a proper abstract simplicial complex. For example the intersection of the 2-simplices marked as a and b consists of two 0-simplices $\{v_0\}, \{v_1\}$, which is not a single simplex. Equivalently the subset of vertices $\{v_0, v_1\}$ doesn't determine a single 1-simplex.

Abstract simplicial complexes are yet another kind of mathematical structures in our toolbox. As with other structures, we can talk about maps of ASCs.

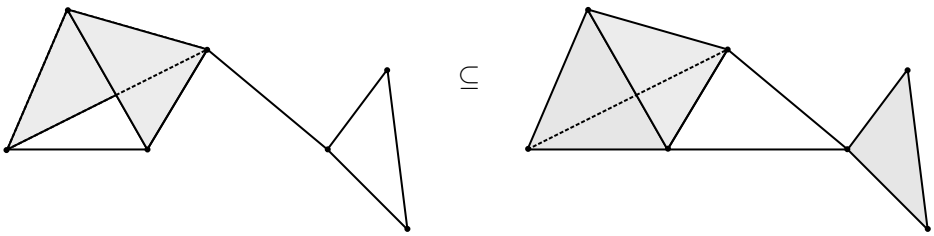
Definition. Let Δ_1 and Δ_2 be ASCs with sets of vertices S_1 and S_2 respectively. A function $f : S_1 \to S_2$ is a **simplicial map** if and only if $X \in \Delta_1$ implies $f(X) \in \Delta_2$. We write $f : \Delta_1 \to \Delta_2$ to denote a simplicial map.

In short: simplicial maps take simplices to simplices (but note that the images of simplices under a simplicial map can be of lower dimension).

Simplicial maps between ASCs induce continuous maps between simplicial complexes – the geometric realizations of the ASCs – by first defining the maps on the points in the simplicial complexes that correspond to vertices in the abstract simplicial complexes and then extending them linearly. The details are not important to us since we will only use the abstract descriptions of simplicial maps.

The examples of simplicials maps that are most important to us are inclusion maps, which we encounter when dealing with subcomplexes.

Definition. Let Δ be an ASC. An ASC Δ' is a **subcomplex** of Δ if and only if $\Delta' \subseteq \Delta$.



If Δ' is a subcomplex of Δ, then in particular the set of vertices of Δ' is contained in the set of vertices of Δ. Therefore the identity map $\Delta' \to \Delta'$ can be thought of as a map to the bigger simplex, $\Delta' \to \Delta$. It is then obviously a simplicial map and is called an inclusion map. Inclusion maps will play an important role later in the book.

We will see in chapter 2 that simplicial complexes allow to easily define and calculate *homology*, an algebraic tool that enables the study of connected components and 'holes' in topological spaces. But our ultimate goal is to study point clouds. What is the connection between simplicial complexes, point clouds, and the space X_ϵ that we've seen previously?

It turns out that X_ϵ is closely related to a certain simplicial complex which can be calculated from the point cloud X and $\epsilon > 0$. The relationship is called *homotopy equivalence*

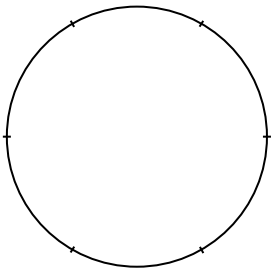
of topological spaces. We will formally define it and discuss it in the last section of the current chapter. Intuitively, homotopy equivalence formalizes the notion of 'continuously deforming' one topological space into another without 'gluing' or 'tearing it apart'. An important fact about homotopy equivalence is that it preserves connected components and holes – the features that we want to study. Thus we don't loose the information that is of interest to us by restricting ourselves to simplicial complexes.

Definition. Let X be a point cloud and $\epsilon > 0$. The **Čech complex** on X with radius ϵ, denoted $\check{C}_\epsilon$, is an abstract simplicial complex defined as follows:

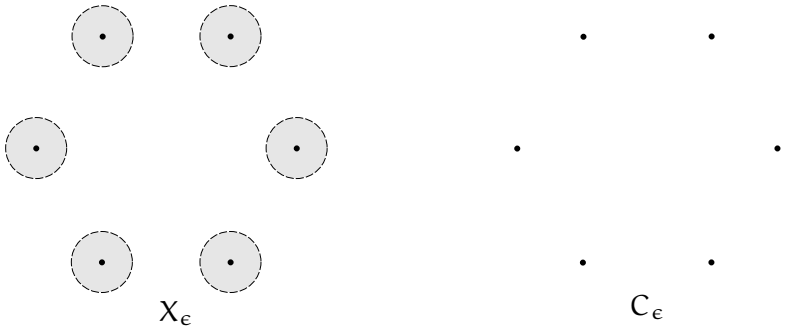
- The set of vertices of $\check{C}_\epsilon$ is the set X,
- For $\sigma \subseteq X$, $\sigma \in \check{C}_\epsilon$ if and only if $\bigcap_{x\in\sigma} B(x,\epsilon) \neq \emptyset$.

In other words, we create a simplex for every subset of points in X such that the balls of radius ϵ centered at each point of the subset intersect. It is clear that the construction gives an ASC.

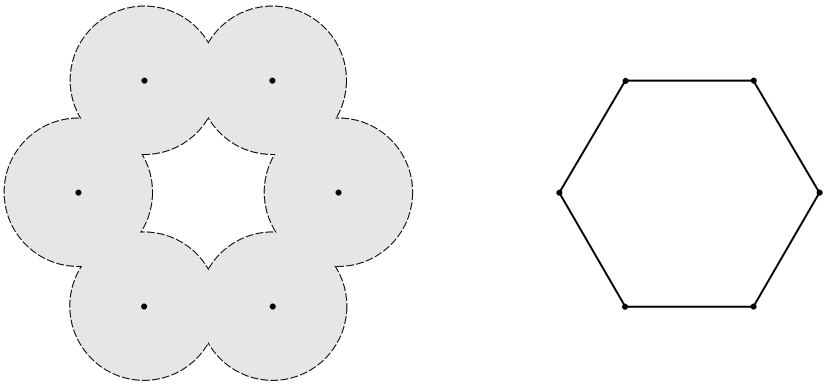
Example 25. Example: Consider $X \subseteq \mathbb{R}^2$ consisting of 6 equally points lying on the unit circle $S^1 = \{x \in \mathbb{R}^2 : \|x\| = 1\}$. To be more specific, take X to be the set of 6th roots of unity: $(1,0)$, $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$, $(-1,0)$, $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$, $(\frac{1}{2}, -\frac{\sqrt{3}}{2})$.



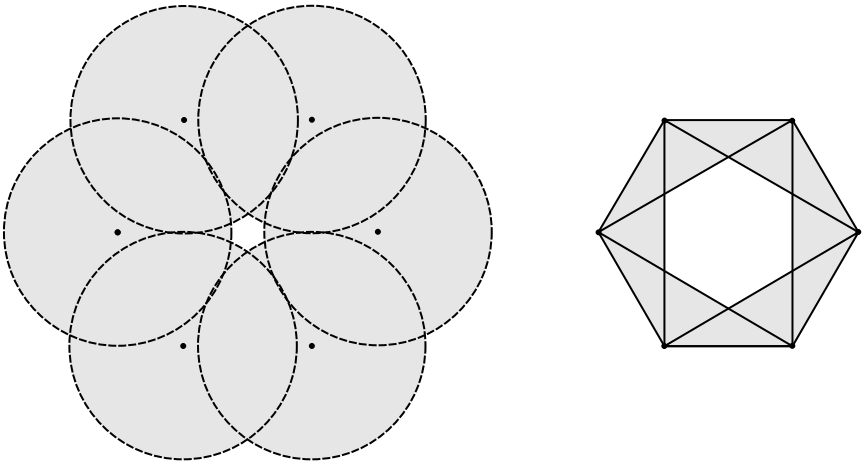
For $\epsilon \in (0, \frac{1}{2} * 1]$ no two distinct balls $B(x,\epsilon)$ intersect, so $\check{C}_\epsilon$ is 0-dimensional, consisting only of the vertices X.



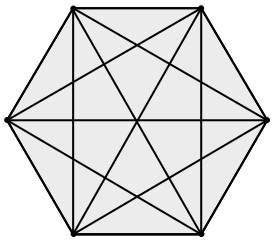
For $\epsilon \in (\frac{1}{2} * 1, \frac{1}{2} * \sqrt{3}]$ pairs of balls corresponding to points of distance 1 intersect, and these are the only intersecting balls. We get a 1-dimensional complex, consisting of the vertices and edges between nearest vertices.



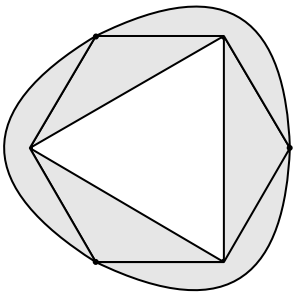
For $\epsilon \in (\frac{1}{2} * \sqrt{3}, \frac{1}{2} * 2]$ we additionally obtain 2-dimensional simplices, since we have triples of intersecting balls, but there are no simplices of higher dimension.



Finally, when $\epsilon > \frac{1}{2} * 2$, all of the balls intersect and the complex becomes a 5-dimensional simplex.



In the pictures above, the drawings of $\check{C}_\epsilon$ for $\epsilon > \frac{1}{2} * \sqrt{3}$ are not 'proper' drawings of simplicial complexes – they contain self-intersections. In fact, for $\epsilon > 1$, $\check{C}_\epsilon$ cannot be 'properly' drawn in $\mathbb{R}^2$. Formally it means that there is no homeomorphism between the geometric realization of $\check{C}_\epsilon$ and a subspace of $\mathbb{R}^2$ – any continuous map from (the geometric realization of) $\check{C}_\epsilon$ to $\mathbb{R}^2$ will not be injective, or in other words will create self-intersections. On the other hand we can draw $\check{C}_\epsilon$ for $\epsilon \in (\frac{\sqrt{3}}{2}, 1]$ if we take some of the 2-simplices 'outside' the hexagon:



For $\epsilon > 1$ if we wanted to embed the complex in Euclidean space we would need 5 dimensions, as the complex contains a 5-dimensional simplex.

Observe that when $\epsilon \leqslant \epsilon'$, $\check{C}_\epsilon$ is a subcomplex of $\check{C}'_\epsilon$. The example above illustrates that fact.

To calculate the Čech complex we have to answer the following question for a given set of points σ: is the intersection of balls of radius ϵ centered at the points of σ non-empty? It is easy to see that this question is equivalent to asking the following: is the radius of the minimum enclosing ball of σ at most ϵ? This problem is a classical problem in computational geometry[11]. Assuming we know how to solve it, we can calculate the Čech complex using a simple algorithm:

Algorithm 1 Computing the Čech complex

Require: X: point cloud, ϵ: positive real number
  $C \leftarrow \emptyset$
  for all $\sigma \subseteq X$ **do**
    if the radius r of the minimum enclosing ball of σ satisfies $r \leqslant \epsilon$ **then**
      $C \leftarrow C \cup \{\sigma\}$
    end if
  end for

This method of computing the Cech complex is probably as naive and inefficient as one can have. In particular the task of finding a minimum enclosing ball for a given set of points is not easy in general and we solve it for every subset of X. We also didn't describe how to enumerate all subsets of X. This can be done recursively; more details about the naive algorithm and a better algorithm can be found in [6]. In any case the amount of memory required to store the complex is at worst exponential in the number of points.

An alternative which is related to the Čech complex is the Vietoris-Rips complex. It can also be constructed from a point cloud, but the definition is more general and works for any finite metric space.

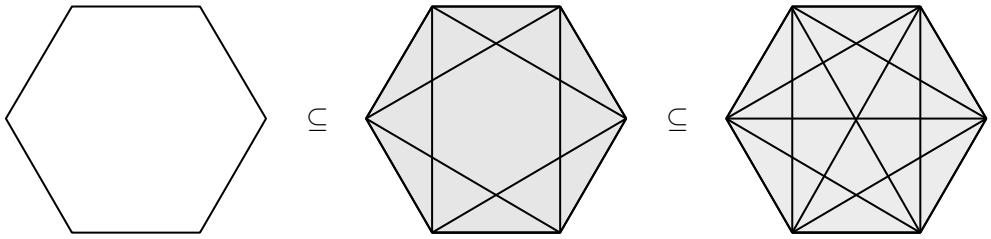
Definition. Let (X, d) be a finite metric space. The **Vietoris-Rips complex** (VR complex in short) on X with radius ϵ, denoted VR_ϵ, is an abstract simplicial complex defined as follows:

- The set of vertices of VR_ϵ is X,
- For $\sigma \subseteq X$, $\sigma \in VR_\epsilon$ if and only if for every $x, y \in \sigma$, $d(x, y) < \epsilon$.

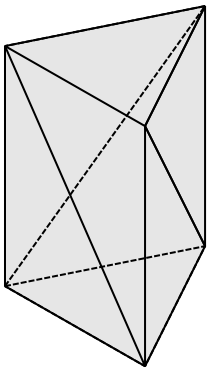
In other words, we create a simplex for every subset of X of diameter smaller than ϵ. It is clear that the construction gives an ASC.

Point clouds in particular are metric spaces (with the Euclidean metric) and we can compare the Čech complex with the VR complex.

Example 26. Let X be the same as in Example 25. For $\epsilon \in (0, \sqrt{3}] \cup (2, \infty)$ we actually have $VR_\epsilon = \check{C}_{\frac{1}{2}\epsilon}$. For $\epsilon \in (\sqrt{3}, 2]$ however, VR_ϵ is strictly bigger than $\check{C}_{\frac{1}{2}\epsilon}$ – we get additional 2-simplices 'in the middle' (see picture below). Indeed, while the corresponding triples of vertices are pairwise distant by less than ϵ, i.e. balls of radius $\frac{1}{2}\epsilon$ centered at these points intersect pairwise, there is no point contained in all three balls at once.



This time we cannot draw VR_ϵ in $\mathbb{R}^2$ for $\epsilon > \sqrt{3}$. However we can make a three-dimensional picture of VR_ϵ for $\epsilon \in (\sqrt{3}, 2]$ – the complex can be drawn as the boundary of a triangular prism, with each of its side face represented by two 2-simplices:



In general, we have the following inclusions of complexes for any $\epsilon > 0$:

$$\check{C}_\epsilon \subseteq VR_{2\epsilon} \subseteq \check{C}_{2\epsilon} \tag{1.1}$$

Proof. Let $\sigma \in \check{C}_\epsilon$. Then for any $x, y \in \sigma$ we have $B(x, \epsilon) \cap B(y, \epsilon) \neq \emptyset$, hence there is some z such that $d(x, z), d(y, z) < \epsilon$, but then $d(x, y) \leqslant d(x, z) + d(z, y) < 2\epsilon$, therefore $\sigma \in VR_{2\epsilon}$. Thus $\check{C}_\epsilon \subseteq VR_{2\epsilon}$.

Let $\sigma \in VR_\epsilon$. Take any $x \in \sigma$. Since $d(x, y) < \epsilon$ for all $y \in \sigma$, $x \in \bigcap_y B(y, \epsilon)$, i.e. $\bigcap_y B(y, \epsilon) \neq \emptyset$, therefore $\sigma \in \check{C}_\epsilon$. Thus $VR_\epsilon \subseteq \check{C}_\epsilon$ (or equivalently $VR_{2\epsilon} \subseteq \check{C}_{2\epsilon}$). □

The VR complex does not have to be homotopy equivalent to X_ϵ, but the above inclusions suggest that a lot of information about the Čech complex (hence about X_ϵ) is preserved, especially when we consider a whole range of ϵs at once.

An upside of the VR complex would be the fact that it works for any metric space, not just point clouds. Thus if our data consists of a set of points (not necessarily in $\mathbb{R}^n$) with some similarity measure defined on them, we can use the VR complex.

Probably the most important reason to use the VR complex is its ease of construction compared to the Čech complex: we only have to check for pairwise distances between the

vertices of our finite metric space. Indeed, a set of $k+1$ vertices in the VR complex forms a k-dimensional simplex if and only if these vertices form a clique in the graph of the complex, i.e. every two vertices in this set are connected with an edge. Thus computing the VR complex becomes much more straightforward:

Algorithm 2 Computing the Vietoris-Rips complex

Require: X: finite metric space, ϵ: positive real number
  $C \leftarrow \emptyset$
  for all $\sigma \subseteq X$ **do**
    if $d(x, y) < \epsilon$ for every $x, y \in \sigma$ **then**
      $C \leftarrow C \cup \{\sigma\}$
    end if
  end for

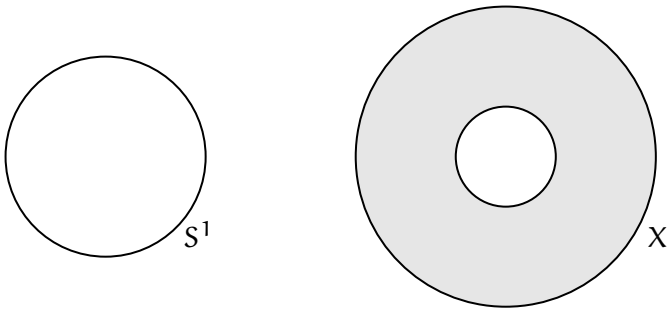
We can also use the property of the VR complex mentioned above and split the construction into two phases. First we compute the subcomplex consisting of its vertices and 1-simplices, called its 1-skeleton or graph. The amount of memory required to store this graph is quadratic in the worst case – much better. Then in the second phase we list all the cliques in this graph to obtain its higher-dimensional simplices. If we are lucky we might not even need to store the higher-dimensional simplices in memory and perform our computations 'online' while listing the simplices so that the used space doesn't go beyond quadratic. Furthermore in some applications we need to list only the simplices up to some fixed dimension – we will see an example of this in chapter 2. For further discussion on the two-phase approach and fast construction of the Vietoris-Rips complex see [16].

The problem with both the Čech complex and the Vietoris-Rips complex is that depending on the choice of ϵ and how our data is placed in space (or the metric), the number of simplices we have to consider might become exponential in the number of data points in the worst case. Attempts to solve this problem include approximating the Čech complex or the VR complex, subsampling points from our data set, or considering different complexes such as the Delaunay complex, the Alpha complex or the Witness complex. For a nice survey of the different complexes see [14, Section 5.2].

1.5. Homotopy equivalence of topological spaces

We've mentioned earlier that the space X_ϵ obtained from a point cloud X by 'thickening' the points is 'homotopy equivalent' to the Čech complex $\check{C}_\epsilon$ on X. But what does that mean? Let us first give a motivating example.

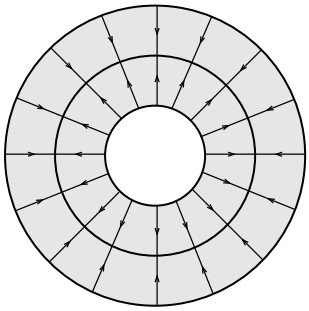
Example 27. Consider S^1, the unit circle in the plane, i.e. the set of points $\{x \in \mathbb{R}^2 : \|x\| = 1\}$ (with the Euclidean topology as usual) and $X = \{x \in \mathbb{R}^2 : \frac{1}{2} \leqslant \|x\| \leqslant \frac{3}{2}\}$, a 'thickened circle'.



Recall that S^1 and X are not homeomorphic (examples 1 and 21; X is homeomorphic to the space g). Indeed, after removing two points from S^1, the obtained space consists of two arcs that are open and disjoint, thus S^1 without two points is disconnected. However, X without any two points is still connected.

Homeomorphism is a very strong notion – if two spaces are homeomorphic, they are essentially the same. A homeomorphism 'renames' the points of a space (being a bijective function), at the same time preserving everything that can be said about its topological features (since it takes open sets to open sets and non-open sets to non-open sets).

We would like to define a type of equivalence of topological spaces that is broader than homeomorphism and formalizes the intuition of 'continuously deforming one shape into another'. For example, imagine the space X defined above being continuously shrinked in time to the circle S^1 contained in X along the segments perpendicular to S^1, as in the picture below:



Every point of X 'moves in time' to a point of S^1 in a 'continuous way'. We would like to formalize this idea and extend it to spaces that are not necessarily contained in one another.

Denote $I = [0, 1]$ and let $t \in I$ – think of t as time. For each point in time we define a continuous function $f_t : X \to X$ using the formula $f_t(x) = (1 - t)x + t\frac{x}{\|x\|}$. Observe what happens when t changes: when $t = 0$, the function is the identity on X, $f_0 = id_X$. For $t = 1$ the function maps each point of X into its corresponding closest point on S^1, $f_1(x) = \frac{x}{\|x\|}$. When t goes from 0 to 1, each point x is 'slided' continuously by f_t from its original position x to its final position $\frac{x}{\|x\|}$. The points already lying on S^1 do not change: on S^1, f_t is the identity for every t. Furthermore, everything is done continuously: the map $F : X \times I \to X$, $F(x, t) = f_t(x)$, is continuous (where $X \times I$, the cartesian product of X and I, can be thought of as a subspace of $\mathbb{R}^3$, X being a subspace of $\mathbb{R}^2$ and I a subspace of $\mathbb{R}$). The family $\{f_t : t \in I\}$ or equivalently the map F is called a deformation retraction of X onto S^1, and S^1 is called a deformation retract of X.

Definition. Let X be a topological space and Y a subspace of X. A **deformation retraction** of X onto Y is a continuous map $F : X \times I \to X$ such that:

- The map $x \mapsto F(x, 0)$ is the identity on X.
- For all $x \in X$, $F(x, 1) \in Y$.
- For all $t \in I$ and $y \in Y$, $F(y, t) = y$.

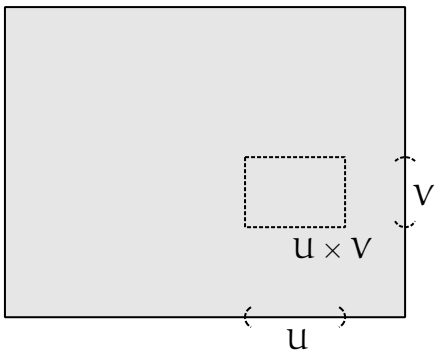
If such a map exists, then Y is a **deformation retract** of X.

There is a problem with the above definition – we didn't yet mention what the topology on the product $X \times I$ is in general. If we restrict ourselves to subsets of the Euclidean space, $X \subseteq \mathbb{R}^n$, then $X \times I$ can be thought of as a subspace of $\mathbb{R}^{n+1}$, hence given the subspace topology. The spaces considered in this book are indeed Euclidean, but for completeness we will give the general definition.

Definition. Let X and Y be topological spaces. An **open box** in $X \times Y$ is a set of the form $U \times V$, where $U \subseteq X$ and $V \subseteq Y$ are open in X and Y respectively.

Definition. Let X and Y be topological spaces. Define a topology on $X \times Y$ as follows: $W \subseteq X \times Y$ is open if and only if for every $p \in W$ there exists an open box $U \times V$ such that $p \in U \times V \subseteq W$. The obtained topology is the **product topology** on $X \times Y$.

One should check that this indeed gives a topology on $X \times Y$.



Example 28. The product topology on $\mathbb{R}^n \times \mathbb{R}^m = \mathbb{R}^{n+m}$, where $\mathbb{R}^n$ and $\mathbb{R}^m$ are given the Euclidean topology, is the Euclidean topology on $\mathbb{R}^{n+m}$.

Armed with the definition of a deformation retract we can proceed onto defining homotopy equivalence of spaces. Two spaces are homotopy equivalent if we can view them both as subspaces of a greater space such that they are both deformation retracts of this space. Formally we require the notion of an embedding of one topological space into another.

Definition. Let X and Y be topological spaces. A map $f : X \to Y$ is an **embedding** of X into Y if f is a homeomorphism between X and its image $f(X) \subseteq Y$. If such an embedding exists, X is said to be embedded into Y.

When a space X embeds into Y, we can be a little sloppy and simply treat it as a subspace of Y.

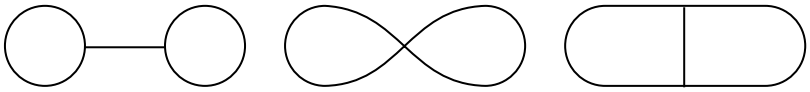
Definition. Let X and Y be topological spaces. X and Y are **homotopy equivalent** if and only if there exists a space Z such that X and Y embed in Z and are deformation retracts of Z under this embedding.

Homotopy equivalent spaces are also said to be *of the same homotopy type*. It is clear that homeomorphic spaces are homotopy equivalent.

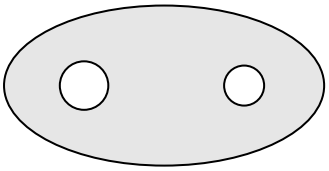
The definition given above is not the usual one given in topology textbooks and it has its flaws compared to the other one, e.g. from this definition it is not clear that homotopy equivalence is transitive. We chose it because of its intuitive geometric appeal – we can 'see' how the space X gets deformed to the space Z and then Y.

Example 29. If X is a deformation retract of Y, then X and Y are homotopy equivalent, since Z is trivially a deformation retract of itself.

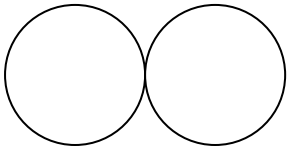
Example 30 (taken from [9])**.** The three spaces drawn below:



are homotopy equivalent to each other, since each is a deformation retract of the following space:



Example 31. The wedge of two circles $X = \{x : \|x - 1\| = 1\} \cup \{x : \|x + 1\| = 1\}$:



is not homotopy equivalent to the single circle S^1. This is because homotopy equivalent spaces have isomorphic homology groups – to be defined in chapter 2 – while S^1 has one-dimensional first homology group and X has two-dimensional first homology group.

The relationship between $\check{C}_\epsilon$ and X_ϵ can be now stated using precise language.

Theorem 2. *For a given set of points X in Euclidean space, its Čech complex $\check{C}_\epsilon$ and the space X_ϵ are homotopy equivalent.*

This result is actually a special case of a more general theorem known as the *nerve theorem* and its proof is beyond the scope of this book. A full treatment can be found in [9, Section 4.G].

Before we move on, one last question remains: what is *shape*? This vague idea has been floating around since the beginning of this book – we want to study 'the shape of our data'. Shape does actually have a precise meaning in mathematics and there is a subfield of topology called *shape theory*[7], but it stays far away from the much more elementary considerations presented in this book. For our purposes we could define shape as follows. First, it is true that homotopy equivalence is actually an equivalence relation, so we can talk about equivalence classes of topological spaces under this relation, i.e. *homotopy types* of spaces. In chapter 2 we will consider *algebraic invariants* of topological spaces that depend

only on their homotopy types, so for practical purposes homotopy type could be what we call shape. However note that even under this terminology we're going to study possibly many different shapes associated to a point cloud, i.e. the spaces X_ϵ for different ϵs which don't have to be homotopy equivalent to each other (and that is the whole point). In summary, by studying 'the shape of our data' we actually mean studying different shapes that can be associated to our data.

Chapter 2

Homology

For this chapter we assume only very basic knowledge of groups and vector spaces by the reader. If necessary, read appendix A for a refresher.

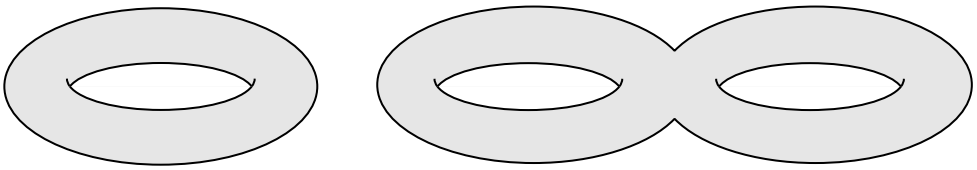
In the previous chapter we've defined and briefly discussed topological spaces which allow us to formally study the notion of shape. We've also seen examples of assigning nontrivial topological spaces to sets of finite points that are embedded in Euclidean spaces or simply come with a metric. In both cases the spaces had the shape (i.e. homotopy type in our terminology) of a simplicial complex, a topological space – inherently an infinite entity – which has a purely combinatorial and finite description. This suggests the possibility of using tools from the mathematical field of topology to study data sets arising in real-world applications, an approach known as *topological data analysis*[13, 3].

Simplicial complexes are some of the 'nicest' spaces out there. One of their properties is that they are *Hausdorff* which means that for any two distinct points we can find their neighbourhoods that are disjoint. There are of course topological spaces without this property, like the two-point indiscrete topological space (Example 15). The particular example of indiscrete spaces might seem trivial but there are a lot of very interesting and important non-Hausdorff spaces such as those arising in *algebraic geometry*. Coming back to simplicial complexes, they satisfy the stronger property of being *metrizable*, i.e. for every simplicial complex there exists a metric such that the topology of the complex is the one obtained from this metric. In fact we can point out a particular metric, the Euclidean metric since simplicial complexes embed in Euclidean spaces. Of course there are other metrics giving the same topology, but the mere fact of being metrizable says a lot about the 'niceness' of the space. All metrizable spaces are Hausdorff but not vice-versa. Moving on, finite simplicial complexes are *compact*, which in the case of metrizable spaces can be characterized as follows: every sequence of points in the space has a convergent subsequence, i.e. a subsequence that has a limit, a point such that every its neighbourhood contains all but finite number of points from the subsequence. Informally speaking compact spaces 'don't extend to infinity' and 'have a boundary'. And of course there are many other properties of simplicial complexes making them 'easy to think about' that we didn't define.

Summarizing the above paragraph, simplicial complexes are in some sense boring, at least from the point of view of *general topology* which is the study of basic definitions and properties of topological spaces that can be expressed starting only with the fundamental idea of an open set. In particular we cannot distinguish different simplicial complexes by searching for the types of pathologies studied in general topology since in this case there are

none. Nevertheless we strongly encourage the reader to consult a more complete treatment of topology such as [15] to witness the vast generality of this field.

Dealing with topological spaces that are 'uninteresting' in the above sense obviously has its upsides. When thinking about such well-behaved topological spaces we can use our geometric intuitions and try to describe whatever features 'visible to the eye' they might have. For example if we look at the torus and the double torus pictured below:



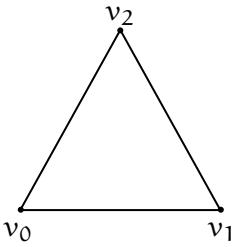
we could argue that the torus has one 'handle' while the double torus has two. This idea can indeed be made precise: the above spaces belong to the class of so called *orientable closed surfaces* and to each such surface we can assign a natural number called its *genus* that formalizes the intuition of 'the number of handles'[1]. This strategy proves to be very fruitful because the genus *classifies* orientable closed surfaces up to homeomorphism: two such surfaces have the same genus if and only if they are homeomorphic! Of course what's important here is that we're looking at a class of topological spaces that satisfy some very rigid conditions – the notion of genus doesn't always make sense. In particular many simplicial complexes which are interesting to us are not surfaces. If the reader finds the topic interesting, a good treatment of surfaces and more generally topological manifolds can be found in [12].

The above example suggests the general strategy of trying to describe features of sufficiently well-behaved topological spaces by assigning them simpler objects such as numbers. These objects should not depend on where we embed our topological space, i.e. homeomorphic spaces should have the same object assigned. If we only care about the homotopy type of a space we could require that homotopy equivalent spaces get the same objects. Such objects are called *invariants*, in particular *homotopy invariants* if they depend only on the homotopy type. These invariants should give us information about the space or its homotopy type – assigning the same object to all spaces would be useless. An ideal situation would be when the invariants completely classify the spaces up to homeomorphism or homotopy equivalence, i.e. non-equivalent spaces get different objects. For example in the world of orientable closed surfaces the genus is such a classifying invariant.

Invariants of topological spaces don't have to be numbers. The field of *algebraic topology* aims to use algebraic objects such as groups or vector spaces to study topological spaces. In this chapter we will describe a formalism called *simplicial homology* where we assign a sequence of vector spaces to a simplicial complex. These vector spaces will only depend on the homotopy type of our topological space. One could intuitively think about homology as detecting holes in topological spaces. This is particularly apparent when studying 2- and 3-dimensional examples. However homology is much more than that and in higher dimensions interesting phenomena can arise. We will see an instance of that later, but before we do, let us study some motivating low-dimensional examples.

[1]The reader is not required to know what an orientable closed surface is. This example is simply to illustrate the power of assigning invariants to topological spaces.

Example 32. Let X be the boundary of a 2-simplex, i.e. 3 segments forming a closed path. We denote the vertices of this simplicial complex by v_0, v_1, v_2. Its segments (1-simplices) are $\{v_0, v_1\}, \{v_1, v_2\}, \{v_2, v_0\}$.



The idea is that X has a hole which can be 'walked around'. 'Walking' usually involves direction, so let us direct our simplices. We will use curvy brackets to denote directed simplices: now (v_0, v_1) is a different simplex than (v_1, v_0) – these are the two different directions of $\{v_0, v_1\}$.

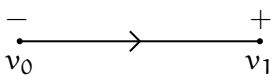
If v, w are vertices, by $[v, w]$ we denote 'walking the segment (v, w) once'. By $-[v, w]$ we denote 'walking the segment (v, w) in the opposite direction once'. Thus $-[v, w] = [w, v]$. Similarly, for n an integer, $n[v, w]$ means 'walking the segment $[v, w]$ n times'. If n is negative, that means walking in the opposite direction. 0 means no walking.

Don't get too attached to the 'walking' idea, it's just for intuition and won't generalize to higher dimensions (2-simplices etc). For now, however, it can give us some geometric view on homology.

A *1-chain* is a finite formal sum of expressions of type $[v, w]$, where v, w is a 1-simplex in our simplicial complex, with integer coefficients. The simplest 1-chain is 0, the trivial chain. Some other examples of 1-chains for the complex X are $[v_1, v_2] + 3[v_0, v_1]$, $[v_0, v_1] + [v_1, v_2] + [v_2, v_0]$, $-5[v_0, v_2]$. Intuitively a 1-chain denotes 'walking on' each of the summands and the integers tell us how many times the segment is walked on and in which direction. The order does not matter and the segments don't have to create a connected path, there is no beginning or no end distinguished in the 1-chain.

A *1-cycle* is a 1-chain in which every vertex is 'entered' the same number of times as it is 'left'. In X, for example, $[v_0, v_1]$ is not a 1-cycle because v_0 is left 1 time but entered 0 times. On the other hand $[v_0, v_1] + [v_1, v_2] + [v_2, v_0]$ is a 1-cycle because for every $i = 0, 1, 2$, the vertex v_i is entered and left exactly one time.

Let us formalize a bit the idea in the above paragraph. A *0-chain* is a formal sum of expressions of type $[v]$, where v is a vertex in our simplicial complex, with integer coefficients. For a 1-chain $[v, w]$ its *boundary* is the 0-chain $[w] - [v]$, which we denote using the following symbol: $\partial[v, w] = [w] - [v]$. Intuitively it can be read as follows: 'walking (v, w) once involves entering w once and leaving v once'. We extend the boundary operator ∂ to all 1-chains linearly, i.e. $\partial \sum_\alpha n_\alpha [v_\alpha, w_\alpha] = \sum_\alpha n_\alpha \partial[v_\alpha, w_\alpha] = \sum_\alpha n_\alpha([w_\alpha] - [v_\alpha])$.



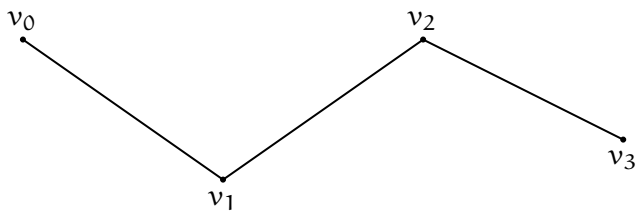
$$\partial[v_0, v_1] = [v_1] - [v_0].$$

Now a *1-cycle* is a 1-chain whose boundary is 0. For example $\partial[v_0, v_1] = [v_1] - [v_0] \neq 0$, thus $[v_0, v_1]$ is not a 1-cycle. On the other hand $\partial([v_0, v_1] + [v_1, v_2] + [v_2, v_0]) = [v_1] - [v_0] + [v_2] - [v_1] + [v_0] - [v_2] = 0$, hence this is a 1-cycle.

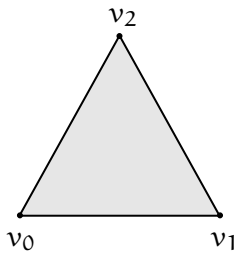
In our 1-dimensional complex X, the 1-cycle $[v_0, v_1] + [v_1, v_2] + [v_2, v_0]$ has the following important properties:

- it is nontrivial, i.e. not equal to 0, unlike, for example, the cycle $[v_0, v_1] + [v_1, v_0]$,
- it *generates all 1-cycles*, i.e. every 1-cycle is a multiple of this cycle, which can be seen using some computations. For example $2[v_1, v_0] + 2[v_0, v_2] + 2[v_2, v_1] = -2([v_0, v_1] + [v_1, v_2] + [v_2, v_0])$.

Example 33. The complex drawn below has no non-trivial 1-cycles.



Example 34. The situation becomes a bit more complicated when we consider higher-dimensional complexes. Let X be a 2-simplex.



We will now introduce *oriented* 2-simplices. This is the 2-dimensional analogue of what we did with 1-simplices when choosing a direction. Again, as with 1-simplices, there will be two ways to assign an orientation to a 2-simplex $\{v, w, u\}$. However, in the case of 1-simplices, there were two vertices, so the orientation could simply be determined by their order: it was either (v, w) or (w, v). For 2-simplices we will say that two orderings of vertices determine the same orientation if and only if they differ by an even permutation. Equivalently, two orderings determine the same orientation if and only if one can be obtained from the other by performing an even number of transpositions (swaps of two vertices). For example we can perform the following transpositions:

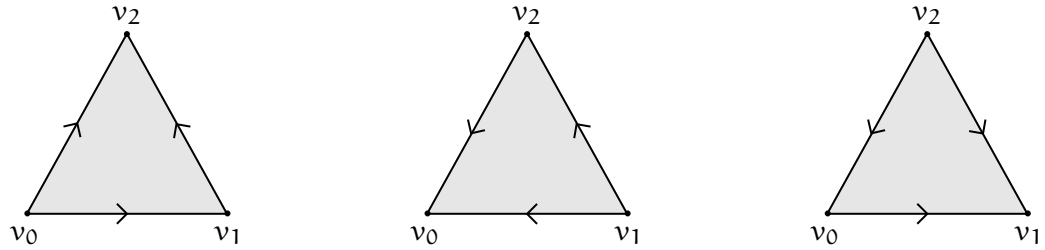
$$(v, w, u) \to (v, u, w) \to (u, v, w)$$

$$(v, w, u) \to (w, v, u) \to (w, u, v)$$

Thus the orderings $(v, w, u), (u, v, w), (w, u, v)$ determine the same orientation of the 2-simplex $\{v, w, u\}$. Similarly, $(v, u, w), (u, w, v), (w, v, u)$ determine the same orientation of the 2-simplex. It is a basic fact about permutations that one ordering cannot be obtained from another both by even and odd number of transpositions. Thus our set of orderings is

partitioned into two disjoint subsets, giving two possible orientations. We denote an oriented simplex by $[v, w, u]$. Hence we have $[v, w, u] = [w, u, v] = [u, v, w]$ and $[v, u, w] = [u, w, v] = [w, v, u]$.

To draw an oriented 2-simplex, we can draw a nonoriented 2-simplex and put arrows on the segments which determine an ordering of the vertices. This gives a number of possible drawings of the same choice of orientation.



Possible drawings of $[v_0, v_1, v_2]$.

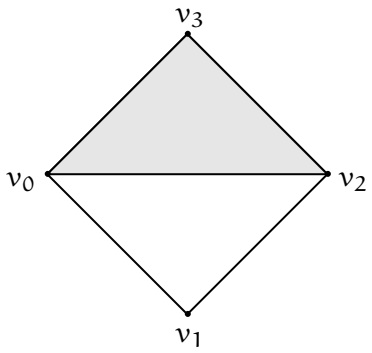
A *2-chain* is a finite formal sum of oriented 2-simplices, i.e. expressions of the form $[v, w, u]$ where $\{v, w, u\}$ is a 2-simplex in our simplicial complex, with integer coefficients. In the case of 1-simplices we had the equality $[v, w] = -[w, v]$. Now we establish that $[v, w, u] = -[w, v, u]$ – we introduce a minus sign whenever we change the orientation of a simplex.

The *boundary* of a 2-chain is a 1-chain defined for single oriented 2-simplices by the equality $\partial[v, w, u] = [w, u] - [v, u] + [v, w]$, which is then extended linearly to all 2-chains, similarly as the boundary of a 1-chain. A *1-boundary* is a 1-chain which is a boundary of some 2-chain. For example, in X, the 1-chain $[v_1, v_2] - [v_0, v_2] + [v_0, v_1]$ is a 1-boundary, since it is the boundary of $[v_0, v_1, v_2]$.

Two 1-chains A and B are called *homologous* if $A - B$ is a boundary. In particular if A is a boundary it is *homologous to* 0.

The 1-chains of X are exactly the same as in Example 32. In particular, the 1-cycles of X are generated by the nontrivial cycle $[v_0, v_1] + [v_1, v_2] + [v_2, v_0]$. However in the previous case there were no 2-simplicies, hence no nontrivial 2-chains, so in particular no nontrivial 1-boundaries. This time our generator is a 1-boundary: $\partial[v_0, v_1, v_2]$. Therefore every 1-cycle is homologous to 0.

Example 35. In the simplicial complex below:



the 1-cycles $[v_0, v_1] + [v_1, v_2] + [v_2, v_3] + [v_3, v_0]$ and $[v_0, v_1] + [v_1, v_2] + [v_2, v_0]$ are homologous. Indeed, their difference $[v_2, v_3] + [v_3, v_0] - [v_2, v_0]$ is equal to $\partial[v_2, v_3, v_0]$.

The examples above suggest that holes can be detected by *cycles*, but we have to be careful in the presence of *boundaries*. Intuitively, when two cycles are homologous to each other, they should not detect different holes. These ideas are formalized using tools from linear algebra. The reader who analyzed and understood the examples above will have no difficulty reading about the general theory below.

2.1. The simplicial chain complex

Definition. Let Δ be an abstract simplicial complex and $\sigma = \{v_0, \ldots, v_n\} \in \Delta$ be a simplex. An **ordering** of the vertices of σ is a sequence $(v_{i_0}, \ldots, v_{i_n})$ such that $0 \leqslant i_0 < \cdots < i_n \leqslant n$ (i.e. the sequence $(i_0, \ldots, i_n)$ is a permutation of $(0, \ldots, n)$). Two orderings $v_{i_0}, \ldots, v_{i_n}$ and $v_{j_0}, \ldots, v_{j_n}$ **have the same orientation** if and only if there exists an even permutation τ of integers $\{0, \ldots, n\}$ such that $(\tau(i_0), \ldots, \tau(i_n)) = (j_0, \ldots, j_n)$. They have **different orientation** if and only if there exists an odd permutation having this property.

Having the same orientation is an equivalence relation on the set of orderings. If $n = 0$ there is only one possible ordering, hence only one equivalence class. For $n > 0$ the relation divides the set of orderings into two classes of equal size.

Definition. An **orientation** is an equivalence class of the above relation for some simplex $\sigma = \{v_0, \ldots, v_n\}$. An **oriented simplex** is a simplex together with an orientation. We denote an oriented simplex by $[v_{i_0}, \ldots, v_{i_n}]$, meaning that the set of vertices is $\{v_0, \ldots, v_n\}$ and the chosen orientation is represented by the ordering $(v_{i_0}, \ldots, v_{i_n})$.

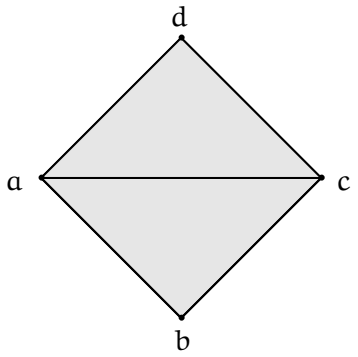
Example 36. An oriented simplex $[v, w, u]$ is a simplex $\{v, w, u\}$ together with the orientation $\{(v, w, u), (w, u, v), (u, v, w)\}$. Thus the symbols $[v, w, u], [w, u, v], [u, v, w]$ represent the same object. Another possible orientation would be $\{(v, u, w), (u, w, v), (w, v, u)\}$.

In the examples above we've considered formal sums of oriented simplices with integer coefficients. This is the usual way to go when defining so called homology groups. However, for reasons that won't be apparent until chapter 3 we will only consider *homology with coefficients in a field*. That is, we will talk about formal sums of oriented simplices with coefficients in some field $\mathbb{F}$. For example, if $\mathbb{F} = \mathbb{Q}$, the field of rational numbers, one such element would be $\frac{1}{2}[v, w] + \frac{5}{3}[w, u]$.

Formally, the object that we will study is obtained by constructing a vector space from a given basis. Recall from linear algebra that every vector space has a basis, i.e. a linearly independent set of vectors which generates the whole space. For example the Euclidean plane $\mathbb{R}^2$ as a vector space over $\mathbb{R}$ has bases such as $(1, 0), (0, 1)$ or $(1, 1), (0, 1)$. Whenever we have a vector space, we can find a basis, usually more than one. We can also go in the other direction – starting with some arbitrary set and a field $\mathbb{F}$ we can construct a vector space over $\mathbb{F}$ such that one of the bases of this vector space will be the set. A formal construction of such an object is given in appendix A. If the reader didn't see it, it might be enlightening, but it's probably not necessary to go through the whole construction. We simply think of the elements of such vector space as (finite) linear combinations of elements of the set (the basis we started with) with coefficients from $\mathbb{F}$.

Example 37. Let $\mathbb{F} = \mathbb{Q}$ and $S = \{a, b, c\}$ – a set with three elements. Let V be a vector space over the field $\mathbb{F}$ with basis S. Then the elements of V are of the form $x_1 a + x_2 b + x_3 c$ where $x_1, x_2, x_3 \in \mathbb{Q}$. The elements a, b, c form a basis of V. $2a + b, b, c$ is another basis of V.

Example 38. Let X be a simplicial complex drawn below:



with vertices named a, b, c, d. Let V be a vector space over $\mathbb{Q}$ with basis the oriented 1-simplices of X. That is, the basis is $\{[a, b], [b, a], [a, c], [c, a], [b, c], [c, b], [c, d], [d, c], [d, a], [a, d]\}$ and V contains elements such as $[a, b] + \frac{3}{4}[d, c]$ etc.

The vector space in Example 38 is almost the one that we would like to study. There is one problem though, namely with the different orientations of a simplex. We would like to have the equalities $[v, w] + [w, v] = 0$ as in the examples at the beginning of the chapter, while Example 38 elements such as $[a, b], [b, a]$ are linearly independent. The construction which allows us to do that is the quotient of a vector space by a subspace.

Definition. Let V be a vector space over a field $\mathbb{F}$ and $W \subseteq V$ be a subspace. We define a relation $\sim$ on V as follows: $a \sim b$ if and only if $a - b \in W$. This is an equivalence relation: symmetry and reflexivity is obvious, and if $a \sim b$, $b \sim c$, then $a - c = (a - b) - (c - b) \in W$, so it is transitive. The set of equivalence classes under this relation is the **quotient of V by W** and is denoted by V/W. The equivalence class of an element $v \in V$ is denoted by $v + W$.

Lemma 5. *This is a vector space over $\mathbb{F}$ under the following operations:*

- *for $k \in \mathbb{F}$, $v + W \in V/W$, $k(v + W) = kv + W$ (multiplication by scalars),*
- *for $v + W, u + W \in V/W$, $(v + W) + (u + W) = v + u + W$ (addition).*

Proof. We will check that the operations are well defined (they don't depend on the choice of representatives of equivalence classes) and leave checking the axioms of a vector space to the reader (they are pretty obvious).

Multiplication by scalars is well defined: let $k \in \mathbb{F}$ and $v + W = v' + W$. Then $v - v' \in W$, hence $k(v - v') \in W$ since W is a subspace. But $k(v - v') = kv - kv'$, hence $kv + W = kv' + W$.

Addition is well defined: if $v + W = v' + W$ and $u + W = u' + W$, then $v + u - (v' + u') = (v - v') + (u - u') \in W$ since W is a subspace, hence $v + u + W = v' + u' + W$. □

Definition. Let $W \subseteq V$ be vector spaces. The map $\pi : V \to V/W$ given by

$$\pi(v) = v + W$$

is the **projection map**.

It is easy to see that π is a linear map which is an epimorphism and its kernel is exactly W.

The question we will ask often is: how do we find a basis of a quotient V/W? One possible way to do that is to find *compatible* bases of W and V, i.e. a basis B of V and a subset B' of B such that B' is a basis of W. Then elements $b + W$ for $b \in B \setminus B'$ form a basis for V/W.

Example 39. Let V be a vector space over $\mathbb{Q}$ with basis $\{a, b, c, d\}$. Let $W = \operatorname{span}\{a, b\}$ (subspace of V generated by the elements a, b). Then $\{c + W, d + W\}$ is a basis of V/W.

Let $W' = \operatorname{span}\{a + b, c + d\}$. Then, since $\{a + b, c + d, a, c\}$ is also a basis of V, $\{a + W', c + W'\}$ is a basis of V/W'. Observe that we have the equalities $a + W' = -b + W'$, $c + W' = -d + W'$ in V/W'.

Definition. Let Δ be an abstract simplicial complex and $\mathbb{F}$ a field. Let $n \geqslant 0$ be an integer. Let V be the vector space over $\mathbb{F}$ with basis the oriented n-simplices of Δ. Let

$$W = \operatorname{span}\{[v_0, \ldots, v_n] + [v_{\tau(0)}, \ldots, v_{\tau(n)}] : [v_0, \ldots, v_n] \in V, \tau \text{ is an odd permutation}\}.$$

That is, W is a subspace of V generated by all sums $\sigma + \sigma'$ where σ, σ' are different orientations of the same simplex. Then

$$C_n = V/W$$

is the **space of n-chains** of the complex Δ over $\mathbb{F}$.

For convenience we will denote elements of C_n by $[v_0, \ldots, v_n]$ (without the '$+W$'). While the definition might seem complicated, we're actually doing a very simple construction: we're simply establishing the equality $[v_0, \ldots, v_n] = -[v_{\tau(0)}, \ldots, v_{\tau(n)}]$ in our vector space for odd permutations τ and the formal way to do this is by dividing by a suitable vector space.

The elements of C_n are simply formal sums of oriented n-simplices of our simplicial complex with the equality $\sigma = -\sigma'$ if σ, σ' are different orientations of the same n-simplex. To get a basis for C_n we simply need to choose an orientation for every simplex.

Example 40. Let X and V be as in Example 38. Let $W = \operatorname{span}\{[a, b] + [b, a], [a, c] + [c, a], [b, c] + [c, b], [c, d] + [d, c], [d, a] + [a, d]\}$. Then by definition $C_1 = V/W$. An example basis for C_1 is $\{[a, b], [a, c], [b, c], [c, d], [d, a]\}$ (again, we omit the '$+W$'). Indeed, $B' = \{[a, b] + [b, a], [a, c] + [c, a], [b, c] + [c, b], [c, d] + [d, c], [d, a] + [a, d]\}$ is a basis for W and $B = B' \cup \{[a, b], [a, c], [b, c], [c, d], [d, a]\}$ is a basis for V. Observe the equalities $[a, b] = -[b, a]$ etc. in C_1.

The spaces of chains C_n are not interesting on their own. Additional structure is given by the boundary operator, which is a linear homomorphism between C_n and C_{n-1}.

Notation. If $[v_0, \ldots, v_n]$ is an oriented simplex in a simplicial complex, then by $[v_0, \ldots, \widehat{v_i}, \ldots, v_n]$ we denote the oriented simplex obtained from $[v_0, \ldots, v_n]$ by removing the vertex v_i, i.e. $[v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n]$.

Definition. Let C_n for $n \geqslant 0$ be the spaces of n-chains of some abstract simplicial complex. Let $\partial_n : C_n \to C_{n-1}$ be a linear homomorphism given on oriented simplices by

$$\partial_n [v_0, \ldots, v_n] = \sum_{i=0}^{n} (-1)^i [v_0, \ldots, \widehat{v_i}, \ldots, v_n]. \tag{2.1}$$

∂_n is the **boundary operator**, also called the boundary homomorphism.

Since for $n > 0$ there are many possible representations $[v_0, \ldots, v_n]$ of the same oriented simplex we should check if ∂_n doesn't depend on the choice of representative. Concretely, we need to show that if τ is an even permutation of $\{0, \ldots, n\}$ then $\partial_n[v_0, \ldots, v_n] = \partial_n[v_{\tau(0)}, \ldots, v_{\tau(n)}]$. Since every even permutation is a composition of an even number of transpositions, it suffices to show that if τ is a transposition then $\partial_n[v_0, \ldots, v_n] = -\partial_n[v_{\tau(0)}, \ldots, v_{\tau(n)}]$. Now every transposition $i \leftrightarrow j$ is a composition of three transpositions: $0 \leftrightarrow i$, $0 \leftrightarrow j$, $0 \leftrightarrow i$, so we only need to check if

$$\partial_n[v_0, \ldots, v_n] = -\partial_n[v_i, \ldots, v_{i-1}, v_0, v_{i+1}, \ldots]$$

where we swapped v_0 with v_i. But

$$\begin{aligned}
&\partial_n[v_i, \ldots, v_{i-1}, v_0, v_{i+1}, \ldots] \\
&= [\ldots, v_{i-1}, v_0, v_{i+1}, \ldots] + \sum_{k=1}^{i-1} (-1)^k [v_i, \ldots, \widehat{v_k}, \ldots, v_{i-1}, v_0, v_{i+1}, \ldots] \\
&+ (-1)^i [v_i, \ldots, v_{i-1}, v_{i+1}, \ldots] + \sum_{k=i+1}^{n} (-1)^k [v_i, \ldots, v_{i-1}, v_0, v_{i+1}, \ldots, \widehat{v_k}, \ldots] \\
&= (-1)^{i+1} [v_0, \ldots, \widehat{v_i}, \ldots] + \sum_{k=1}^{i-1} (-1)^{k+1} [v_0, \ldots, \widehat{v_k}, \ldots] \\
&+ (-1)^{2i+1} [v_1, \ldots] + \sum_{k=i+1}^{n} (-1)^{k+1} [v_0, \ldots, \widehat{v_k}, \ldots] \\
&= -\sum_{k=0}^{n} (-1)^k [\ldots, \widehat{v_k}, \ldots] = -\partial_n [v_0, \ldots, v_n].
\end{aligned}$$

This proves that ∂_n is well defined on the set of oriented n-simplices. To conclude that it gives a homomorphism on the entire space C_n we observe two facts:

- the oriented n-simplices generate C_n, that is, every element of C_n is a linear combination of the oriented n-simplices,
- the formulas for ∂_n on different generators are compatible with each other: if $\sigma = -\sigma'$, then $\partial_n \sigma = -\partial_n \sigma'$. This follows from the previous paragraph, since we've seen how $\partial_n[v_0, \ldots, v_n]$ changes when we perform a transposition of the vertices $v_0, \ldots, v_n$, so we also know how it changes when we perform an odd permutation (which is a composition of an odd number of transpositions).

We've seen how the boundary operator ∂_2 acts on 2-chains in Example 34. We usually omit the index indicating the dimension of chains and write simply ∂. Which operator is chosen is deduced from the context – it depends on the type of chain we act on.

What is ∂_0? For $n < 0$ we can define $C_n = 0$ (the trivial vector space) and the only choice for ∂_0 is $\partial_0 = 0$.

Lemma 6. *The boundary of a boundary is zero, i.e.* $\partial_{n-1} \circ \partial_n = 0$.

Proof.

$$\partial_{n-1}\partial_n[v_0,\dots,v_n] = \partial_{n-1}\sum_{i=0}^{n}(-1)^i[v_0,\dots,\hat{v_i},\dots,v_n]$$

$$= \sum_{i=0}^{n}\sum_{j=0}^{i-1}(-1)^{i+j}[v_0,\dots,\hat{v_j},\dots,\hat{v_i},\dots,v_n] + \sum_{i=0}^{n}\sum_{j=i+1}^{n}(-1)^{i+j-1}[v_0,\dots,\hat{v_i},\dots,\hat{v_j},\dots,v_n]$$

$$= \sum_{0\leqslant j<i\leqslant n}(-1)^{i+j}[v_0,\dots,\hat{v_j},\dots,\hat{v_i},\dots,v_n] - \sum_{0\leqslant i<j\leqslant n}(-1)^{i+j}[v_0,\dots,\hat{v_i},\dots,\hat{v_j},\dots,v_n] = 0$$

□

We have constructed a sequence of vector spaces C_n, $n \geqslant 0$, and homomorphisms between them, $\partial_n : C_n \to C_{n-1}$, satisfying the condition $\partial_{n-1}\partial_n = 0$. This is an example of a general concept in algebra that has a name of its own.

Definition. A **chain complex** $(C_\bullet, \partial_\bullet)$ is a sequence of vector spaces and homomorphisms between them:

$$\dots \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \dots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} 0$$

satisfying $\partial_{n-1}\partial_n = 0$ for all $n > 0$. The elements of C_n are called n-chains.

Chain complexes arise in different parts of mathematics. The one we focus on for now is the **simplicial chain complex** obtained by considering ordered simplices in a simplicial complex as we have done. We will see another example of a chain complex in chapter 3. The following definitions make sense for any chain complex, which is a purely algebraic object, even though the names suggest a geometric meaning.

Definition. Let $(C_\bullet, \partial_\bullet)$ be a chain complex and $n \geqslant 0$.

The kernel of ∂_n is the **space of n-cycles** and denoted Z_n. The elements of Z_n are called n-cycles.

The image of ∂_{n+1} is the **space of n-boundaries** and denoted B_n. The elements of B_n are called n-boundaries.

Observe that every 0-chain is a cycle since $\partial_0 = 0$. We've seen some examples of cycles and boundaries in the context of a simplicial chain complex at the beginning of the chapter. In terms of cycles and boundaries the condition $\partial_{n-1}\partial_n = 0$ says that every boundary is a cycle: $B_n \subseteq Z_n$.

Definition. $A, B \in Z_n$ are **homologous** if $A - B \in B_n$. A cycle is **bounding** if it is homologous to 0.

Being homologous is an equivalence relation and we can consider equivalence classes of homologous cycles. Actually we've seen this situation before – this is the quotient of two vector spaces.

Definition. The **n-th homology group** is the quotient Z_n/B_n, denoted H_n.

Observe that a cycle being bounding means exactly that it is zero in the homology group.

Remark. Our homology groups are much more than just groups – they are vector spaces, since we're considering *chain complexes of vector spaces*. However we will still use the classical term 'homology groups'. We will also see in chapter 3 a more general notion of a chain complex.

We now return to the concrete situation of a simplicial chain complex. If X is an (abstract) simplicial complex and $\mathbb{F}$ is a field, by $C_\bullet(X,\mathbb{F})$ we denote the simplicial chain complex over $\mathbb{F}$ associated to X. We will often omit the $\bullet$. $C_n(X,\mathbb{F})$ is the n-th chain space of this chain complex and analogously for Z_n, B_n and H_n in place of C_n. When the space X is known from the context or if we want to make a general statement irrespective of a particular simplicial complex we will omit X, and similarly for the field $\mathbb{F}$, so we will use symbols such as $C_n(X)$, $C_n(\mathbb{F})$, or simply C_n.

Let us calculate a few examples to get a feeling of what homology is.

Example 41. Take a simplicial complex consisting of 3 vertices v_0, v_1, v_2 and no higher dimensional simplices. It then has 3 connected components, each consisting of a single vertex. The spaces C_n are 0 for $n > 0$ and C_0 is a 3-dimensional vector space with example basis $[v_0], [v_1], [v_2]$. This is then a basis for Z_0 since $Z_0 = C_0$. Furthermore $B_0 = 0$ since $C_1 = 0$. Hence $H_0 = Z_0/\{0\} = Z_0$ is a 3-dimensional vector space.

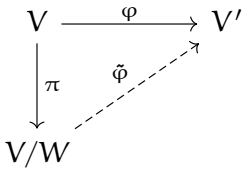
Example 42. Take a simplicial complex with vertices as in the previous example, but this time add an edge $\{v_0, v_1\}$. Our complex now has 2 connected components – one is the 1-simplex $\{v_0, v_1\}$ and one is the vertex $\{v_2\}$. Z_0 is the same as before, but now the space of 0-boundaries B_0 is a 1-dimensional vector space with example basis $[v_1] - [v_0]$. We can find a compatible basis for Z_0: $[v_0], [v_1] - [v_0], [v_2]$. Now $H_0 = Z_0/B_0$ is a 2-dimensional vector space with example basis $[v_0] + B_0, [v_2] + B_0$.

As the examples above suggest H_0 is related to the connected components of the simplicial complex. The dimension of H_0 is equal to the number of connected components and we can always find a basis for H_0 represented by vertices each lying in a different connected component.

Theorem 3. *Let X be a simplicial complex. There exists a linear isomorphism between $H_0(X,\mathbb{F})$ and a vector space over $\mathbb{F}$ with basis the connected components of X.*

Before we prove the theorem let us state a general fact about homomorphisms of vector spaces and quotients.

Lemma 7. *Let $\varphi : V \to V'$ be a linear map of vector spaces and $W \subseteq V$ be a subspace of V satisfying $W \subseteq \ker\varphi$, i.e. $\varphi(W) = \{0\}$. Let $\pi : V \to V/W$ be the projection map. There exists a unique homomorphism $\tilde{\varphi} : V/W \to V'$ satisfying $\tilde{\varphi} \circ \pi = \varphi$; in other words the diagram*



commutes.

Proof. Simply define $\tilde{\varphi}$ by $\tilde{\varphi}(v+W) = \varphi(v)$. We need to check that $\varphi(v)$ doesn't depend on the choice of the representative v of $v+W$. But if $v+W = v'+W$ then $v-v' \in W$ by definition, so $\varphi(v-v') = 0$ as $W \subseteq \ker\varphi$, hence $\varphi(v) = \varphi(v')$.

This is obviously a linear map which satisfies $\tilde{\varphi}\circ\pi = \varphi$. Furthermore any map ψ satisfying $\psi \circ \pi = \varphi$ is given by $\psi(v+W) = \psi(\pi(v)) = \varphi(v)$, so $\psi = \tilde{\varphi}$, which gives uniqueness. □

The map $\tilde{\varphi}$ from the above lemma is said to be induced from φ.

Corollary 1 (First isomorphism theorem). *Let $\varphi : V \to V'$ be a linear map of vector spaces. There exists a unique isomorphism $\tilde{\varphi}$ between $V/\ker\varphi$ and $\operatorname{im}\varphi$, where $\ker\varphi$ is the kernel of φ and $\operatorname{im}\varphi$ is the image of φ, satisfying $\tilde{\varphi}\circ\pi = \varphi$, where π is the projection map. In particular, if φ is an epimorphism, we get an isomorphism $V/\ker\varphi \simeq V'$.*

Proof. Take $W = \ker\varphi$ in the above lemma. Since $\tilde{\varphi} \circ \pi = \varphi$ and π is an epimorphism, $\operatorname{im}\tilde{\varphi} = \operatorname{im}\varphi$. In particular if φ is an epimorphism then so is $\tilde{\varphi}$. $\tilde{\varphi}$ is also a monomorphism. Indeed, if $\tilde{\varphi}(v+\ker\varphi) = \tilde{\varphi}(v'+\ker\varphi)$, then by definition $\varphi(v) = \varphi(v')$, i.e. $\varphi(v-v') = 0$, so $v-v' \in \ker\varphi$, but that means $v+\ker\varphi = v'+\ker\varphi$. □

We can finally prove theorem 3. If X is a simplicial complex, by $\pi_0(X)$ we denote the set of connected components of X. For v a vertex in a simplicial complex X, by $C(v) \in \pi_0(X)$ we denote the connected component of v.

Proof of theorem 3. Let V be a vector space over the field $\mathbb{F}$ with basis $\pi_0(X)$. Let $\varphi : Z_0 \to V$ be a linear homomorphism given on the basis of Z_0 by $\varphi([v]) = C(v)$. This is obviously an epimorphism, since every connected component contains at least one vertex. We will prove that its kernel is B_0, from which we obtain an induced isomorphism $H_0 = Z_0/B_0 \simeq V$ by corollary 1.

Suppose that A is a 0-boundary, $A = \partial\sum_\alpha k_\alpha[v_\alpha, w_\alpha] = \sum_\alpha k_\alpha([w_\alpha] - [v_\alpha])$ for some coefficients $k_\alpha \in \mathbb{F}$ and 1-simplices $\{v_\alpha, w_\alpha\}$ in X. Then for each α the vertices w_α, v_α are connected with an edge, so they lie in the same connected component. Thus

$$\varphi(A) = \sum_\alpha k_\alpha(C(w_\alpha) - C(v_\alpha)) = 0$$

which proves that every 0-boundary is in the kernel of φ.

On the other hand, let A be an element of the kernel of φ, $A = \sum_\alpha k_\alpha[v_\alpha]$ for some $k_\alpha \in \mathbb{F}$ and v_α vertices in X, $0 = \varphi(A) = \sum_\alpha k_\alpha C(v_\alpha)$. Group the last sum by the components of X:

$$\sum_{C\in\pi_0(X)} \Big(\sum_{C(v_\alpha)=C} k_\alpha\Big)C = 0.$$

Since the components of X form a basis for V we get that for every $C \in \pi_0(X)$

$$\sum_{C(v_\alpha)=C} k_\alpha = 0. \qquad (*)$$

Let us restrict our attention to a particular component C for which there exists α such that $C(v_\alpha) = C$ and $k_\alpha \neq 0$. We will prove that the sum

$$\sum_{C(v_\alpha)=C} k_\alpha[v_\alpha]$$

is the boundary of some 1-chain consisting of 1-simplices contained in the component C. Let v be one of the vertices v_α such that $k_\alpha \neq 0$. Let k be its coefficient. From equation (*) we obtain

$$k = -\sum_{C(v_\alpha)=C, v_\alpha \neq v} k_\alpha$$

hence

$$\sum_{C(v_\alpha)=C} k_\alpha[v_\alpha] = k[v] + \sum_{C(v_\alpha)=C, v_\alpha \neq v} k_\alpha[v_\alpha] = \sum_{C(v_\alpha)=C, v_\alpha \neq v} k_\alpha([v_\alpha] - [v])$$

but each summand in the last expression is a boundary of some 1-chain. Indeed, for each α such that $C(v_\alpha) = C$, since v_α and v lie in the same component C, there is a path of edges in C

$$\{w_0, w_1\}, \{w_1, w_2\}, \ldots, \{w_{n-1}, w_n\}$$

where $w_0 = v$ and $w_n = v_\alpha$. Then if we take P_α to be the 1-chain $[w_0, w_1] + \cdots + [w_{n-1}, w_n]$, we get $\partial P_\alpha = [v_\alpha] - [v]$, thus

$$\partial \sum_{C(v_\alpha)=C, v_\alpha \neq v} k_\alpha P_\alpha = \sum_{C(v_\alpha)=C} k_\alpha[v_\alpha].$$

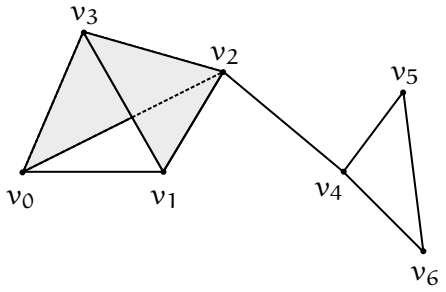
By doing that for each component C, we get that

$$A = \sum_\alpha k_\alpha[v_\alpha] = \sum_{C \in \pi_0(X)} \sum_{C(v_\alpha)=C} k_\alpha[v_\alpha]$$

is a boundary. □

The following examples focus on H_1 and H_2.

Example 43. Let X be the complex pictured below.



Its 2-simplices are $\{v_1, v_2, v_3\}, \{v_0, v_2, v_3\}$. To calculate H_1 we can use the algorithm described in section 2.2 or do some simple calculations by hand and find a basis for Z_1 together with a compatible basis for B_1. In any case, an example basis for Z_1 is:

$$[v_0, v_1] + [v_1, v_3] + [v_3, v_0], [v_0, v_2] + [v_2, v_3] + [v_3, v_0],$$
$$[v_1, v_2] + [v_2, v_3] + [v_3, v_1], [v_4, v_5] + [v_5, v_6] + [v_6, v_4].$$

A compatible basis for B_1 is

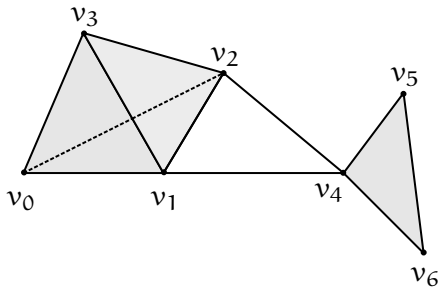
$$[v_0, v_2] + [v_2, v_3] + [v_3, v_0] = \partial[v_0, v_2, v_3], [v_1, v_2] + [v_2, v_3] + [v_3, v_1] = \partial[v_1, v_2, v_3],$$

therefore the obtained basis for H_1 would be

$$[v_0, v_1] + [v_1, v_3] + [v_3, v_1], [v_4, v_5] + [v_5, v_6] + [v_6, v_4]$$

and we see in particular that H_1 is a 2-dimensional vector space. There are no cycles of higher dimension, so $H_n = 0$ for $n \geqslant 2$.

Example 44. Let Y be the complex drawn below.



Its 2-simplices are all possible 2-simplices obtained from the vertices v_0, v_1, v_2, v_3 and the simplex $\{v_4, v_5, v_6\}$. We will consider two cases, depending whether we take the 3-simplex $\{v_0, v_1, v_2, v_3\}$ into account.

X from the previous example is a subcomplex of Y. An example basis for $Z_1(Y)$ contains all the chains listed as the basis for $Z_1(X)$ in the previous example, and additionally

$$[v_1, v_2] + [v_2, v_4] + [v_4, v_1].$$

However we also get additional elements in a basis for $B_1(Y)$ compared to the basis for $B_1(X)$:

$$\partial[v_0, v_1, v_3], \partial[v_4, v_5, v_6],$$

so the obtained basis for $H_1(Y)$ would be

$$[v_1, v_2] + [v_2, v_4] + [v_4, v_1].$$

This time we also have a 2-cycle which forms a basis for Z_2:

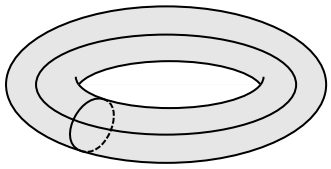
$$[v_1, v_2, v_3] + [v_0, v_3, v_2] + [v_0, v_1, v_3] + [v_0, v_2, v_1].$$

If Y contains the 3-simplex $\{v_0, v_1, v_2, v_3\}$, the above 2-chain is a boundary and $H_2 = 0$. Otherwise it forms a basis for H_2 which is then 1-dimensional. For $n \geqslant 3$, $H_n = 0$.

Example 45. Let X be the torus triangulated as in Example 24. Using the names of vertices given there we can calculate, e.g. using the algorithm from section 2.2, that an example basis for H_1 is

$$[v_0, v_3] + [v_3, v_4] + [v_4, v_0], [v_0, v_1] + [v_1, v_2] + [v_2, v_0].$$

We can draw these two cycles on the three-dimensional picture of the torus:



It also turns out that if we add all the 2-simplices in the triangulation with suitable orientations, we get a 2-cycle, which forms a basis for H_2. Thus H_1 is 2-dimensional and H_2 is 1-dimensional.

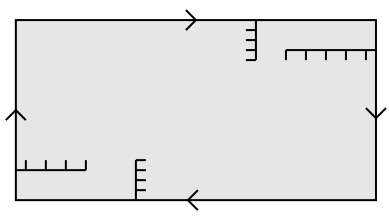
We see that in some sense H_1 and H_2 'detect' holes of different type: the dimension of H_1 might increase when we add simplices of dimension 1 (which might add a circular hole, corresponding to a new non-bounding cycle appearing) and might decrease when adding simplices of dimension 2 (which might close a circular hole, corresponding to a non-bounding cycle becoming bounding). Similarly the dimension of H_2 might increase when adding simplices of dimension 2 (adding a void – a new non-bounding 2-cycle appears) and decrease when adding simplices of dimension 3 (closing a void – a non-bounding 2-cycle becomes bounding). Higher-dimensional simplices are not visualized so easily, but the general idea is that H_n detects 'n-dimensional holes' for $n > 0$. Of course we didn't really say what a 'hole' is – homology is probably the closest we can get to formally talk about this concept. In particular, if we find k linearly independent vectors in H_n, we can say that we've found k different n-dimensional holes, and if we find the dimension of H_n as a vector space, that would be the number of n-dimensional holes.

That would be the end of the story... if we only considered finite simplicial complexes which embed in $\mathbb{R}^3$, such as all the examples considered until now. However the world of low-dimensional objects is not where the interesting things happen. The power of (persistent) homology and more generally topological data analysis lies in the ability to infer robust information about high-dimensional objects, and one of the merits of (algebraic) topology is the ability to reveal interesting phenomena happening in high dimensions that would be hard to imagine without the mathematical machinery at our disposal.

The problem we didn't think about is how do homology groups of a simplicial complex depend on the choice of the field $\mathbb{F}$. First of all, theorem 3 has been proven for every field, so H_0 is taken care of. It is also true that if we restrict ourselves to finite simplicial complexes which embed in $\mathbb{R}^3$, the dimension of $H_n(\mathbb{F})$ for $n = 1, 2$ doesn't depend on $\mathbb{F}$ (proving that claim is far beyond the scope of this book) and $H_n = 0$ for $n \geqslant 3$. In that case we could use the simplest possible field $\mathbb{F} = \mathbb{Z}_2$ and obtain all the necessary information. Then the calculations become much simpler as $\mathbb{Z}_2$ constains only two elements, 0 and 1. We can in particular forget about the signs in the boundary formula 2.1 since in $\mathbb{Z}_2$, $-1 = 1$. On the other hand the situation complicates when we consider higher-dimensional objects such as the one in the next example.

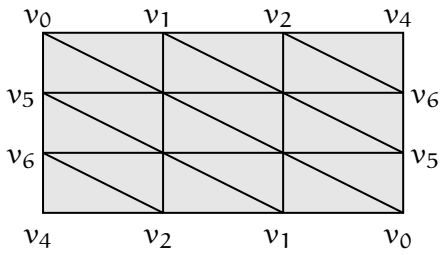
Example 46. The topological space we shall consider is the real projective plane, denoted $\mathbb{R}P^2$. It cannot be embedded in $\mathbb{R}^3$ (the smallest possible dimension required is 4), but we can easily describe it as a simplicial complex.

Similarly to the torus in Example 24, $\mathbb{R}P^2$ can be thought of as a rectangle in which opposite edges have been identified, but in this case we identify them in opposite directions, as in the following picture:



The arrows indicate the directions of gluing. The left edge gets identified with the right edge so that the top left corner becomes the bottom right corner and the bottom left corner becomes the top right corner. Similarly for the top and bottom edges. The comb-shaped objects have been drawn for reference: we see that when passing an edge, the teeth of a comb change directions.

To define $\mathbb{R}P^2$ formally and say what 'identifying edges' actually means we would have to discuss quotient topological spaces which we have decided not to do in this book. However we can easily define $\mathbb{R}P^2$ by simply giving it a simplicial complex structure, as in the picture below.



The vertices on the edges have been named to point out which ones are identified. This gives a correct 2-dimensional abstract simplicial complex: each subset of vertices defines either exactly one simplex or none.

We will compute $H_1(\mathbb{R}P^2, \mathbb{F})$ for $\mathbb{F}$ the fields $\mathbb{Q}$ and $\mathbb{Z}_p$, p prime. To do that, we will consider chains with integer coefficients, i.e. formal sums of the form $\sum n_\alpha \sigma_\alpha$ where σ_α is an oriented simplex and n_α is an integer. Every such n-chain can be thought of as an element of $C_n(\mathbb{F})$ for any $\mathbb{F}$. Indeed, since every field has a 1, integers also make sense: for $n \in \mathbb{Z}$ we have $n = 1 + \cdots + 1$ (added n times) if n is positive and $n = -(1 + \cdots + 1)$ if n is negative, so n is naturally an element of the field. For example if $\mathbb{F} = \mathbb{Z}_2$ we have

$$2\sigma_1 + 5\sigma_2 + 4\sigma_3 + 3\sigma_4 = \sigma_2 + \sigma_4$$

since $2 = 1 + 1 = 0$, $5 = 2 + 2 + 1 = 1$, $3 = 2 + 1 = 1$ in $\mathbb{Z}_2$. We will see that by studying only chains with integer coefficients we can say a lot about what happens in a general field.

Let

$$A = [v_4, v_6] + [v_6, v_5] + [v_5, v_0] + [v_0, v_1] + [v_1, v_2] + [v_2, v_4].$$

First we make the following observations about the chain A:

1. A is a cycle for every $\mathbb{F}$: simply apply the boundary formula.

2. For every 1-cycle B with integer coefficients there exists a 2-cycle C with integer coefficients and $n \in \mathbb{Z}$ such that $nA - B = \partial C$. This not only says that B is homologous to an integer multiple of A, but also that it is 'homologous over integers', i.e. at least one of the cycles C satisfying $nA - B = \partial C$ has integer coefficients. We will later discuss how to prove this fact.

3. There exists a 2-cycle B with integer coefficients such that $\partial B = 2A$. To find B add all the 2-simplices of with suitable orientations.

4. There is no 2-cycle B with integer coefficients such that $\partial B = A$. Again we postpone the method of proving this fact.

From the above properties we will deduce that when $\mathbb{F}$ is one of the fields $\mathbb{Q}$ or $\mathbb{Z}_p$, then $\{A\}$ generates Z_1 and A is a boundary if and only if $\mathbb{F} = \mathbb{Z}_2$. Therefore $\mathbb{H}_1(\mathbb{Z}_2) = \mathbb{Z}_2$ and $\mathbb{H}_1(\mathbb{F}) = 0$ for $\mathbb{F} = \mathbb{Q}$ or $\mathbb{Z}_p$, $p \neq 2$.

For any of the considered fields $A \in Z_1$ by observation 1. Furthermore A is a generator of H_1, i.e. every cycle is homologous to a multiple of A. When $\mathbb{F} = \mathbb{Z}_p$ this is immediate from observation 2 since in these fields all coefficients are integers: for any cycle B simply take C as in the observation and we get that $\partial C = (n \mod p)A - B$. For $\mathbb{Q}$ write B as a linear combination of oriented simplices with rational coefficients and find a common denominator of all the coefficients so that $B = \frac{1}{k}B'$ where B' has integer coefficients and $k \in \mathbb{Z}$. By observation 2 we have $n \in \mathbb{Z}$ and $C \in C_2$ with integer coefficients such that $nA - B' = \partial C$, hence $\frac{n}{k}A - B = \partial\frac{1}{k}C$.

Now if $\mathbb{F} \neq Z_2$, A is a boundary by observation 3 since if $2A = \partial B$ then $A = \partial\frac{1}{2}B$.

In $\mathbb{Z}_2$ we cannot divide by 2 (which is equal to 0) and in fact this together with other observations implies that A is not a boundary. Indeed, suppose otherwise and let B be such that $\partial B = A$. B has integer coefficients (all equal to 1) and if we calculate its boundary over the integers (without taking remainders of division by 2) we find that $\partial B = A + 2C$ for some chain C. C is a cycle over the integers: $2\partial C = \partial 2C = \partial(\partial B - A) = 0$, hence $\partial C = 0$. By observation 2, $C = nA + \partial D$ for some $n \in \mathbb{Z}$, D a 2-cycle with integer coefficients. Let B' be a 2-cycle with integer coefficients such that $\partial B' = 2A$ from observation 3. Then

$$A = \partial B - 2(nA + \partial D) = \partial B - \partial D - n2A = \partial(B - D - nB')$$

which contradicts observation 4.

In the above example, the cycle A detects a special type of 'hole'. If we allow only integer coefficients then A is non-bounding: this is observation 4 above. $2A$ is always bounding by observation 3. We call this phenomenon *torsion*.

If we think of holes as obstacles that we can walk around but not 'into', then we've just found a path that walked once 'goes around an obstacle', but when we walk it twice in the same direction we actually see no obstacle – we've simply walked around the interior of the square seen in the previous picture. In light of this we could either give up on the idea of a hole or argue that there are different types of holes, including 'torsional' ones which are only harder to imagine for humans living in three dimensions. With the exception of mathematicians for whom torsion is a completely natural thing.

In the above calculation we've used integer coefficients. This is actually the usual way to define homology: instead of defining the space of n-chains as a vector space over some field with basis the oriented n-simplices of our simplicial complex (with change of orientation of a simplex equivalent to a change of sign), we define $C_n(\mathbb{Z})$ as the *free abelian group* with basis the oriented n-simplices (with the same rule concerning orientations and signs). Elements of this abelian group are exactly formal sums of oriented n-simplices with integer coefficients. We then define the boundary homomorphism and the spaces of cycles $Z_n(\mathbb{Z})$ and boundaries $B_n(\mathbb{Z})$ as usual. We can also take quotients of groups as we do with vector spaces and we define $H_n(\mathbb{Z}) = Z_n(\mathbb{Z})/B_n(\mathbb{Z})$. However not every abelian group is *free*, i.e. it doesn't need to have a basis, a set of elements such that every element of the group can be uniquely written as a linear combination (with integer coefficients) of the basis elements. For Example $\mathbb{Z}_n$ are such groups since any element is always linearly dependent: multiplied by n it gives 0.

While Z_n and B_n are free, H_n doesn't have to be, and $\mathbb{R}P^2$ is such a space – we actually have $H_1(\mathbb{R}P^2, \mathbb{Z}) = \mathbb{Z}_2$.

We will see a generalization of both abelian groups and vector spaces in chapter 3 called modules. Then, in chapter 4, we will describe a general method for calculating homology over certain types of modules, abelian groups included, which will give us a way to prove observations 2 and 4 in the above example. The general algorithm is a bit more complicated than the one we will soon see in section 2.2. In the following chapters we also explain why we consider homology groups with coefficients in fields and not just integers.

Another remark that should be given is that the method presented in the above example – using integer coefficients to calculate homology in fields – is actually a very special case of a general theorem, the *universal coefficient theorem*, which rougly says that homology groups with coefficients in a field, or more generally in a group, can be calculated knowing only the standard integer homology groups, without even knowing the entire chain complex. To some extent it works in both directions: using non-integer coefficients we can deduce facts about integer homology groups. For example if we know that $H_1(\mathbb{Z}_2) = \mathbb{Z}_2$ as above we can deduce that $H_1(\mathbb{Z})$ contains a *torsional element of order* 2, an element g such that $2g = 0$.

In particular the universial coefficient theorem implies that the *rank* of $H_n(\mathbb{Z})$, i.e. the maximal number of linearly independent elements (where linear independence is defined analogously to vector spaces), is equal to the dimension of $H_n(\mathbb{Q})$ as a vector space. This can be thought of as the number of 'usual' holes in a simplicial complex.

Definition. For a simplicial complex X, $\beta_n = \dim H_n(X, \mathbb{Q})$ is the **n-th Betti number**.

We've defined so called **simplicial homology**. Homology is a much more general concept in algebraic topology and there are many *homology theories*. In particular there's a generalization of simplicial homology to arbitrary topological spaces called **singular homology**, see e.g. [9, Chapter 2]. Singular homology doesn't require any additional structure on the topological space such as a simplicial complex structure. It turns out that singular homology groups of simplicial complexes are isomorphic to their simplicial homology groups. Furthermore we have the following theorem:

Theorem 4. *If two topological spaces are homotopy equivalent, their singular homology groups are isomorphic.*

A proof can also be found in [9, Chapter 2]. Thus homology is an invariant of a topological space up to homotopy equivalence. This formalizes the intuitive idea that continuous deformation of shape doesn't change its components and holes.

We know from chapter 1 that for a point cloud X and $\epsilon > 0$, the Cech complex $\check{C}_\epsilon$ for X is homotopy equivalent to the space X_ϵ obtained by summing a family of balls around the points of X. From the above theorem, $\check{C}_\epsilon$ and X_ϵ have the same homology, so by calculating the simplicial homology of $\check{C}_\epsilon$ we also know the singular homology of X_ϵ. An interesting collorary is that if X lies in $\mathbb{R}^n$, the k-th homology of $\check{C}_\epsilon$ is zero for $k \geqslant n$. This is because singular homology of an open set in $\mathbb{R}^n$, such as X_ϵ, is zero in dimensions n and higher, which is another nontrivial result of algebraic topology[9, Proposition 3.29].

In contrast, for the VR complex we don't have any result regarding homotopy equivalence to some simple space in $\mathbb{R}^n$. It turns out that it is possible to obtain nontrivial higher homology for VR_ϵ.

Example 47. Let X be the point cloud from Example 25, the 6th roots of unity. X is a subset of $\mathbb{R}^2$ and according to the above considerations any open subset of $\mathbb{R}^2$ has trivial singular homology groups in dimension 2. However we will find out that the simplicial homology group H_2 of VR_ϵ for $\epsilon = 2$ is nonzero.

Name the vertices $v_0, \ldots, v_5$ with the counter-clockwise order of appearance on the circle, starting with $v_0 = (1, 0)$. VR_2 has no 3-dimensional simplices and has the following 2-simplices:

$$\{v_0, v_1, v_2\}, \{v_1, v_2, v_3\}, \{v_2, v_3, v_4\}, \{v_3, v_4, v_5\}, \{v_4, v_5, v_0\}, \{v_5, v_0, v_1\},$$

$$\{v_0, v_2, v_4\}, \{v_1, v_3, v_5\}.$$

Observe that the 2-simplices listed in the first line are exactly the two simplices of C_1. VR_2 differs from C_1 by the simplices listed in the second line. The following 2-chain:

$$\begin{aligned}&[v_0, v_2, v_4] + [v_0, v_1, v_2] + [v_0, v_4, v_5] + [v_2, v_3, v_4]\\ &- [v_1, v_2, v_3] - [v_0, v_1, v_5] - [v_3, v_4, v_5] - [v_1, v_3, v_5]\end{aligned}$$

is a non-bounding 2-cycle – calculate its boundary to find that it's zero. It cannot be bounding as there are no 3-simplices. Indeed, the picture in Example 26 already suggested that this complex has a void inside.

The above example proves that VR_ϵ is not homotopy equivalent to $C_{2\epsilon}$ in general. We have witnessed the power of homology – an algebraic tool allows us to prove facts about topology. Perhaps it can help us study our data sets?

We have also seen that the Vietoris-Rips complex might exhibit 'weird' behavior, like having 2-dimensional holes for points on the plane. Because of the inclusions (1.1) we expect this to happen rarely, i.e. for small ranges of ϵ. In return for efficiency, the information we obtain by studying the Vietoris-Rips complex is an approximation of the information obtained by studying the Cech complex (or X_ϵ) directly.

2.2. Computing homology

Given a simplicial complex, how do we compute its homology groups in practice? The first question we should ask about H_n is its dimension, which tells us if there are any non-trivial holes in our complex. Then we might want to dig deeper and ask for non-bounding cycles. Finding multiple cycles that are linearly independent in H_n means finding multiple holes. Finally, if we find a basis of H_n – a maximal linearly independent set of cycles in H_n – we know both the dimension and all possible non-bounding cycles as they are linear combinations of the elements of the basis.

So finding the interesting information amounts to finding a basis for H_n. Recall that to find a basis of a quotient V/W we can find compatible bases for the space V and the subspace W. So in our case we want to find a basis $b_1, \ldots, b_k$ of B_n and a set of vectors $b_{k+1}, \ldots, b_{k+l} \in Z_n$ such that the set $b_1, \ldots, b_{k+l}$ is a basis of Z_n. Then

$$b_{k+1} + B_n, \ldots, b_{k+l} + B_n$$

will be a basis for H_n.

How do we find such a set of vectors? Let $n \geqslant 1$ and suppose we have found a basis $b_1, \ldots, b_k$ of Z_n. This is the kernel of ∂_n, which is a subspace of C_n, so in particular the vectors $b_1, \ldots, b_k$ form a linearly independent subset of the vector space C_n and can be extended to a basis of C_n by some vectors $b_{k+1}, \ldots, b_{k+l}$. An interesting observation follows: the vectors $\partial_n(b_{k+1}), \ldots, \partial_n(b_{k+l})$ form a basis of $B_{n-1} = \operatorname{im} \partial_n$. Indeed: first of all, they span the space $\operatorname{im} \partial_n$, since all the vectors $\partial_n(b_1), \ldots, \partial_n(b_{k+l})$ span $\operatorname{im} \partial_n$ being the images of a basis of C_n, but the first k vectors $\partial_n(b_1), \ldots, \partial(b_k)$ are all 0 being the images of vectors from the kernel of ∂_n. Secondly, the considered vectors are linearly independent: suppose $\alpha_1 \partial_n(b_{k+1}) + \cdots + \alpha_l \partial_n(b_{k+l}) = 0$ for some $\alpha_1, \ldots, \alpha_l \in \mathbb{F}$. By linearity, $\partial_n(\alpha_1 b_{k+1} + \cdots + \alpha_l b_{k+l}) = 0$, or in other words, $\alpha_1 b_{k+1} + \cdots + \alpha_l b_{k+l}$ is an element of Z_n. But that means it is a linear combination of $b_1, \ldots, b_k$. By linear independence of the vectors $b_1, \ldots, b_{k+l}$ we get $\alpha_1 = \cdots = \alpha_l = 0$.

Let U be the subspace of C_n spanned by $b_{k+1}, \ldots, b_{k+l}$. We see that in some sense C_n is composed of two parts: Z_n, the kernel of ∂_n, and U, which we have just shown to be isomorphic to $\operatorname{im} \partial_n$, $\partial_n|_U$ being the isomorphism. More specifically, we have that $Z_n \cap U = \{0\}$ by independence of the vectors b_i, and $Z_n + U = C_n$ (the expression on the left denotes a subspace of C_n formed by considering all linear combinations of vectors from Z_n and U) by the fact that b_i span C_n. We write $Z_n \oplus U = C_n$ and say that C_n is the **direct sum** of Z_n and U. The result should not be surprising in light of the first isomorphism theorem. In fact the argument above could be made into another proof of corollary 1 with little additional commentary. We have also obtained the classic *rank-nullity theorem*: $\dim \operatorname{im} \partial_n + \dim \ker \partial_n = l + k = \dim C_n$.

For convenience let us reorder the vectors b_i and suppose that $b_1, \ldots, b_l$ form a basis of U while $b_{l+1}, \ldots, b_{l+k}$ form a basis of Z_n. Let $b'_i = \partial_n(b_i)$ for $i = 1, \ldots, l$. It is a basis of B_{n-1} and can be extended to a basis of C_{n-1} by some vectors $b'_{l+1}, \ldots, b'_{l+m}$. Now the matrix of ∂_n in the bases b_i, b'_i has the following form:

$$\begin{bmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{bmatrix}.$$

There are l nonzero columns, the i-th column having a 1 in the i-th row and 0 everywhere else, for $i = 1, \ldots, l$. Indeed, the coefficients of $\partial_n(b_i)$ in the basis $b'_1, \ldots, b'_{l+m}$ are 0 except the coefficient at b_i, which is 1, which means exactly that $\partial_n(b_i) = b'_i$. The other vectors, $b_{l+1}, \ldots, b_{l+k}$, are from the kernel of ∂_n, which is why the other columns are zero. Warning: the above picture might suggest that the matrix is square, which obviously doesn't have to be the case, and usually isn't: $k \neq m$ in general. But the area with 1s on the diagonal is square.

Definition. A matrix with coefficients in a field $\mathbb{F}$ in the form

$$\begin{bmatrix} \alpha_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 & \dots & 0 \\ 0 & 0 & \dots & \alpha_k & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{bmatrix},$$

i.e. with nonzero elements $\alpha_i \in \mathbb{F}$ on the diagonal up to some point and zero everywhere else, is in the **Smith normal form**.

So we have obtained a matrix in the Smith normal form with the coefficients α_i all equal to 1. This isn't important for our discussion: multiplying the vectors of a basis of some space by nonzero scalars simply gives another basis of the same space.

We can reason in the other direction: suppose we are given some bases b_i, b'_i of C_n, C_{n-1} respectively such that the matrix of ∂_n in those bases is in Smith normal form. By multiplying the basis vectors by appropriate scalars we can assume that the nonzero coefficients are equal to 1. Then we can deduce that the vectors $b'_1, \dots, b'_l$, where l is the number of nonzero rows (and columns), form a basis of B_{n-1}, since they span the image of ∂_n, and the vectors $b_{l+1}, \dots, b_{l+k}$, where k is the number of zero columns, form a basis of Z_n, since they span the kernel of ∂_n.

The above discussion suggests the following strategy: we can start with some bases $\mathfrak{B}$, $\mathfrak{B}'$ of C_n, C_{n-1} respectively and a representation of ∂_n in those bases as a matrix. Then, using elementary operations on rows and columns, reduce the matrix to the Smith normal form with a standard algorithm (Gaussian elimination). Each elementary operation on the columns corresponds to a change of $\mathfrak{B}$ and on the rows – to a change of $\mathfrak{B}'$ (see appendix A). Having reduced the matrix, the elements of $\mathfrak{B}'$ corresponding to nonzero rows form a basis of B_{n-1} and the elements of $\mathfrak{B}$ corresponding to zero columns form a basis of Z_n.

How do we find the bases to start with and a representation of ∂_n as a matrix in those bases? Easy: choose an orientation of every simplex in our simplicial complex. Among the chosen oriented simplices, the ones of dimension n form a basis for C_n, and of dimension $n-1$ – a basis for C_{n-1}. Then, for every chosen oriented n-simplex σ, use formula (2.1) to find coefficients of $\partial_n(\sigma)$ in the chosen bases. We will see an example calculation later.

Choosing an orientation is also an easy task, because usually the vertices come stored in some order. This order gives an ordering of every simplex, so in particular an orientation.

Thus for every $n \geqslant 0$ we can find a basis of B_n and Z_{n+1}. Since $Z_0 = C_0$, the vertices of the simplicial complex form an example basis of Z_0. But we wanted to find *compatible* bases of B_n and Z_n and the above procedure might give us completely different sets of vectors. We would like our basis for B_n to be a subset of the basis for Z_n.

The problem exists right at the beginning of the procedure: we start with a representation of ∂_n as a matrix in a basis of C_n and *some* basis of C_{n-1}, which has nothing to do with any basis of Z_{n-1} that we might have already found, and then reduce the matrix. In effect the obtained basis of B_{n-1} has no relationship to the basis of Z_{n-1}. The fix is easy: first find a basis of Z_{n-1} – say $\mathfrak{B}'$, then extend it to a basis of C_{n-1} – let's name it $\widehat{\mathfrak{B}}'$ – then represent ∂_n in a basis of C_n and basis $\widehat{\mathfrak{B}}'$. Now, after reducing, we know how to write the obtained basis of B_{n-1} in terms of $\mathfrak{B}'$.

Actually, we don't even have to extend the basis $\mathfrak{B}'$ of Z_{n-1} to a basis of the whole space C_{n-1}. This is precisely because $B_{n-1} \subseteq Z_{n-1}$, i.e. the image of ∂_n is contained in the space Z_{n-1}, so we can think of ∂_n as a linear map between the spaces C_n and Z_{n-1}. In the matrix seen previously, the rows corresponding to elements of $\hat{\mathfrak{B}}' \setminus \mathfrak{B}'$ would be zero anyway.

So assuming we have a basis for Z_{n-1}, say $\mathfrak{B}'$, and a representation of ∂_n as a matrix in some basis of C_n and $\mathfrak{B}'$, reduce the matrix to obtain: a new basis for Z_{n-1} (during the reduction we might have performed row operations), a basis for B_{n-1} which is a subset of the basis for Z_{n-1} (vectors corresponding to the nonzero rows), and a basis for Z_n (vectors corresponding to the zero columns).

One last problem remains: how to obtain a representation of ∂_n as a matrix in a basis of C_n and our basis of Z_{n-1}? Our input data consists of some bases of C_n for each n, say $\mathfrak{B}_n$, and a representation of ∂_n as a matrix in the bases $\mathfrak{B}_n$ and $\mathfrak{B}_{n-1}$ for $n \geqslant 1$. Assuming we have solved the problem for $n-1$, we have a representation of ∂_{n-1} as a matrix in basis $\mathfrak{B}_{n-1}$ of C_{n-1} and some basis $\mathfrak{B}'_{n-2}$ of Z_{n-2}. We start reducing the matrix of ∂_{n-1}, which might perform column operations, and those correspond to operations on the basis $\mathfrak{B}_{n-1}$. While reducing the matrix of ∂_{n-1}, whenever we perform a column operation – thus an operation on the basis $\mathfrak{B}_{n-1}$ – simply perform simultaneously the corresponding operation on the rows of the matrix of ∂_n. Finally, when the reduction is done, we have obtained a new basis for C_{n-1}, say $\widetilde{\mathfrak{B}_{n-1}}$, and we look at the zero columns of the reduced matrix of ∂_{n-1} to read our new basis $\mathfrak{B}'_{n-1}$ for Z_{n-1}. This is a subset of $\widetilde{\mathfrak{B}_{n-1}}$ and the rows of the new matrix of ∂_n corresponding to this subset give us the representation of ∂_n in the bases $\mathfrak{B}_n$ and $\mathfrak{B}'_{n-1}$.

The problem is already solved for ∂_1, since $\mathfrak{B}_0$ is already a basis of $Z_0 = C_0$. By induction we know how to calculate all the required bases for every n.

The above considerations lead us to the algorithm in figure 3, which works for any chain complex of finite-dimensional vector spaces $(C_\bullet, \partial_\bullet)$ over some field $\mathbb{F}$ and calculates compatible bases of B_n and Z_n up to some integer N. In the case of a simplicial chain complex, the chain spaces are zero in dimensions high enough, so we can calculate all the homology groups. The input of the algorithm consists of finite sequences $\mathfrak{B}_n$, assumed to be (ordered) bases of the chain spaces C_n, and matrices M_{n+1} over the field $\mathbb{F}$ of dimensions $|\mathfrak{B}_n| \times |\mathfrak{B}_{n+1}|$, assumed to be the representations of ∂_{n+1} in the bases $\mathfrak{B}_{n+1}$ and $\mathfrak{B}_n$, for $n \geqslant 0$. In particular the matrices have to satisfy the boundary homomorphism property: $M_n M_{n+1} = 0$. The output consists of sets $\mathfrak{B}''_n \subseteq \mathfrak{B}'_n$, bases of B_n and Z_n, represented as linear combinations of elements of $\mathfrak{B}_n$. For a matrix M, the expression $M(i,j)$ denotes the element of M in row i and column j, $M(i,\bullet)$ denotes the ith row of M and $M(\bullet,j)$ the jth column. For a sequence of elements $\mathfrak{B}$, $\mathfrak{B}(i)$ denotes the ith element of the sequence.

Starting with $n = 1$ and going up, we reduce the matrices M_n to the Smith normal form. After first $n-1$ iterations of the outer loop the matrix M_n is represented in bases $\mathfrak{B}_n, \mathfrak{B}'_{n-1}$ of C_n, Z_{n-1} respectively. While performing column operations on M_n, we perform the corresponding operations on $\mathfrak{B}_n$ and rows of M_{n+1}. While performing row operations on M_n, we perform the corresponding operations on $\mathfrak{B}'_{n-1}$.

Algorithm 3 Finding compatible bases for Z_n and B_n

Require:

N: non-negative integer,
$\mathfrak{B}_n$: finite sequence for $0 \leqslant n \leqslant N+1$,
M_n: matrix of dimensions $|\mathfrak{B}_{n-1}| \times |\mathfrak{B}_n|$ for $1 \leqslant n \leqslant N+1$ satisfying $M_n M_{n+1} = 0$.

$\mathfrak{B}'_0 \leftarrow \mathfrak{B}_0$
for $n \leftarrow 1, \ldots, N$ **do**
    $numPivots \leftarrow$ ColumnReduce$(M_n, \mathfrak{B}_n, M_{n+1})$
    $\mathfrak{B}'_n \leftarrow \mathfrak{B}_n$
    for $j \leftarrow numPivots, \ldots, 1$ **do**
        Remove $\mathfrak{B}'_n(j)$
        Remove $M_{n+1}(j, \bullet)$
    end for
    RowReduce$(M_n, \mathfrak{B}'_{n-1}, numPivots)$
    $\mathfrak{B}''_{n-1} \leftarrow \emptyset$
    for $i \leftarrow 1, \ldots, numPivots$ **do**
        $\mathfrak{B}''_{n-1} \leftarrow \mathfrak{B}''_{n-1} \cup \{\mathfrak{B}'_{n-1}(i)\}$
    end for
end for

Algorithm 4 Reduction to column-echelon form

```
1: function ColumnReduce(M_n, 𝔅_n, M_{n+1})
2:     rows ← numRows(M_n), cols ← numCols(M_n)
3:     pivotCol ← 1, pivotRow ← 1
4:     while pivotCol ⩽ cols do
5:         while pivotRow ⩽ rows ∧ ∀j ⩾ pivotCol: M_n(pivotRow, j) = 0 do
6:             pivotRow ← pivotRow + 1
7:         end while
8:         if pivotRow > rows then
9:             return pivotCol − 1
10:        end if
11:        k ← min{j : M_n(pivotRow, j) ≠ 0}

12:        swap(M_n(•, k), M_n(•, pivotCol))
13:        swap(𝔅_n(k), 𝔅_n(pivotCol))
14:        swap(M_{n+1}(k, •), M_{n+1}(pivotCol, •))

15:        for j ← pivotCol + 1, ..., cols do
16:            if M_n(pivotRow, j) ≠ 0 then
17:                α ← M_n(pivotRow, j)/M_n(pivotRow, pivotCol)
18:                M_n(•, j) ← M_n(•, j) − αM_n(•, pivotCol)
19:                𝔅_n(j) ← 𝔅_n(j) − α𝔅_n(pivotCol)
20:                M_{n+1}(pivotCol, •) ← M_{n+1}(pivotCol, •) + αM_{n+1}(j, •)
21:            end if
22:        end for
23:    end while
24:    return pivotCol − 1
25: end function
```

Algorithm 5 Row reduction of a matrix in column-echelon form to Smith normal form

```
1: procedure RowReduce(M_n, B'_{n-1}, numPivots)
2:     rows ← rows(M_n)
3:     for j ← 1, ..., numPivots do
4:         pivotRow ← min{i : M_n(i, j) ≠ 0}
5:         swap(M_n(pivotRow, •), M_n(j, •))
6:         swap(B'_{n-1}(pivotRow), B'_{n-1}(j))
7:         for i ← j + 1, ..., rows do
8:             if M_n(i, j) ≠ 0 then
9:                 α ← M_n(j, j)/M_n(i, j)
10:                M_n(i, •) ← M_n(i, •) − αM_n(j, •)
11:                B'_{n-1}(j) ← B'_{n-1}(j) + αB'_{n-1}(i)
12:            end if
13:        end for
14:    end for
15: end procedure
```

The reduction starts with bringing the matrix M_n to so called **column-echelon form**:

$$\begin{bmatrix} \boxed{*} & 0 & & \dots & 0 \\ * & 0 & & \dots & 0 \\ * & \boxed{*} & 0 & \dots & 0 \\ * & * & \boxed{*} & 0 \dots & 0 \\ * & * & * & 0 \dots & 0 \end{bmatrix}$$

A matrix is in colum-echelon form if for every column $j \geqslant 2$, if the column is nonzero, then column $j-1$ is also nonzero and the first nonzero element (starting from the top) in column $j-1$ is *higher* than the first nonzero element in column j. The first nonzero element in a column is a **pivot**. In the above picture pivots are marked using boxes. A row (column) containing a pivot is a **pivot row** (**pivot column**). So the first few columns on the matrix are pivot columns, every consecutive pivot is positioned lower than the previous pivot, and the other columns are zero.

The function ColumnReduce in figure 4 performs the reduction to column-echelon form. We eliminate columns of the matrix M_n using the elementary operations swapping columns i, j and adding column i column multiplied by a scalar α to a column j. These operations correspond to swapping the elements i, j of the basis $\mathfrak{B}_n$ and adding element i multiplied by α to the element j respectively. In turn the corresponding operations on the rows of M_{n+1} are: swapping rows i, j and subtracting column j multipled by α from column i (notice the difference; see appendix A). We find a pivot row, put the pivot column into its place using swaps, then eliminate elements to the right of the pivot. Then we repeat for the next (lower) pivot unless there are no more pivots. The function returns the number of pivots, i.e. the number of nonzero columns.

After performing ColumnReduce the algorithm will do no more column operations on M_n. Furthermore RowReduce doesn't change the pivots. Thus a column is zero in the

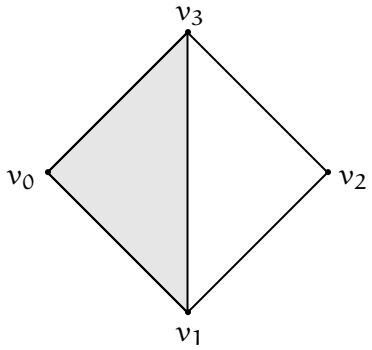
column-echelon form if and only if it will be zero in the Smith normal form at the end of the algorithm. Due to this fact we can right now say which elements of $\mathfrak{B}_n$ will form a basis $\mathfrak{B}'_n$ of Z_n: these are exactly the elements of $\mathfrak{B}_n$ corresponding to zero columns in the column-echelon form. So in the next step we construct the basis $\mathfrak{B}'_n$ by removing the elements of $\mathfrak{B}_n$ corresponding to nonzero columns. At the same time we remove the corresponding rows of M_{n+1} to obtain a representation of ∂_{n+1} in the bases $\mathfrak{B}_{n+1}$ and $\mathfrak{B}'_n$.

We finish the reduction using procedure RowReduce in figure 5. We eliminate elements under the pivots and put the pivots on the diagonal using elementary row operations. At the same time we perform corresponding operations on the basis $\mathfrak{B}'_{n-1}$. We don't need to modify the matrix M_{n-1} as it is of no more use to us. After RowReduce has finished the matrix is in Smith normal form.

The obtained set $\mathfrak{B}'_{n-1}$ is the final basis of Z_{n-1} and we can take the subset of $\mathfrak{B}'_{n-1}$ corresponding to nonzero rows of M_n to obtain a compatible basis $\mathfrak{B}''_{n-1}$ of B_{n-1}.

When implementing the above algorithm(s) we might ask how to represent the output $\mathfrak{B}''_n \subseteq \mathfrak{B}'_n$. If our input bases $\mathfrak{B}_n$ are abstract sets of elements, we might want to represent the vectors in $\mathfrak{B}'_n$ as formal linear combinations of the elements of $\mathfrak{B}_n$. A 'sparse' representation would be to store each vector as a list of elements of $\mathfrak{B}_n$ with their coefficients, keeping only these that have nonzero coefficients. We then need to have a way to add, subtract, and multiply such lists by scalars. Another direction would be to represent $\mathfrak{B}'_n$ as a matrix, where each column corresponds to an element of $\mathfrak{B}'_n$ and contains the coefficients of this element in the basis $\mathfrak{B}_n$. In practice if we use a sparse-matrix representation these two ideas amount to the same thing.

Example 48. We will use the algorithm to calculate the homology groups of the simplicial chain complex over the field $\mathbb{Q}$ of the following simplicial complex:



There is a natural ordering of the vertices which gives an orientation of every simplex. Thus our chosen bases for C_n for n $0, 1, 2$ are:

$$\mathfrak{B}_0 = ([v_0], [v_1], [v_2], [v_3]),$$

$$\mathfrak{B}_1 = ([v_0, v_1], [v_0, v_3], [v_1, v_2], [v_1, v_3], [v_2, v_3]),$$

$$\mathfrak{B}_2 = ([v_0, v_1, v_3]).$$

The bases have to be ordered to talk about matrices. We did the most natural thing and ordered them lexicographically. For $n > 2$ $C_n = 0$ so the bases in higher dimensions are empty. We want to run the algorithm for $N = 2$ so that it calculates in particular a basis

for Z_2 – we know that $B_2 = 0$. Formally the algorithm would require a matrix M_3 and a sequence $\mathfrak{B}_3$. Let's say that for $n = 2$ the operations involving M_{n+1} in the algorithm are no-ops. If necessary the algorithm can either be modified to condition on this edge case or can be given a 0 matrix M_3 of dimensions $|\mathfrak{B}_2| \times 1$ and a sequence $\mathfrak{B}_3 = (0)$.

Formula 2.1 gives the following representations of ∂_n as matrices in bases $\mathfrak{B}_n, \mathfrak{B}_{n-1}$ for $n = 1, 2$:

$$M_1 = \begin{bmatrix} -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}, M_2 = \begin{bmatrix} 1 \\ -1 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Let '$c_i \leftrightarrow c_j$' denote swapping columns i and j and '$c_i \leftarrow c_i + \alpha c_j$' adding the jth column multiplied by α to the column i. The matrix operated on will be known from the context. We will use a similar notation for row operations, using letter w instead of c.

First we reduce M_1 to the column-echelon form using ColumnReduce. The algorithm performs the operations

$$c_2 \leftarrow c_2 - c_1, c_3 \leftarrow c_3 - c_2, c_4 \leftarrow c_4 - c_2, c_5 \leftarrow c_5 + c_3$$

which gives the column-echelon form of M_1

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

Simultaneously it performs the corresponding operations on $\mathfrak{B}_1$, which changes it to

$$([v_0, v_1], [v_0, v_3] - [v_0, v_1], [v_1, v_2] - [v_0, v_3] + [v_0, v_1], \\ [v_1, v_3] - [v_0, v_3] + [v_0, v_1], [v_2, v_3] + [v_1, v_2] - [v_0, v_3] + [v_0, v_1]).$$

At the same time, M_2 gets modified by the corresponding row operations

$$w_1 \leftarrow w_1 + w_2, w_2 \leftarrow w_2 + w_3, w_2 \leftarrow w_2 + w_4, w_3 \leftarrow w_3 - w_5$$

which gives the matrix

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

The first three columns of M_1 are now the pivot columns and the last two columns are zero. Therefore we take the last two vectors of the modified basis $\mathfrak{B}_1$ of C_1 to obtain

$$\mathfrak{B}_1' = ([v_1, v_3] - [v_0, v_3] + [v_0, v_1], [v_2, v_3] + [v_1, v_2] - [v_0, v_3] + [v_0, v_1]),$$

a basis for Z_1. As expected, the first three rows of M_2 are now zero – this is because B_1, the image of ∂_2, is contained in Z_1, and the last two rows of M_1 correspond to $\mathfrak{B}_1'$. They give us a new M_2 – the representation of $\partial_2 : C_2 \to Z_1$ in bases $\mathfrak{B}_2$ and $\mathfrak{B}_1'$:

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

Finally the algorithm reduces M_1 using RowReduce, performing the operations

$$w_2 \leftarrow w_2 + w_1, w_4 \leftarrow w_4 + w_2, w_4 \leftarrow w_4 + w_3$$

to obtain

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and simultaneously performs the corresponding operations on $\mathfrak{B}'_0 = \mathfrak{B}_0$, which gives a modified basis of Z_0

$$([v_0] - [v_1], [v_1] - [v_3], [v_2] - [v_3], [v_3]).$$

Since the Smith normal form of M_1 has 3 pivots, the first 3 elements form the set $\mathfrak{B}''_0$, a basis of B_0.

Finally, observe that the modified M_2 is already in the Smith normal form, so the algorithm doesn't perform any modifications of the matrices or the bases in step $n = 2$, but based on M_2 returns the set $\mathfrak{B}''_1$ consting of the first element of $\mathfrak{B}'_1$

$$\mathfrak{B}''_1 = ([v_1, v_3] - [v_0, v_3] + [v_0, v_1])$$

and gives $\mathfrak{B}'_2 = \emptyset$ as there are no zero columns in this matrix.

We deduce that $H_2 = 0$ and example bases for H_1 and H_0 are $([v_2, v_3] + [v_1, v_2] - [v_0, v_3] + [v_0, v_1] + B_1), ([v_3] + B_0)$ respectively. In particular $\dim H_1 = \dim H_0 = 1$.

Let's analyze the complexity of the algorithm. We will assume for simplicity that the performed operations on the field, i.e. adding, subtracting and multiplying scalars in $\mathbb{F}$ take constant time. Depending on the field and the implementation this might not always be the case. Fixing $n \geqslant 1$, let $k = |\mathfrak{B}_{n-1}|$ and $l = |\mathfrak{B}_n|$ be the number of rows and columns of M_n respectively.

Function ColumnReduce starts the outer **while** by looking for the pivot. Lines 5 and 11 might have to pass the entire row, so they are $O(l)$. Since every iteration of the loop increases $pivotRow$ at least once, these lines are executed at most k times. Other operations involved in looking for the pivot take constant time. Thus lines 5 to 11 take $O(kl)$ time during the whole execution of the function.

Next we perform swaps in lines 12 to 14. These can be performed in $O(k)$ time since k is the length of a column of M_n, which is also the length of a row of M_{n+1}, and we assume a matrix representation of $\mathfrak{B}_n$ (a sparse representation cannot perform worse). They are executed for every found pivot, i.e. $O(k)$ times, so during the whole execution they take $O(k^2)$ time.

Finally, the **for** loop at line 15 performs $O(l)$ iterations, where each iteration might take $O(k)$ time, doing operations on entire columns of M_n (and rows of M_{n+1}). As with the swaps, the **for** is executed for every found pivot, i.e. $O(k)$ times. Thus it takes $O(k^2 l)$ in total. In summary, the function takes $O(kl + k^2 + k^2 l) = O(k^2 l)$ time.

A very similar analysis shows that RowReduce also takes $O(k^2 l)$ time. Furthermore, we can easily see that the rest of the **for** iteration in algorithm 3 can be performed in $O(kl)$ time, so a single **for** iteration takes $O(k^2 l + k^2 l + kl) = O(k^2 l)$ time. Summing over all n we we that the complexity of the algorithm is $O(\sum_{n=1}^{N} |\mathfrak{B}_{n-1}|^2 \times |\mathfrak{B}_n|)$.

Remark 1. We have cheated a bit in the previous paragraph, saying that lines 8 to 12 in algorithm 3 can be executed in $O(kl) = O(|\mathfrak{B}_{n-1}| \times |\mathfrak{B}_n|)$ time. Depending on the implementation we might have to construct the matrix M_{n+1} anew using only the rows that are left. But we can safely assume that this can be done in $O(|\mathfrak{B}_{n+1}| \times |\mathfrak{B}_n|)$ time, which is then taken into account in the final sum.

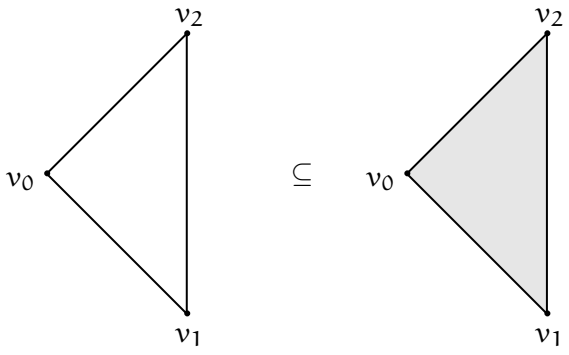
Remark 2. If we were a bit more careful we would observe that the number of pivots is bounded by $\min(k, l)$, so the complexity of a single **for** iteration in algorithm 3 can be lowered to $O(\min(k, l)kl)$.

Remark 3. To calculate H_n we only need to know the $n+1$ skeleton of our simplicial complex X, i.e. the subcomplex of X consisting of all simplices of dimensions at most $n+1$. In particular when working with the Vietoris-Rips complex, if we compute it using the two-stage approach described earlier and we're only interested in H_d for $d \leqslant n$, we never need to look at simplices of dimension $n+1$ and higher. This allows us to reduce the complexity of our computations in certain situations.

2.3. Functoriality

Whenever we have a relationship between two simplicial complexes, their homology groups are also related.

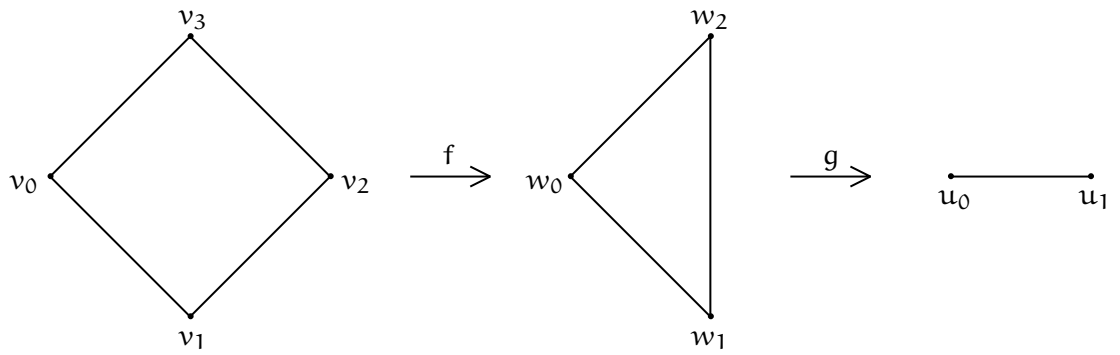
Example 49. Suppose we have an inclusion of complexes:



The first complex has a non-bounding cycle $[v_0, v_1] + [v_1, v_2] + [v_2, v_0]$. When we consider it in homology (take its equivalence class), it is nonzero, and even forms a basis for the first homology group. Now when we 'add' a 2-simplex inside, i.e. we look at the bigger complex on the right, the cycle becomes bounding, so it is zero in homology. How to properly (formally) describe this situation?

Recall that inclusion of complexes can be thought of as a special case of a map between complexes, where each vertex in the 'smaller' complex gets mapped to itself in the 'bigger' complex; it is then called an inclusion map. So let us ask a more general question: if we have a map between (abstract) simplicial complexes, what relationship does it give between their homology groups, if any?

Example 50. Take the following maps:



v	v_0	v_1	v_2	v_3
$f(v)$	w_0	w_1	w_1	w_2

v	w_0	w_1	w_2
$g(v)$	u_0	u_1	u_1

The tables define the maps f and g by telling which vertices get mapped to which. It is easy to see that they are simplicial maps, i.e. they take simplices to simplices. We would like to say that under f the cycle $[v_0, v_1] + [v_1, v_2] + [v_2, v_3] + [v_3, v_0]$ 'still lives' (is nonzero) but after applying g it 'collapses' (becomes zero).

Definition (Induced map)**.** Let $f : X \to Y$ be a map of abstract simplicial complexes. Let C_n^X, C_n^Y denote the n-th chain spaces of X, Y respectively. The linear map $f_{*,n} : C_n^X \to C_n^Y$ defined for $n \geqslant 0$ by the formula

$$f_{*,n}([v_0, \ldots, v_n]) = \begin{cases} [f(v_0), \ldots, f(v_n)] & \text{if } f(v_0), \ldots, f(v_n) \text{ are pairwise distinct} \\ 0 & \text{otherwise} \end{cases}$$

is the **map of chain spaces induced by** f. We will denote it by f_* for brevity if the dimension n is not important or known from the context.

There are of course a few things to check in the above definition. The situation is pretty much the same as it was with the boundary homomorphism in formula 2.1.

First of all f_* is well defined on the set of oriented simplices: suppose $[v_0, \ldots, v_n] = [w_0, \ldots, w_n]$, i.e. the sequence $(v_0, \ldots, v_n)$ is an even permutation of the sequence $(w_0, \ldots, w_n)$. Then $f(v_0), \ldots, f(v_n)$ are pairwise distinct if and only if $f(w_0), \ldots, f(w_n)$ are pairwise distinct and the sequence $(f(w_0), \ldots, f(w_n))$ is an even permutation of $(f(v_0), \ldots, f(v_n))$, so $[f(v_0), \ldots, f(v_n)] = [f(w_0), \ldots, f(w_n)]$.

Secondly f_* extends to a linear map on the entire chain space C_n^X: it is given on a set of generators of C_n^X (the oriented n-simplices of X) and the values for different generators are compatible with each other, i.e. if $\sigma = -\sigma'$ then $f_*(\sigma) = -f_*(\sigma')$ (using the same argument as in the previous paragraph but with odd permutations).

Example 51. In Example 50 f_* takes the 1-cycle $[v_0, v_1] + [v_1, v_2] + [v_2, v_3] + [v_3, v_0]$ to the 1-cycle $[w_0, w_1] + 0 + [w_1, w_2] + [w_2, w_0]$, which after applying g_* becomes $[u_0, u_1] + 0 + 0 + [u_1, u_0] = 0$.

What makes the induced map useful is its compatibility with the boundary homomorphism, as stated in the next lemma.

Lemma 8. *Let X, Y be abstract simplicial complexes and $(C^X_\bullet, \partial^X_\bullet)$, $(C^Y_\bullet, \partial^Y_\bullet)$ be their corresponding simplicial chain complexes. Let $f : X \to Y$ be a simplicial map. Then for each $n \geqslant 1$ the induced map satisfies*

$$\partial^Y_n \circ f_{*,n} = f_{*,n-1} \circ \partial^X_n.$$

The equality is shortly written $\partial f_* = f_* \partial$. If the reader similarly to the author prefers diagrams, the lemma states that the diagram

$$\begin{array}{ccc} C^X_n & \xrightarrow{f_{*,n}} & C^Y_n \\ \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} \\ C^X_{n-1} & \xrightarrow{f_{*,n-1}} & C^Y_{n-1} \end{array}$$

commutes.

Proof. It is enough to check the equality on oriented n-simplices since they generate C^X_n. Assuming $f(v_0), \dots, f(v_n)$ are pairwise distinct, we have

$$\partial f_*[v_0, \dots, v_n] = \partial[f(v_0), \dots, f(v_n)] = \sum_{i=1}^{n} (-1)^i [f(v_0), \dots, \widehat{f(v_i)}, \dots, f(v_n)]$$
$$= \sum_{i=1}^{n} (-1)^i f_*[v_0, \dots, \widehat{v_i}, \dots, v_n] = f_* \sum_{i=1}^{n} (-1)^i [v_0, \dots, \widehat{v_i}, \dots, v_n] = f_* \partial [v_0, \dots, v_n].$$

On the other hand, if $f(v_k) = f(v_l)$ for some $k \neq l$, then

$$f_* \partial [v_0, \dots, v_n] = (-1)^k f_*[v_0, \dots, \widehat{v_k}, \dots, v_n] + (-1)^l f_*[v_0, \dots, \widehat{v_l}, \dots, v_n]$$

since for $i \neq k, l$, $f_*[v_0, \dots, \widehat{v_i}, \dots, v_n] = 0$. Now if $f(v_0), \dots, \widehat{f(v_k)}, \dots, f(v_n)$ are not pairwise distinct then the above expression becomes zero. Otherwise it is equal to

$$(-1)^k [f(v_0), \dots, \widehat{f(v_k)}, \dots, f(v_n)] + (-1)^l [f(v_0), \dots, \widehat{f(v_l)}, \dots, f(v_n)].$$

Now we again use that $f(v_l) = f(v_k)$ and perform $|l-k-1|$ transpositions in the second term to get

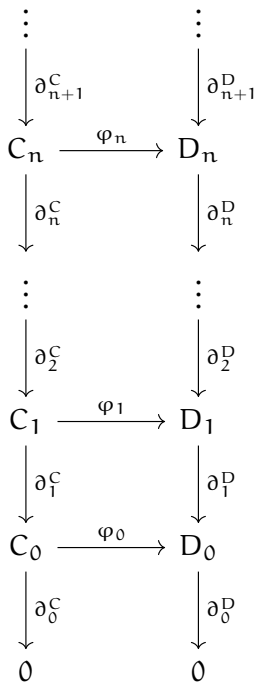
$$(-1)^k [f(v_0), \dots, \widehat{f(v_k)}, \dots, f(v_n)] + (-1)^{k+l-k-1} [f(v_0), \dots, \widehat{f(v_k)}, \dots, f(v_n)] = 0$$

which proves that $f_* \partial [v_0, \dots, v_n] = 0 = \partial f_* [v_0, \dots, v_n]$. □

This property of f_* is the defining property of a *chain map*, which is another purely algebraic concept.

Definition (Chain map)**.** Let $(C_\bullet, \partial^C_\bullet)$, $(D_\bullet, \partial^D_\bullet)$ be a chain complex. A **chain map** φ

between the complexes $C_\bullet$ and $D_\bullet$ is a sequence of homomorphisms $\varphi_n : C_n \to D_n$



satisfying $\partial^D_n \circ \varphi_n = \varphi_{n-1} \circ \partial^C_n$ for every $n \geqslant 1$. In other words every square in the above diagram commutes.

For brevity, when evaluating ∂^C_n on $x \in C_n$, we will often write $\partial(x)$ instead of $\partial^C_n(x)$. Which ∂ is used can be deduced from the type of x. Similarly, for a chain map φ we will write $\varphi(x)$ instead of $\varphi_n(x)$.

Lemma 9. *Let $\varphi : (C_\bullet, \partial^C_\bullet) \to (D_\bullet, \partial^D_\bullet)$ be a chain map. Let Z^C_n, B^C_n be the spaces of cycles and boundaries of $C_\bullet$ and similarly for $D_\bullet$. Then $\varphi_n(Z^C_n) \subseteq Z^D_n$ and $\varphi_n(B^C_n) \subseteq B^D_n$ – chain maps take cycles to cycles and boundaries to boundaries.*

Proof. Let $A \in Z^C_n$, that is $\partial(A) = 0$. If $n = 0$ then of course $\varphi(A)$ is a cycle. If $n \geqslant 1$ then from the property of chain maps $\partial(\varphi(A)) = \varphi(\partial(A)) = \varphi(0) = 0$, i.e. $\varphi(A) \in Z^D_n$.

Now let $A \in B^C_n$, so there is some $B \in C_{n+1}$ such that $\partial(B) = A$. Then $\varphi(B) \in D_{n+1}$ and $\varphi(A) = \varphi(\partial(B)) = \partial(\varphi(B))$, i.e. $\varphi(A) \in B^D_n$. □

Thanks to the above lemma if we restrict φ_n to Z^C_n we obtain a homomorphism into Z^D_n. Composing it with the projection map $\pi^D : Z^D_n \to Z^D_n / B^D_n = H^D_n$, we get $\pi^D \circ \varphi_n|_{Z^C_n} : Z^C_n \to H^D_n$. Again using the above lemma we conclude that this map takes every boundary to zero (because the kernel of π^D is B^D_n and φ_n takes boundaries to boundaries). Then using lemma 7 we get an induced homomorphism between $\psi_n : H^C_n \to H^D_n$ which is given by the formula $\psi_n(x + B^C_n) = \varphi_n(x) + B^D_n$ for $x \in Z^C_n$.

Definition (Induced map on homology groups)**.** Let $\varphi : (C_\bullet, \partial^C_\bullet) \to (D_\bullet, \partial^D_\bullet)$ be a chain map. For every $n \geqslant 0$, the map $\varphi_{*,n} : H^C_n \to H^D_n$, where H^C_n and H^D_n are the homology groups of the chain complexes $C_\bullet$, $D_\bullet$, given by

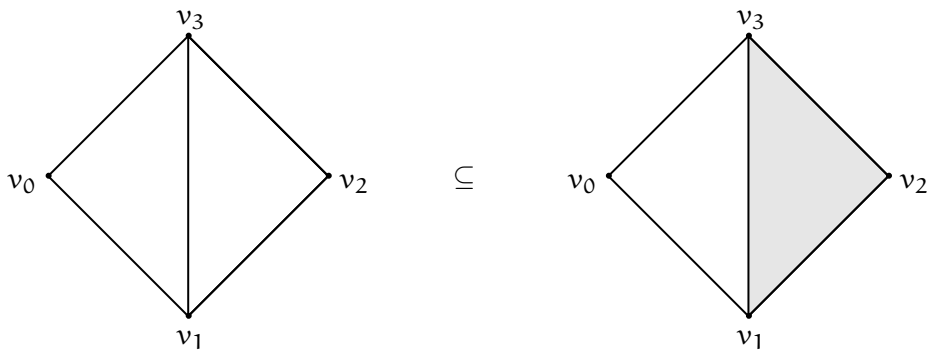
$$\varphi_{*,n}(x + B^C_n) = \varphi_n(x) + B^D_n$$

is the **induced map on n-th homology groups**. It is well defined by the considerations in the above paragraph.

In particular if we have a map f of simplicial complexes, it induces a map of their corresponding simplicial chain complexes, which in turn induces maps between their homology groups. We will not call them 'maps induced by the map induced by ...', but simply the induced maps (of homology groups). We will often abuse notation and use the symbol f_* to denote both the induced map of chain complexes and the maps between homology groups. Which one is being considered (and for which n) should be clear from the context.

Example 52. In Example 49 the inclusion map induces a map between the first homology groups. H_1 of the first complex is nonzero but H_1 of the bigger complex is zero, so the induced map is also zero.

Example 53. The following inclusion



induces a map of the first homology groups. An example basis of H_1 of the first complex is $[v_0, v_1] + [v_1, v_3] + [v_3, v_0] + B_1, [v_0, v_1] + [v_1, v_2] + [v_2, v_3] + [v_3, v_0] + B_1$. The induced map takes both elements of this basis to the same element of H_1 of the second complex: $[v_0, v_1] + [v_1, v_3] + [v_3, v_0] + B_1$, which forms a basis of this H_1. Informally speaking, adding the 2-simplex $[v_1, v_2, v_3]$ to the first complex makes the two cycles of the original basis homologous.

The operation of 'taking the induced map' of homology groups given a simplicial map satisfies minimal usefulness properties that we'd expect: $id_* = id$ (where the first identity is a simplicial map and the second a map on homology groups) and if $f : X \to Y$, $g : Y \to Z$ are simplicial maps, then $(g \circ f)_* = g_* \circ f_*$. These properties can be easily checked and we leave it to the reader.

Hence we've defined a method of assigning a vector space $H_n(X)$ to every simplicial complex X and a map of vector spaces $H_n(X) \to H_n(Y)$ to every map of simplicial complexes $X \to Y$, and this method satisfies the properties mentioned above. Mathematically speaking we've defined a *functor* from the category of simplicial complexes to the category of vector spaces (in fact we've defined a functor for every $n \geqslant 0$ – taking the n-th homology groups).

Chapter 3

Persistent homology

3.1. Filtrations and persistence complexes

The above considerations allow us to determine the homology groups of a single simplicial complex. In the common computational setting of having a discrete set of points, one necessarily has to define a suitable simplicial complex on this set that would correspond to the natural notions of shape and distance inherited from the ambient Euclidean space $\mathbb{R}^n$. It can be done in a plethora of ways, including the Čech or Vietoris–Rips complexes for various values of ε.

This however requires a particular value of ε to even start considering the complex and its homology groups. One can think that the choice of a reasonably 'correct' value of ε is crucial.

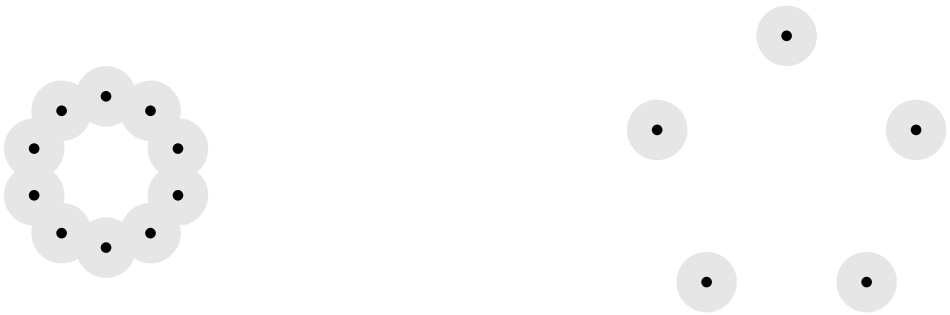
Should the ε be too big, the balls around the points in the data set will intersect too much, possibly causing loss of information about interesting topological structure of the data set. In extreme cases, the complex will have one connected component and no holes. This roughly corresponds to underfitting in statistical data analysis: our 'model' is not precise enough to convey any useful information.

On the other hand, a too small value ε will lead to the counterpart of overfitting: the topology of the complex will be mostly influenced by local noise in the data, e.g. causing small random perturbations in the imperfect input to be detected as holes. In the extreme case of a minuscule ε, each point will form a connected component on its own and the homology groups will be otherwise trivial.

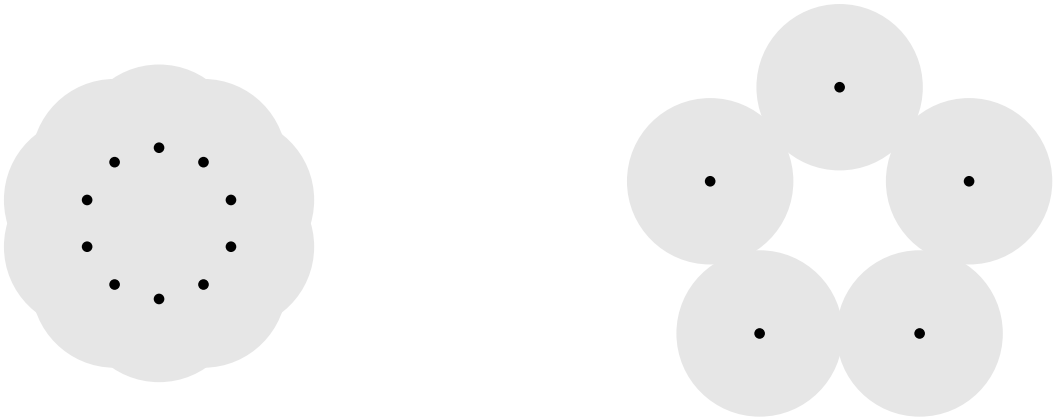
As one can see, different values of ε can show different aspects of the structure of the data set. There might not be a single ε that accurately describes the data (c.f. figure 3.1). However, topological data analysis allows us to consider multiple (or effectively **all**) possible values of ε, which is much stronger than just being able to find the 'right' one. By examining the complexes for all values of ε simultaneously, we can possibly infer much more interesting information about the data set than by considering just one complex.

Clearly, when ε increases, more and more balls around the dataset points intersect each other. Formally, for $\varepsilon_1 < \varepsilon_2$ the Čech (or Vietoris–Rips) complex X^1 for $\varepsilon = \varepsilon_1$ is a subcomplex of the Čech (or Vietoris–Rips) complex X^2 for $\varepsilon = \varepsilon_2$.

Hence, X^2 might have more simplices than X^1 and therefore it might have more cycles, and the non-bounding cycles already present in X^1 may be bounding in X^2. This allows us to ask questions that refer to both of those complexes simultaneously, e.g. ask which cycles in



(a) A small ε detects a hole in the left half of the data set, but fails to do so in the right one.



(b) A large ε detects a hole in the right half of the data set, but fails to do so in the left one.

Figure 3.1: There might not be a single ε that accurately describes the data.

X^1 remain non-bounding even in X^2, i.e. when the ε is increased to ε_2. Note that short-lived cycles which are non-bounding only for a small interval of ε are likely to be caused by noise in the input data set and should be disregarded during the analysis of the data. Thus, we are predominantly interested in cycles which are non-bounding for a large interval of values of ε — those correspond to presumably 'interesting' homologies.

We can extend the above consideration to more than two complexes, which leads to the following definition:

Definition (Filtration)**.** A sequence of complexes (X^k) is called a **filtration** iff X^n is a subcomplex of X^m whenever $n < m$.

As a consequence of the above, any sequence $0 = \varepsilon_0 < \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_n$ yields a corresponding filtration $X^0 \subseteq X^1 \subseteq X^2 \subseteq \cdots \subseteq X^n$ of Čech (or Vietoris–Rips) simplicial complexes. One can easily see, that given a finite set of points there are only finitely many nonzero values of ε that really matter, e.g. in the case of Vietoris-Rips those are all the $\binom{|X|}{2}$ pairwise distances of elements of the data set X. There is no other Vietoris-Rips complex that can be formed than when using one of the above values of ε.

In practice, even not all of those values are needed: as mentioned above, the very large ones are unlikely to yield interesting results, because they coalesce too much, and the very small are unable to capture the big picture of the dataset's shape. Hence, we may skip some of

them for computational efficiency reasons, because we do not expect anything of importance to arise from them.

For a filtration (X^k) we use the standard notation of $C_n^k, Z_n^k, B_n^k, H_n^k$ for n-dimensional chains, cycles, boundaries and homologies of the k-th chain, respectively. However, the additional structure given by the filtration allows us to consider n-dimensional holes of X^k which manage to survive at least until X^{k+p}, i.e. those n-cycles of X^k which not only are non-bounding in X^k, but also keep being non-bounding even in X^{k+p}.

Definition (Persistent homology groups)**.** Let (X^k) be a filtration. The **p-persistent n-dimensional homology group of a complex** X^k is defined as:

$$H_n^{k,p} = Z_n^k / \left(Z_n^k \cap B_n^{k+p}\right)$$

The intersection on the right hand side of the following definition is needed because X^{k+p} might have more n-cycles than X^k, so B_n^{k+p} is not necessarily a subspace of Z_n^k, we are however only interested in the n-cycles that have been already present in X^k.

Formally speaking, we used the functoriality of chain spaces, viz. lifted the inclusion mapping between complexes to a mapping between their respective chain spaces, obtaining chain maps between the chain complexes. By applying Lemma 9 we obtain a map $Z_n^k \to Z_n^{k+p}$, which, having been induced from inclusion, can be easily seen to be a monomorphism. Thus we have $Z_n^k \subseteq Z_n^{k+p}$ and both the numerator and the denominator are subspaces of Z_n^{k+p}.

This method of considering homologies spanning across different filtration levels can be generalised further to arbitrary chain complexes, not necessarily simplicial ones.

Definition (Persistence complex)**.** A **persistence complex** is a sequence of chain complexes (C_*^k) together with chain maps: $i^k : C_*^k \to C_*^{k+1}$, such that the diagram shown in figure 3.2 commutes. Note: i^k are usually inclusions and, for the sake of readability, have been marked as such in the diagram.

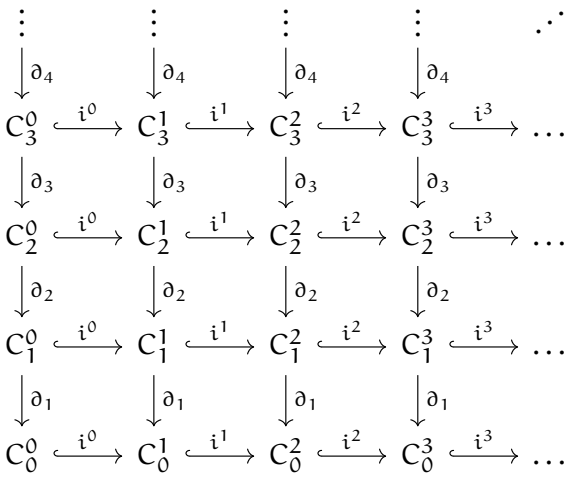
In fact, a filtration of chain complexes together with the appropriate inclusions gives a persistence complex.

3.2. Persistence modules

The notion of persistence complexes allows us to study homology groups of the respective complexes for various ε simultaneously, viz. compute the persistent homology groups. However, very natural question arise: how to compute said homology groups and whether they can be expressed using a unified algebraic framework as a simple object, how to compute bases for them, are those bases related in any way, ...?

A suitable algebraic structure that would describe n-dimensional cycles in a persistence complex should behave roughly like vector spaces used to talk about n-dimensional cycles in ordinary (i.e. not persistence) complexes. However, it should be able to express the additional structure, viz. the persistence.

The reader certainly knows a an algebraic construct which packs multiple values into a single object while preserving useful algebraic properties, viz. polynomials. A polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ represents the sequence of values $(a_0, a_1, \ldots, a_n)$. Polynomial



(a) The full diagram.

(b) A simplified notation for the above diagram.

Figure 3.2: A persistence complex

addition corresponds to pointwise addition of values. It turns out that this is the correct way forward in the present case.

To this end, one needs to relax slightly the conditions imposed on vector spaces: because polynomials are not necessarily invertible, invertibility of elements in the underlying field needs to be given up. By doing this, we obtain the notion of a module over a ring (instead of a vector space over a field). A full formal definition is presented below for the sake of completeness.

3.2.1. A bit of algebra

Reader interested in reading more about this topic is referred to any commutative algebra textbook, such as the one by Atiyah and Macdonald[1] or Bourbaki[2].

Definition (Ring)**.** A set R together with two operations:

- $+_R : R \times R \to R$
- $\cdot_R : R \times R \to R$

is a **ring** iff it satisfies the following conditions:

- R with $+_R$ is a commutative group, i.e.:
  - $+_R$ is commutative, i.e. $r_1 +_R r_2 = r_2 +_R r_1$ for all $r_1, r_2 \in R$;
  - $+_R$ is associative, i.e. $(r_1 +_R r_2) +_R r_3 = r_1 +_R (r_2 +_R r_3)$ for all $r_1, r_2, r_3 \in R$;

- there exists an element $0_R \in R$ s.t. $0_R +_R r = r +_R 0_R = r$ for all $r \in R$ (note that such a 0_R is unique);
- for every $r_1 \in R$ there exists $r_2 \in R$ denoted $-r_1 := r_2$ s.t. $r_1 + r_2 = 0_R$ (note that such an r_2 is unique);

- $\cdot_R$ is associative, i.e. $(r_1 \cdot_R r_2) \cdot_R r_3 = r_1 \cdot_R (r_2 \cdot_R r_3)$ for all $r_1, r_2, r_3 \in R$;
- $\cdot_R$ is distributive over $+_R$, i.e.:
  - $r_1 \cdot_R (r_2 +_R r_3) = (r_1 \cdot_R r_2) +_R (r_1 \cdot_R r_3)$ for all $r_1, r_2, r_3 \in R$;
  - $(r_1 +_R r_2) \cdot_R r_3 = (r_1 \cdot_R r_3) +_R (r_2 \cdot_R r_3)$ for all $r_1, r_2, r_3 \in R$.

Whenever it does not lead to confusion, the subscripts denoting which ring the operations are caried out in will be omitted.

Definition (Commutative ring)**.** A ring $(R, +_R, \cdot_R)$ is said to be **commutative** iff $r_1 \cdot_R r_2 = r_2 \cdot_R r_1$ for every $r_1, r_2 \in R$.

Definition (Unital ring)**.** A ring $(R, +_R, \cdot_R)$ is said to be **unital** (or a **ring with unity**) iff there exists an element $1_R \in R$ s.t. $1_R \cdot_R r = r \cdot_R 1_R = r$ for every $r \in R$. Note that such a 1_R is unique if it exists.

Example 54. Every field is a commutative unital ring.

Example 55. For every natural $n > 0$ the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a ring, where addition and multiplication are carried out modulo n.

For example, in $\mathbb{Z}_6$ one has $4 + 5 = 3$ and $2 \cdot 3 = 0$.

Example 56. If R is a (commutative, unital) ring, then the set of polynomials with one variable t and coefficients from R, denoted by $R[t]$, is a (comutative, unital) ring too. Addition and multiplication are defined in the natural way, similarly to the well-known polynomials over the reals. Note however, that the familiar property of $\deg(f \cdot g) = \deg f + \deg g$ may fail to hold for some R, e.g. in $\mathbb{Z}_6$ we have $2x \cdot (3x^2 + 1) = 2x$.

Definition (Ring homomorphism)**.** Let R_1 and R_2 be rings. A function $\phi : R_1 \to R_2$ is a **homomorphism** iff it preserves the ring structure, i.e.:

- $\phi(0_{R_1}) = 0_{R_2}$;
- $\phi(r +_{R_1} r') = \phi(r) +_{R_2} \phi(r')$ for all $r, r' \in R_1$;
- $\phi(r \cdot_{R_1} r') = \phi(r) \cdot_{R_2} \phi(r')$ for all $r, r' \in R_1$;

If R_1 and R_2 are assumed to be unital rings, we also require $\phi(1_{R_1}) = 1_{R_2}$.

Definition (Kernel)**.** Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ a homomorphism.

The set:

$$\ker \phi = \{r_1 \in R_1 : \phi(r_1) = 0_{R_2}\}$$

is called the **kernel** of ϕ.

Definition (Image)**.** Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ a homomorphism.

The set:

$$\operatorname{im}\phi = \{r_2 \in R_2 : \exists_{r_1 \in R_1} \phi(r_1) = r_2\}$$

is called the **image** of ϕ.

Definition (Module)**.** Let $(R, +_R, \cdot_R)$ be a commutative ring with unity[1]. A set M together with two operations:

- $+_M : M \times M \to M$
- $\cdot_M : R \times M \to M$

is a **module over** R (or R-module for short) iff it satisfies the following conditions:

- M with $+_M$ is a commutative group, i.e.:
  - $+_M$ is commutative, i.e. $m_1 +_M m_2 = m_2 +_M m_1$ for all $m_1, m_2 \in M$;
  - $+_M$ is associative, i.e. $(m_1 +_M m_2) +_M m_3 = m_1 +_M (m_2 +_M m_3)$ for all $m_1, m_2, m_3 \in M$;
  - there exists an element $0_M \in M$ s.t. $0_M +_M m = m +_M 0_M = m$ for all $m \in M$;
  - for every $m_1 \in M$ there exists $m_2 \in M$ denoted $-m_1 := m_2$ s.t. $m_1 + m_2 = 0_M$ (note that such an m_2 is unique);
- $r_1 \cdot_M (r_2 \cdot_M m) = (r_1 \cdot_R r_2) \cdot_M m$ for all $r_1, r_2 \in R$ and $m \in M$
- $1_R \cdot_M m = m$ for all $m \in M$;
- $(r_1 +_R r_2) \cdot_M m = (r_1 \cdot_M m) +_M (r_2 \cdot_M m)$ for all $r_1, r_2 \in R$ and $m \in M$;
- $r \cdot_M (m_1 +_M m_2) = (r \cdot_M m_1) +_M (r \cdot_M m_2)$ for all $r \in R$ and $m_1, m_2 \in M$.

Whenever it does not lead to confusion, the subscripts distinguishing between ring and module operations will be omitted.

Example 57. Every vector space over a field F is also a module over F, because all fields are commutative rings with unity. Moreover, modules over F are precisely vector spaces.

Example 58. Modules over the ring of integers $\mathbb{Z}$ are precisely abelian groups. For every abelian group the multiplication by integers is defined as:

$$n \cdot a = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{(-n) \text{ times}} & \text{if } n < 0 \end{cases}$$

[1]This notion can be generalised to arbitrary rings. However, all rings in this work will be commutative and unital.

Example 59. This example will not be needed in this work, but is of great importance in many areas of mathematics, so it is included here for the sake of completeness.

Let G be a finite group and R be a ring. By $R[G]$ we denote the set of all mappings $f : G \to R$. This is clearly a module, with addition being defined pointwise $(f_1 + f_2)(g) = f_1(g) + f_2(g)$ and multiplication by elements of R given as $(r \cdot f)(g) = r \cdot f(g)$. Moreover, this is a ring with multiplication given as:

$$(f_1 \cdot f_2)(g) = \sum_{\substack{g_1, g_2 \\ g_1 \cdot g_2 = g}} f_1(g_1) f_2(g_2)$$

This structure is called the **group ring** of G over R.

One can extend this definition further, using more advanced topics in calculus and measure theory. If G is not necessarily finite, but is a topological group (i.e. is a topological space and the group operations are continuous) that is Hausdorff and locally compact, then it admits a unique (up to a positve multiplicative factor) left-invariant countably additive non-trivial measure μ on its Borel subsets — this measure is called the Haar measure. Then we may define $R[G]$ as the set of all integrable functions $f : G \to R$ with operations as above, however multiplication is given as:

$$(f_1 \cdot f_2)(g) = \int_G f_1(s) f_2(s^{-1} g) d\mu(s)$$

Definition (Module homomorphism)**.** Let R be a ring and M_1, M_2 modules over F. A function $\phi : M_1 \to M_2$ is a **homomorphism** iff it preserves the structure of modules, i.e.:

- $\phi(0_{M_1}) = 0_{M_2}$;
- $\phi(m +_{M_1} m') = \phi(m) +_{M_2} \phi(m')$ for all $m, m' \in M_1$;
- $\phi(rm) = r\phi(m)$ for all $r \in R$ and $m \in M_1$.

Example 60. The following example will be of crucial significance in this work.

Let R be a ring and M be a module over the ring of polynomials $R[t]$. Then M is clearly also a module over R and is equipped with an R-module homomorphism $\phi : M \to M$ given as $\phi(m) = t \cdot m$.

On the other hand, when given an R-module M together with an R-module homomorphism $\phi : M \to M$, we can view M as an $R[t]$-module in the following way:

- addition is inherited from the R-module structure;
- multiplication by scalars is defined as $\left(a_0 + a_1 t + a_2 t^2 + \cdots + a_n c^n\right) \cdot m = a_0 \cdot m + a_1 \cdot \phi(m) + a_2 \cdot \phi^2(m) + \cdots + a_n \cdot \phi^n(m)$, where ϕ^k denotes the k-th iterate of ϕ.

One can easily check that all module axioms hold.

Definition (Kernel)**.** Let R be a ring, M_1, M_2 modules over F, and $\phi : M_1 \to M_2$ a homomorphism.

The set:

$$\ker \phi = \{m_1 \in M_1 : \phi(m_1) = 0_{M_2}\}$$

is called the **kernel** of ϕ.

Definition (Image)**.** Let R be a ring, M_1, M_2 modules over F, and $\phi : M_1 \to M_2$ a homomorphism.

The set:

$$\operatorname{im}\phi = \{m_2 \in M_2 : \exists_{m_1 \in M_1} \phi(m_1) = m_2\}$$

is called the **image** of ϕ.

Definition (Epimorphism)**.** Let R be a ring, M_1, M_2 modules over F. A homomorphism $\phi : M_1 \to M_2$ is an **epimorphism** iff its image is equal to the whole module M_2, i.e. ϕ is surjective.

Definition (Monomorphism)**.** Let R be a ring, M_1, M_2 modules over F. A homomorphism $\phi : M_1 \to M_2$ is a **monomorphism** iff its kernel is equal to $\{0_{M_2}\}$, i.e. ϕ is injective.

Definition (Isomorphism)**.** Let R be a ring, M_1, M_2 modules over F. A homomorphism $\phi : M_1 \to M_2$ is an **isomorphism** iff it is both an epimorphism and a monomorphism, i.e. it is bijective.

Example 61. If M_1, M_2 are two modules over the same ring R we can equip their Cartesian product $M_1 \times M_2$ with the structure of an R-module. Every operation is defined componentwise, e.g. $(m_1, m_2) + (m_1', m_2') = (m_1 + m_1', m_2 + m_2')$. We can also define projections $\pi_i : M_1 \times M_2 \to M_i$ by $\pi_1((m_1, m_2)) = m_1$ and $\pi_2((m_1, m_2)) = m_2$.

This can be easily generalised to arbitrary products, even infinite ones. For the latter, $\prod_i M_i$ is defined as the set of all sequences $(m_i)_i$ such that $m_i \in M_i$.

This object is called the **direct product** of modules and satisfies the following universal property: If Z is an R-module and $f_i : Z \to M_i$ are homomorphisms for $i \in \{1, 2\}$, then there exists a unique homomorphism $f_1 \times f_2 : Z \to M_1 \times M_2$ such that $f_i = \pi_i \circ (f_1 \times f_2)$.

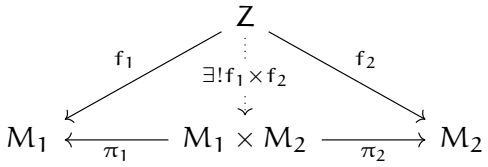


Figure 3.3: The universal property of direct product of two modules.

This universal property easily extends to arbitrary finite and infinite products.

Remark. The above universal property defined the product uniquely, up to isomorphism. This is a general fact that holds for various universal properties. A reader not familiar with the proof of this fact is encouraged to think about it and realise that general abstract nonsense may indeed be sufficient to prove a fact.

Example 62. We may reverse the arrows in the diagram in Example 61. Again, the resulting construction, if exists, is unique up to isomorphism.

We denote it by $M_1 \oplus M_2$ and call it the **direct sum** of modules. It satisfies the following universal property: If Z is an R-module and $f_i : M_i \to Z$ are homomorphisms for $i \in \{1, 2\}$, then there exists a unique homomorphism $f_1 \oplus f_2 : M_1 \oplus M_2 \to Z$ such that $f_i = (f_1 \oplus f_2) \circ \iota_i$.

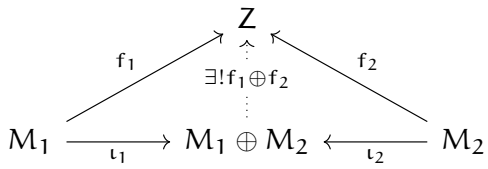


Figure 3.4: The universal property of direct sum of two modules.

This can be easily generalised to arbitrary sums, even infinite ones.

It turns out that finite direct sums are equal to the corresponding direct products, with $\iota_1(m_1) = (m_1, 0_{M_2})$ and $\iota_2(m_2) = (0_{M_1}, m_2)$. However, for infinite ones, $\bigoplus_i M_i$ is defined as the set of all sequences $(m_i)_i$ such that $m_i \in M_i$ and only finitely many values m_i are nonzero.

Definition (Generating set)**.** Let R be a ring and M be an R-module. A subset $S \subseteq M$ is a **generating set** iff every element of M can be expressed as a linear combination of finitely many elements in S, i.e. for every $m \in M$ there exist $k \in \mathbb{N}$, $s_1, s_2, \ldots, s_k \in S$, and $r_1, r_2, \ldots, r_k \in R$ such that $m = r_1 s_1 + r_2 s_2 + \cdots + r_k s_k$.

Module M is said to be **finitely generated** iff it admits a finite generating set.

Definition (Linearly independent set)**.** Let R be a ring and M be an R-module. A subset $S \subseteq M$ is a **linearly independent set** iff for every $k \in \mathbb{N}$, $s_1, s_2, \ldots, s_k \in S$, and $r_1, r_2, \ldots, r_k \in R$ such that $r_1 s_1 + r_2 s_2 + \cdots + r_k s_k = 0_M$ one necessarily has $r_1, \ldots, r_k = 0_R$.

Definition (Basis)**.** Let R be a ring and M be an R-module. A subset $S \subseteq M$ is a **basis** iff it is both generating and linearly independent. We often equip S with an order, i.e. S is often a sequence, not a set.

As opposed to vector spaces, modules do not necessarily have a basis.

Definition (Zero divisor)**.** An element r of a commutative ring R is called a **zero divisor** iff there exists an element $q \in R \setminus \{0\}$ s.t. $r \cdot q = 0$.

Definition (Torsion element)**.** An element m of a module M over ring R is called a **torsion element** iff there exists an element $r \in R$ that is not a zero divisor, s.t. $r \cdot m = 0$.

Example 63. $\mathbb{Z}_{42}$ is an abelian group, and hence a module over $\mathbb{Z}$. However, every nonzero element is a torsion element as $42a = 0$ for all $a \in \mathbb{Z}_{42}$, hence any nonempty set is not linearly independent. Thus, $\mathbb{Z}_{42}$ has no basis.

Example 64. Consider the ring of polynomials with integer coefficients ($\mathbb{Z}[t]$). The set

$$(2, t) = \{2p(t) + tq(t) : p(t), q(t) \in \mathbb{Z}[t]\}$$

is clearly a $\mathbb{Z}[t]$-module and it is generated by 2 and t. Moreover, none of these generators is a linear combination of the other generators (in this case: neither is a multiplicity of the other). However, they are not independent, because there is a linear combination of 2 and t with nonzero coefficients in $\mathbb{Z}[t]$, viz. $2 \cdot t - t \cdot 2 = 0$, that evalutes to zero. It can be checked that this module has no basis.

Zero divisors are somewhat problematic and the theory behind rings and modules is much easier (but therefore less interesting!) when we assume that there are none.

Definition (Integral domain)**.** A commutative unital ring without zero divisors is called an **integral domain**.

Example 65. Fields and $\mathbb{Z}$ are integral domains.

Example 66. For $n > 1$, the ring $\mathbb{Z}_n$ is an integral domain iff n is a prime.

Example 67. $R[t]$ is an integral domain iff R is one. Moreover, in this case the familiar equality $\deg(f \cdot g) = \deg f + \deg g$ holds.

Many natural constructions can be carried out on rings and modules: the notions of homomorphisms, products, direct sums etc. are straightforward, as presented above. However, quotients of rings are a little bit more problematic. The reader likely knows that quotients of any vector space by its subspace, or of any abelian group by its subgroup are well-defined, but in case of general groups this requires an additional constraint: the subgroup must be normal. The general idea is that there should be a quotient map from the outer object to its quotient by the inner object. This sometimes necessitates additional constraints on the inner object: in the case of rings, one obtains the notion of ideals. As usual in this work, we will only consider the commutative case.

Definition (Ideal)**.** Let R be a commutative ring. A nonempty subset I of R is an **ideal** iff it satisfies the following conditions:

- $(I, +)$ is a subgroup of $(R, +)$, i.e.:
  - $x + y \in I$ for all $x, y \in I$;
  - $-x \in I$ for all $x \in I$;
- $rx \in I$ for all $r \in R$ and $x \in I$.

Remark. Let R be a commutative ring. Every ideal $I \subseteq R$ is a module over R.

Example 68. Let R be a commutative ring and $S \subseteq R$. The set

$$(S) = \{a_1 r_1 + a_2 r_2 + \cdots + a_k r_k : a_1, a_2, \ldots, a_k \in R, r_1, r_2, \ldots, r_k \in S\}$$

is an ideal, called the ideal generated by S.

We have already seen this object in Example 64. It can easily be seen that it is the smallest ideal in R containing S.

In particular, the set of multiplicities of a single given element $r \in R$, i.e. (r), is an ideal. An ideal of such form is called **principal**.

Remark. The inclusion $(r_1) \subseteq (r_2)$ means precisely that $r_1 \in (r_2)$, i.e. there exists $r \in R$ such that $r_1 = r r_2$. In this case r_2 is a divisor of r_1, which we denote $r_2 \mid r_1$.

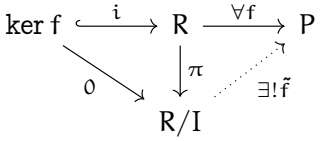
Remark. Let $\phi : R_1 \to R_2$ be a ring homomorphism. Then $\ker \phi$ is an ideal.

Moreover, the converse holds: if $I \subseteq R$ is an ideal, it is the kernel of a homomorphism from R to some other module:

Lemma 10. *Let* R *be a ring and* $I \subseteq R$ *be an ideal. There exists a ring* R/I *with a morphism* $\pi : R \to R/I$*, s.t.* $\ker \pi = I$*, constructed in the proof below. This ring is called the quotient ring, and the mapping — the quotient mapping.*

Proof. Let $\sim \subseteq R \times R$ be the relation defined as: $x \sim y \iff x - y \in I$. Let R/I be the set of equivalence classes of $\sim$. One can define the operations on equivalence classes in a straightforward manner: $[r_1]_\sim + [r_2]_\sim = [r_1 + r_2]_\sim$, similarly for multiplication. The proof that I being an ideal implies that this is well-defined (i.e. does not depend on the choice of r_1, r_2 from the appropriate equivalence classes) is left to the reader. The quotient map is defined as $\pi(r) = [r]_\sim$. □

Lemma 11. *The quotient* R/I *satisfies the following universal property: Let* $f : R \to P$ *be any ring homomorphism s.t.* $I \subseteq \ker f$*. Then there exists a unique ring homomorphism* $\tilde{f} : R/I \to P$ *s.t.* $f = \tilde{f} \circ \pi$*.*



Proof. The condition $f = \tilde{f} \circ \pi$ is equivalent to:

$$\forall_{r \in R}\ \tilde{f}([r]_\sim) = f(r)$$

This is well defined, because if $r \sim r'$, then $r - r' \in I \subseteq \ker f$, so $f(r) = f(r')$. Furthermore, one can trivially check that $\tilde{f}$ is indeed a homomorphism. □

Remark. Every R/I is a module over R with multiplication given by $r \cdot [r']_\sim = [rr']_\sim$.

Example 69. Every field has only trivial ideals, namely the zero ideal and the whole field.

Example 70. The nonzero ideals of $\mathbb{Z}$ can be shown to be precisely the sets of integers divisible by a fixed integer $d \neq 0$. The quotient ring is $\mathbb{Z}/(d) = \mathbb{Z}_d$.

The above considerations can be generalised to submodules:

Definition (Submodule)**.** Let R be a commutative ring and M a module over R. A nonempty subset N of M is a **submodule** iff it satisfies the following conditions:

- $(N, +)$ is a subgroup of $(M, +)$, i.e.:
  - $x + y \in I$ for all $x, y \in N$;
  - $-x \in I$ for all $x \in N$;
- $rx \in I$ for all $r \in R$ and $x \in N$.

Quotient modules, quotient maps and their universal property are given as in the case of ideals.

Example 71. The ideal generated by $S \subseteq R$ in a ring R defined in Example 68 is a submodule of R, for which S is a generating set in the sense of modules.

Definition (Principal ideal domain)**.** An integral domain R is a **principal ideal domain** (PID) iff every ideal is generated by one element: for every ideal $I \subseteq R$ there exists an $r \in I$ s.t. $I = (r)$.

Example 72. If F is a field, then the map $\phi : \mathbb{Z} \ni n \mapsto n \cdot 1_F \in F$ is a ring homomorphism. Its kernel $\ker \phi$ is an ideal in a principal ideal domain $\mathbb{Z}$, and hence is generated by a single element n. Without loss of generality, n may be assumed to be non-negative. This value n is called the **characteristic** of F and denoted $\operatorname{char} F$.

This can be generalised to:

Definition (Noetherian ring)**.** A ring R is **Noetherian** iff every ideal in R is finitely generated: for every ideal $I \subseteq R$ there exists a finite sequence $r_1, r_2, \ldots, r_n \in I$ s.t. $I = (r_1, r_2, \ldots, r_n)$.

Remark. Every principal ideal domain is Noetherian.

Definition (Noetherian module)**.** A module M is **Noetherian** iff every submodule in M is finitely generated: for every submodule $N \subseteq M$ there exists a finite sequence $m_1, m_2, \ldots, m_n \in I$ s.t. $N = (m_1, m_2, \ldots, m_n)$.

Remark. Every Noetherian ring is a Noetherian module over itself, since submodules of rings coincide with ideals.

One can build many modules using quotients and direct sums, e.g.: $R \oplus R/I_1 \oplus R/I_2 \oplus R/I_3 \oplus \cdots \oplus R/I_n$. In the Chapter 4, we will show that if R is a PID and the module is finitely generated, those are the only possible cases up to isomorphism..

Because modules over PIDs can be classified, we need a simple fact that the rings we will be working with are indeed PIDs.

Lemma 12. *Let F be a field. Then $F[t]$, i.e. the ring of polynomials with coefficients in F, is a principal ideal domain.*

Proof. Trivially, if $P(t), Q(t) \in F[t]$ are two nonzero polynomials, then their product $(P \cdot Q)(t)$ must be nonzero too, because the leading coefficient of $P \cdot Q$ is the product of leading coefficients of P and Q.

It remains to be shown that every ideal $I \subseteq F[t]$ is generated by a single polynomial. If $I = 0$, then this is obviously the case. Otherwise, let $P(t) \in I$ be a nonzero polynomial with the smallest possible degree among such polynomials. If there are more than one polynomials with minimal degree, choose one arbitrarily.

One can see that $I = (P(t))$. Suppose to the contrary, that some $Q(t) \in I$ were such that $Q(t) \notin (P(t))$, i.e. $P(t) \nmid Q(t)$. Then, by employing the familiar long divison of polynomials, one gets $Q(t) = R_1(t)P(t) + R_2(t)$, where $R_1(t), R_2(t) \in F[t]$. This yields that $R_2(t) = Q(t) - R_1(t)P(t) \in I$, because $Q(t), P(t) \in I$. Moreover, $R_2(t)$, being the remainder, has smaller degree than $P(t)$, whence one obtains a contradiction, because the degree of $P(t)$ was assumed to be minimal among all the polynomials in I. □

3.2.2. Description of persistence modules

Definition (Persistence module)**.** A sequence of modules over a ring R

$$M^0 \xrightarrow{i^0} M^1 \xrightarrow{i^1} M^2 \xrightarrow{i^2} M^3 \xrightarrow{i^3} \dots$$

is called a **persistence module**.

Given a persistence complex $C^0_* \hookrightarrow C^1_* \hookrightarrow C^2_* \hookrightarrow \dots$, over a field F, for each dimension n one has a vector space of chains C^j_n for every j separately.

Hence, for every dimension n we have a persistence module C^*_n:

$$C^0_n \xrightarrow{i^0} C^1_n \xrightarrow{i^1} C^2_n \xrightarrow{i^2} C^3_n \xrightarrow{i^3} \dots$$

This is not the only persistence module that we met before, e.g. homologies also form one, but it will be the most important one for us hereafter.

Define: $C_n = \bigoplus_i C^i_n$. This is obviously a vector space over F, however one can equip it with more structure, which will encompass persistence, viz. the structure of a module over $F[t]$. As addition and multiplication by elements of F is already defined, one only needs to define multiplication by t. The action of t should express a shift to the next filtration level, so we define it as:

$$t \cdot (m_0, m_1, m_2, \dots) = \left(0, i^0(m_0), i^1(m_1), i^2(m_2), \dots\right)$$

This is an instance of the phenomenon described in Example 60.

Moreover, we have $F[t]$-module homomorphisms: $\partial_n : C_n \to C_{n-1}$, defined in the straightforward way: $\partial_n((m_0, m_1, m_2, \dots)) = \left(\partial^0_n(m_0), \partial^1_n(m_1), \dots\right)$. One can easily check that this is indeed a $F[t]$-module homomorphism, because i^* form a chain map.

This structure of a $F[t]$-module extends to cycles, boundaries and homologies: instead of taking images, kernels and quotients of vector spaces, we need to perform the respective operations on modules. One can easily check that none of the considerations made previously about those spaces require division in the underlying field. We will use the straightforward notation Z_k, B_k, H_k for n-dimensional cycles, boundaries and homologies, respectively.

An important question arises: why limit ourselves to F being a field? Although one can consider such structures, and even compute interesting invariants about them, the case of fields allows a very useful decomposition, which is crucial to the analysis of persistent homologies. Namely, using techniques developed in the following chapter (in particular, Corollary 4) we will obtain:

$$H_n = \bigoplus_i t^{\alpha_i} F[t] \oplus \bigoplus_i (t^{\beta_i} F[t])/(t^{\gamma_i}) \tag{3.1}$$

for some $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$ such that $\beta_i < \gamma_i$, where $t^k F[t]$ denotes polynomials in t divisible by t^k.

Of course, having such a classification for $F = \mathbb{Z}$ would be much more useful, as we could utilise the universal coefficient theorem to completely determine homology groups for every other F being an abelian group. Unfortunately, no such classification is known[17].

The next chapter will be devoted to showing that the algorithms presented in the Chapter 2 need hardly any change to compute persistent homologies. For now, the reader may assume without proof that the required changes are:

- replacement of ± 1 in the matrices by certain monomials $\pm t^k$ — the power k corresponds to the difference between filtration levels of the basis elements associated with the row and column;
- addition of an additional step that sorts the rows of the aforementioned matrices (together with their associated basis elements) in the order of decreasing filtration levels.

3.2.3. Barcodes and persistence diagrams

The above considerations yield, for every dimension n, a decomposition given in equation (3.1).

This gives some n-dimensional cycles which appear in X^{α_i} and remain non-bounding in every successive X^k for $k \geqslant \alpha_i$, and some n dimensional cycles which appear in X^{β_i} and remaing non-bounding in X^k for $\beta_i \leqslant k < \gamma_i$, and finally become a boundnary in X^{γ_i}.

The decomposition (3.1) allows us to recover the persistsent homology groups $H_n^{k,p}$. To obtain the basis of the latter, we just have basis elements corresponding to those summands in equation (3.1) that either:

- are of the type $t^{\alpha_i}F[t]$ and $\alpha_i \leqslant k$ — since they correspond to cycles that appear at most at level k, and never become bounding; or
- are of the type $(t^{\beta_i}F[t])/(t^{\gamma_i})$ and $\beta_i \leqslant k$, but $k + p > \gamma_i$ — since they correspond to cycles that appear at most at level k, and survive as non-bounding at least until level $k + p$ inclusive.

In the case of filtered complexes discussed above, that arise from taking various values of ε, we can associate with the former cycles an interval $[\varepsilon_{\alpha_i}, \infty)$ and with the latter: $\left[\varepsilon_{\beta_i}, \varepsilon_{\gamma_i}\right)$. This interval represents the range of values of ε for which a particular element of the homology group (intuitively: 'hole') exists.

As ε increases, new cycles may appear and some of the old ones may become bounding. A short interval likely represents noise in the data, as it corresponds to a short-lived homology: a cycle became bounding shortly after it started existing at all. On the other hand, a long interval represents a long-lived homology (intuitively: 'hole'), which is likely to correspond to inherent topological features of the data. Hence, when examining those intervals, we mostly care about the longest ones, as they convey the most information about the data set.

The collection of those intervals is called the **barcode** of the persistence complex C in dimension n. If the exact correspondence between the intervals and cycles is not needed in a particular application, we may simplify the algorithms from Chapter 2 and forget about bases, caring only about the invariant factor decomposition itself. An example barcode can be found in figure 3.5.

One can also represent every such an interval $[x, y)$ as a point $(x, y) \in (\mathbb{R} \cup \{\infty\})^2$. The collection of those points (possibly with repetitions, i.e. a multiset), together with all the diagonal points (x, x) for $x \in \mathbb{R} \cup \{\infty\}$ counted with infinite multiplicity is called a **persistence diagram**.

3.2.4. Stability

Barcodes (or, equivalently, persistence diagrams) are useful mostly because they are robust against noise. This means that small perturbations of the data induce small perturbations of the persistence diagrams, whence the structure inferred from the homologies of a sampled data set is likely to be similar to the structure of the actual data.

More precisely, one may consider a metric on the space of persistence diagrams, called the **bottleneck distance**:

$$d_B(D_1, D_2) = \inf_{\xi} \sup_{d_1 \in D_1} \|d_1 - \xi(d_1)\|_\infty$$

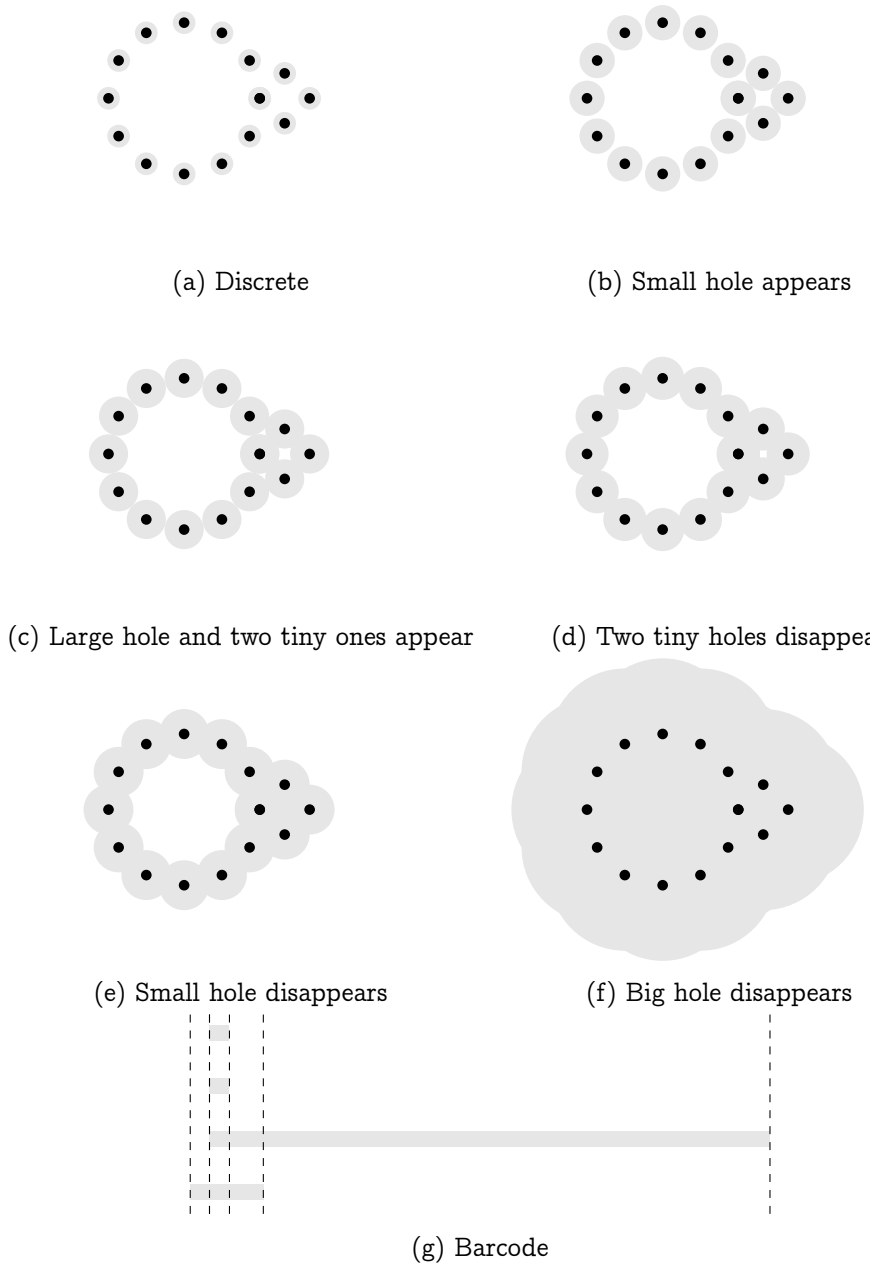
where $\xi : D_1 \xhookrightarrow{} D_2$ ranges over all bijections from D_1 to D_2.

For a finite data set $X \subseteq \mathbb{R}^n$ we may consider a continuous function $f_X : \mathbb{R}^n \to \mathbb{R}$ which assigns to every point its distance from the set X. Then the sublevel set $f_X^{-1}((-\infty, \varepsilon])$ is precisely equal to the union of balls of radius ε around points from X, which is homotopy equivalent to the Čech complex $\check{C}_\varepsilon$ by Theorem 2.

One can show that if X_1 and X_2 are two data sets with persistence diagrams D_1 and D_2 respectively, then

$$d_B(D_1, D_2) \leqslant \|f_{X_1} - f_{X_2}\|_\infty \tag{3.2}$$

Proof of this inequality is omitted from this work. Actually, a stronger statement can be proven[4] about persistence diagrams of sublevel sets of arbitrary continuous functions under certain mild assumptions, however this result corresponds directly to the inequality 3.2 in the case considered in this work.



(a) Discrete

(b) Small hole appears

(c) Large hole and two tiny ones appear

(d) Two tiny holes disappear

(e) Small hole disappears

(f) Big hole disappears

(g) Barcode

Figure 3.5: Barcode for a simple data set. One clearly sees two long-lived, presumably important holes and two short-lived, presumably irrelevant ones.

Chapter 4

Finitely generated modules over a principal ideal domain

The purpose of this chapter is to show that every finitely generated module M over a principal ideal domain R decomposes into simple factors[2], up to isomorphism. More precisely, that $M \simeq \bigoplus_i R \oplus \bigoplus_i R/(I_i)$, that is: M consists of a finite number of copies of R and a finite number of quotients of R. Of course, R is a quotient of itself, so the above formula could be simplified, but by factoring out the free and torsion parts the structure can be seen more easily. One may require that $I_i | I_{i+1}$ and every $I_i \neq 0$. This is then called the 'invariant factor decomposition'.

Theorem 5. *Let R be a principal ideal domain and M a finitely generated module over R. Then*

$$M \simeq \bigoplus_i R \oplus \bigoplus_i R/I_i$$

Moreover, the number of summands of either kind is determined uniquely.

Moreover, the proof will be essentially algorithmic, i.e. it will allow to compute this decomposition if a finite presentation of M will be given.

Definition (Presentation)**.** A module M over ring R is **finitely presented** iff there exists an epimorphism (surjective homomorphism) $\phi : R^k \twoheadrightarrow M$ s.t. $\ker \phi$ is finitely generated.

One can think of a finite presentation as specifying a finite set of generators (the R^k) and a finite set relations between them (the kernel of ϕ).

Example 73. The module $\mathbb{Z}[x, y, z]/(x^2 - y^3, z^2 - xz)$, i.e. polynomials over the integers with variables x, y, z, where $x^2 = y^3$ and $z^2 = xz$, is finitely presented.

Example 73 actually describes the way modules will be presented as the input to the algorithms presented in this book.

4.1. Every finitely generated module over PID is finitely presented

First, we will prove that every finitely generated over PID is finitely presented. As said above, this result will not be needed for the algorithmic part of this work, hence a less proof-oriented

reader may skip this section altogether. However, the reader might still prefer to read this section to get more acquainted with modules and related notions.

Lemma 13. *Let M, N be modules over a ring R and $\phi : M \twoheadrightarrow N$ be a surjective homomorphism between them. Suppose that M is Noetherian. Then N is Noetherian too.*

Proof. Let $P \subseteq N$ be any submodule of N. One can easily check that the preimage $\phi^{-1}(P)$ is a submodule of M, and hence is finitely generated, so there exist $m_1, m_2, \ldots, m_n$, s.t. $\phi^{-1}(P) = (m_1, m_2, \ldots, m_n)$. Then $\phi(m_1), \ldots, \phi(m_n)$ generate P, because every element $p \in P$ is by surjectivity an image of $m \in M$, which necessarily must belong to $\phi^{-1}(P)$, and so is of the form $m = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n$ for some $a_1, \ldots, a_n \in M$. Hence, $p = \phi(m) = \phi(a_1)\phi(m_1) + \phi(a_2)\phi(m_2) + \cdots + \phi(a_n)\phi(m_n)$, so indeed $\phi(m_1), \ldots, \phi(m_n)$ generate P. □

Lemma 14. *Let R_1, R_2 be commutative unital rings. Ideals of $R_1 \oplus R_2$ are of the form $I_1 \oplus I_2$ where $I_1 \subseteq R_1$ and $I_2 \subseteq R_2$ are ideals of R_1, R_2 respectively.*

Proof. Let $I \subseteq R_1 \oplus R_2$ be an ideal and let $I_1 = \{i_1 : (i_1, i_2) \in I\} \subseteq R_1$ and $I_2 = \{i_2 : (i_1, i_2) \in I\} \subseteq R_2$.

Clearly, I_1, I_2 are ideals: if $i_1, i_1' \in I_1$, then there exist $i_2, i_2' \in R_2$ such that $(i_1, i_2), (i_1', i_2') \in I$, whence $(i_1 + i_1', i_2 + i_2') \in I$, therefore $i_1 + i_1' \in I_1$. Moreover, if $i_1 \in I_1$ and $r \in R_1$, then there exists $i_2 \in R_2$ such that $(i_1, i_2) \in I$, whence $(r, 1) \cdot (i_1, i_2) = (ri_1, i_2) \in I$, therefore $ri_1 \in I_1$.

Trivially, $I \subseteq I_1 \oplus I_2$. On the other hand, if $i_1 \in I_1$ and $i_2' \in I_2$ then there exist $i_2 \in R_2$, $i_1' \in R_1$ such that $(i_1, i_2), (i_1', i_2') \in I$. Therefore, $(1,0)\cdot(i_1, i_2) + (0,1)\cdot(i_1', i_2') = (i_1, i_2') \in I$. Thus, $I = I_1 \oplus I_2$. □

Lemma 15. *If M, N are two Noetherian modules over a ring R, then their direct sum $M \oplus N$ is Noetherian, too.*

Proof. We have the canonical injection $i : M \to M \oplus N$ and the canonical projection $\pi : M \oplus N \to N$. They can easily be seen to satisfy the relation $\ker \pi = \operatorname{im} i$.

Take any submodule $S \subseteq M \oplus N$. Then $\pi(S) \subseteq N$ and $i^{-1}(S) \subseteq M$ can be easily seen to be submodules of N and M respectively, whence they are finitely generated: $\pi(S) = (n_1, n_2, \ldots, n_k)$ and $i^{-1}(S) = (m_1, m_2, \ldots, m_l)$. Let $\widetilde{n}_1, \widetilde{n}_2, \ldots, \widetilde{n}_k \in S$ be such that $\pi(\widetilde{n}_i) = n_i$ for every $i = 1, 2, \ldots, k$, and let $\widetilde{m}_i = i(m_i) \in S$ for every $i = 1, 2, \ldots, l$.

One can easily see that $S = (\widetilde{n}_1, \widetilde{n}_2, \ldots, \widetilde{n}_k, \widetilde{m}_1, \widetilde{m}_2, \ldots, \widetilde{m}_l)$ as follows:

For every $s \in S$ we can decompose $\pi(s)$ as $r_1 n_1 + r_2 n_2 + \cdots + r_k n_k$ for some $r_1, r_2, \ldots, r_k \in R$, whence, for $\widetilde{s} = r_1 \widetilde{n}_1 + r_2 \widetilde{n}_2 + \cdots + r_k \widetilde{n}_k$, we have $\pi(s) = \pi(\widetilde{s})$. Thus $s - \widetilde{s} \in \ker \pi = \operatorname{im} i$, therefore $s - \widetilde{s}$ can be written as $i(t_1 m_1 + t_2 m_2 + \cdots + t_l m_l) = t_1 \widetilde{m}_1 + t_2 \widetilde{m}_2 + \cdots + t_l \widetilde{m}_l$ for some $t_1, t_2, \ldots, t_l \in R$, which finally yields $s = r_1 \widetilde{n}_1 + r_2 \widetilde{n}_2 + \cdots + r_k \widetilde{n}_k + t_1 \widetilde{m}_1 + t_2 \widetilde{m}_2 + \cdots + t_l \widetilde{m}_l$. □

Corollary 2. *If $M_1, \ldots, M_n$ are Noetherian modules over a ring R, then $\bigoplus_{i=1}^{n} M_i$ is Noetherian, too.*

Proof. Apply Lemma 15 inductively. □

Lemma 16. *Every finitely generated module over a Noetherian ring is Noetherian and finitely presented.*

Proof. A module M over R is finitely generated iff there exists a surjective homomorphism $\phi : R^k \twoheadrightarrow M$ where k is the number of generators. By Corollary 2, R^k is Noetherian, and hence, by Lemma 13, its homomorphic image M is Noetherian too. Moreover, $\ker \phi$ is a submodule of R^k, so it is finitely generated, whence M is finitely presented. □

Actually, for the common case of M being a commutative algebra over R[1], one can give a different elegant proof[1], based on the Hilbert's basis theorem:

Definition (Commutative algebra)**.** A module M over a commutative unital ring R is a commutative algebra if it also a commutative unital ring and satisfies $r(xy) = (rx)y = x(ry)$ for $r \in R$, and $x, y \in M$.

Theorem 6 (Hilbert's basis theorem)**.** *Let* R *be a Noetherian ring. Then* $R[x]$ *is a Noetherian ring, too.*

Proof. Let $I \subseteq R[x]$ be an ideal in $R[x]$. Define inductively: $f_n \in I$ as the polynomial in I that is not a linear combination of $f_1, \ldots, f_{n-1}$, i.e. does not belong to the ideal $I_n = (f_1, \ldots, f_{n-1})$. If there are multiple such polynomials, pick arbirtrarily one with the smallest degree. Note that f_1 is just an arbitrary polynomial in I with the smallest degree. Observe that $\deg f_i \leqslant \deg f_j$ if $i \leqslant j$.

If this construction stops at some step n then the polynomials $f_1, \ldots, f_{n-1}$ generate I, so I is finitely generated. Suppose then to the contrary that it does not stop. Let a_n be the coefficient of the highest degree monomial of f_n, e.g. if $f_n = \sum_{i=0}^{k} \alpha_i x^i$ where $\alpha_k \neq 0$, then $a_n = \alpha_k$.

The ideal in R generated by all the $a_1, a_2, a_3, \ldots$ is finitely generated by the assumption on Noetherianness of M. Hence, some a_n must be a linear combination of $a_1, \ldots, a_{n-1}$: $a_n = \sum_{i=0}^{n-1} \beta a_i$. Let $g = \sum_{i=0}^{n-1} \beta f_i x^{\deg f_n - \deg f_i}$ be a polynomial in $R[x]$. Clearly, g is a linear combination of $f_1, \ldots, f_{n-1}$, so $g \in I_n$. Hence, $f_n - g \notin I_n$, because otherwise we would get $f_n \in I_n$, which is absurd. But $f_n - g$ has smaller degree than f_n because g was chosen so that the highest degree monomial of f_n would vanish when g is subtracted — a contradiction.

Hence, I is finitely generated. □

Corollary 3. *If* R *be a Noetherian ring, then* $R[x_1, x_2, \ldots, x_n]$ *is Noetherian, too.*

Proof. Apply Theorem 6 inductively. □

Lemma 17. *Every finitely generated commutative algebra over a Noetherian ring is Noetherian and finitely presented.*

Proof. A module M over R is finitely generated iff there exists a surjective homomorphism $\phi : R^k \twoheadrightarrow M$ where k is the number of generators. By Corollary 3, $R[x_1, \ldots, x_k]$ is Noetherian, and hence, by Lemma 13, its homomorphic images R^k and M are Noetherian too. Moreover, $\ker \phi$ is a submodule of R^k, so it is finitely generated, whence M is finitely presented. □

[1] In particular, only such cases will arise in this work.

4.2. Finitely presented modules over a PID

This section contains a purely algorithmic proof that every finitely presented module M over a principal ideal domain P decomposes as $M \simeq \bigoplus_i R \oplus \bigoplus_i R/(I_i)$.

To this end, consider the presentation $\phi : R^r \to M$, where r is the number of generators of M. Denote the said generators by $g_1, g_2, \ldots, g_r$. Moreover, let $s_1, \ldots, s_p$ be the generators of $\ker \phi$ — those are sometimes called **relations**. Then, every s_i is a linear combination of $g_1, g_2, \ldots, g_r$. One can think of those combinations as expressions in terms of g_i's that should evaluate to zero.

This easily yields a linear map $\psi : R^p \to R^r$, where the i-th basis element in the domain is sent to s_i.

Observation. In the above notation: $M = R^r / \operatorname{im} \psi$.

Example 74. Consider $R = \mathbb{Q}[t]$ and $M = \mathbb{Q}[t]^3$ with generators a, b, c. Let $I = (a - t^2 b, tb - t^3 c)$, then $N = M/I$ is generated by $g_1, g_2, g_3 = a, b, c$ and the relations are simply: $s_1 = a - t^2 b, s_2 = tb - t^3 c$.

The map ψ can be represented as matrix:

$$\begin{bmatrix} 1 & 0 \\ -t^2 & t \\ 0 & -t^3 \end{bmatrix}$$

where each column corresponds to a single relation, written down in terms of the generators.

In every case that will arise algorithmically in this work, the setting will be very much akin to the one in Example 74, i.e. we will have an explicitly specified set of generators and relations between them. This is, to the authors' best knowledge, probably the most natural way to think of finite presentations.

We will use the letter ψ interchangeably for either the map itself or its matrix representation with respect to a given set of generators and relations. A matrix representation, apart from providing a compact textual notation or being well suited to being stored in computer memory, is mostly useful when we are about to perform some computations on it.

Many algorithms that operate on matrices repeatedly employ a couple of so called elementary operations, i.e. multipliying a row/column by an invertible constant, adding a multiple of a row/column to another one, and swapping two rows/columns. Those operations are often sufficient over fields, however over PIDs we need a generalisation: we will left- and right-multiply the matrix in question by invertible matrices.

Definition (Invertible homomorphism)**.** A module homomorphism $\phi : M_1 \to M_2$ is **invertible** iff there exists a module homomorphism $\psi : M_2 \to M_1$ such that $\phi \circ \psi = \mathrm{id}_{M_2}$ and $\psi \circ \phi = \mathrm{id}_{M_1}$. We write $\phi^{-1} := \psi$.

Over fields, multiplication by an invertible matrix is equivalent to applying a sequence of elementary row/column operations. On the other hand, over principal ideal domains, every elementary row/column operation can be expressed as a left- or right-multiplication by an invertible matrix, but the other implication does not hold for all PIDs.

To wit, one can easily check that for:

$$A_{i,j} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 1 \end{bmatrix}$$

$$B_{i,j,\alpha} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & \alpha & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 1 \end{bmatrix}$$

$$C_{i,\alpha} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & \alpha & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

the matrices $A_{i,j}, B_{i,j,\alpha}$ are invertible for all indices i, j and any $\alpha \in R$, and the matrices $C_{i,\alpha}$ are invertible iff α is invertible.

They directly correspond to elementary operations: left-multiplication to row operations and right-multiplication to column operations, e.g.:

$$\begin{bmatrix} | & | & \cdots & | & \cdots & | & \cdots & | \\ c_1 & c_2 & \cdots & c_i & \cdots & c_j & \cdots & c_k \\ | & | & \cdots & | & \cdots & | & \cdots & | \end{bmatrix} \cdot A_{i,j} = \begin{bmatrix} | & | & \cdots & | & \cdots & | & \cdots & | \\ c_1 & c_2 & \cdots & c_j & \cdots & c_i & \cdots & c_k \\ | & | & \cdots & | & \cdots & | & \cdots & | \end{bmatrix}$$

$$\begin{bmatrix} | & | & \cdots & | & \cdots & | & \cdots & | \\ c_1 & c_2 & \cdots & c_i & \cdots & c_j & \cdots & c_k \\ | & | & \cdots & | & \cdots & | & \cdots & | \end{bmatrix} \cdot B_{i,j,\alpha} = \begin{bmatrix} | & | & \cdots & | & \cdots & | & \cdots & | \\ c_1 & c_2 & \cdots & c_i & \cdots & c_j + \alpha c_i & \cdots & c_k \\ | & | & \cdots & | & \cdots & | & \cdots & | \end{bmatrix}$$

$$\begin{bmatrix} | & | & \cdots & | & \cdots & | \\ c_1 & c_2 & \cdots & c_i & \cdots & c_k \\ | & | & \cdots & | & \cdots & | \end{bmatrix} \cdot C_{i,\alpha} = \begin{bmatrix} | & | & \cdots & | & \cdots & | \\ c_1 & c_2 & \cdots & \alpha c_i & \cdots & c_k \\ | & | & \cdots & | & \cdots & | \end{bmatrix}$$

One can easily see how those operations correspond to changes in the choice of generators or relations.

Lemma 18. *Left-multiplication by an invertible matrix* E *corresponds to applying* E^{-1} *to the generators of the module* M.

In particular, the elementary matrix operations on the rows of the matrix ψ *correspond to operations on the generators of the module* M*, viz.:*

- *multiplying the* i*-th row by an invertible constant* $c \in R$ *corresponds to dividing the generator* g_i *by* c*;*
- *swapping the* i*-th and* j*-th row corresponds to swapping the* i*-th and* j*-th generators;*
- *adding the* i*-th row multiplied by* $c \in R$ *to the* j*-th row corresponds to replacing* g_j *with* $g_j - cg_i$.

Lemma 19. *Right-multiplication by an invertible matrix* E *corresponds to applying* E^{-1} *to the relations of the module* M.

In particular, the elementary matrix operations on the columns of the matrix ψ *correspond to operations on the relations of* M*, viz.:*

- *multiplying the* i*-th column by an invertible constant* $c \in R$ *corresponds to dividing the relation* s_i *by* c*;*
- *swapping the* i*-th and* j*-th column corresponds to swapping the* i*-th and* j*-th relations;*
- *adding the* i*-th column multiplied by* $c \in R$ *to the* j*-th column corresponds to replacing* s_j *with* $s_j - cs_i$.

Lemma 20. *If a matrix* ψ *corresponds to a presentation of a module* M*, then every matrix* ψ' *obtained by performing an arbitrary sequence of multiplications by an invertible matrix corresponds to a presentation of the same module* M*. Moreover, the relationship between those presentations can be easily computed given the sequence of multiplications.*

Proof. Proceed by induction on the number of multiplications performed, using either Lemma 18 or Lemma 19 in each step.

This of course could be stated more concisely by multiplying all the invertible matrices together (left- and right-factors separately) and applying the aforementioned lemmas only once, but often the matrices will be very simple (e.g. correspond to elementary row operations), so the inductive process might be computationally cheaper. □

Similarly as in various other computational tasks pertaining to matrices, our goal will be to reduce the matrix ψ to a simpler form using the aforementioned operations. More precisely, we will reduce it to the Smith normal form.

Definition (Smith normal form)**.** Let A be a matrix over a principal ideal domain R. We

say that A is in **Smith normal form** iff

$$A = \begin{bmatrix} \alpha_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \alpha_3 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_k & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

for some $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k \in R$ such that each α_i divides the next one, i.e. $\alpha_i | \alpha_{i+1}$.

Because the values α_i are unique up to multiplication by unit[2], one frequently speaks of **the** Smith normal form instead of **a** Smith normal form. The values α_i are called **invariant factors** of matrix A.

The reason for the reduction is that it immediately yields an invariant factor decomposition of the module M itself. Indeed, if we succeed in reducing ψ to the Smith normal form, we will obtain the invariant factor decomposition of M:

Lemma 21. *Let M be a finitely presented module over a principal ideal domain R. Suppose that $\psi : R^s \to R^r$ corresponds to a presentation of M and the matrix ψ is in Smith normal form with invariant factors $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k$ (note that this implies $k \leqslant \min(s, r)$). Then*

$$M \simeq \bigoplus_{i=1}^{r-k} R \oplus \bigoplus_{i=1}^{k} R/(\alpha_i)$$

Proof. This follows from the fact $M = R^r / \operatorname{im} \psi$. More verbosely: every column which consists only of zeroes, corresponds to a free factor R in the invariant decomposition, because the respective generator is not cancelled out by any relation. Every other column corresponds to a generator of M whose α_i-multiplicity is zero, and hence yields a $R/(\alpha_i)$ term in the said decomposition. □

Hence, it only remains to show an algorithm which converts an arbitrary matrix over a principal ideal domain R to its Smith normal form. Observe that if R was guaranteed to be a field, this task would reduce to merely performing the Gaussian elimination, as in Algorithms 4 and 5 in Chapter 2. However, if R is merely a ring, Gaussian elimination needs some modifications, because division is not always possible.

Fortunately, a couple of observations will render those modifications unnecessary in the cases mentioned in this work, i.e. computing persistent homology. Thus, they are provided for the sake of completeness and will not be elaborated upon in great detail and only the required changes to the algorithms will be presented, without explicitly providing the pseudocode.

We will rely heavily on the following extremely simple yet useful lemma:

Definition (Greatest common divisor)**.** Let R be a principal ideal domain and $x, y \in R$. Then $d \in R$ is said to be a **divisor** of x (denoted $d \mid x$) iff $(d) \supseteq (x)$. Furthermore, d is said

[2]Proof of this fact is omitted from this work, as it is not relevant.

to be the **greatest common divisor** of x, y iff it is a common divisor of x and of y, and every other common divisor d' of x and y is a divisor of d.

One can easily observe that if d_1, d_2 are both greatest common divisors of x, y, then $(d_1) = (d_2)$, i.e. d_1 and d_2 differ by multiplication by an invertible factor. This justifies the use of the definite pronoun 'the'.

Lemma 22 (Bezout's identity). *Let* R *be a principal ideal domain and* $x, y \in R$. *Then their greatest common* $d \in R$ *exists, and there exist* $k, l \in R$ *such that* $kx + ly = d$.

Proof. Let $I = (x, y)$ be the ideal generated by x, y. Since R is a principal ideal domain, there exists $d \in R$ such that $I = (d)$. One can easily check that it is indeed the greatest common divisor of x, y.

Moreover, $d \in I = (x, y)$ means that d is a linear combination of elements x and y, whence $d = kx + ly$ for some $k, l \in R$. □

Examine the only problematic step of Gaussian elimination, i.e. $M(j, \bullet) := M(j, \bullet) - \alpha M(i, \bullet)$ where $\alpha = \frac{M(j,i)}{M(i,i)}$. We cannot perform this step unless $x = M(i, i)$ is a divisor of $y = M(j, i)$. However, by Lemma 22, we have $k, l \in R$ such that $kx + ly = d$ for $d \in R$ being the greatest common divisor of x, y, whence $k\frac{x}{d} + l\frac{y}{d} = 1$. Hence, the matrix

$$\begin{bmatrix} k & l \\ -\frac{y}{d} & \frac{x}{d} \end{bmatrix}$$

is invertible:

$$\begin{bmatrix} k & l \\ -\frac{y}{d} & \frac{x}{d} \end{bmatrix} \cdot \begin{bmatrix} \frac{x}{d} & -l \\ \frac{y}{d} & k \end{bmatrix} = \begin{bmatrix} \frac{x}{d} & -l \\ \frac{y}{d} & k \end{bmatrix} \cdot \begin{bmatrix} k & l \\ -\frac{y}{d} & \frac{x}{d} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Now observe that

$$\begin{bmatrix} k & l \\ -\frac{y}{d} & \frac{x}{d} \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} kx + ly \\ -\frac{yx}{d} + \frac{xy}{d} \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

By scattering those 4 values to the i-th and j-th column and row we obtain an invertible matrix

$$A = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & k & 0 & \cdots & 0 & l & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & -\frac{y}{d} & 0 & \cdots & 0 & -\frac{x}{d} & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 1
\end{bmatrix}$$

which, when applied on the left of the matrix ψ, changes the i-th and j-th row so that $\psi(i,i)$ divides $\psi(j,i)$. This then allows the Gaussian elimination to proceed.

However, when this method is employed to perform reduction to the Smith normal form, one difficulty arises: when this is applied in the row reduction algorithm, it may destroy the property achieved before by the column reduction and vice versa. This can be mitigated by running row reduction and column reduction alternately until the requested Smith normal form is found.

Obviously, this is a priori no longer guaranteed to halt. Fortunately, for every pivot element (for simplicity: $\psi(i,i)$), this algorithm does not shrink the ideal generated by the said pivot element. Moreover, every step described above (to avoid division) makes this ideal strictly larger. We will prove that in a PID (precisely: in every Noetherian ring), there are no infinite ascending sequences of ideals. This will imply that we can indeed reduce any matrix ψ to its Smith normal form, except that the divisibility criterion does not need to be satisfied.

Lemma 23. *Let R be a Noetherian ring. There cannot exist an infinite ascending sequence of ideals: $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$.*

Proof. Suppose to the contrary, that such a sequence exists. Let $I = \bigcup_i I_i$ be the sum of all the ideals in this sequence. One can easily check that I is an ideal in a Notherian ring R, so it must be finitely generated: $I = (g_1, g_2, \ldots, g_k)$.

Every g_i belongs to I, so it must belong to I_{k_i} for some $k_i \in \mathbb{N}$. Take the maximum of all the numbers k_i: $k = \max\{k_1, k_2, \ldots, k_n\}$. Then $g_1, g_2, \ldots, g_k \in I_k$, whence $I = (g_1, g_2, \ldots, g_k) \subseteq I_k \subsetneq I_{k+1} \subseteq I$ — a contradiction. □

Transforming the matrix further, so that the divisibility criterion holds, is left as an easy exercise for the reader. It will not be needed for applications that are considered in this thesis.

4.3. The case of $F[t]$

We will show how the above algorithm can be greatly simplified in the case described in this work, i.e. computing persistent homology. Moreover, the additional structure of $F[t]$, viz. polynomial degrees, will allow a more precise characterisation of modules.[3]

To this end, first consider an example[4].

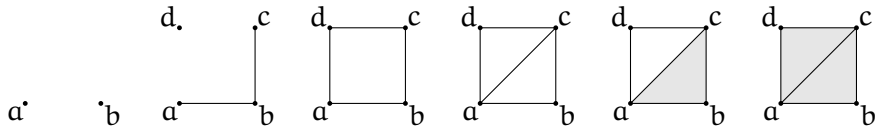
Example 75. Considered the following filtered complex:

Its homology groups in dimension 0 arise from taking the quotient of cycles Z_0 by boundnaries B_0. Let $F = \mathbb{Z}_2$, so that we can concentrate on the persistence part and not the correct signs. If we fix the basis of C_1 as (ab, bc, cd, ad, ac) and the basis of C_0 as (a, b, c, d), we get:

$$\partial_1 = \begin{bmatrix} t & 0 & 0 & t^2 & t^3 \\ t & t & 0 & 0 & 0 \\ 0 & 1 & t & 0 & t^2 \\ 0 & 0 & t & t & 0 \end{bmatrix}$$

[3]This can be generalised further to the notion of graded modules over graded rings, but we apply it only to this special case to ease explanation.

[4]This example has been described by Zomorodian and Carlsson[17].



(a) X^0 (b) X^1 (c) X^2 (d) X^3 (e) X^4 (f) X^5

Figure 4.1: Example of a filtered complex

The higher powers of t arise from the fact, that e.g. ac belongs to C^3, but a belongs to C^0. Hence, if we want to lift a to C^3, we need to multiply it by $t^{3-0} = t^3$. Similarly, c belongs to C^1, so if we want to lift it to C^3, we have to multiply it by $t^{3-1} = t^2$. Thus, the boundnary homomorphism maps ac to $t^3a + t^2c$ (we work in $\mathbb{Z}_2[t]$ in order not to be concerned with orientation, which could possibly hinder the ease of understanding).

We can therefore assign to every simplex s its **degree**: the smallest index i such that s appears in C^i. Similarly, we define the degree of a monomial in C_k: $\deg t^k f s = k + \deg s$ if $f \in F$, and s is a simplex. An element of C_k is called **homogeneous** iff it is the sum of monomials having the same degree.

If we fix any homogeneous bases for C_k and C_{k-1} (viz. every element of the basis is homogeneous), the matrix ∂_k will consist only of zeroes and powers of t, as above, possibly multiplied by base field elements. The degree of $\partial_k(i,j)$ is the difference between the degree of the j-th element of the basis of C_k and the degree of the i-th element of the basis of C_{k-1}.

Observation. The above property is preserved by every step of the algorithm shown in the previous section.

This allows us to refine the definition of invariant factor decomposition in the following way: the original exposition preserved only the structure of R-module, and not the degrees of elements. However, the observation above allows us to see that every summand R or $R/(\alpha_i)$ in Lemma 21 is actually shifted upwards by the degree of the corresponding generator (i.e. column), viz. it is equal to $t^{\deg g}R$ or $t^{\deg g}(R/(\alpha_i))$. This yields

Corollary 4. *In this case, we have the following degree-preserving isomorphism:*

$$H_n \simeq \bigoplus_i t^{\alpha_i} F[t] \oplus \bigoplus_i (t^{\beta_i} F[t])/(t^{\gamma_i})$$

4.4. Simplification of the algorithm

The following observation allows us to employ Algorithms 3, 4, and 5 from Chapter 2 almost directly, without having to employ the PID-related additions to the Gaussian elimination-like algorithms.

Observation. Sort any homogeneous basis of C_{k-1} in the order of descending degrees. Then every column of ∂_k consists of increasing degrees of powers of t (multiplied by elements from the field F), interspersed by zeroes. This property is preserved by every step of the column-echelon form reduction algorithm, and hence every division requested by it is possible.

Example 76. In the Example 75, fix the basis of C_1 as (ab, bc, cd, ad, ac) and the basis of C_0 as (d, c, b, a) (the latter ordered by decreasing degrees). Then:

$$\partial_1 = \begin{bmatrix} 0 & 0 & t & t & 0 \\ 0 & 1 & t & 0 & t^2 \\ t & t & 0 & 0 & 0 \\ t & 0 & 0 & t^2 & t^3 \end{bmatrix}$$

By applying the Algorithm 4 from Chapter 2, we get:

$$\tilde{\partial}_1 = \begin{bmatrix} \boxed{t} & 0 & 0 & 0 & 0 \\ t & \boxed{1} & 0 & 0 & 0 \\ 0 & t & \boxed{t} & 0 & 0 \\ 0 & 0 & t & 0 & 0 \end{bmatrix}$$

obtaining a new homogeneous basis for C_1, namely: (cd, bc, ab, z_1, z_2), where $z_1 = ad - cd - t \cdot bc - t \cdot ab$ and $z_2 = ac - t^2 \cdot bc - t^2 \cdot ab$. Therefore, (z_1, z_2) is a homogeneous basis for Z_1.

Moreover, we see that the resulting matrix still satisfies the degree condition, i.e. each column consists of increasing powers of t, possibly interspersed by zeroes. Hence, we can perform the ordinary row reduction, and obtain the Smith normal form — applying no PID-related modifications at all.

Example 77. In the Example 75, we obtain that the invariant factors of ∂_1 are $1, t, t$.

If row i in the column-echelon form of ∂_k contains a pivot t^r, then it contributes $F[t]/(t^r)$ to the invariant factor decomposition of H_{k-1}. However, this $F[t]/(t^r)$ is shifted upwards by the degree of z_i, where z_i is the i-th element of the homogeneous basis of Z_{k-1} used to express ∂_k. Hence, row i contributes $(t^{\deg z_i} F[t])/(t^{r+\deg z_i})$, i.e. there is a $(k-1)$-dimensional homology that appears in $C^{\deg z_i}$ and becomes bounding in $C^{r+\deg z_i}$.

On the other hand, if row i lacks a pivot element, then the cycle it represents never gets bounding, whence this row contributes $t^{\deg z_i} F[t]$ to the invariant factor decomposition.

Summing up, we obtain:

Lemma 24. *The above algorithm, given a homogeneous basis for Z_{k-1} and matrix ∂_k expressed with respect to the said basis and the standard basis of C_k, computes:*

- *the invariant factor decomposition of H_{k-1} (together with information which cycles from the given basis of Z_{k-1} correspond to which factors);*
- *a homogeneous basis for Z_k*

The only difference from the algorithms described in Chapter 2 is that the matrices M_n mentioned therein have entries from $F[t]$ instead of F and that we have to sort the basis $\mathfrak{B}_n$ in the order of decreasing degrees before performing the reduction. Furthermore, by noting down the exact pivot values we can recover the decomposition of H_n as

$$H_n = \bigoplus_i t^{\alpha_i} F[t] \oplus \bigoplus_i (t^{\beta_i} F[t])/(t^{\gamma_i})$$

Appendix A

Groups and vector spaces

This appendix serves as a collection of elementary definitions and facts (without proofs) relating to groups and vector spaces. It is meant as a quick refresher for a reader with little mathematical background.

Definition (Group)**.** A set G together with an operation $\cdot_G : G \times G \to G$ is a **group**[2] iff it satisfies the following conditions:

- $\cdot_G$ is associative, i.e. $(g_1 \cdot_G g_2) \cdot_G g_3 = g_1 \cdot_G (g_2 \cdot_G g_3)$ for all $g_1, g_2, g_3 \in G$;
- there exists an element $1_G \in G$, called the identity element, s.t. $1_G \cdot_G g = g \cdot_G 1_G = r$ for all $g \in G$ (note that such a 1_G is unique);
- for every $g_1 \in G$ there exists $g_2 \in G$ called the inverse of g_1 and denoted $g_1^{-1} := g_2$ s.t. $g_1 \cdot_G g_2 = 1_G = g_2 \cdot_G g_1$ (note that such a g_2 is unique);

Whenever it does not lead to confusion, the subscripts denoting which group the operations are caried out in will be omitted.

Definition (Commutative group)**.** A group G is **commutative** (or **abelian**) iff $g_1 \cdot_G g_2 = g_2 \cdot_G g_1$ for all $g_1, g_2 \in G$.

When dealing with groups that are not necessarily abelian the operation is usually written as $\cdot$, so when performing the operation on two elements g_1, g_2 we write $g_1 \cdot g_2$. Often we omit the operation symbol and simply concatenate the elements: $g_1 g_2$. This is the **multiplicative** notation. However, when the group is abelian and we wish to emphasize this fact, we prefer to use the $+$ symbol to denote the operation, writing expressions such as $g_1 + g_2$. We also denote the inverse by $-g$ instead of g^{-1}. This is the **additive** notation.

Example 78. The set of integers, $\mathbb{Z}$, together with the operation of addition, is an abelian group.

Example 79. By $\mathbb{Z}_n$ where n is a natural number we denote the set $\{0, \ldots, n-1\}$. This is an abelian group when considered with the operation of adding numbers modulo n.

Example 80. The set of real numbers, $\mathbb{R}$, together with the operation of addition, is an abelian group. However, when considered with the operation of multiplication, it is not a group: 0 has no inverse element. However, $\mathbb{R} \setminus \{0\}$ with multiplication is an abelian group.

Example 81. The unit circle considered as a subset of the complex plane, $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, is an abelian group with the operation of complex multiplication.

Example 82. Let X be a set. The set of all bijections from X to itself, with the operation of composition of functions, is a group. If X has 3 or more elements the group is nonabelian.

Definition (Field)**.** A set F together with two operations:

- $+_F : F \times F \to F$
- $\cdot_F : F \times F \to F$

is a **field**[2] iff it satisfies the following conditions:

- F with $+_F$ is a commutative group;
- $F \setminus \{0_F\}$ with $\cdot_F$ is a commutative group;
- $\cdot_F$ is distributive over $+_F$, i.e.:
  - $f_1 \cdot_F (f_2 +_F f_3) = (f_1 \cdot_F f_2) +_F (f_1 \cdot_F f_3)$ for all $f_1, f_2, f_3 \in F$;
  - $(f_1 +_F f_2) \cdot_F f_3 = (f_1 \cdot_F f_3) +_F (f_2 \cdot_F f_3)$ for all $f_1, f_2, f_3 \in F$.

Whenever it does not lead to confusion, the subscripts denoting which field the operations are caried out in will be omitted.

Example 83. The sets of rational numbers, real numbers, and complex numbers, denoted $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ respectively, are fields. These should be familiar to any reader who finished a basic linear algebra course.

Example 84. If p is a prime number, then $\mathbb{Z}_p$ is a field. Multiplication is defined as standard integer multiplication modulo p. What is not obvious is the existence of an inverse element for $n \in \mathbb{Z}_p$, $n \neq 0$. This follows from *Bézout's identity*: since n and p are relatively prime, there exist integers a, b such that $an + bp = 1$. Taking this equality modulo p we get that $an = 1$ in $\mathbb{Z}_p$.

Definition (Vector space)**.** Let $(F, +_F, \cdot_F)$ be a field. A set V together with two operations:

- $+_V : V \times V \to V$
- $\cdot_V : R \times V \to V$

is a **vector space**[2, 8] iff it satisfies the following conditions:

- V with $+_V$ is a commutative group;
- $f_1 \cdot_V (f_2 \cdot_V v) = (f_1 \cdot_F f_2) \cdot_V v$ for all $f_1, f_2 \in F$ and $v \in V$;
- $1_F \cdot_V v = v$ for all $v \in V$;
- $(f_1 +_F f_2) \cdot_V v = (f_1 \cdot_V v) +_V (f_2 \cdot_V v)$ for all $f_1, f_2 \in F$ and $v \in V$;
- $f \cdot_V (v_1 +_V v_2) = (r \cdot_V v_1) +_V (r \cdot_V v_2)$ for all $f \in F$ and $v_1, v_2 \in V$.

The elements of V are called **vectors** and the elements of F are called **scalars**. The operation $+_V$ is called addition and $\cdot_V$ is called multiplication by scalars.

Whenever it does not lead to confusion, the subscripts distinguishing between field and vector space operations will be omitted.

Example 85. If F is a field then F^n, the set of sequences $(f_1, \ldots, f_n)$ where $f_1, \ldots, f_n \in F$, is a vector space over F, with addition and multiplication by scalars performed coordinate-wise.

Example 86. If F is a field, a polynomial over F with variable x is an expression of the form $a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n$ where $a_i \in F$. The set of polynomials over F with variable x, denoted $F[x]$, is a vector space over F, with addition and multiplication by scalars defined in the obvious way.

Definition (Subspace)**.** Let F be a field and V a vector space over F. Subset $V' \subseteq V$ is a **subspace** of V iff it is a vector space when equipped with the inherited operations $+_V$, $\cdot_V$.

Definition (Homomorphism)**.** Let F be a field and V_1, V_2 vector spaces over F. A function $\phi : V_1 \to V_2$ is a **homomorphism** (equivalently a **linear map**) iff it preserves the structure of vector spaces, i.e.:

- $\phi(0_{V_1}) = 0_{V_2}$;
- $\phi(v +_{V_1} v') = \phi(v) +_{V_2} \phi(v')$ for all $v, v' \in V_1$;
- $\phi(fv) = f\phi(v)$ for all $f \in F$ and $v \in V_1$.

Definition (Kernel)**.** Let F be a field, V_1, V_2 vector spaces over F, and $\phi : V_1 \to V_2$ a homomorphism.

The set:

$$\ker \phi = \{v_1 \in V_1 : \phi(v_1) = 0_{V_2}\}$$

is called the **kernel** of ϕ and can easily be checked to be a subspace of V_1.

Definition (Image)**.** Let F be a field, V_1, V_2 vector spaces over F, and $\phi : V_1 \to V_2$ a homomorphism.

The set:

$$\operatorname{im} \phi = \{v_2 \in V_2 : \exists_{v_1 \in V_1} \phi(v_1) = v_2\}$$

is called the **image** of ϕ and can easily be checked to be a subspace of V_2.

Definition (Generating set)**.** Let V be a vector space over a field F. A set of vectors $S \subseteq V$ is a **generating set** for V (equivalently **generates** or **spans** V) if and only if every $v \in V$ can be expressed as a linear combination of vectors from S, viz. there exist $v_1, \ldots, v_n \in S$ and $f_1, \ldots, f_n \in F$ such that $v = f_1 v_1 + \cdots + f_n v_n$.

Definition (Linearly independent set)**.** Let V be a vector space over F. A set of vectors $S \subseteq V$ is **linearly independent** if and only if every linear combination of elements of this set over F which is 0 must be trivial, i.e. for every $v_1, \ldots, v_n \in S$ and $f_1, \ldots, f_n$, the following implication holds:

$$f_1 v_1 + f_2 v_2 + \ldots + f_n v_n = 0 \implies f_1 = f_2 = \ldots = f_n = 0$$

Definition (Basis)**.** Let V be a vector space over F. A set of vectors $\mathfrak{B} \subseteq V$ is a **basis** if and only if it is a linearly independent and spans V.

Example 87. In example 85 the set $(1,0,\ldots,0),(0,1,\ldots,0),(0,0,\ldots,1)$ is a basis for F^n.

Example 88. In example 86 the set $1, x, x^2, \ldots$ is a basis for $F[x]$.

Lemma 25. *Every vector space V has a basis. For vector spaces which lack a finite basis, this requires the axiom of choice[10].*

The cardinality of every basis of V is the same, and is called the ***dimension*** *of V.*

Lemma 26. *Let V be a vector space over F and $\mathfrak{B}$ be a subset of V. The following conditions are equivalent:*

1. *$\mathfrak{B}$ is a basis for V.*
2. *$\mathfrak{B}$ is a maximal linearly independent set in V (maximal with respect to inclusion).*
3. *$\mathfrak{B}$ is a minimal generating set in V (minimal with respect to inclusion).*
4. *For every $v \in V$ there exists a unique set of scalars f_b, one for each vector $b \in \mathfrak{B}$, such that all but a finite number of the f_b are 0 and $v = \sum_b f_b b$.*

Example 89 (Ordered basis)**.** Let V be a vector space over F. An ordered basis for V is a basis with a total order on its elements. If V has finite dimension, an ordered basis for V can be thought of as a sequence of vectors $(v_1,\ldots,v_n)$ such that the set $\{v_1,\ldots,v_n\}$ is a basis for V.

Definition (Coordinates)**.** Let $\mathfrak{B}$ be an ordered basis of a vector space V over F. For any vector $v \in V$, the unique set of scalars f_b for $b \in \mathfrak{B}$ from lemma 26, condition 4, associated to the basis $\mathfrak{B}$ and ordered correspondingly, is the set of **coordinates** for v. If $\mathfrak{B} = (b_1,\ldots,b_n)$ is finite, then the coordinates of v form a sequence $(f_1,\ldots,f_n)$ such that $v = \sum_{i=1}^{n} f_i b_i$.

Example 90. Let $F = \mathbb{R}$ and $V = F^3 = \mathbb{R}^3$. The vector $(1,2,3) \in V$ is equal to $1(1,0,0) + 2(0,1,0) + 3(0,0,1)$, so its coordinates in the ordered basis $((1,0,0),(0,1,0),(0,0,1))$ are $(1,2,3)$. On the other hand, its coordinates in the ordered basis $((1,0,0),(0,1,0),(0,1,1))$ are $(1,-1,3)$.

Notation. If V is a finite-dimensional vector space over F and $\mathfrak{B} = (b_1,\ldots,b_n)$ is an ordered basis for V, then the column vector

$$\begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix}_{\mathfrak{B}}$$

denotes the vector $v \in V$ given by the coordinates $(f_1,\ldots,f_n)$, viz. $v = \sum_{i=1}^{n} f_1 v_i$. If the basis is understood, we omit the subscript $\mathfrak{B}$ in the column vector.

Example 91. Let $V = \mathbb{R}^3$ over $\mathbb{R}$, $\mathfrak{B}_1 = ((1,0,0),(0,1,0),(0,0,1))$, $\mathfrak{B}_2 = ((1,0,0),(0,1,0),(0,1,1))$. Then for $v = (1,2,3) \in V$ we have

$$v = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}_{\mathfrak{B}_1} = \begin{bmatrix} 1 \\ -1 \\ 3 \end{bmatrix}_{\mathfrak{B}_2}.$$

Definition (Matrix of homomorphism)**.** Let $\varphi : V \to W$ be a homomorphism between finite-dimensional vector spaces V, W over F. Let $\mathfrak{A} = (a_1, \ldots, a_n)$, $\mathfrak{B} = (b_1, \ldots, b_m)$ be ordered bases of V, W respectively. Let $\varphi(a_i) = c_{1i}b_1 + \cdots + c_{mi}b_m$ for $i = 1, \ldots, n$, i.e. $c_{1i}, \ldots, c_{mi}$ are coordinates of $\varphi(a_i)$ in $\mathfrak{B}$. The matrix

$$\begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

is the **matrix of φ in the bases $\mathfrak{A}$, $\mathfrak{B}$**, denoted $M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}}$. We say that the i-th column of this matrix corresponds to the i-th vector of the basis $\mathfrak{A}$ for $i = 1, \ldots, n$ and the i-th row of this matrix corresponds to the i-th vector of the basis $\mathfrak{B}$ for $i = 1, \ldots, m$.

Example 92. Let $V = \mathbb{R}^2$, $\mathfrak{B} = ((1,0),(0,1))$. Let $\varphi : V \to V$ be given by $\varphi(x,y) = (x+y, 2x-y)$. Then

$$M(\varphi)^{\mathfrak{B}}_{\mathfrak{B}} = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}.$$

Lemma 27. *Let $\varphi : V \to W$ be a homomorphism between finite-dimensional vector spaces V, W over F. Let $\mathfrak{A} = (\alpha_1, \ldots, \alpha_n)$, $\mathfrak{B} = (\beta_1, \ldots, \beta_m)$ be bases of V, W respectively. Suppose that*

$$v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}_{\mathfrak{A}} \quad \text{and} \quad \varphi(v) = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}_{\mathfrak{B}}.$$

Then

$$\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}} \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

where $\cdot$ denotes matrix multiplication (by a column vector).

Lemma 28 (Matrix of composition)**.** *Let $\varphi : V \to W$, $\psi : W \to U$ be homomorphisms of vector spaces V, W, U over F. Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ be bases of V, W, U respectively. Then*

$$M(\psi \circ \varphi)^{\mathfrak{C}}_{\mathfrak{A}} = M(\psi)^{\mathfrak{C}}_{\mathfrak{B}} \cdot M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}}$$

where $\psi \circ \varphi : V \to U$ is the composition of ψ with φ and $\cdot$ denotes matrix multiplication.

Lemma 29 (Elementary operations)**.** *Let $\varphi : V \to W$ be a homomorphism between finite-dimensional vector spaces V, W over F. Let $\mathfrak{A} = (a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n)$, $\mathfrak{B} = (b_1, \ldots, b_k, \ldots, b_l, \ldots, b_m)$ be ordered bases of V, W respectively.*

Suppose

$$M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}} = \begin{bmatrix} c_1 & \ldots & c_i & \ldots & c_j & \ldots & c_n \end{bmatrix}$$

so that $c_1, \ldots, c_n$ are the columns of the matrix.

- *If $\mathfrak{A}' = (a_1, \ldots, a_j, \ldots, a_i, \ldots, a_n)$ (the i-th basis vector has been swapped with the j-th basis vector in the domain), then*

$$M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}'} = \begin{bmatrix} c_1 & \cdots & c_j & \cdots & c_i & \cdots & c_n \end{bmatrix},$$

i.e. the i-th column has been swapped with the j-th column;

- *if α is a scalar and $\mathfrak{A}' = (a_1, \ldots, \alpha a_i, \ldots, a_j, \ldots, a_n)$ (the i-th basis vector has been multiplied by α in the domain), then*

$$M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}'} = \begin{bmatrix} c_1 & \cdots & \alpha c_i & \cdots & c_j & \cdots & c_n \end{bmatrix},$$

  i.e. the i-th column has been multiplied by α;

- *if α is a scalar and $\mathfrak{A}' = (a_1, \ldots, a_i + \alpha a_j, \ldots, a_j, \ldots, a_n)$ (the j-th basis vector multiplied by α has been added to the i-th basis vector in the domain), then*

$$M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}'} = \begin{bmatrix} c_1 & \cdots & c_i + \alpha c_j & \cdots & c_j & \cdots & c_n \end{bmatrix},$$

  i.e. the j-th column multiplied by α has been added to the i-th column.

Now suppose

$$M(\varphi)^{\mathfrak{B}}_{\mathfrak{A}} = \begin{bmatrix} r_1 \\ \vdots \\ r_i \\ \vdots \\ r_j \\ \vdots \\ r_n \end{bmatrix}$$

so that $r_1, \ldots, r_n$ are the rows of the matrix.

- *If $\mathfrak{B}' = (b_1, \ldots, b_j, \ldots, b_i, \ldots, b_n)$ (the i-th basis vector has been swapped with the j-th basis vector in the codomain), then*

$$M(\varphi)^{\mathfrak{B}'}_{\mathfrak{A}} = \begin{bmatrix} r_1 \\ \vdots \\ r_j \\ \vdots \\ r_i \\ \vdots \\ r_n \end{bmatrix},$$

  i.e. the i-th row has been swapped with the j-th row;

- *if α is a scalar and $\mathfrak{B}' = (b_1, \ldots, \alpha b_i, \ldots, b_j, \ldots, b_n)$ (the i-th basis vector has been multiplied by α in the codomain), then*

$$M(\varphi)^{\mathfrak{B}'}_{\mathfrak{A}} = \begin{bmatrix} r_1 \\ \vdots \\ \alpha^{-1} r_i \\ \vdots \\ r_j \\ \vdots \\ r_n \end{bmatrix},$$

  i.e. the i-th row has been multiplied by α^{-1};

- *if α is a scalar and $\mathfrak{B}' = (b_1, \ldots, b_i + \alpha b_j, \ldots, b_j, \ldots, b_n)$ (the j-th basis vector multiplied by α has been added to the i-th basis vector in the codomain), then*

$$M(\varphi)_{\mathfrak{A}}^{\mathfrak{B}'} = \begin{bmatrix} r_1 \\ \vdots \\ r_i \\ \vdots \\ r_j - \alpha r_i \\ \vdots \\ r_n \end{bmatrix},$$

i.e. the i-th row multiplied by α has been subtracted from the j-th row. Notice the difference with the previous situation!

□

Construction of a vector space with a given basis.

Let S be a set and F be a field. There exists a vector space $F^{(S)}$ over F and a function $i : S \to F^{(S)}$ such that $\{i(s) : s \in S\}$ is a basis of $F^{(S)}$.

Indeed, let

$$F^{(S)} = \{f : S \to F \mid f(s) = 0 \text{ for all but a finite number of } s \in S\}.$$

This is a vector space over F: addition and multiplication by scalars is defined point-wise, i.e. for $f, f' \in F^{(S)}$ and $\alpha \in F$, $(f + f')(s) = f(s) + f'(s)$ and $(\alpha f)(s) = \alpha f(s)$ for $s \in S$. The zero element in $F^{(S)}$ is the constant 0 function.

Let $i : S \to F^{(S)}$ be given by

$$i(s)(s') = \begin{cases} 1 & \text{if } s = s' \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{i(s) : s \in S\}$ is a basis of $F^{(S)}$. Indeed, suppose that $s_1, \ldots, s_n$ are pairwise different and $\alpha_1 i(s_1) + \cdots + \alpha_n i(s_n) = 0$ for some $\alpha_1, \ldots, \alpha_n \in F$, where 0 denotes the constant 0 function . Then for each $j = 1, \ldots, n$ we have $0 = \alpha_1 i(s_1)(s_j) + \cdots + \alpha_n i(s_n)(s_j) = \alpha_j$ by the definition of i, which proves linear independence of $\{i(s) : s \in S\}$. Furthermore if $f \in F^{(S)}$, then $f = \sum_{s \in S} f(s) i(s)$ – this sum is a finite sum since f is nonzero only for a finite amount of $s \in S$. This proves that $\{i(s) : s \in S\}$ spans $F^{(S)}$.

Since i is an injection, we can use it to identify elements of S with their images under i, so instead of writing $i(s) \in F^{(S)}$ we simply write $s \in F^{(S)}$. Then elements of $F^{(S)}$ can be thought of as finite formal linear combinations of elements from S.

Appendix B

Authors' contribution

Kamil's contribution

Chapters 1 and 2, appendix.

Krzysztof's contribution

Chapters 3 and 4, appendix.

Bibliography

[1] Atiyah, M. F., and Macdonald, I. G. *Introduction to commutative algebra*. Addison-Wesley-Longman, 1969.

[2] Bourbaki, N. *Éléments de mathématique: algèbre*. Actualités scientifiques et industrielles. Hermann, 1939.

[3] Carlsson, G. Topology and data. *Bulletin of the American Mathematical Society 46*, 2 (2009), 255–308.

[4] Cohen-Steiner, D., Edelsbrunner, H., and Harer, J. Stability of persistence diagrams. *Discrete & Computational Geometry 37*, 1 (2007), 103–120.

[5] Croom, F. H. *Principles of topology*. Courier Dover Publications, 2016.

[6] Dantchev, S., and Ivrissimtzis, I. Efficient construction of the Čech complex. *Computers & Graphics 36*, 6 (2012), 708–713.

[7] Dydak, J., and Segal, J. *Shape theory: An introduction*, vol. 688. Springer, 2006.

[8] Grassmann, H. *Die lineale Ausdehnungslehre ein neuer Zweig der Mathematik: dargestellt und durch Anwendungen auf die übrigen Zweige der Mathematik, wie auch auf die Statik, Mechanik, die Lehre vom Magnetismus und die Krystallonomie erläutert*. His Die Wissenschaft der extensiven Grösse, oder die Ausdehnungslehre. O. Wigand, 1844.

[9] Hatcher, A. *Algebraic Topology*. Cambridge University Press, 2002.

[10] Jech, T. *Set theory*. Springer Science & Business Media, 2013.

[11] Larsson, T. Fast and tight fitting bounding spheres. In *SIGRAD 2008. The Annual SIGRAD Conference Special Theme: Interaction; November 27-28; 2008 Stockholm; Sweden* (2008), no. 034, Linköping University Electronic Press, pp. 27–30.

[12] Lee, J. *Introduction to topological manifolds*, vol. 940. Springer Science & Business Media, 2010.

[13] Lum, P. Y., Singh, G., Lehman, A., Ishkanov, T., Vejdemo-Johansson, M., Alagappan, M., Carlsson, J., and Carlsson, G. Extracting insights from the shape of complex data using topology. *Scientific reports 3* (2013), srep01236.

[14] Otter, N., Porter, M. A., Tillmann, U., Grindrod, P., and Harrington, H. A. A roadmap for the computation of persistent homology. *EPJ Data Science 6*, 1 (2017), 17.

[15] Steen, L. A., Seebach, J. A., and Steen, L. A. *Counterexamples in topology*, vol. 18. Springer, 1978.

[16] Zomorodian, A. Fast construction of the vietoris-rips complex. *Computers & Graphics 34*, 3 (2010), 263–271.

[17] Zomorodian, A., and Carlsson, G. Computing persistent homology. *Discrete & Computational Geometry 33*, 2 (2005), 249–274.