ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institute of Theoretical Computer Science
Patrick Schnider

Introduction to Topological Data Analysis **Scribe Notes 3** **HS22**

Scribe notes by Simon Weber. Please contact me for corrections.
Lecture date: March 2, 2023
Last update: Thursday 2nd March, 2023, 14:42

A brief recap of algebra

Definition 1. *A group* $(G, +)$ *is a set* G *together with a binary operation "+" such that*

1. $\forall a, b \in G$: $a + b \in G$
2. $\forall a, b, c \in G$: $(a + b) + c = a + (b + c)$ *(Associativity)*
3. $\exists 0 \in G$: $a + 0 = 0 + a = a \ \forall a \in G$
4. $\forall a \in G \exists -a \in G$: $a + (-a) = 0$

$(G, +)$ *is* abelian *if we also have*

5. $\forall a, b \in G$: $a + b = b + a$ *(Commutativity)*

Examples:

$(\mathbb{Z}, +)$ is a group (even an abelian one), but not $(\mathbb{N}, +)$.

The moves of a Rubik's cube also form a group (with the operation being concatenation), but not an abelian one.

Definition 2. *Let* $(G, +)$ *be a group.*
A subset $A \subseteq G$ *is a* generator *if every element of* G *can be written as a finite sum of elements of* A *and their inverses.*
A subset $B \subseteq G$ *is a* basis *if every element of* G *can be* uniquely *written as a finite sum of elements of* B *and their inverses (ignoring trivial cancellations, i.e.,* $a + c + (-c) + (-b) = a + (-b)$*).*
An abelian group that has a basis is called free.

Examples:

The six standard moves of the Rubik's cube (rotating the top, bottom, front, back, left, or right layer clockwise by 90) are a generator for the Rubik's cube moves.

$\{1\}$ is a basis of $(\mathbb{Z}, +)$.

Definition 3. *For some group* $(G, +)$*,* $H \subseteq G$ *is a* subgroup*, if* $(H, +)$ *is also a group.*

Example: The even integers (including 0) are a subgroup of $(\mathbb{Z}, +)$.

Definition 4. *Let* $H \subseteq G$ *be a subgroup of* $(G, +)$*, and* $a \in G$*.*
The left coset $a + H$ *is the set* $a + H := \{a + b \mid b \in H\}$*, and the* right coset $H + a := \{b + a \mid b \in H\}$*. If* G *is abelian,* $a + H = H + a$*, and they are simply called the* coset*.*
For G *abelian, the* quotient group of G by H*, denoted by* G/H*, is the group on cosets* $\{a + H, a \in G\}$ *with the operation* $\oplus$ *defined as* $(a + H) \oplus (b + H) = (a + b) + H$*,* $\forall a, b \in G$*.*

Examples:

Let $G = (\mathbb{Z}, +)$ and $H = n\mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$. Then, $G/H = \{0 + \mathbb{Z}, 1 + \mathbb{Z}, \dots, (n-1) + \mathbb{Z}\}$ is the group usually referred to as $\mathbb{Z}_n$, the group of modular arithmetic modulo n.

$\mathbb{R}/\mathbb{Z}$ is the circle group (the multiplicative group of all complex numbers of absolute value 1).

But if we say a group *is* another group, what exactly do we mean? We again define equivalences by the existence of certain maps between the groups.

Definition 5. *A map* $h : G \to H$ *between* $(G, +)$ *and* $(H, \star)$ *is a* homomorphism *if* $h(a + b) = h(a) \star h(b)$, $\forall a, b \in G$*.*
A bijective homomorphism is called an isomorphism*, and then we write* $G \cong H$ *and say that* G *and* H *are* isomorphic*.*

kernel $\ker h := \{a \in G \mid h(a) = 0\}$

image $\operatorname{im} h := \{b \in H \mid \exists a \in G \text{ with } h(a) = b\}$

cokernel $\operatorname{coker} h := H / \operatorname{im} h$

What are we assuming in our definition of the cokernel? For the definition of a quotient group to apply, we need the divisor group to be a subgroup of the dividend group. Luckily, the following lemma says that $\operatorname{im} h$ is always a subgroup of H.

Lemma 6. $\ker h$ *and* $\operatorname{im} h$ *are subgroups of* $(G, +)$ *and* $(H, \star)$*, respectively.*

Proof. We first prove this for $\ker h$.

1. $a, b \in \ker h \Rightarrow h(a) = h(b) = 0$. By definition of homomorphism, $h(a + b) = h(a) \star h(b) = 0 \star 0 = 0$, and thus by definition of $\ker h$, $a + b \in \ker h$. We conclude that $\ker h$ is closed under $+$.
2. Associativity follows from associativity of $+$ in G, since $\ker h \subseteq G$.
3. $\forall a \in G: \ h(0) \star h(a) = h(0 + a) = h(a)$, and thus $h(0) = 0$, from which $0 \in \ker h$ follows.

4. Let $a \in \ker h$. Then, $0 = h(0) = h(a - a) = h(a) \star h(-a) = 0 \star h(-a) = h(-a)$, and thus $-a \in \ker h$.

The proof for $\operatorname{im} h$ is left as an exercise. □

Definition 7. $(R, +, \cdot)$ *is a* ring, *if*

1. $(R, +)$ *is an abelian group.*
2. $\forall a, b, c \in R$*:*
   $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *and* *(Associativity of* $\cdot$*)*
   $a \cdot (b + c) = a \cdot b + a \cdot c,$
   $(b + c) \cdot a = b \cdot a + c \cdot a$ *(Distributivity)*
3. $\exists 1 \in R$*, such that* $a \cdot 1 = 1 \cdot a = a \; \forall a \in R$*.* *(Multiplicative identity)*

If $\cdot$ *is commutative, we say that* R *is* commutative*.*

Definition 8. *A commutative ring in which every non-zero element has a multiplicative inverse (*$\forall a \in R \setminus \{0\}, \exists b \in R : a \cdot b = 1$*) is called a* field*.*

Definition 9. *Given a ring* $(R, +, \cdot)$ *with multiplicative identity* 1*, an* R-module M *is an abelian group* $(M, \oplus)$ *with an operation* $\otimes : R \times M \to M$ *such that for all* $r, r' \in R$ *and* $x, y \in M$*, we have*

1. $r \otimes (x + y) = (r \otimes x) \oplus (r \otimes y)$
2. $(r + r') \otimes x = (r \otimes x) \oplus (r' \otimes x)$
3. $1 \otimes x = x$
4. $(r \cdot r') \otimes x = r \otimes (r' \otimes x)$

If R *is a field, the* R*-module is called a* vector space*.*

In the literature, we often use the same symbol $(\cdot)$ for both operations $\cdot$ and $\otimes$, and $+$ for both $+$ in R and $\oplus$ in M. For a vector space, this should feel quite normal, since for the vector space $\mathbb{R}^n$ (which is an $\mathbb{R}$-module), we also write $\cdot$ for multiplying scalars to both scalars and vectors, and $+$ for addition of both scalars and vectors.