

Mathematics Bootcamp

Department of Statistical Sciences, University of Toronto

Emma Kroell

Last updated: May 12, 2022

Contents

Preface	3
1 Review of proof techniques with examples from algebra and analysis	4
1.1 Propositional logic	4
1.1.1 Truth values	4
1.1.2 Logical equivalence	4
1.2 Types of proof	5
1.2.1 Direct Proof	5
1.2.2 Proof by contrapositive	5
1.2.3 Proof by contradiction	5
1.2.4 Summary	6
1.2.5 Induction	6
1.3 Exercises	6
1.3.1 Axioms of a field	7
1.3.2 Exercises	7
1.4 References	7
1.4.1 Exercises	7
2 Linear Algebra	8
2.1 Vector spaces	8
2.1.1 Axioms of a vector space	8
2.1.2 Subspaces	8
2.1.3 Exercises	9
2.2 Linear (in)dependence and bases	9
2.3 Exercises	10
2.4 Linear transformations	10
2.5 Determinants	10
2.6 Spectral theory	10
2.7 Inner product spaces	11
2.8 Matrix decomposition	11
2.9 References	11
3 Set theory	11
4 Metric spaces and sequences	11
5 Topology	11
6 Differentiation and integration	11

Preface

These notes were prepared for the inaugural Department of Statistical Sciences Graduate Student Bootcamp at the University of Toronto, which is to be held in July 2022.

References are provided for each section. All references are freely available online, though some may require a University of Toronto library log-in to access.

1 Review of proof techniques with examples from algebra and analysis

1.1 Propositional logic

Propositions are statements that could be true or false. They have a corresponding **truth value**. We will use capital letters to denote propositions.

ex. “ n is odd” and “ n is divisible by 2” are propositions .

Let’s call them P and Q . Whether they are true or not (i.e. their truth value) depends on what n is.

We can negate statements: $\neg P$ is the statement “ n is not odd”

We can combine statements:

- $P \wedge Q$ is the statement “ n is odd and n is divisible by 2”.
- $P \vee Q$ is the statement “ n is odd or n is divisible by 2”. We always assume the inclusive or unless specifically stated otherwise.

Examples:

- If it’s not raining, I won’t bring my umbrella.
- I’m a banana or Toronto is in Canada.
- If I pass this exam, I’ll be both happy and surprised.

1.1.1 Truth values

Example 1.1. Write the following using propositional logic *If it is snowing, then it is cold out.*

It is snowing.

Therefore, it is cold out.

Solution. $P \implies Q$

P

Conclusion: Q



To examine if statement is true or not, we use a truth table

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

1.1.2 Logical equivalence

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg P$	$\neg P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

What is $\neg(P \implies Q)$?

1.2 Types of proof

- Direct
- Contradiction
- Contrapositive
- Induction

1.2.1 Direct Proof

Approach: Use the definition and known results.

Example 1.2. *The product of an even number with another integer is even.*

Approach: use the definition of even.

Definition 1.3. *We say that an integer n is **even** if there exists another integer j such that $n = 2j$. We say that an integer n is **odd** if there exists another integer j such that $n = 2j + 1$.*

Proof. Let $n, m \in \mathbb{Z}$, with n even. By definition, there $\exists j \in \mathbb{Z}$ such that $n = 2j$. Then

$$nm = (2j)m = 2(jm)$$

Therefore nm is even by definition. □

1.2.2 Proof by contrapositive

Example 1.4. *If an integer squared is even, then the integer is itself even.*

How would you approach this proof?

$$P \implies Q \qquad \neg P \implies \neg Q$$

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg P$	$\neg Q$	$\neg Q \implies \neg P$
T	T	F	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Proof. We prove the contrapositive. Let n be odd. Then there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. We compute

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus n^2 is odd. □

1.2.3 Proof by contradiction

Example 1.5. *The sum of a rational number and an irrational number is irrational.*

Proof. Let $q \in \mathbb{Q}$ and $r \in \mathbb{R} \setminus \mathbb{Q}$. Suppose in order to derive a contradiction that their sum is rational, i.e. $r + q = s$ where $s \in \mathbb{Q}$. But then $r = s - q \in \mathbb{Q}$. Contradiction. □

1.2.4 Summary

In sum, to prove $P \implies Q$:

- Direct proof: assume P , prove Q
- Proof by contrapositive: assume $\neg Q$, prove $\neg P$
- Proof by contradiction: assume $P \wedge \neg Q$ and derive something that is impossible

1.2.5 Induction

Theorem 1.6 (Well-ordering principle for \mathbb{N}). *Every nonempty set of natural numbers has a least element.*

Theorem 1.7 (Principle of mathematical induction). *Let n_0 be a non-negative integer. Suppose P is a property such that*

1. (base case) $P(n_0)$ is true
2. (induction step) For every integer $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for every integer $n \geq n_0$

Note: Principle of strong mathematical induction: For every integer $k \geq n_0$, if $P(n)$ is true for every $n = n_0, \dots, k$, then $P(k+1)$ is true.

Example 1.8. $n! > 2^n$ if $n \geq 4$.

Proof. We prove this by induction on n .

Base case: Let $n = 4$. Then $n! = 4! = 24 > 16 = 2^4$.

Inductive hypothesis: Suppose for some $k \geq 4$, $k! > 2^k$.

Then

$$(k+1)! = (k+1)k! > (k+1)2^k > 2(2^k) = 2^{k+1}.$$

□

Example 1.9. *Every integer $n \geq 2$ can be written as the product of primes.*

Proof. We prove this by induction on n .

Base case: $n = 2$ is prime.

Inductive hypothesis: Suppose for some $k \geq 2$ that one can write every integer n such that $2 \leq n \leq k$ as a product of primes.

We must show that we can write $k+1$ as a product of primes.

First, if $k+1$ is prime then we are done.

Otherwise, if $k+1$ is not prime, by definition it can be written as a product of some integers a, b such that $1 < a, b < k+1$. By the induction hypothesis, a and b can both be written as products of primes, so we are done. □

1.3 Exercises

1. Prove De Morgan's Laws: $\neg(P \wedge Q) = \neg P \vee \neg Q$ and $\neg(P \vee Q) = \neg P \wedge \neg Q$.
2. Prove the Fundamental Theorem of Arithmetic, that every integer $n \geq 2$ has a unique prime factorization (i.e. prove that the prime factorization from the last proof is unique).

1.3.1 Axioms of a field

- (A1) *Commutativity in addition:* $x + y = y + x$
- (A2) *Commutativity in multiplication:* $x \times y = y \times x$
- (B1) *Associativity in addition:* $x + (y + z) = (x + y) + z$
- (B2) *Associativity in multiplication:* $x \times (y \times z) = (x \times y) \times z$
- (C) *Distributivity:* $x \times (y + z) = x \times y + x \times z$
- (D1) *Existence of a neutral element, addition:* There exists a number 0 such that $x + 0 = x$ for every x .
- (D2) *Existence of a neutral element, multiplication:* There exists a number 1 such that $x \times 1 = x$ for every x .
- (E1) *Existence of an inverse, addition:* For each number x , there exists a number $-x$ such that $x + (-x) = 0$.
- (E2) *Existence of an inverse, multiplication:* For each number $x \neq 0$, there exists a number $1/x$ such that $x \times 1/x = 1$.

[EK: This section to be worked on later]

1.3.2 Exercises

1. For any $a, b \neq 0$, $1/(ab) = 1/a \times 1/b$
 2. For $a > 0$, $1/(-a) = -1/a$.
 3. For $a, b \neq 0$, $1/(a/b) = b/a$
- (A1) *Commutativity in addition:* $x + y = y + x$
 - (A2) *Commutativity in multiplication:* $x \times y = y \times x$
 - (B1) *Associativity in addition:* $x + (y + z) = (x + y) + z$
 - (B2) *Associativity in multiplication:* $x \times (y \times z) = (x \times y) \times z$
 - (C) *Distributivity:* $x \times (y + z) = x \times y + x \times z$
 - (D1) *Existence of a neutral element, addition:* There exists a number 0 such that $x + 0 = x$ for every x .
 - (D2) *Existence of a neutral element, multiplication:* There exists a number 1 such that $x \times 1 = x$ for every x .
 - (E1) *Existence of an inverse, addition:* For each number x , there exists a number $-x$ such that $x + (-x) = 0$.
 - (E2) *Existence of an inverse, multiplication:* For each number $x \neq 0$, there exists a number $1/x$ such that $x \times 1/x = 1$.

1.4 References

A good resource for this is Gerstein (2012). Lakins (2016) is also a great resource, but sadly it is not freely available online or at U of T.

1.4.1 Exercises

1. For any $a, b \neq 0$, $1/(ab) = 1/a \times 1/b$
2. For $a > 0$, $1/(-a) = -1/a$.
3. For $a, b \neq 0$, $1/(a/b) = b/a$

2 Linear Algebra

2.1 Vector spaces

2.1.1 Axioms of a vector space

Let V be a set and let \mathbb{F} be a field.

Definition 2.1. We call V a **vector space** if the following hold:

Addition:

- (A) Commutativity in addition: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ for all $\mathbf{u}, \mathbf{v} \in V$
- (B) Associativity in addition: $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$
- (C) Existence of a neutral element, addition: There exists a vector $\mathbf{0}$ such that for any $\mathbf{v} \in V$, $\mathbf{0} + \mathbf{v} = \mathbf{v}$
- (D) Additive inverse: For every $\mathbf{v} \in V$, there exists another vector, which we denote $-\mathbf{v}$, such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.

Multiplication by a scalar:

- (E) Existence of a neutral element, multiplication: For any $\mathbf{v} \in V$, $1 \times \mathbf{v} = \mathbf{v}$
- (F) Associativity in multiplication: Let $\alpha, \beta \in \mathbb{F}$. For any $\mathbf{v} \in V$, $(\alpha\beta)\mathbf{v} = \alpha(\beta\mathbf{v})$

Associativity:

- (G) Let $\alpha \in \mathbb{F}, \mathbf{u}, \mathbf{v} \in V$. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \beta\mathbf{v}$.
- (H) Let $\alpha, \beta \in \mathbb{F}, \mathbf{v} \in V$. $(\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}$.

Elements of the vector space are called vectors.

Most often we will assume $\mathbb{F} = \mathbb{C}$ or \mathbb{R} .

Examples of vector spaces: \mathbb{R}^n , \mathbb{C}^n , $M_{m \times n}$ (matrices of size $m \times n$), \mathbb{P}_n (polynomials of degree n , $p(x) = a_0 + a_1x + \dots + a_nx^n$).

Lemma 2.2. For every $\mathbf{v} \in V$, we have $-\mathbf{v} = (-1) \times \mathbf{v}$.

Proof. Our goal is to show that $(-1) \times \mathbf{v}$ is the additive inverse of \mathbf{v} . We show this as follows:

$$\mathbf{v} + (-1) \times \mathbf{v} = \mathbf{v} \times (1 + (-1)) = \mathbf{v} \times 0 = \mathbf{0}$$

The last step uses Exercise 2.8. **[EK: Do by hand in class]** □

2.1.2 Subspaces

Definition 2.3. A subset U of V is called a **subspace** of V if U is also a vector space (using the same addition and scalar multiplication as on V).

Proposition 2.4. A subset U of V is a subspace of V if and only if U satisfies the following three conditions:

1. $\mathbf{0} \in U$
2. Closed under addition: $\mathbf{u}, \mathbf{w} \in U$ implies $\mathbf{u} + \mathbf{w} \in U$
3. Closed under scalar multiplication: $\alpha \in \mathbb{F}$ and $\mathbf{u} \in U$ implies $\alpha\mathbf{u} \in U$

Proof. \Rightarrow If U is a subspace of V , then U satisfies these 3 properties by Definition 2.1.

\Leftarrow Suppose U satisfies the given 3 conditions. Then for any $\mathbf{v} \in U$, there must exist $-\mathbf{v} \in U$ by property 3, since $-\mathbf{v} = (-1) \times \mathbf{v}$ by Lemma 2.2 (property D). Property 1 assures property C. Properties 2 and 3, and the fact that $U \subset V$, assure the remaining properties hold. □

This characterisation allows us to easily show that the intersection of subspaces is again a subspace.

Proposition 2.5. *Let V be a vector space and let $U_1, U_2 \subseteq V$ be subspaces. Then $U_1 \cap U_2$ is also a subspace of V .*

Proof. We use the characterization in Proposition 2.4. First, since $\mathbf{0} \in U_1$ and $\mathbf{0} \in U_2$, we have $\mathbf{0} \in U_1 \cap U_2$. Second, for $\mathbf{u}, \mathbf{v} \in U_1 \cap U_2$, since in particular $\mathbf{u}, \mathbf{v} \in U_1$ and $\mathbf{u}, \mathbf{v} \in U_2$ and U_1, U_2 are subspaces, $\mathbf{u} + \mathbf{v} \in U_1$ and $\mathbf{u} + \mathbf{v} \in U_2$. Thus, $\mathbf{u} + \mathbf{v} \in U_1 \cap U_2$. Similarly, one shows $\alpha \mathbf{u} \in U_1 \cap U_2$ for $\alpha \in \mathbb{F}$. \square

On the contrary the union of two subspaces is not a subspace in general (see Exercise 2.12). However, the next definition introduces the smallest subspace containing the union.

Definition 2.6. *Suppose U_1, \dots, U_m are subsets of V . The sum of U_1, \dots, U_m , denoted $U_1 + \dots + U_m$, is the set of all possible sums of elements of U_1, \dots, U_m . More precisely,*

$$U_1 + \dots + U_m = \{\mathbf{u}_1 + \dots + \mathbf{u}_m : \mathbf{u}_1 \in U_1, \dots, \mathbf{u}_m \in U_m\}$$

Proposition 2.7. *Suppose U_1, \dots, U_m are subspaces of V . Then $U_1 + \dots + U_m$ is the smallest subspace of V containing U_1, \dots, U_m .*

2.1.3 Exercises

Exercise 2.8 (1.1.7 in Treil 2017). Show that $0\mathbf{v} = \mathbf{0}$ for $\mathbf{v} \in V$.

Exercise 2.9 (1.B.1 in Axler 2015). Show that $-(-v) = v$ for $\mathbf{v} \in V$.

Exercise 2.10 (1.B.2 in Axler 2015). Suppose that $\alpha \in \mathbb{F}, \mathbf{v} \in V$, and $\alpha \mathbf{v} = \mathbf{0}$. Prove that $\alpha = 0$ or $\mathbf{v} = \mathbf{0}$.

Exercise 2.11 (1.B.4 in Axler 2015). Why is the empty space not a vector space?

Exercise 2.12 (7.4.1 in Treil 2017). Let U_1 and U_2 be subspaces of a vector space V . Prove that $U_1 \cup U_2$ is a subspace of V if and only if $U_1 \subseteq U_2$ or $U_2 \subseteq U_1$.

2.2 Linear (in)dependence and bases

Definition 2.13. *A linear combination of vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ of vectors in V is a vector of the form*

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n = \sum_{k=1}^n \alpha_k \mathbf{v}_k$$

where $\alpha_1, \dots, \alpha_n \in \mathbb{F}$.

Definition 2.14. *The set of all linear combinations of a list of vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ in V is called the **span** of $\mathbf{v}_1, \dots, \mathbf{v}_n$, denoted $\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. In other words,*

$$\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \{\alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n : \alpha_1, \dots, \alpha_n \in \mathbb{F}\}$$

The span of the empty list is defined to be $\{\mathbf{0}\}$.

Definition 2.15. *A system of vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ is called a **basis** (for the vector space V) if any vector $\mathbf{v} \in V$ admits a unique representation as a linear combination*

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n = \sum_{k=1}^n \alpha_k \mathbf{v}_k$$

In undergrad, you likely thought about this as: the equation $\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$, where the α_i are unknown, has a unique solution.

Example of bases:

For \mathbb{R}^n : $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \dots, 0)$, \dots , $\mathbf{e}_n = (0, \dots, 0, 1)$

For \mathbb{P}^n : $1, x, x^2, \dots, x^n$

Definition 2.16. *The linear combination $\alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$ is called **trivial** if $\alpha_k = 0$ for every k .*

Proposition 2.17. *A system of vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ is a basis if and only if it is linearly independent and complete (generating).*

[EK: Proof done by hand]

2.3 Exercises

From Harvard: Exercise: Suppose v_1, v_2, v_3, v_4 (a) spans V and (b) is linearly independent. Prove that the list

$$v_1 - v_2, v_2 - v_3, v_3 - v_4, v_4$$

also (a) spans V and (b) is linearly independent.

Exercise: Suppose v_1, \dots, v_m is linearly independent in V and $w \in V$. Prove that if $v_1 + w, \dots, v_m + w$ is linearly dependent, then $w \in \text{span}(v_1, \dots, v_m)$.

Exercise: Suppose that v_1, \dots, v_m is linearly independent in V and $w \in V$. Show that v_1, \dots, v_m, w is linearly independent if and only if

$$w \notin \text{span}(v_1, \dots, v_m)$$

onExercises Exercise: Suppose v_1, v_2, v_3, v_4 (a) spans V and (b) is linearly independent. Prove that the list

$$v_1 - v_2, v_2 - v_3, v_3 - v_4, v_4$$

also (a) spans V and (b) is linearly independent.

Exercise: Suppose v_1, \dots, v_m is linearly independent in V and $w \in V$. Prove that if $v_1 + w, \dots, v_m + w$ is linearly dependent, then $w \in \text{span}(v_1, \dots, v_m)$.

Exercise: Suppose that v_1, \dots, v_m is linearly independent in V and $w \in V$. Show that v_1, \dots, v_m, w is linearly independent if and only if

$$w \notin \text{span}(v_1, \dots, v_m)$$

[EK: Add a few from books]

2.4 Linear transformations

Definition 2.18. A **transformation** T from domain X to codomain Y is a rule that assigns an output $y = T(x) \in Y$ to each input $x \in X$

Definition 2.19. A transformation from a vector space U to a vector space V is **linear** if

$$T(\alpha \mathbf{u} + \beta \mathbf{v}) = \alpha T(\mathbf{u}) + \beta T(\mathbf{v}) \quad \text{for any } \mathbf{u}, \mathbf{v} \in V, \alpha, \beta \in \mathbb{F}$$

Examples: differentiation, rotation of vectors, reflection of vectors

[EK: transpose, adjoint]

2.5 Determinants

2.6 Spectral theory

Let $T: V \rightarrow V$ be a linear map, where V is a vector space. We would like to describe the action of this linear map in a particularly nice way. For example, if there exists a basis $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ of V such that $T\mathbf{v}_i = \alpha_i \mathbf{v}_i$ where $\alpha_i \in \mathbb{F}$ for $i = 1, \dots, n$, then T acts on this particular basis merely by scaling the basis vectors. If we look at the matrix of T with respect to this basis, T is a diagonal matrix with α_i in the diagonal.

Definition 2.20. Let V be a vector space. Given a linear map $T: V \rightarrow V$ and $\alpha \in \mathbb{F}$, α is called an **eigenvalue** of T if there exists a non-zero vector $\mathbf{v} \in V \setminus \{\mathbf{0}\}$ such that $T\mathbf{v} = \alpha \mathbf{v}$. We call such \mathbf{v} an **eigenvector** of T with eigenvalue α .

Note that $T\mathbf{v} = \alpha \mathbf{v}$ can be rewritten as $(T - \alpha I)\mathbf{v} = \mathbf{0}$. Thus, if α is an eigenvalue, the map $T - \alpha I$ is not invertible, since it must have non-trivial kernel. Using the known characterizations of invertability, this gives the following characterization for eigenvalues.

Theorem 2.21. Let V be a vector space and $T: V \rightarrow V$ be a linear map. The following are equivalent

1. $\alpha \in \mathbb{F}$ is an eigenvalue of T ,

2. $(T - \alpha I)\mathbf{x} = 0$ has a non-trivial solution,

3. $\det(T - \alpha I) = 0$.

Note that the last part is to be understood as the determinant of a matrix description of T with respect to a basis of V . We call the polynomial $p_A(\alpha) = \det(T - \alpha I)$ characteristic polynomial of T . Hence, the eigenvalues of T are the zeros of the characteristic polynomial. Recall that basis transformations can be expressed as invertible matrices, thus this is well-defined, since the characteristic polynomial and therefore the eigenvalues are independent of the choice of basis. We will now examine when there exists a basis of eigenvectors.

2.7 Inner product spaces

2.8 Matrix decomposition

2.9 References

The following texts:

Linear Algebra Done Right Axler 2015

Linear Algebra Done Wrong Treil 2017

3 Set theory

4 Metric spaces and sequences

5 Topology

6 Differentiation and integration

7 Multivariable calculus

References

- Axler, Sheldon (2015). *Linear Algebra Done Right*. 3rd ed. Undergraduate Texts in Mathematics. Springer.
URL: <https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/978-3-319-11080-6>.
- Gerstein, Larry J. (2012). *Introduction to Mathematical Structures and Proofs*. Undergraduate Texts in Mathematics. URL: <https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/978-1-4614-4265-31>.
- Lakins, Tamara J. (2016). *The Tools of Mathematical Reasoning*. Pure and Applied Undergraduate Texts.
- Treil, Sergei (2017). *Linear Algebra Done Wrong*. URL: <https://www.math.brown.edu/streil/papers/LADW/LADW.html>.