TTIC 31150/CMSC 31150
Mathematical Toolkit (Spring 2023)

Avrim Blum and Ali Vakilian

TAs: Xiao Luo and Kumar Kshitij Patel

Lecture 1: Fields and Vector Spaces

Welcome to Mathematical Toolkit

Course goal: develop basic mathematical tools useful in various areas of CS. Focus on linear algebra and probability: both underlying theory and various applications.

- Canvas site and webpage
- Lecture notes on webpage
- Homework 1 out today, due March 29.
- Optional but recommended discussion session [Fri 2:00-2:50 in TTIC 529]
- Coursework: 5 homeworks (12% each, 60% total), 1 midterm (15%), 1 final (25%).

Let's get started!

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*

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

Field? No.

Fact. If $a \cdot b = 0_{\mathbb{F}}$, then at least one of a or b is equal to $0_{\mathbb{F}}$

- Additive identity: $0_{\mathbb{Q}^2} = (0,0)$.
- $(1,-1)\cdot(1,1) = (0,0)$

Another Argument: Multiplicative identity must be (1,0), but then no inverse for (1,-1).

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

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

Field? No. Multiplicative identity must be (1,0), but then no inverse for (1,-1).

However, for any prime p*, the following operations* do *define a field* [Will verify on homework]

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

This is equivalent to taking $\mathbb{F}=\{a+b\sqrt{p} \mid a,b\in\mathbb{Q}\}$ *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.

[Equivalently, one can be written as a linear combination of the others]

Let's consider $\mathbb{R}^2$

- Give an example of 3 vectors that are linearly dependent.

- Give an example of 2 vectors that are linearly independent.

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 $\mathsf{C}([0,1], \mathbb{R}) = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$ *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 $b_1, \dots, b_n \in \mathbb{R}$ 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 $f_1, \dots, f_n$ 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. ■

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.*

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.*

- If B satisfies 3.3 then also satisfies 3.4:
- If B satisfies 3.4 then also satisfies 3.3:

Proposition 3.5 (Steinitz exchange principle) *Let* $\{v_1, \ldots, v_k\}$ *be linearly independent and* $\{v_1, \ldots, v_k\} \subseteq \operatorname{Span}(\{w_1, \ldots, w_n\})$. *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 $j \in [n], w_j \in \operatorname{Span}(\{v_1, \ldots, v_k\} \setminus \{v_i\})$. However, this implies

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

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., $k = n$.*

- Use Exchange principle to successively replace v's with w's.
- Never use same w twice (since always linearly indep of current set).
- End with a subset of B_2 which means $k \leq n$.
- Go in other direction to get $n \leq k$.

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., $k = n$.*

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).*

- If not linearly independent, pick some element that can be written as a linear combination of the others and remove it. Repeat.

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., $k = n$.*

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 $S \subseteq B$.*

- Recall Proposition 3.4: a basis is a maximal linearly independent set.
- If S is not a basis, there must exist some $v \in V \setminus S$ such that $S \cup \{v\}$ is linearly independent. Add it into S and repeat.

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., $k = n$.*

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.*

- If not, you could grow it using Prop 3.4, and get two bases of different size.