Lecture 1: March 20, 2023

Lecturer: Ali Vakilian (notes based on notes from Madhur Tulsiani)

The primary goal of this course is to collect a set of basic mathematical tools which are often useful in various areas of computer science. We will mostly focus on linear algebra and probability, both their underlying theory and various applications. Please see the course webpage for a more detailed list of topics.

The course will be evaluated on the basis of the following:

- Homeworks: 60% (five homeworks worth 12% each)
- Midterm: 15%
- Final: 25%

1 Fields

A field, often denoted by $\mathbb{F}$, is simply a nonempty set with two associated operations $+$ and $\cdot$ mapping $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$, which satisfy:

- **commutativity**: $a + b = b + a$ and $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{F}$.
- **associativity**: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{F}$.
- **identity**: There exist elements $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathbb{F}$ such that $a + 0_{\mathbb{F}} = a$ and $a \cdot 1_{\mathbb{F}} = a$ for all $a \in \mathbb{F}$.
- **inverse**: For every $a \in \mathbb{F}$, there exists an element $(-a) \in \mathbb{F}$ such that $a + (-a) = 0_{\mathbb{F}}$. For every $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, there exists $a^{-1} \in \mathbb{F}$ such that $a \cdot a^{-1} = 1_{\mathbb{F}}$.
- **distributivity of multiplication over addition**: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{F}$.

Example 1.1 $\mathbb{Q}$, $\mathbb{R}$ *and* $\mathbb{C}$ *with the usual definitions of addition and multiplication are fields. But* $\mathbb{Z}$ *with the usual definitions is not (why?).*

Example 1.2 *Consider defining addition and multiplication on* $\mathbb{Q}^2$ *as*

$$(a,b) + (c,d) = (a+c, b+d) \qquad \text{and} \qquad (a,b)\cdot(c,d) = (ac+bd, ad+bc)\,.$$

These operations do not *define a field. While various properties of addition are indeed satisfied, inverses may not always exist for multiplication as defined above. Check that the multiplicative identity needs to be* $(1,0)$ *but then the element* $(1,-1)$ *has no multiplicative inverse.*

However, for any prime p*, the following operations* do *define a field*

$$(a,b) + (c,d) = (a+c, b+d) \qquad \text{and} \qquad (a,b)\cdot(c,d) = (ac+pbd, ad+bc)\,.$$

This is equivalent to taking $\mathbb{F} = \left\{a + b\sqrt{p} \mid a,b \in \mathbb{Q}\right\}$ *with the same notion of addition and multiplication as for real numbers. Alternatively, one can also define a field by taking* $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$ *(why?)*

Example 1.3 *For any prime* p*, the set* $\mathbb{F}_p = \{0,1,\ldots,p-1\}$ *(also denoted as GF(p)) is a field with addition and multiplication defined modulo* p*.*

2 Vector Spaces

A vector space V over a field $\mathbb{F}$ is a nonempty set with two associated operations $+ : V \times V \to V$ (vector addition) and $\cdot : \mathbb{F} \times V \to V$ (scalar multiplication) which satisfy:

- **commutatitivity of addition**: $v + w = w + v$ for all $v, w \in V$.
- **associativity of addition**: $u + (v + w) = (u + v) + w\ \forall u, v, w \in V$.
- **pseudo-associativity of scalar multiplication**: $a \cdot (b \cdot v) = (a \cdot b) \cdot v\ \forall a, b \in \mathbb{F}, v \in V$.
- **identity for vector addition**: There exists $0_V \in V$ such that for all $v \in V$, $v + 0_V = v$.
- **inverse for vector addition**:$\forall v \in V,\ \exists(-v) \in V$ such that $v + (-v) = 0_V$.
- **distributivity**: $a \cdot (v + w) = a \cdot v + a \cdot w$ and $(a + b) \cdot v = a \cdot v + b \cdot v$ for all $a, b \in \mathbb{F}$ and $v, w \in V$.
- **identity for scalar multiplication**: $1_{\mathbb{F}} \cdot v = v$ for all $v \in V$.

Definition 2.1 (Linear Dependence) *A set* $S \subseteq V$ *is* linearly dependent *if there exist distinct* $v_1, \ldots, v_n \in S$ *and* $a_1, \ldots, a_n \in \mathbb{F}$ *not all zero, such that* $\sum_{i=1}^n a_i \cdot v_i = 0_V$*. A set which is not linearly dependent is said to be* linearly independent.

Example 2.2 $\mathbb{R}$ *is a vector space over* $\mathbb{Q}$*.*

Example 2.3 *The set* $\left\{1, \sqrt{2}, \sqrt{3}\right\}$ *is linearly independent in the vector space* $\mathbb{R}$ *over the field* $\mathbb{Q}$.

Example 2.4 $\mathbb{R}[X]$ *is a vector space over* $\mathbb{R}$. *(This is the set of polynomials in X with real-valued coefficients).*

Example 2.5 $C([0,1], \mathbb{R}) = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$ *is a vector space over* $\mathbb{R}$.

Example 2.6 $\mathsf{Fib} = \left\{f \in \mathbb{R}^{\mathbb{N}} \mid f(n) = f(n-1) + f(n-2)\ \forall n \geq 2\right\}$ *is a vector space over* $\mathbb{R}$.

Proposition 2.7 *Let* $b_1, \ldots, b_n \in \mathbb{R}$ *be distinct and let* $g(x) = \prod_{i=1}^{n}(x - b_i)$. *Define*

$$f_i(x) = \frac{g(x)}{x - b_i} = \prod_{j \neq i}(x - b_j),$$

where we extend the function at point b_i *by continuity. Prove that* $f_1, \ldots, f_n$ *are linearly independent in the vector space* $\mathbb{R}[x]$ *over the field* $\mathbb{R}$.

Proof: First of all, 0_V is the zero polynomial. For contradiction, assume the f_i are linearly dependent, so there exists $a_1, ..., a_n$ not all zero such that $a_1 f_1(x) + ... + a_n f_n(x)$ is the zero polynomial (i.e., it equals 0 no matter what value is given for x). Let a_i be some nonzero coefficient (we are guaranteed there is at least one). If we feed in $x = b_i$, then all terms of the polynomial become 0 except for $a_i f_i(b_i)$. This term is non-zero because the b's are all distinct and $a_i \neq 0$. Contradiction. ∎

Example 2.8 *The set of functions*

$$S = \{1\} \cup \{\sin(kx) \mid k \in \mathbb{N}, k \geq 1\} \cup \{\cos(kx) \mid k \in \mathbb{N}, k \geq 1\},$$

is linearly independent in the vector space of continuous real-valued functions over $\mathbb{R}$.

3 Linear Independence and Bases

Definition 3.1 *Given a set* $S \subseteq V$, *we define its* span *as*

$$\text{Span}(S) = \left\{\sum_{i=1}^{n} a_i \cdot v_i \mid a_1, \ldots, a_n \in \mathbb{F}, v_1, \ldots, v_n \in S, n \in \mathbb{N}\right\}.$$

Note that we only include finite *linear combinations.*

Remark 3.2 *Note that the definition above and the previous definitions of linear dependence and independence, all involve only finite linear combinations of the elements. Infinite sums cannot be said to be equal to a given element of the vector space without a notion of convergence or distance, which is not necessarily present in an abstract vector space.*

Definition 3.3 (Basis) *A set B is said to be a basis for the vector space V if B is linearly independent and* $\text{Span}(B) = V$.

It is often useful to use the following alternate characterization of a basis.

Proposition 3.4 *Let V be a vector space and let $B \subseteq V$ be a maximal linearly independent set i.e., B is linearly independent and for all $v \in V \setminus B$, $B \cup \{v\}$ is linearly dependent. Then B is a basis.*

In particular, if B satisfies Definition 3.3 then it satisfies Proposition 3.4 since any $v \in V \setminus B$ can be written as a finite linear combination of vectors in B. In the other direction, if B satisfies Proposition 3.4 then it satisfies Definition 3.3 because if it didn't, then $B \cup \{v\}$ would be linearly independent for any $v \in V \setminus Span(B)$.

The following proposition and its proof will be very useful.

Proposition 3.5 (Steinitz exchange principle) *Let $\{v_1, \ldots, v_k\}$ be linearly independent and $\{v_1, \ldots, v_k\} \subseteq \text{Span}(\{w_1, \ldots, w_n\})$. Then $\forall i \in [k]$ $\exists j \in [n]$ such that $w_j \notin \{v_1, \ldots, v_k\} \setminus \{v_i\}$ and $\{v_1, \ldots, v_k\} \setminus \{v_i\} \cup \{w_j\}$ is linearly independent.*

Proof: Assume not. Then, there exists $i \in [k]$ such that for all w_j, either $w_j \in \{v_1, \ldots, v_k\} \setminus \{v_i\}$ or $\{v_1, \ldots, v_k\} \setminus \{v_i\} \cup \{w_j\}$ is linearly dependent. Note that this means we cannot have $v_i \in \{w_1, \ldots, w_n\}$. (In that case, $w_j = v_i$ would fail.)

The above gives that for all $j \in [n]$, $w_j \in \text{Span}(\{v_1, \ldots, v_k\} \setminus \{v_i\})$. However, this implies

$$\{v_1, \ldots, v_k\} \subseteq \text{Span}(\{w_1, \ldots, w_n\}) \subseteq \text{Span}(\{v_1, \ldots, v_k\} \setminus \{v_i\}) ,$$

which is a contradiction. ■

3.1 Finitely generated spaces

A vector space V is said to be finitely generated if there exists a finite set T such that $\text{Span}(T) = V$. The following is an easy corollary of the Steinitz exchange principle.

Corollary 3.6 *Let $B_1 = \{v_1, \ldots, v_k\}$ and $B_2 = \{w_1, \ldots, w_n\}$ be two bases of a finitely generated vector space V. Then, they must have the same size i.e., $k = n$.*

Proof Sketch: Use the exchange principle to successively replace elements from B_1 by those from B_2. Since we need to replace k elements and no element of B_2 can be used twice (why?) we must have $k \leq n$. By symmetry, we must also have $n \leq k$. $\square$

The above proves that all bases of a finitely generated vector space (if they exist!) have the same size. It is easy to see that a similar argument can also be used to prove that a basis must always exist.

Exercise 3.7 *Prove that a finitely generated vector space with a generating set T has a basis (which is a subset of the generating set T).*

The above argument can also be used to prove the following statement.

Exercise 3.8 *Let V be a finitely generated vector space and let $S \subseteq V$ be any linearly independent set. Then S can be "extended" to a basis of V i.e., there exists a basis B such that $S \subseteq B$.*

The size of all bases of a vector space is called the dimension of the vector space, denoted as $\dim(V)$. Using the above arguments, it is also easy to check that *any* linearly independent set of the right size must be a basis.

Exercise 3.9 *Let V be a finitely generated vector space and let S be a linearly independent set with $|S| = \dim(V)$. Prove that S must be a basis of V.*