Learning Uni Maths

gispisquared

If only I had the theorems! Then I should find the proofs easily enough.

Bernhard Riemann

Contents

CHAPTER 1

Set Theory

AXIOM 1 (Existence). *There exists a set.*

REMARK 2. This is implied by the Axiom of Infinity; however, we include it here so that we may define the empty set.

DEFINITION 3. A *sentence* is made by combining assertions of belonging (eg $x \in A$) and/or assertions of equality (eg $A = B$) using the usual logical operators: *and, or, not, implies, if and only if, there exists, for all.*

DEFINITION 4. Let A and B be sets. If every element of A is an element of B, we say that A is a *subset* of B, denoted $A \subseteq B$.

PROPOSITION 1. *If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

AXIOM 5 (Extensionality). *$A = B$ iff $A \subseteq B$ and $B \subseteq A$.*

AXIOM 6 (Specification). *For every set A and every sentence $S(x)$ there is a set B whose elements are exactly those elements x of A for which $S(x)$ holds.*

DEFINITION 7. We notate this set B by $\{x \in A : S(x)\}$.

PROPOSITION 2. *There exists a unique set X such that for any x, the sentence $x \in X$ is false.*

DEFINITION 8. We call this set the *empty set*, notated $\emptyset$.

PROPOSITION 3. *For every set A there is a set B such that $B \notin A$.*

AXIOM 9 (Pairing). *For any two sets A and B there is a set X with $A \in X$ and $B \in X$.*

PROPOSITION 4. *There is a unique set Y such that for any a, a is in Y iff $a = A$ or $a = B$.*

DEFINITION 10. This set is called the *unordered pair* formed by A and B, denoted $\{A, B\}$.

DEFINITION 11. The set $\{A, A\}$ is denoted $\{A\}$, and called the *singleton* of A.

AXIOM 12 (Union). *For any set X of sets there exists a set Y such that for any A in X, and any a in A, a is in Y.*

PROPOSITION 5. *For a nonempty set X of sets there is a unique set Z such that a is in Z if and only if there exists an A in X such that a is in A.*

DEFINITION 13. This set is called the *union* of X, denoted $\bigcup X$.
For two sets A and B we define $A \cup B = \bigcup\{A, B\}$.

Definition 14. Let A and B be sets. The *intersection* of A and B, notated $A \cap B$, is $\{x \in A : x \in B\}$.

If $A \cap B = \emptyset$ then A and B are called *disjoint*.

Proposition 6. *We have*

- $A \cup \emptyset = A$,
- $A \cup B = B \cup A$ *(commutative)*,
- $A \cup (B \cup C) = (A \cup B) \cup C$ *(associative)*,
- $A \cup A = A$ *(idempotent)*,
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributive)*,
- $A \subseteq B$ *iff* $A \cup B = B$,
- $A \cap \emptyset = A$,
- $A \cap B = B \cap A$ *(commutative)*,
- $A \cap (B \cap C) = (A \cap B) \cap C$ *(associative)*,
- $A \cap A = A$ *(idempotent)*,
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributive)*,
- $A \subseteq B$ *iff* $A \cap B = A$.

Proposition 7. *For every nonempty set C of sets, there is a unique set Y such that $x \in Y$ iff $x \in X$ for each X in C.*

Definition 15. This set Y is called the *intersection* of C, denoted $\bigcap C$.

Axiom 16 (Powers). *For each set X there is a set that contains all subsets of X.*

Proposition 8. *There is a unique set Y such that $x \in Y$ iff $x \subseteq X$.*

Definition 17. This set Y is called the *power set* of X, denoted $\mathcal{P}(X)$.

Definition 18. The *ordered pair* of a and b is the set defined as

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Proposition 9. *For any a, b, c, d, we have $(a, b) = (c, d)$ iff $a = c$ and $b = d$.*

Definition 19. Let A and B be sets. The *Cartesian product* $A \times B$ is

$$\{(x, y) : x \in A,\ y \in B\}.$$

Proposition 10. *For any set R of ordered pairs there are sets A and B such that $R \subseteq A \times B$.*

Definition 20. A *binary relation* R over sets A and B is a subset of $A \times B$. If (a, b) is in R we write aRb.

If $A = B$ then we call it a *binary relation over* A.

Definition 21. An *equivalence relation* is a binary relation $\sim$ over A such that

- $a \sim a$ (reflexive),
- $a \sim b \iff b \sim a$ (symmetric), and
- if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitive).

The *equivalence class* of a under $\sim$ is

$$[a] = \{x \in A : x \sim a\}.$$

Definition 22. A *partition* of a set A is a disjoint set of subsets of A whose union is A.

A partition X of A *induces* a relation $\sim$, where $a \sim b$ iff a and b belong to the same element of X.

Proposition 11. *The set of equivalence classes of an equivalence relation exists and is a partition.*

Definition 23. This partition is called the partition *induced* by the equivalence relation $\sim$.

Proposition 12. *The equivalence relation induced by a partition induces that partition; the partition induced by an equivalence relation induces that relation.*

Definition 24. For any set X we define $X^+ = X \cup \{X\}$.

Axiom 25 (Infinity). *There exists a set S containing $\emptyset$ and containing X^+ for every X in S.*

Proposition 13. *There exists a unique set ω which is a subset of all such sets S.*

Proposition 14. *For any $a, b \in \omega$, exactly one of $a \in b$, $a = b$, $b \in a$ is true.*

Proposition 15. *For any $a \in \omega$ and any $b \in a$, $b \subseteq a$.*

Definition 26. A *function* $f : A \to B$ is a relation f over A and B such that for each $a \in A$ there is exactly one $b \in B$ such that afb. We usually write this as $f(a) = b$.

A function f is *injective* if for each b in B, there is at most one a in A such that $f(a) = b$. It is *surjective* if for each b in B there is at least one a in A such that $f(a) = b$. A function which is both injective and surjective is *bijective*.

Theorem 16 (Recursion theorem). *If a is an element of a set X, and if $f : X \to X$ is a function, then there is a function $g : \omega \to X$ such that $u(0) = a$ and $u(n^+) = f(u(n))$ for all n in ω.*

Axiom 27 (Substitution). *If $S(a, b)$ is a sentence such that for each a in a set A there exists a set B_a such that $b \in B_a \iff S(a, b)$, then there exists a function F with domain A such that $F(a) = B_a$ for each a in A.*

Axiom 28 (Foundation). *Every set X contains a set Y such that X and Y are disjoint.*

Axiom 29 (Choice). *Let X be a set of sets whose members are all nonempty. Then there exists a function $f : X \to \bigcup X$ such that $f(Y) \in Y$ for all $Y \in X$.*

Definition 30. A *partial order* is a binary relation $\leq$ on a a set A such that

- $a \leq a$ (reflexive),
- if $a \leq b$ and $b \leq a$ then $a = b$ (antisymmetric), and
- if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitive).

We define $a < b$ if $a \leq b$ and $a \neq b$.

If for all a and b we have $a \leq b$ or $b \leq a$ (strongly connected), then $\leq$ is a *total order*.

A *chain* is a totally ordered subset of a partially ordered set.

DEFINITION 31. If X is a partially ordered set, and if $a \in X$, the set $s(a) = \{x \in X : x < a\}$ is called the *initial segment* determined by a.

DEFINITION 32. Two partially ordered sets X and Y are *similar* if there is a bijection $f : X \to Y$ such that $a \leq b \iff f(a) \leq f(b)$. This bijection is called a *similarity*.

DEFINITION 33. Let S be a subset of a partially ordered set A, and let a be an element of A. If $s \leq a$ for every s in S, then we call a an *upper bound* of S. If $a \leq s$ for every s in S, then we call a a *lower bound* of S. If a is an upper bound of S and a lower bound of the set of upper bounds of S, then we call a a *least upper bound* of S.

DEFINITION 34. A *well-order* on A is a total order $\leq$ on A such that every nonempty subset S of A has an element a which is a lower bound for S. The set A together with the relation $\leq$ is then called *well-ordered*.

PROPOSITION 17. *If two well-ordered sets are similar, then the similarity is unique.*

THEOREM 18. *If X and Y are well-ordered, then either X and Y are similar, or one is similar to an initial segment of the other.*

DEFINITION 35. An *ordinal number* is a well-ordered set α such that for any $\xi \in \alpha$ we have $s(\xi) = \xi$.

PROPOSITION 19. *ω is an ordinal number.*

PROPOSITION 20. *If α is an ordinal number then so is α^+, and so is any element of α.*

THEOREM 21. *If two ordinal numbers are similar, then they are equal.*
Otherwise, one is an element of the other.

PROPOSITION 22. *If a set α can be well-ordered such that it is an ordinal, then the ordering is unique.*

PROPOSITION 23. *Every well-ordered set is similar to a unique ordinal number.*

PROPOSITION 24. *There is no set of all ordinal numbers.*

THEOREM 25 (Zorn's Lemma). *Suppose a partially ordered set P has the property that every chain in P has an upper bound in P. Then there is an element $a \in P$ such that the only upper bound for $\{a\}$ is a.*

THEOREM 26 (Well-Ordering Theorem). *Every set has a well-ordering.*

DEFINITION 36. Two sets A and B are said to have the same *cardinality* (written $|A| = |B|$) if there is a bijection $f : A \to B$.

A set A has cardinality at most the cardinality of B ($|A| \leq |B|$) if there is an injection $f : A \to B$.

A set A has cardinality less than the cardinality of B ($|A| < |B|$) if $|A| \leq |B|$ and $|A| \neq |B|$.

THEOREM 27. *If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

THEOREM 28. *For any set A, $|\mathcal{P}(A)| > |A|$.*

DEFINITION 37. A *cardinal number* is an ordinal number α such that for any ordinal number β with $|\alpha| = |\beta|$ we have $\alpha \subseteq \beta$.

PROPOSITION 29. *For any set S, there is a unique cardinal number α with $|\alpha| = |S|$.*

DEFINITION 38. For these sets S and α we define $|S| = \alpha$.

DEFINITION 39. A set A is said to be *finite* if $|A| \in \omega$, and *infinite* otherwise.

PROPOSITION 30. *A set is infinite if and only if it has the same cardinality as some proper subset.*

DEFINITION 40. An infinite set A is said to be *countable* if $|A| = \omega$, and *uncountable* otherwise.

PROPOSITION 31. *A countable set does not have any uncountable subsets. An uncountable set has a countable subset.*

References.

- *Naive Set Theory*, Halmos
- *Set Theory*, Jech

CHAPTER 2

Number Systems

DEFINITION 41. A *binary operation* on A is a function $\cdot : A \times A \to A$. We usually write $\cdot(a, b) = c$ as $a \cdot b = c$.

It is *associative* if $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a,\ b,\ c$ in A.

It is *commutative* if $a \cdot b = b \cdot a$ for any $a,\ b$ in A.

DEFINITION 42. A *monoid* is an ordered pair $(A, \cdot)$ of a set A and an associative binary operation $\cdot$ on A such that there exists an element 1, called the *identity*, such that $a \cdot 1 = 1 \cdot a = a$ for all a.

REMARK 43. There are two main notations for monoid-type structures. These are

- Multiplicative notation, in which the operation is notated $a \cdot b$ or simply ab, and the identity element is 1; and
- Additive notation, in which the operation is notated $a + b$ and the identity element is 0.

DEFINITION 44. A *group* is a monoid $(A, \cdot)$ such that for each element a of A there is an element b of A such that $ab = 1 = ba$.

A group is *abelian* if the operation is commutative.

PROPOSITION 32. *If* $ab = ba = 1$ *and* $ac = 1$ *or* $ca = 1$ *then* $b = c$.

DEFINITION 45. The element b of A such that $ab = ba = 1$ is called the *inverse* of a. In multiplicative notation, the inverse of a is notated a^{-1}. In additive notation, the inverse of a is notated $-a$.

REMARK 46. We often define $\frac{a}{b} = ab^{-1}$ in multiplicative notation, and $a - b = a + (-b)$ in additive notation.

DEFINITION 47. A *ring* is an ordered triple $(A, +, \cdot)$ such that $(A, +)$ is an abelian group, $(A \setminus \{0\}, \cdot)$ is a monoid, and the *distributive laws* hold:

$$a \cdot (b + c) = ab + ac \quad \text{and} \quad (a + b) \cdot c = ac + bc.$$

It is *commutative* if $\cdot$ is commutative.

It is *ordered* if there is a total order $\leq$ on A satisfying

- if $a \leq b$ then $a + c \leq b + c$, and
- if $0 \leq a$ and $0 \leq b$ then $0 \leq ab$.

DEFINITION 48. A *field* is a commutative ring $(A, +, \cdot)$ such that $(A \setminus \{0\}, \cdot)$ is a group.

An *ordered field* is a field that is also an ordered ring.

DEFINITION 49. In an ordered ring R, the *absolute value* $|a|$ of an element a of R is a if $0 \leq a$, otherwise $-a$.

PROPOSITION 33. $|a+b| \le |a| + |b|$.

DEFINITION 50. Let X and Y be similar well-ordered sets, and let A and B be the least elements of X and Y respectively. Assume that all other elements of X and Y are operations on A and B respectively, and let f be the similarity between A and B.

A function $\varphi : A \to B$ is said to be a *homomorphism* if for every $a, b \in A$ and every $\cdot \in X \setminus \{A\}$ we have

$$\varphi(a \cdot b) = \varphi(a) f(\cdot) \varphi(b).$$

An *isomorphism* is a bijective homorphism.

If there exists an isomorphism from A to B, then we say A and B are *isomorphic.*

PROPOSITION 34. *The property of being isomorphic is reflexive, symmetric and transitive.*

REMARK 51. We don't say that isomorphism is an equivalence relation, since it would imply there exists a set of all well-ordered sets of this type.

Such a set does not exist because if it did it would contain (S, Id_S) for each set S. Then we could use specification to extract the set containing exactly those elements, and Proposition 10 to extract a set of all sets.

THEOREM 35. *There exists a unique ordered ring $\mathbb{Z}$ (up to isomorphism) such that $\{x \in \mathbb{Z} : x \ge 0\}$ is well-ordered.*

$\mathbb{Z}$ is commutative.

DEFINITION 52. The *integers*, $\mathbb{Z}$, are a well-ordered ring. The *non-negative integers* $\mathbb{Z}_{\ge 0}$ are $\{n \in \mathbb{Z} : n \ge 0\}$. The *positive integers* $\mathbb{Z}^+$ are $\mathbb{Z}_{\ge 0} \setminus \{0\}$.

REMARK 53. We avoid use of the term *natural numbers*, and the symbol $\mathbb{N}$, since some use them to mean the positive integers and others use them to mean the nonnegative integers.

PROPOSITION 36. *$\mathbb{Z}_{\ge 0}$ is similar to ω.*

REMARK 54. Thus, we may identify ω with $\mathbb{Z}_{\ge 0}$. In particular, the cardinality of a finite set is a nonnegative integer.

PROPOSITION 37. *Every ordered ring contains a unique subring isomorphic to $\mathbb{Z}$.*

DEFINITION 55. In $\mathbb{Z} \times \mathbb{Z}^+$, we define the operations

$$(a, b) + (c, d) = (ad + bc, bd), \qquad (a, b)(c, d) = (ac, bd).$$

We also define an equivalence relation $\sim$ where $(a, b) \sim (c, d) \iff ad = bc$.

We define the *rational numbers* $\mathbb{Q}$ as the partition of $\mathbb{Z} \times \mathbb{Z}^+$ induced by this equivalence relation, with $[(a, b)] + [(c, d)] = [(ad + bc, ac + bd)]$ and $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$.

PROPOSITION 38. *The relation $\sim$ is an equivalence relation. Moreover, the operations $+$ and $\cdot$ are uniquely defined. With these operations, $\mathbb{Q}$ is a field.*

PROPOSITION 39. *Every ordered field contains a unique subfield isomorphic to $\mathbb{Q}$.*

DEFINITION 56. A totally ordered set S is *complete* if every nonempty subset that has an upper bound in S has a least upper bound in S.

THEOREM 40. *There exists a unique complete ordered field, up to isomorphism.*

DEFINITION 57. We call this field $\mathbb{R}$.

DEFINITION 58. We define $\mathbb{Q}_{\geq 0}$, $\mathbb{Q}^+$, $\mathbb{R}_{\geq 0}$, $\mathbb{R}^+$ in an analogous way to $\mathbb{Z}_{\geq 0}$ and $\mathbb{Z}^+$.

DEFINITION 59. We define the *complex numbers* $\mathbb{C}$ as $\mathbb{R}^2$, with the operations

$$(a,b)+(c,d)=(a+c,b+d), \qquad (a,b)\cdot(c,d)=(ac-bd,ad+bc).$$

We usually write (a,b) as $a+bi$. We define the *conjugate* of $a+bi$ to be $\overline{a+bi}=a-bi$.

PROPOSITION 41. $\mathbb{C}$ *is a field under these operations.*

PROPOSITION 42. *There are unique homomorphisms* $\mathbb{Z}\to\mathbb{Q}$, $\mathbb{Q}\to\mathbb{R}$ *and* $\mathbb{Q}\to\mathbb{C}$. *There is also a homomorphism* $\mathbb{R}\to\mathbb{C}$.

REMARK 60. Because of this, we usually take $\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$.

PROPOSITION 43. *Let* $a\in\mathbb{C}$. *Then,* $a\overline{a}\in\mathbb{R}_{\geq 0}$.

PROPOSITION 44. *Let* $b\in\mathbb{R}_{\geq 0}$. *There exists a unique* $x\in\mathbb{R}_{\geq 0}$ *such that* $x\cdot x=b$.

DEFINITION 61. We call x the *square root* of b, denoted $\sqrt{b}$.
We call $\sqrt{a\overline{a}}$ the *modulus* of a, denoted $|a|$.

PROPOSITION 45. $|a+b|\leq|a|+|b|$.

THEOREM 46. $|\mathbb{Z}^+|=|\mathbb{Z}_{\geq 0}|=|\mathbb{Z}|=|\mathbb{Q}|=\omega$, *but* $|\mathbb{R}|=|\mathbb{C}|=|\mathcal{P}(\omega)|$.

CHAPTER 3

Linear Algebra

DEFINITION 62. Let $\mathbb{F}$ be a field. A *vector space over* $\mathbb{F}$ is an abelian group V (of *vectors*) together with a function $\cdot : \mathbb{F} \times V \to V$ (*scalar multiplication*) such that

- $a(bv) = (ab)v$ (compatible),
- $1v = v$ (identity), and
- $a(u + v) = au + av$ and $(a + b)v = av + bv$ (distributive).

DEFINITION 63. Let S be a subset of V. A *linear combination* of elements of S is a vector of the form

$$\sum_{i=1}^{n} a_i s_i,$$

where each s_i is a distinct element of S.

DEFINITION 64. A *basis* of a vector space V is a set $S \subseteq V$ such that each element of V can be uniquely represented as a linear combination of elements of S.

REMARK 65. For an infinite-dimensional vector space, there are multiple different notions of a basis. This one is usually called a *Hamel basis*.

THEOREM 47. *Let V be a vector space.*

- *V has a basis.*
- *Any two bases of V have the same cardinality.*

DEFINITION 66. The *dimension* of V is the cardinality of a basis of V. If $\dim V$ is an integer, V is said to be *finite-dimensional*; otherwise, it is *infinite-dimensional*.

DEFINITION 67. A *subspace* W of V is a nonempty subset of V which is also a vector space over $\mathbb{F}$.

PROPOSITION 48. *A subset W of V is a subspace iff the following conditions hold:*

- *W is nonempty;*
- *$u, v \in W$ implies $u + v \in W$ (closed under addition); and*
- *if $a \in \mathbb{F}$ and $u \in W$ then $au \in W$ (closed under scalar multiplication).*

DEFINITION 68. The *span* of a subset S of V is the intersection of all linear subspaces of V that contain S.

PROPOSITION 49. *The span of S is the set of linear combinations of elements of S. It is also a subspace of V.*

DEFINITION 69. A subset S of V is *linearly independent* if any linear combination of elements of S that produces 0 has all coefficients equal to 0. Otherwise, it is *linearly dependent*.

Proposition 50. *A subset S of V is a* basis *iff it is linearly independent and its span is V.*

Proposition 51. *Let V be finite-dimensional with dimension d. Let S be a set of vectors in V with $|S| = d$. Then S is linearly independent iff it spans V.*

Definition 70. A *linear map* from V to W is a group homomorphism $T : V \to W$ such that $T(\lambda v) = \lambda T(v)$ for all $\lambda \in \mathbb{F}$.
The *product* of linear maps S and T is $ST = S \circ T$.

Proposition 52. *The space of linear maps from V to W is a vector space.*

Definition 71. The *null space* of a linear map T is the subset of its domain that T maps to 0.

Proposition 53. *Let V be finite-dimensional, and let $T : V \to W$ be a linear transformation. Then the null space of T is a subspace of V, the image of T is a subspace of W, and the sum of the dimensions of these two subspaces equals* $\dim V$.

Definition 72. A linear map $T : V \to W$ is *invertible* if there is a linear map $S : W \to V$ such that ST is the identity on V and TS is the identity on W. In this case, S is called an *inverse* of T.

Definition 73. An *isomorphism* is an invertible linear map.

Proposition 54. *Two vector spaces over $\mathbb{F}$ are isomorphic iff they have the same dimension.*

Proposition 55. *Suppose V and W are finite-dimensional and isomorphic, and T is a linear transformation from V to W. The following are equivalent:*

- *T is invertible.*
- *T is injective.*
- *T is surjective.*

Definition 74. The *product* of vector spaces is the Cartesian product, where addition and scalar multiplication are defined componentwise.

Proposition 56. *Suppose U is a subspace of V. Define the relation $a \sim b \iff b - a \in V$. Then $\sim$ is an equivalence relation, and addition and scalar multiplication are invariant under it. The partition induced by this relation is a vector space.*

Definition 75. This vector space is called the *quotient space* of V over U, denoted V/U.

Proposition 57. *Suppose T is a linear transformation with domain V, and let U be the null space of T. Then T is an isomorphism from V/U to the range of T.*

Definition 76. A *linear functional* on V is a linear map from V to $\mathbb{F}$.

Definition 77. The space of linear functionals on V is the *dual space* of V, denoted V'.

Definition 78. If $v_1, \ldots, v_n$ is a basis of V, then the *dual basis* is the list of elements φ_j of V', where $\varphi_j v_k$ is 1 if $j = k$ and 0 otherwise.

Proposition 58. *The dual basis of a basis of V is a basis of V'.*

Definition 79. The *dual map* of T is the linear map $T' : W' \to V'$ defined by $T'\varphi = \varphi T$ for each $\varphi \in W'$.

Proposition 59. *T' is a linear map. The dimensions of the range of T' and the range of T coincide.*

Definition 80. Suppose V and W have finite bases $\{v_i\}_1^m$ and $\{w_i\}_1^n$ respectively. The *matrix* A of T with respect to these bases is defined by

$$T_{v_k} = \sum_{i=1}^{n} A_{i,k} w_i.$$

We also identify $1 \times n$ and $n \times 1$ matrices with elements of $\mathbb{F}^n$.

Proposition 60. *This defines a bijection between the space of $m \times n$ matrices and the space of linear transformations $\mathbb{F}^n \to \mathbb{F}^m$.*

Definition 81. Thus, we identify the two, and can therefore talk of the image, null space, etc of a matrix.

Definition 82. The *rank* of a matrix is the dimension of its image.
The *transpose* of a matrix is the matrix obtained by reflecting over the diagonal.

Proposition 61. *Let $T : V \to W$ be a linear transformation, where V and W are finite-dimensional. Pick bases $\{v_i\}$ and $\{w_i\}$ of V and W. The matrix of T' with respect to the dual bases of $\{v_i\}$ and $\{w_i\}$ is the transpose of the matrix of T with respect to $\{v_i\}$ and $\{w_i\}$.*

Corollary 62. *The rank of a matrix equals the rank of its transpose.*

Definition 83. Let U, V, W be finite-dimensional vector spaces, and let $A : U \to W$ and $B : V \to W$ be linear maps. We *augment* A with B to get the linear map

$$(A|B) : U \times V \to W,\ (A|B)(x, y) = Ax + By.$$

Proposition 63. *For any $x : V \to U$ we have $Ax = B \iff (A|B)(x, -I) = 0$.*

Remark 84. Thus, to solve the linear system $Ax = B$ it suffices to find the null space of $(A|B)$. Notice also that the matrix of $(A|B)$ is simply the matrix formed by concatenating the matrices of A and B.

Proposition 64. *Let T and S be linear maps from V to W. The following are equivalent:*

- *The null spaces of T and S are the same.*
- *The images of T' and S' coincide.*
- *There is an invertible linear map $A : V \to V$ such that $AT = S$.*

Definition 85. Such linear maps are called *equivalent*.

Definition 86. A *pivot* is the first nonzero entry in a row of a matrix.
A matrix is in *row echelon form (REF)* if all rows consisting of only zeroes are at the bottom and the pivot of a nonzero row is strictly to the right of the pivot of the row above it.
A matrix is in *reduced row echelon form (RREF)* if it is in REF, all pivots are 1, and each column containing a pivot has zeroes everywhere else in the column.

PROPOSITION 65. *Every matrix is equivalent to a unique matrix in RREF.*

DEFINITION 87. An *elementary matrix* is a matrix that differs from the identity in exactly one entry, where that entry is nonzero in the elementary matrix.

PROPOSITION 66. *A matrix is invertible iff it is a product of elementary matrices.*

REMARK 88. The null space of a matrix in RREF is easy to find. Thus, to find the null space of a matrix, we left-multiply by elementary matrices to find an equivalent matrix in RREF. This process is known as *Gaussian elimination.* It is efficient because multiplying by an elementary matrix has simple consequences:

- An elementary matrix which has a nonzero entry on the main diagonal multiplies a row by a scalar.
- An elementary matrix which has a nonzero entry off the main diagonal adds a scalar multiple of one row to another.

Most authors add a third (redundant) type of row operation and elementary matrix: swapping two rows.

The next proposition shows that Gaussian elimination also helps us find bases for the span of a set of vectors.

PROPOSITION 67. *Let T be a matrix which is equivalent to a matrix S in REF. Then,*

- *The rows of S with pivots form a basis for the span of the rows of T.*
- *Consider the columns of S with pivots. The corresponding columns of T form a basis for the span of the columns of T.*

DEFINITION 89. An *inner product space* is a vector space V over a field $\mathbb{F}$ which is either $\mathbb{R}$ or $\mathbb{C}$, together with a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ satisfying

- $\langle x, y \rangle = \overline{\langle y, x \rangle}$ (conjugate symmetry)
- $\langle ax + by, z \rangle = a\langle x, z \rangle + b\langle y, z \rangle$ (linearity in the first argument), and
- $\langle x, x \rangle = 0 \implies x = 0$.

PROPOSITION 68. *Any linear functional f on a finite-dimensional inner product space can be written as $f(x) = \langle x, v \rangle$ for some fixed vector v.*

DEFINITION 90. A *normed vector space* is a vector space V over $\mathbb{R}$ or $\mathbb{C}$ on which there is a *norm*: a function $\| \cdot \| : V \to \mathbb{C}$ satisfying

- $\|x\| \geq 0$, with $\|x\| = 0 \iff x = 0$,
- $\|ax\| = |a|\|x\|$, and
- $\|x + y\| \leq \|x\| + \|y\|$ (the triangle inequality).

PROPOSITION 69. *If V is an inner product space, then $\langle x, x \rangle$ is real for all x. Moreover, $\|x\| = \sqrt{\langle x, x \rangle}$ is a norm on V.*

DEFINITION 91. Two vectors x and y are *orthogonal* if $\langle x, y \rangle = 0$.

A set of vectors is *orthonormal* if each vector in the set has norm 1 and is orthogonal to all other vectors in the set.

PROPOSITION 70. *Any finite-dimensional inner product space has an orthonormal basis.*

References.

- *Linear Algebra Done Wrong*, Treil
- *Linear Algebra Done Right*, Axler
- *Finite-Dimensional Vector Spaces*, Halmos

APPENDIX A

Proofs