Learning Uni Maths

Andres Buritica Monroy

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

Bernhard Riemann

Contents

CHAPTER 1

Undergraduate

1. Set Theory

DEFINITION 1. We define a *set*, or *collection*, as an object which has a notion of *elements* — for any set A and any object B, either B is an element of A or it isn't.

AXIOM 2 (Existence). There exists a set.

DEFINITION 3. 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 4. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

AXIOM 5 (Extensionality). Let A and B be sets. We have $A \subseteq B$ and $B \subseteq A$ iff $A = B$.

DEFINITION 6. 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.*

AXIOM 7 (Specification). For every set A, every set p and every sentence $S(x, p)$ there is a set B whose elements are exactly those elements x of A for which $S(x, p)$ holds.

DEFINITION 8. We notate this set B by $\{x \in A : S(x, p)\}$.

PROPOSITION 9. There exists a unique set X such that for any x, the sentence $x \in X$ is false.

DEFINITION 10. We call this set the *empty set*, notated $\emptyset$.

PROPOSITION 11. For every set A there is a set B such that $B \notin A$.

AXIOM 12 (Pairing). For any two sets A and B there is a set X with $A \in X$ and $B \in X$.

PROPOSITION 13. There is a unique set Y such that for any a, a is in Y iff $a = A$ or $a = B$.

DEFINITION 14. This set is called the *unordered pair* formed by A and B, denoted $\{A, B\}$.

DEFINITION 15. The set $\{A, A\}$ is denoted $\{A\}$, and called the *singleton* of A.

AXIOM 16 (Union). For any collection 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 17. For a nonempty collection 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 18. This set is called the *union* of X, denoted $\bigcup X$.
For two sets A and B we define $A \cup B = \bigcup\{A, B\}$.

PROPOSITION 19. For every nonempty collection C of sets, there is a unique set Y such that $x \in Y$ iff $x \in X$ for each X in C.

DEFINITION 20. This set Y is called the *intersection* of C, denoted $\bigcap C$.

DEFINITION 21. Let A and B be sets. The *intersection* of A and B, notated $A \cap B$, is $\bigcap\{A, B\}$.
If $A \cap B = \emptyset$ then A and B are called *disjoint*.

AXIOM 22 (Powers). For each set X there is a collection that contains all subsets of X.

PROPOSITION 23. There is a unique collection Y such that $x \in Y$ iff $x \subseteq X$.

DEFINITION 24. This set Y is called the *power set* of X, denoted $\mathcal{P}(X)$.

DEFINITION 25. The *ordered pair* of a and b is the set defined as

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

PROPOSITION 26. For any a, b, c, d, we have $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

PROPOSITION 27. For any sets A and B, the set

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

exists.

DEFINITION 28. This set is called the *Cartesian product* of A and B, denoted $A \times B$.

PROPOSITION 29. For any set R of ordered pairs there are sets A and B such that $R \subseteq A \times B$.

DEFINITION 30. A *binary relation* R from A to 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 31. 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 32. A *partition* of a set A is a disjoint collection of nonempty subsets of A whose union is A.
A partition X of A *induces* a relation A/X, where $a\ A/X\ b$ iff a and b belong to the same element of X.

PROPOSITION 33. The collection of equivalence classes of an equivalence relation exists and is a partition.

DEFINITION 34. This partition is called the partition *induced* by the equivalence relation $\sim$, denoted $X/\sim$.

PROPOSITION 35. The equivalence relation induced by a partition induces that partition; the partition induced by an equivalence relation induces that relation.

DEFINITION 36. The *natural projection* $\pi : X \to X/\sim$ sends every element to its equivalence class.

DEFINITION 37. For a relation R from X to Y we define the *inverse* relation $R^{-1} : Y \to X$ by $xRy \iff yR^{-1}x$.

DEFINITION 38. 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 $f(a) = b$.

PROPOSITION 39. The set of functions from A to B exists.

DEFINITION 40. We denote it by B^A.

PROPOSITION 41. Let $F : X \to Y$ be a function and let $\sim$ be an equivalence relation on X. There is a function $G : X/\sim \to Y$ such that $F = G\pi$ iff the image of every equivalence class is a singleton.

DEFINITION 42. In this case G is the function *induced* on $X/\sim$ by F.

DEFINITION 43. The *identity* function $I_A : A \to A$ is defined by $I_A(a) = a$ for each $a \in A$.

DEFINITION 44. Let $f : A \to B$ and $g : B \to A$ be functions. If $f \circ g = I_A$, then f is a *left inverse* of g and g is a *right inverse* of f. If both $f \circ g = I_B$ and $g \circ f = I_B$, then f is called the *two-sided inverse* or simply *inverse* of g.

DEFINITION 45. For a set $E \subseteq A$, we define the *image* of E under f as $f(E) = \{f(x) : x \in E\}$. For a set $E \subseteq B$, we define the *inverse image* of E under F as $f^{-1}(E) = \{x \in A : f(x) \in E\}$.

DEFINITION 46. 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*.

PROPOSITION 47. A function whose domain is nonempty is injective iff it has a left inverse.

PROPOSITION 48. A function is bijective iff it has an inverse, which equals any left- or right-inverse of the function.

DEFINITION 49. If $A \subseteq B$ and $f : B \to C$, the *restriction* of f to A is $f|_A : A \to C,\ f|_A(x) = f(x)$.

DEFINITION 50. For functions $f : W \to X$ and $g : Y \to Z$, where $Y \subseteq X$, we define the *composite* $f \circ g : W \to Z$ as $(f \circ g)(x) = f(g(x))$ for all x.

DEFINITION 51. A function x from a set I (the *index set*) to a set X is called an *indexed family* of X, and its range is an *indexed set*. We notate the indexed set by $\{x_i\}_{i \in I}$.

DEFINITION 52. For any set X we define $X^+ = X \cup \{X\}$.

AXIOM 53 (Infinity). There exists a set S containing $\emptyset$ and containing X^+ for every X in S.

PROPOSITION 54 (Peano Axioms). There exists a unique set ω satisfying

- $\emptyset \in \omega$. We define $0 = \emptyset$.
- If $n \in \omega$ then $n^+ \in \omega$.
- If $S \subseteq \omega$ such that $\emptyset \in S$ and $n \in S \implies n^+ \in S$ then $S = \omega$.
- $n^+ \neq \emptyset$ for all $n \in \omega$.
- If n and m are in ω, and if $n^+ = m^+$, then $n = m$.

THEOREM 55 (Recursion). 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.

PROPOSITION 56. The set S^n, defined by $S^1 = S$ and $S^{n+1} = S^n \times S$, exists for each $n \in \omega \setminus \{\emptyset\}$.

DEFINITION 57. 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 58. 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 59. 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 60. 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 61. 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*.

THEOREM 62 (Transfinite Induction). Let S be a subset of a well-ordered set A such that for any $x \in A$, if $s(x) \subseteq S$ then $x \in S$. Then $S = A$.

DEFINITION 63. If a is an element of a well-ordered set A, and X is an arbitrary set, then a *sequence of type* a is an family of X indexed by $s(a)$.

A *sequence function* of type A is a function whose domain consists of all sequences of type a for each $a \in A$, and whose codomain is A.

PROPOSITION 64 (Transfinite Recursion). If A is a well-ordered set, and if f is a sequence function of type A in X, then there is a unique function $U : A \to X$ such that $U(a) = f(U|s(a))$ for each a in W.

PROPOSITION 65. If two well-ordered sets are similar, then the similarity is unique.

THEOREM 66. 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 67. An *ordinal number* is a well-ordered set α such that for any $\xi \in \alpha$ we have $s(\xi) = \xi$.

We define the ordinals $0 = \emptyset$ and $1 = 0^+$.

PROPOSITION 68. There is no set of all ordinal numbers.

PROPOSITION 69. ω is an ordinal number.

PROPOSITION 70. If α is an ordinal number then so is α^+, and so is any element of α.

PROPOSITION 71. If α is an ordinal number, then either $\alpha = (\bigcup \alpha)^+$ or $\alpha = \bigcup \alpha$.

DEFINITION 72. In the first case, α is a *successor ordinal*; in the second, it is a *limit ordinal*.

THEOREM 73. If two ordinal numbers are similar, then they are equal.

Otherwise, one is an element of the other.

AXIOM 74 (Substitution). If p is a set and $S(a, b, p)$ is a sentence such that for each a in a set A there exists a set B_a such that $b \in B_a \iff S(a, b, p)$, then there exists a function F with domain A such that $F(a) = B_a$ for each a in A.

AXIOM 75 (Foundation). Every set X contains a set Y such that X and Y are disjoint.

AXIOM 76 (Choice). Let X be a collection 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 $Y \in X$.

PROPOSITION 77. Every relation includes a function with the same domain.

THEOREM 78 (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 79 (Well-Ordering Theorem). Every set has a well-ordering.

PROPOSITION 80. Every well-ordered set is similar to a unique ordinal number.

PROPOSITION 81. If S is an ordinal and A is a family of ordinals indexed by A, consider the set T of ordered pairs (s, a) such that $s \in S$ and $a \in A_s$. We define the relation $(s_1, a_1) \leq (s_2, a_2)$ if $s_1 < s_2$ or $s_1 = s_2$ and $a_1 \leq a_2$. This relation well-orders T.

DEFINITION 82. The ordinal corresponding to T under this well-ordering is the *ordinal sum* of A, denoted $\sum A$.

PROPOSITION 83. For any pair of ordinals (a, b) with $a \leq b$ there is an ordinal c such that $a + c = b$.

COROLLARY 84. If $a < b$ then for any c we have $c + a < c + b$ and $a + c \leq b + c$.

PROPOSITION 85. If A and B are ordinals, the ordering on $A \times B$ where $(a, b) \leq (c, d)$ iff $b < d$ or both $b = d$ and $a \leq c$ is a well-ordering on $A \times B$.

DEFINITION 86. The ordinal corresponding to $A \times B$ under this well-ordering is the *ordinal product* of A and B, denoted AB or $A \cdot B$.

PROPOSITION 87. If $a < b$ then for any c we have $ca < cb$ and $ac \leq bc$.

PROPOSITION 88. For every family $\{a_i\}$ of ordinals indexed by an ordinal b, there exists an ordinal c and a unique function $f : b^+ \to c$ such that $f(\emptyset) = 1$ and

$$f(x) = \begin{cases} f(\bigcup x)a_x & \bigcup x \neq x \\ \bigcup_{y \in x} f(y) & \bigcup x = x \end{cases}.$$

The graph of f is the same no matter which ordinal c is used.

DEFINITION 89. We define $\prod a_i = f(I)$. If all a_i equal a, then we define $a^b = f(b)$.

PROPOSITION 90. If $a \leq b$, then for any c we have $a^c \leq b^c$. If additionally $c > 1$, then $c^a \leq c^b$.

PROPOSITION 91. With ordinal sums, products and exponents as defined,

$$\begin{aligned} a + 0 = 0 + a &= a \\ a + 1 &= a^+ \\ a + (b + c) &= (a + b) + c \\ a(bc) &= (ab)c \\ a \sum B_i &= \sum aB_i \\ a^{\sum B_i} &= \prod a^{B_i} \\ a^{bc} &= (a^b)^c. \end{aligned}$$

However, ordinal addition and multiplication are not commutative and not right-distributive. Also, $(ab)^c$ is generally distinct from $a^c b^c$.

PROPOSITION 92. For $c > 1$ and $a \geq 1$, we have $c^a \geq a$.

DEFINITION 93. 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 $|A| \neq |B|$.

A set A is *enumerable* if $|A| = |\omega$, *countable* if it is finite or enumerable, and *uncountable* otherwise.

PROPOSITION 94. If there exists a surjection $f : A \to B$ then $|B| \leq |A|$.

THEOREM 95 (Schröder-Bernstein). If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

THEOREM 96 (Cantor). For any set A, $|\mathcal{P}(A)| > |A|$.

DEFINITION 97. A set S is *dense* if for any $a \in S$, the least upper bound of $s(a)$ is a. It is *unbordered* if it has no least upper bound or greatest lower bound.

PROPOSITION 98. All enumerable unbordered dense totally ordered sets are similar.

PROPOSITION 99. If A and B are collections of disjoint sets and $f : A \to B$ is a bijection such that $|f(a)| = |a|$ for each $a \in A$, then $|\bigcup A| = |\bigcup B|$, and $|\prod A| = |\prod B|$.

PROPOSITION 100. For any set C and any indexed family of sets A we have

$$\left|\prod C^{A_i}\right| = \left|C^{\bigcup A}\right|.$$

DEFINITION 101. We define $\sum |A_i| = |\bigcup A_i|$, $\prod |A_i| = |\prod A_i|$, and $|A|^{|B|} = |A^B|$.

PROPOSITION 102. For every set of cardinal numbers there is a cardinal number strictly greater than all of them.

THEOREM 103 (König). Let $\{A_i\}$ and $\{B_i\}$ be indexed families of disjoint sets, such that for each i we have $|A_i| < |B_i|$. Then, $|\bigcup A_i| < |\bigcup B_i|$.

DEFINITION 104. A *cardinal number* is an ordinal number α such that for any ordinal number β with $|\alpha| = |\beta|$ we have $\alpha \subseteq \beta$.

PROPOSITION 105. If a and b are ordinals, then $|a + b| = |a| + |b|$, $|ab| = |a||b|$ and $|a^b| = |a|^{|b|}$. Here, ordinal operations are used on the left side and cardinal operations are used on the right.

PROPOSITION 106. Every element of ω, as well as ω itself, is a cardinal number.

PROPOSITION 107. For any set S, there is a unique cardinal number α with $|\alpha| = |S|$.

DEFINITION 108. For these sets S and α we define $|S| = \alpha$.

DEFINITION 109. A set A is said to be *finite* if $|A| \in \omega$, and *infinite* otherwise.

PROPOSITION 110. A set is infinite if and only if it has the same cardinality as some proper subset.

PROPOSITION 111. A countable set does not have any uncountable subsets. An uncountable set has a subset with cardinality equal to ω.

PROPOSITION 112. A union of countably many countable sets is countable.

PROPOSITION 113. If a and b are cardinal numbers such that $a \geq \omega$ and $a \geq b$, then $a + b = a \times b = a$. If b is finite we also have $a^b = a$.

COROLLARY 114. If b is infinite and $a = c^b$ for some c, then $a^b = a$.

PROPOSITION 115. Let $\beta > 1$ be an arbitrary ordinal. Every ordinal can be represented uniquely as a finite sum $\sum_i \beta^{\alpha_i}\gamma_i$, where all α_i are distinct and each γ_i is smaller than β.

DEFINITION 116. For each infinite cardinal a, consider the set $c(a)$ of all infinite cardinals strictly smaller than a. Since $c(a)$ is well-ordered, it is similar to some ordinal α; we write $a = \aleph_\alpha$.

PROPOSITION 117. The set of ordinals with cardinality $\aleph_\alpha$ has cardinality $\aleph_{\alpha+1}$.

References.

- Halmos, *Naive Set Theory*
- Kamke, *Theory of Sets*

2. Number Systems

DEFINITION 118. For a nonnegative integer n, we define an *operation of arity* n on a set S as a function $f : S^n \to S$. We use the convention $S^0 = 1 = \{0\}$, so an operation of arity 0 selects an element of S.

DEFINITION 119. A *binary operation* $\cdot$ is an operation of arity 2. 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 120. An *algebraic structure* is an ordered pair (S, O) where S is a set and O is an indexed set of operations on S.

DEFINITION 121. A *semigroup* is a set A together with an associative binary operation on A.

REMARK 122. There are two main notations for semigroups. These are

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

DEFINITION 123. An element $e \in A$ is called an *identity* for $\cdot$ if for each x we have $x \cdot e = e \cdot x = x$.

DEFINITION 124. A *monoid* is a semigroup with a nullary operation that selects an identity.

DEFINITION 125. A partial order $\leq$ and a binary operation $\cdot$ are said to be *compatible* if $x \leq y$ implies $ax \leq ay$ and $xa \leq ya$.

DEFINITION 126. Let X be a monoid with a compatible partial order $\geq$. The sets $X_{\geq 0}$ and $X_{>0} = X^+$ are defined as $\{x \in X : x \geq 0\}$ and $X_{\geq 0} \setminus \{0\}$.

DEFINITION 127. A *group* is a monoid A with a unary operation $\cdot^{-1}$ such that for each $a \in A$ we have $aa^{-1} = a^{-1}a = 1$.

A group is *abelian* if its binary operation is commutative.

DEFINITION 128. A *rng* is an (additive) abelian group A with a binary operation $\cdot$ such that $(A, \cdot)$ is a semigroup, 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 compatible with $+$ such that $A_{\geq 0}$ is closed under $\cdot$.

It is a *ring* if $(A, \cdot)$ is a monoid.

REMARK 129. Some authors use "ring" for what we call a rng, and "ring with identity" or similar for what we call a ring.

DEFINITION 130. A *field* is a ring $(A, +, \cdot)$ such that $(A \setminus \{0\}, \cdot)$ is an abelian group.

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

DEFINITION 131. Let (A, X) and (B, Y) be algebraic structures such that X and Y are indexed by the same set.

A function $\varphi : A \to B$ is said to be a *homomorphism*, or *morphism*, if for every $a, b \in A$ and every i we have have

$$\varphi(aX_ib) = \varphi(a)Y_i\varphi(b).$$

DEFINITION 132. An *isomorphism* is a bijective homomorphism. An isomorphism from a set to itself is an *automorphism*.

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

PROPOSITION 133. The property of being isomorphic is reflexive, symmetric and transitive.

REMARK 134. We don't say that isomorphism is an equivalence relation, since this would imply the existence of a set of all sets. (Consider the union of all sets isomorphic to the trivial group.)

DEFINITION 135. Let A be a [group, ring, etc] and let S be a subset of A. If S is also a [group, ring, etc], then S is called a *sub*[group, ring, etc] of A. Conversely, A is a [group, ring, etc] *extension* of S.

PROPOSITION 136. The intersection of any collection of sub[group, ring, etc]s of G is again a sub[group, ring, etc] of G.

DEFINITION 137. The *direct product* of an indexed set $\{G_i\}_{i\in I}$ of algebraic structures is the set of sequences $\{g_i\}_{i\in I}$ such that each g_i is in G_i, with operations defined componentwise.

PROPOSITION 138. The direct product of a set of [groups, rings, etc][1] is again a [group, ring, etc].

PROPOSITION 139. Let R be a commutative ring and let $x \notin R$. There exists a unique ring extension $R[x]$ of R up to isomorphism such that for every ring extension S of R and every element y of S, there is a unique ring homomorphism $f_y : R[x] \to S$ which fixes R and sends x to y.

DEFINITION 140. This ring is called the *polynomial ring* over R; if $p \in R[x]$, we define p to be a function on S by $f_y(p) = p(y)$.

PROPOSITION 141. Every element in $R[x]$ can be uniquely written as $\sum_{i=1}^{\infty} r_i x^i$, where all but finitely many r_is are 0.

DEFINITION 142. The *degree* of a polynomial is the largest i such that $r_i \neq 0$.

DEFINITION 143. An equivalence relation $\sim$ and a binary operation $\cdot$, both over A, are said to be *compatible* if $a_1 \sim a_2$ and $b_1 \sim b_2$ imply $a_1 \cdot b_1 \sim a_2 \cdot b_2$. In this case, we may define the operation $\cdot$ *induced* on $A/\sim$ by $\cdot$ as $[a] \cdot [b] = [a \cdot b]$.

PROPOSITION 144. If A is a [monoid, group, etc] and $\sim$ is a nontrivial equivalence relation compatible with all of its operations, then $A/\sim$ is a [monoid, group, etc] under the operations induced on it.

DEFINITION 145. A partially ordered set S is *complete* if every nonempty subset that has an upper bound in S has a least upper bound in S.

[1] except for fields

PROPOSITION 146. Let S be a complete partially ordered set. Every nonempty subset that has a lower bound in S has a greatest lower bound in S.

THEOREM 147. There are structures $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ satisfying the following properties:

- $\mathbb{Z}$ is a ring, and if R is a ring, there is a unique homomorphism $f : \mathbb{Z} \to R$.
- $\mathbb{Q}$ is a field, and if F is a field containing $\mathbb{Z}$, there is a unique homomorphism $f : \mathbb{Q} \to F$.
- $\mathbb{R}$ is a complete totally ordered field.

Moreover, each of these properties defines the corresponding structure up to unique isomorphism.

PROPOSITION 148. There are unique orders on $\mathbb{Z}$ and $\mathbb{Q}$ compatible with $+$ such that $1 \geq 0$.

PROPOSITION 149 (Principle of Mathematical Induction). If $S \subseteq \mathbb{Z}^+$ such that $1 \in S$ and if $x \in S$ then $x + 1 \in S$, then $S = \mathbb{Z}^+$.

DEFINITION 150. The structures thus defined are the *nonnegative integers*, *integers*, *rational numbers* and *real numbers* respectively.

REMARK 151. We avoid the symbol $\mathbb{N}$ and the term *natural numbers*, since some sources take it to mean $\mathbb{Z}_{>0}$ and others take it to mean $\mathbb{Z}_{\geq 0}$.

DEFINITION 152. We define the *complex numbers* $\mathbb{C}$ as $\mathbb{R}[x]/\sim$, where $\sim$ is the equivalence relation given by $a \sim b \iff \exists c : a = b + c(x^2 + 1)$. The equivalence class of x is denoted i.

PROPOSITION 153. There is a unique nontrivial automorphism of $\mathbb{C}$ fixing $\mathbb{R}$.

DEFINITION 154. This automorphism is called *complex conjugation*; the image of a is denoted $\overline{a}$.

PROPOSITION 155. If $a \in \mathbb{C}$, then $a\overline{a} \in \mathbb{R}_{\geq 0}$.

PROPOSITION 156. Let $b \in \mathbb{R}_{\geq 0}$. There exists a unique $x \in \mathbb{R}_{\geq 0}$ such that $x \cdot x = b$.

DEFINITION 157. We call x the *square root* of b, denoted $\sqrt{b}$.

DEFINITION 158. We call $\sqrt{a\overline{a}}$ the *modulus* of a, denoted $|a|$.

PROPOSITION 159 (Triangle Inequality). If a and b are complex numbers, then $|a + b| \leq |a| + |b|$.

THEOREM 160 (Fundamental Theorem of Algebra). For all $P \in \mathbb{C}[x] \setminus \mathbb{C}$, there is a complex number z such that $P(z) = 0$.

REMARK 161. We assume this theorem for now, and prove it in the section on complex analysis.

THEOREM 162. $|\mathbb{Z}^+| = |\mathbb{Z}_{\geq 0}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega$, but $|\mathbb{R}| = |\mathbb{C}| = |\mathcal{P}(\omega)|$.

References.

- Landau, *Foundations of Analysis*
- Birkhoff and Mac Lane, *A Survey of Modern Algebra*

3. Linear Algebra

DEFINITION 163. 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 164. 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.

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

THEOREM 166. Let V be a vector space.

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

DEFINITION 167. 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 168. A *subspace* W of V is a nonempty subset of V which is also a vector space over $\mathbb{F}$.

PROPOSITION 169. 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).

PROPOSITION 170. The intersection of any collection of subspaces of V is again a subspace of V.

DEFINITION 171. The *span* of a subset S of V is the intersection of all subspaces of V which contain S.

PROPOSITION 172. The span of S is the set of all linear combinations of S.

DEFINITION 173. Given two subspaces X and Y of V, their *sum* $X + Y$ is the intersection of all subspaces of V which contain both X and Y.

If $X + Y = V$ and $X \cap Y = \{0\}$ then X is said to be a *complement* of Y.

PROPOSITION 174. $X + Y = \{x + y : x \in X, y \in Y\}$.

DEFINITION 175. 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 176. A subset S of V is a *basis* iff it is linearly independent and its span is V.

PROPOSITION 177. 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 178. A *linear map*, or *linear transformation*, from V to W is a group homomorphism $T : V \to W$ such that $T(\lambda v) = \lambda T(v)$ for all $\lambda \in \mathbb{F}$. A linear map from a vector space to itself is an *operator*.

The *product* of linear maps S and T is $ST = S \circ T$.

PROPOSITION 179. The set $\mathcal{L}(V, W)$ of linear maps from V to W is a vector space. Right-multiplication by a linear map $T : U \to V$ defines a linear map from $\mathcal{L}(V, W)$ to $\mathcal{L}(U, W)$. Left-multiplication by T defines a linear map from $\mathcal{L}(W, U)$ to $\mathcal{L}(W, V)$.

DEFINITION 180. An *algebra* is a set A over a field K with operations of addition, multiplication and scalar multiplication which is both a vector space and a ring, such that multiplication is bilinear.

PROPOSITION 181. The set of operators from a vector space to itself is an algebra.

DEFINITION 182. The *null space* of a linear map T is the subset of its domain that T maps to 0.

PROPOSITION 183. The null space and image of a linear map are both vector spaces.

PROPOSITION 184. The null space of a linear map is $\{0\}$ iff the map is injective.

PROPOSITION 185. If a linear map is injective, then its left inverse is linear. If a linear map is surjective, then it has a linear right inverse.

PROPOSITION 186. Let V be finite-dimensional. A linear map $T : V \to V$ is injective iff it is surjective.

DEFINITION 187. The *product* of vector spaces is the Cartesian product, where addition and scalar multiplication are defined componentwise.

PROPOSITION 188. The product of a collection S of vector spaces is a vector space whose dimension is the sum of the dimensions of the elements of S.

COROLLARY 189. The product $\mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F}$ is a vector space over $\mathbb{F}$.

PROPOSITION 190. Suppose U is a subspace of V. Define the relation $a \sim b \iff b - a \in V$. Then $\sim$ is an equivalence relation compatible with addition and scalar multiplication. The partition induced by this relation is a vector space. If V is finite-dimensional, this vector space has dimension $\dim V - \dim U$.

DEFINITION 191. This vector space is called the *quotient space* of V over U, denoted V/U.

PROPOSITION 192. Suppose T is a linear transformation with domain V, and let U be the null space of T. Then T induces an isomorphism from V/U to the image of T.

COROLLARY 193 (Rank-Nullity). 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 194. A *linear functional* on V is a linear map from V to $\mathbb{F}$.
The space of linear functionals on V is the *dual space* of V, denoted V^*.

PROPOSITION 195. If V is infinite-dimensional, $\dim V^* > \dim V$.

PROPOSITION 196. If $v_1, \ldots, v_n$ is a finite basis of V, then there exists a basis of n elements φ_j of V^*, where $\varphi_j v_k$ is 1 if $j = k$ and 0 otherwise.

DEFINITION 197. This basis is called the *dual basis* of $v_1, \ldots, v_n$.

PROPOSITION 198. If V is finite-dimensional, then for every $z \in (V^*)^*$ there is an $x \in V$ such that for every $y \in V^*$ we have $z(y) = y(x)$. The correspondence $x \to z$ is an isomorphism.

REMARK 199. Thus, $(V^*)^*$ and V are often identified for finite-dimensional vector spaces.

DEFINITION 200. For $U \subseteq V$, the *annihilator* of U is

$$U^0 = \{\varphi \in V^* : \varphi(u) = 0 \ \forall u \in U\}.$$

PROPOSITION 201. $\dim U + \dim U^0 = \dim V$.

PROPOSITION 202. $(U^0)^0 = U$.

PROPOSITION 203. If M and N are complementary subspaces of V, then M^0 and N^0 are complementary subspaces of V^*. The restriction $|_M$ is an isomorphism between N^0 and M^*.

DEFINITION 204. 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 205. The image of T' is the annihilator of the null space of T. The null space of T' is the annihilator of the image of T.

DEFINITION 206. 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

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

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

PROPOSITION 207. This defines a bijection between the space of $m \times n$ matrices and $\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$.

DEFINITION 208. Thus, we identify the two, and can therefore talk of the image, null space, etc of a matrix. Matrix addition and multiplication are defined in the same way as addition and multiplication of linear transformations.

DEFINITION 209. The *rank* of a matrix is the dimension of its image.
The *transpose* of a matrix is the matrix obtained by swapping rows and columns: $A^T_{j,k} = A_{k,j}$.

PROPOSITION 210. 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 $\{w_i\}$ and $\{v_i\}$ is the transpose of the matrix of T with respect to $\{v_i\}$ and $\{w_i\}$.

PROPOSITION 211. The image of A equals the image of AA^T.

COROLLARY 212. The ranks of the matrices A, A^T, AA^T and A^TA are equal.

DEFINITION 213. 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 214. For any $x : V \to U$ we have $Ax = B \iff (A|B)(x, -I) = 0$.

REMARK 215. 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 216. 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' are the same.
- There is an invertible linear map $A : V \to V$ such that $AT = S$.

DEFINITION 217. Such linear maps are called *equivalent*.

DEFINITION 218. A linear transformation $T : V \to V$ is a *projection* onto U if U is its image and $Tu = u$ for each $u \in U$.

PROPOSITION 219. Every linear transformation is equivalent to a projection.

COROLLARY 220. Every linear transformation T is a sum of r transformations of rank one, where r is the rank of T.

DEFINITION 221. 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 222. Every matrix is equivalent to a unique matrix in RREF.

PROPOSITION 223 (LU Factorisation). If a matrix A is square, then there are a permutation matrix P, an invertible lower-triangular matrix L and a matrix U in REF such that $PA = LU$.

REMARK 224. The null space of a matrix in REF is easy to find by *back-substitution*. Thus, to find the null space of a matrix, we factorise it into into $P^{-1}LU$ and find the null space of U. This process is known as *Gaussian elimination*.

PROPOSITION 225. 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 226. Let $T : V \to V$ be a linear transformation. A subspace U of V is called *invariant* under T if $u \in U \implies Tu \in U$.

DEFINITION 227. A nonzero vector $v \in V$ is called an *eigenvector* of T if there is some $\lambda \in \mathbb{F}$ such that $Tv = \lambda v$. We call λ an *eigenvalue* of T.

PROPOSITION 228. λ is an eigenvalue of T if and only if $T - \lambda I$ is not invertible.

PROPOSITION 229. Any set of eigenvectors of T with distinct eigenvalues is linearly independent.

PROPOSITION 230. Suppose $T : V \to W$ is linear, U is a subspace of V, and $\pi_1 : V \to V/U$ and $\pi_2 : W \to W/T(U)$ are natural projections. There is a unique linear map $T/U : V/U \to W/T(U)$ such that $T/U \circ \pi_1 = \pi_2 \circ T$.

DEFINITION 231. This map is the *quotient map*.

DEFINITION 232. Suppose $T : V \to V$ is a linear transformation and

$$p(z) = \sum a_i z^i,$$

where each $a_i \in \mathbb{F}$. Then $p(T) = \sum a_i T^i$.

THEOREM 233. Every operator on a finite-dimensional nonzero complex vector space has an eigenvalue.

DEFINITION 234. In defining the *matrix* of an operator, we choose the same basis for the domain and codomain.

PROPOSITION 235. Suppose V is a finite-dimensional vector space and $T : V \to V$ is an operator. Then T has an upper-triangular matrix with respect to some basis of V.

PROPOSITION 236. Suppose $T : V \to V$ has an upper-triangular matrix with respect to some basis of V. Then the eigenvalues of T are precisely the entries on the diagonal of that matrix.

DEFINITION 237. An operator is *diagonalisable* if it has a diagonal matrix with respect to some basis of the space.

PROPOSITION 238. Let $T : V \to V$ be an operator over a finite-dimensional vector space. Then T is diagonalisable iff V has a basis consisting of eigenvectors of T.

DEFINITION 239. 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 240. The dot product, defined by

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = \sum a_i \overline{b_i},$$

is an inner product over both $\mathbb{R}^n$ and $\mathbb{C}^n$.

PROPOSITION 241 (Cauchy-Schwarz). $|\langle u, v\rangle| \leq \|u\|\|v\|$.

DEFINITION 242. A *normed vector space* is a vector space V over $\mathbb{R}$ or $\mathbb{C}$ on which there is a *norm*: a function $\|\cdot\| : V \to \mathbb{R}$ satisfying

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

PROPOSITION 243. 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 244. 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 245 (Gram-Schmidt). Suppose V is finite-dimensional. Then every orthonormal list of vectors in V can be extended to an orthonormal basis of V.

REMARK 246. Thus, we may identify a finite-dimensional inner product space over $\mathbb{F}$ with $\mathbb{F}^n$ under the usual dot product.

THEOREM 247 (Schur). An operator over a finite-dimensional inner product space has an upper-triangular matrix with respect to an orthonormal basis of the space.

THEOREM 248 (Riesz Representation). 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.

PROPOSITION 249. Let $T : V \to W$ be linear. There exists a unique function $T^* : W \to V$ such that

$$\langle Tv, w\rangle = \langle v, T^*w\rangle$$

for every $v \in V$ and every $w \in W$. The function T^* is linear, and we have $(T^*)^* = T$.

DEFINITION 250. We call T^* the *adjoint* of T.

PROPOSITION 251. The images of T and TT^* are the same; the images of T^* and T^*T are the same.

COROLLARY 252. The ranks of T and T^* are the same.

PROPOSITION 253. Let $T : V \to W$ be linear, where V and W are real or complex vector spaces. Let $\{v_i\}$ be an orthonormal basis for V, and let $\{w_i\}$ be an orthonormal basis for W. Then, the matrix of T^* with respect to $\{w_i\}$ and $\{v_i\}$ is the conjugate transpose of the matrix of T with respect to $\{v_i\}$ and $\{w_i\}$.

DEFINITION 254. Let T be an operator. If $T^* = T$, then T is *self-adjoint*. If $TT^* = T^*T$, then T is *normal*.

PROPOSITION 255. Every eigenvalue of a self-adjoint operator is real.

THEOREM 256 (Spectral). Let $T : V \to V$ be normal, where V is finite-dimensional. Then T has a diagonal matrix with respect to some orthonormal basis of V.

REMARK 257. Thus, we may write $T = UBU^*$, where $UU^* = U^*U = I$ and B is diagonal.

PROPOSITION 258. If A is normal, then B commutes with A iff B commutes with A^*.

DEFINITION 259. Let U and V be vector spaces over $\mathbb{F}$. A function $w : U \times V \to \mathbb{F}$ is called a *bilinear form* if $w(u, v_0)$ and $w(u_0, v)$ are linear for fixed u_0 and v_0.

PROPOSITION 260. The dimension of the space of bilinear forms on $U \times V$ is the product of the dimensions of U and V.

PROPOSITION 261. For any two vector spaces V and W there is a unique (up to isomorphism) vector space $V \otimes W$ and a bilinear map $\otimes : V \times W \to V \otimes W$ such that for any bilinear function $h : V \times W \to Z$ there is a unique linear function $\bar{h} : V \otimes W \to Z$ such that $h(v, w) = \bar{h}(v \otimes w)$.

DEFINITION 262. The space $U \otimes V$ is the *tensor product* of U and V, and for $u \in U$ and $v \in V$ we call $u \otimes v$ the *tensor product* of u and v.

PROPOSITION 263. The following spaces are canonically isomorphic:

- $U^* \otimes V^*$
- $(U \otimes V)^*$
- The space of bilinear functions on $U \times V$.

PROPOSITION 264. If X and Y are bases in U and V, then the set $\{x \otimes y : x \in X, y \in Y\}$ is a basis in $U \otimes V$.

PROPOSITION 265. Let U and V be finite-dimensional vector spaces. There is a unique isomorphism $f : \mathcal{L}(U) \otimes \mathcal{L}(V) \to \mathcal{L}(U \otimes V)$ satisfying

$$f(A \otimes B)(u \otimes v) = Au \otimes Bv.$$

DEFINITION 266. Thus, we identify these two spaces and speak of the tensor product of two operators as an operator on the tensor product of the underlying spaces.

PROPOSITION 267. For each bilinear form f on a finite-dimensional inner product space there is a unique linear map A such that $Q(x, y) = \overline{\langle Ax, y \rangle}$ for all $x, y \in V$. The form f is conjugate symmetric — that is, $f(x, y) = \overline{f(y, x)}$ — iff A is self-adjoint.

DEFINITION 268. A *quadratic form* Q on V is defined by $Q(x) = f(x, x)$, where $f : V \times V \to \mathbb{F}$ is bilinear.

PROPOSITION 269. If Q is a quadratic form on a complex vector space such that its image is contained in $\mathbb{R}$, then there exists a unique conjugate symmetric bilinear form f such that $Q(x) = f(x, x)$.

DEFINITION 270. Two self-adjoint linear maps X and Y are *congruent* if there is some invertible linear map S such that $X = SYS^*$.

PROPOSITION 271. If $Q = \langle Ax, x \rangle$ and $R(y) = \langle By, y \rangle$ are two quadratic forms on V, then there is an invertible linear map L such that $Q(Lx) = R(x)$ iff A and B are congruent.

PROPOSITION 272 (Sylvester's Law of Inertia). If two diagonal matrices are congruent, the numbers of positive, negative, and zero entries are equal in each.

DEFINITION 273. A quadratic form $Q(x) = f(x, x)$ on an inner product space, where f is conjugate symmetric, is called

- *Positive definite* if $Q(x) > 0$ for all $x \neq 0$;
- *Positive semidefinite* if $Q(x) \geq 0$ for all x;
- *Negative definite* if $Q(x) < 0$ for all $x \neq 0$;
- *Negative semidefinite* if $Q(x) \leq 0$ for all x; and
- *Indefinite* otherwise.

A self-adjoint linear map A is called *positive definite* (etc) if the corresponding quadratic form $\langle Ax, x\rangle$ is positive definite (etc).

PROPOSITION 274. T is positive semidefinite iff there exists an operator R such that $T = R^*R$. The matrix R may be taken to be upper triangular, and is invertible iff T is positive definite.

DEFINITION 275. An operator F is a *square root* of an operator T if $R^2 = T$.

PROPOSITION 276. Every positive semidefinite operator has a unique positive semidefinite square root.

DEFINITION 277. If T is a positive semidefinite operator, then $\sqrt{T}$ denotes the unique positive semidefinite square root of T.

DEFINITION 278. Let U be a finite-dimensional subspace of V. The *orthogonal projection* of V onto U is the operator $P_U : V \to V$ defined by $P_U v = u$ where $u \in U$ and $\langle v - u, x\rangle = 0\ \forall x \in U$.

PROPOSITION 279. The orthogonal projection is well defined, and satisfies

$$\|P_u v\| \leq \|v\|.$$

For any $u \in U$, we have

$$\|v - P_U v\| \leq \|v - u\|.$$

PROPOSITION 280. Let A be injective. Then A^*A is invertible, and the projection onto the image of A is $A(A^*A)^{-1}A^*$.

COROLLARY 281 (Least Squares Regression). For any vector b, the vector x that minimises $\|b - Ax\|$ is $(A^*A)^{-1}A^*b$.

DEFINITION 282. A linear transformation is an *isometry* if it preserves norms. An operator which is also an isometry is *unitary*.

PROPOSITION 283. An linear map T is an isometry iff $T^*T = I$.

THEOREM 284 (QR Decomposition). Let $A : V \to W$ be linear, and pick orthonormal bases on V and W. There There exists a unitary operator Q and an upper triangular matrix R such that $A = QR$.

PROPOSITION 285. If $A = QR$ as above and A is injective, then $(A^*A)x = A^*b$ implies $Rx = Q^*b$.

THEOREM 286 (Polar Decomposition). For each operator T, there exists a unitary operator S such that $T = S\sqrt{T^*T}$.

DEFINITION 287. The *singular values* of T are the eigenvalues of $\sqrt{T^*T}$, where each eigenvalue λ is counted the same number of times as the dimension of its eigenspace.

PROPOSITION 288. The nonzero singular values of T and of T^* coincide.

THEOREM 289 (Singular Value Decomposition). Suppose $T : V \to W$ has singular values $s_1, \ldots, s_n$. Then there exist orthonormal bases $e_1, \ldots, e_n$ of V and $f_1, \ldots, f_n$ of W such that

$$Tv = \sum_i s_i \langle v, e_i \rangle f_i$$

for all $v \in V$.

PROPOSITION 290. Let $T : V \to W$ be a linear transformation. There exists a unique linear transformation $T^+ : W \to V$ such that

- $TT^+T = T$;
- $T^+TT^+ = T^+$;
- TT^+ and T^+T are self-adjoint.

DEFINITION 291. This transformation T^+ is known as the *pseudoinverse* of T.

PROPOSITION 292. If T is injective, then $T^+T = I$. If T is surjective, then $TT^+ = I$.

PROPOSITION 293. The perpendicular projection onto the image of T is TT^+.

DEFINITION 294. A vector v is called a *generalised eigenvector* of T corresponding to an eigenvalue λ if $v \neq 0$ and $(T - \lambda I)^j v = 0$ for some positive integer j.

The *generalised eigenspace* of T corresponding to λ is the set of all generalised eigenvectors of T corresponding to λ, along with the 0 vector.

PROPOSITION 295. For finite-dimensional V, v is a generalised eigenvector of T iff $(T - \lambda I)^{\dim V} v = 0$.

PROPOSITION 296. Generalised eigenvectors corresponding to distinct eigenvalues are linearly independent.

PROPOSITION 297. Suppose V is a finite-dimensional complex vector space, and T is an operator on V. Then there is a basis of V consisting of generalised eigenvectors of T.

DEFINITION 298. The *multiplicity* of an eigenvalue λ of T is the dimension of the corresponding generalised eigenspace.

PROPOSITION 299. If T is diagonalisable, then the multiplicity of λ equals the number of times that λ appears in the diagonal matrix of T with respect to any basis.

PROPOSITION 300. Every operator on a nonzero finite-dimensional real vector space has an invariant subspace of dimension 1 or 2.

DEFINITION 301. A linear transformation T is *nilpotent* if $T^q = 0$ for some positive integer q. The least positive integer q such that this is true is called the *index* of T.

DEFINITION 302. If X is a complement of Y, and X and Y are both invariant under T, then T is said to be *decomposed* by X and Y.

PROPOSITION 303. For every linear transformation A on a finite-dimensional vector space V, there are unique subspaces X and Y on V such that A is decomposed by X and Y, $A|_X$ is nilpotent, and $A|_Y$ is invertible.

PROPOSITION 304. If A is nilpotent with index q on a finite-dimensional vector space V, then there exist positive integers $r, q = q_1 \geq \cdots \geq q_r$ and vectors $x_1, \ldots, x_r$ such that $\{A^j x_i : 1 \leq i \leq r, j < q_r\}$ is a basis for V and $A^{q_i} x_i = 0$ for all i.

DEFINITION 305. A *block diagonal matrix* is a square matrix of the form

$$\begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix},$$

where each A_i is a square matrix lying along the diagonal and all other entries of the matrix are 0.

THEOREM 306 (Jordan Form). If T is an operator on a finite-dimensional complex vector space, then there is a basis such that the matrix of T with respect to this basis is block diagonal with blocks of the form

$$\begin{pmatrix} \lambda_i & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{pmatrix},$$

where each λ_i is a distinct eigenvalue of T.

DEFINITION 307. The *trace* of a square matrix A is the sum of the diagonal entries of A.

PROPOSITION 308. If T is an operator over a finite-dimensional vector space V, and $\{a_i\}$ and $\{b_i\}$ are two bases for V, then the trace of the matrix of T with respect to $\{a_i\}$ equals the trace of the matrix of T with respect to $\{b_i\}$.

DEFINITION 309. We call this quantity the *trace* of T.

PROPOSITION 310. The trace is additive; further, the traces of $AB + kI$ and of $BA + kI$ are equal.

PROPOSITION 311. If V is complex, then the trace of T equals the sum of the eigenvalues of T counted according to multiplicity.

DEFINITION 312. We define $\otimes^k V^*$ to be the n-times tensor product of V^* with itself, identifying it with the space of functions on V^k which are linear in each element. Its elements are called *k-linear forms*.

DEFINITION 313. A k-linear form on V is *alternating* if its value is 0 whenever two of its arguments are equal. The set of alternating k-linear forms on V is denoted $\wedge^k V^*$.

PROPOSITION 314. If $x_1, \ldots, x_k$ are linearly dependent vectors and w is an alternating k-linear form, then $w(x_1, \ldots, x_k) = 0$.

DEFINITION 315. We define $Alt(f) = \frac{1}{k!}\sum_\pi \operatorname{sign}(\pi) f \circ \pi$ and $\operatorname{Alt} = \frac{1}{k!} Alt$.

PROPOSITION 316. The function Alt is a projection from the space of k-linear forms to the space of alternating k-linear forms.

PROPOSITION 317. If $\operatorname{Alt}(f_1) = \operatorname{Alt}(f_2)$ and $\operatorname{Alt}(g_1) = \operatorname{Alt}(g_2)$ then $\operatorname{Alt}(f_1 \otimes g_1) = \operatorname{Alt}(f_2 \otimes g_2)$.

DEFINITION 318. We define the *wedge product* as $\operatorname{Alt}(f) \wedge \operatorname{Alt}(g) = \operatorname{Alt}(f \otimes g)$.

REMARK 319. Conventions differ here; some instead define $Alt(f) \wedge Alt(g) = Alt(f \otimes g)$. This is nicer for some applications (especially integration) since the wedge product of a dual basis $\{b_i^*\}$, evaluated on the basis $\{b_i\}$, gives 1 instead of $\frac{1}{n!}$.

PROPOSITION 320. A subset of V^* is linearly independent iff its wedge product (taken in any order) is nonzero.

PROPOSITION 321. If V is an n-dimensional vector space for $n > 0$, then $\wedge^n V^*$ has dimension $\binom{m}{n}$.

PROPOSITION 322. Let $A : V \to W$ be linear, and let n be fixed. There is a unique operator $\wedge^n A : \wedge^n W^* \to \wedge^n V^*$ such that for each $p \in \wedge^n W^*$ we have $p(Av_1, \ldots, Av_n) = \wedge^n A p(v_1, \ldots, v_n)$. We have $\wedge^n AB = \wedge^n A \wedge^n B$.

DEFINITION 323. If $V = W$ has dimension n, then $\wedge^n A$ must be equivalent to multiplication by some scalar. We call this scalar $|A|$ the *determinant* of A, also denoted $\det A$.

PROPOSITION 324. A is invertible iff $\det A \neq 0$.

PROPOSITION 325. $\det A = \det A' = \det A^*$.

COROLLARY 326. If A is unitary, then $\det A = \pm 1$.

PROPOSITION 327. Let $a, b \in \mathbb{R}^3$. There exists a unique vector $a \times b$ such that for for any vector c, $(a \times b) \cdot c$ is the determinant of the operator which sends the standard basis to a, b, c.

DEFINITION 328. This vector is the *cross product* of a and b.

PROPOSITION 329. We have the following identities:

- $a \times b + b \times a = 0$
- $a \times (b \times c) + b \times (c \times a) + c \times (a \times b) = 0$.

DEFINITION 330. If π is a permutation of $\{1, 2, \ldots, n\}$, the sign of π is -1^k, where $k = |\{(a, b) \in \{1, 2, \ldots, n\} : a < b,\ \pi(a) > \pi(b)\}|$.

PROPOSITION 331. Let A be $n \times n$. The determinant of the linear transformation defined by A equals

$$\sum_\pi \operatorname{sign}(\pi) \prod_{i=1}^n A_{\pi(i),i},$$

where the sum is taken over all permutations π of $\{1, 2, \ldots, n\}$.

DEFINITION 332. Let V be finite-dimensional. An *orientation* of V is a function f from the set of bases of V to $\{-1, 1\}$ such that $f(\{u_i\})f(\{v_i\})$ has the same sign as the determinant of the linear map that takes each u_i to the corresponding v_i.

DEFINITION 333. For an $n \times n$ matrix A, let $A_{j,k}$ denote the $(n-1) \times (n-1)$ matrix obtained from A by crossing out row number j and column number k. The numbers $C_{j,k} = (-1)^{j+k} \det A_{j,k}$ are the *cofactors* of A. Let C be the matrix whose entries are the cofactors of a given matrix A.

THEOREM 334 (Cofactor expansion). $AC^T = (\det A)I$.

COROLLARY 335 (Cramer's rule). For an invertible matrix A, the kth component of the solution of the equation $Ax = b$ is given by

$$x_k = \frac{\det B_k}{\det A},$$

where the matrix B_k is obtained from A by replacing the kth column of A by B.

PROPOSITION 336. If V is a complex vector space, then the determinant of T equals the product of the eigenvalues of T counted according to multiplicity.

DEFINITION 337. Let T be an operator on a finite-dimensional vector space. The *characteristic polynomial* p of T is defined by

$$p(\lambda) = \det(T - \lambda I).$$

THEOREM 338 (Cayley-Hamilton). Let p be the characteristic polynomial of T. Then $p(T) = 0$.

PROPOSITION 339. If T is an operator on a finite-dimensional complex vector space, then the characteristic polynomial p of T satisfies

$$p(z) = \prod(\lambda_i - z),$$

where λ_i are the eigenvalues of T counted according to multiplicity.

COROLLARY 340. All eigenvalues of A are positive iff A is positive definite.

PROPOSITION 341 (Sylvester's Criterion). Let A be self-adjoint. Then A is positive definite iff for each k, the determinant of the top-left $k \times k$ submatrix of A is positive.

References.

- Strang, *Linear Algebra and its Applications*
- Treil, *Linear Algebra Done Wrong*
- Axler, *Linear Algebra Done Right*
- Halmos, *Finite-Dimensional Vector Spaces*

4. Analysis

DEFINITION 342. A *topology* on a set X is a collection T of *open sets* in X such that $\emptyset, X \in T$, and T is closed under arbitrary unions and finite intersections. A set for which a topology has been specified is a *topological space*. Given $x \in X$, a *neighbourhood* of x is an element $U \in T$ such that $x \in U$.

DEFINITION 343. If X is a set, a *basis* for a topology on X is a collection B of subsets of X such that $\bigcup B = X$, and if $B_1, B_2 \in B$ have nonempty intersection then there is a $B_3 \in B$ contained in their intersection.

PROPOSITION 344. If B is a basis for a topology on X, the collection of all unions of elements of B defines a topology on X.

DEFINITION 345. This is the topology *generated* by B.

PROPOSITION 346. Let X be a topological space with topology T. If Y is a subset of X, the collection $T_Y = \{Y \cap U : U \in T\}$ is a topology on Y.

DEFINITION 347. This is the *subspace topology*.

DEFINITION 348. Let E be a subset of a topological space M.

- A point p is a *limit point* of E if neighbourhood of p contains a point $q \neq p$ such that $q \in E$.
- A point p is a *condensation point* of E if every neighbourhood o fp contains uncountably many points of E.
- A point p is an *interior point* of E if there is a neighbourhood of p which is a subset of E.
- E is *closed* if every limit point of E is a point of E.
- E is *open* if every point of E is an interior point of E.
- E is *perfect* if E is closed and every point of E is a limit point of E.
- The *complement* E^c of a set E is the set $M \setminus E$.
- The *interior* of E is the set of interior points of E.
- The *boundary* ∂E of E is the set of points of M that are limit points of both E and E^c.
- The *closure* of E is the set $\overline{E} = E \cup \partial E$.

PROPOSITION 349. The interior and boundary of E are disjoint, and their union is E.

PROPOSITION 350. The following are equivalent:

- E is its own interior.
- $E \cap \partial E = \emptyset$.
- E^c contains its limit points.
- $\partial E \subseteq E^c$.

PROPOSITION 351. The closure of E is closed; the interior of E is open.

Any closed set which contains E contains the closure of E. Any open set which is contained in E is contained in the interior of E.

DEFINITION 352. A sequence $\{a_n\}$ is *convergent* if there is a point L such that every neighbourhood of L contains all but finitely many a_n. We write $\lim_{n\to\infty} a_n = L$, or $a_n \to L$ as $n \to \infty$.

DEFINITION 353. A set E is *connected* if the only subsets of E that are both open and closed in E are the empty set and E itself; otherwise, it is *disconnected*. It is *path-connected* if for all $x, y \in E$ there is a continuous function $f : [0, 1] \to E$ such that $f(0) = x$ and $f(1) = y$. It is *contractible* if there is a continuous map $f : [0, 1] \times E \to E$ such that $f(0, x) = x$ and $f(1, x)$ is constant.

PROPOSITION 354.

- Every open connected set is path-connected.
- Every path-connected set is connected.
- Every contractible set is path-connected.

PROPOSITION 355. A topological space is disconnected iff it is the union of two disjoint nonempty open sets.

DEFINITION 356. We say that f is *continuous* at p if for each neighbourhood B of $f(p)$, there is a neighbourhood A of p such that $f(A) \subseteq B$.

We say that f is *continuous* on X, or simply *continuous*, if it is continuous at every point in X.

PROPOSITION 357. A function is continuous iff the inverse image of every open set is open.

PROPOSITION 358. A continuous image of a connected set is connected.

PROPOSITION 359. A monotonic function $f : [a, b] \to \mathbb{R}$ has at most countably many discontinuities.

DEFINITION 360. An *open cover* of a topological space E is a set of open sets whose union contains E.

DEFINITION 361. A set E is said to be *compact* if every open cover of E contains a finite subcover.

PROPOSITION 362. Suppose $X \subseteq M$. A subset E of X is compact relative to X (under the subspace topology) iff E is compact relative to M.

PROPOSITION 363. If S is a collection of closed subsets of a compact space such that any finite intersection of elements of S is nonempty, then $\bigcap S$ is nonempty.

PROPOSITION 364. A continuous image of a compact set is compact.

DEFINITION 365. A topological space is *Hausdorff* if for every pair (a, b) of distinct points, there are disjoint neighbourhoods A of a and B of b.

PROPOSITION 366. If $f : X \to Y$ is a continuous bijection, X is compact, and Y is Hausdorff, then f^{-1} is continuous.

DEFINITION 367. A *metric space* is a nonempty set M together with a function $d : M \times M \to \mathbb{R}$ (the *metric*) such that

- $d(x, y) = 0 \iff x = y$,
- $d(x, y) = d(y, x)$ (symmetry),
- $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

DEFINITION 368. In a metric space, the *open ball* $B_r(x)$ with centre x and radius r is the set of all points y with $d(x, y) < r$.

The *closed ball* $\overline{B_r(x)}$ with centre x and radius r is the set of all points y with $d(x, y) \leq r$.

PROPOSITION 369. In a normed vector space, the function $d(x, y) = \|x - y\|$ is a metric.

DEFINITION 370. We call this the *induced metric*.

PROPOSITION 371. The set of open balls on a metric space is a basis for a topology.

PROPOSITION 372. Suppose $\{a_n\}$ and $\{b_n\}$ are sequences of complex numbers which converge to a and b respectively. Then the sequences $\{a_n + b_n\}, \{a_n b_n\}, \{\frac{a_n}{b_n}\}$ converge to $a + b, ab, \frac{a}{b}$ respectively (where in the last one we require $b_n \neq 0$ for each n, and $b \neq 0$).

DEFINITION 373. Let E be a subset of a metric space X.

- E is *bounded* if it is contained in some open ball.
- E is *totally bounded* if for any $\varepsilon > 0$ there are a finite number of open balls of radius ε which cover E.

THEOREM 374 (Monotone Convergence). A monotonic sequence in $\mathbb{R}$ converges iff it is bounded.

DEFINITION 375. A sequence $\{p_n\}$ in a metric space is *Cauchy* if for every $\varepsilon > 0$ there is an integer N such that $d(p_n, p_m) < \varepsilon$ if $m, n \geq N$.
A metric space is *complete* if every Cauchy sequence converges.

PROPOSITION 376. Every convergent sequence is Cauchy.

PROPOSITION 377. A sequence in $\mathbb{R}^n$ or $\mathbb{C}^n$ converges iff it converges coordinatewise.

COROLLARY 378. $\mathbb{R}^n$ and $\mathbb{C}^n$ are complete.

PROPOSITION 379. Let M be a metric space. The following are equivalent:

- M is compact.
- M is complete and totally bounded.
- Every infinite set in M contains a limit point.
- Every sequence of open sets $S_1 \subseteq S_2 \subseteq \cdots$ fails to cover M.

COROLLARY 380 (Weierstrass). Every bounded infinite subset of $\mathbb{R}^n$ has a limit point.

COROLLARY 381 (Extreme Value Theorem). If the domain of f is compact and the codomain of f is $\mathbb{R}$, then the image of f is closed and bounded. In particular, f attains its minimum and maximum.

PROPOSITION 382. Let $S \subseteq \mathbb{R}$. The following are equivalent:

- S is connected.
- If $a, b \in S$ and $a \leq c \leq b$ then $c \in S$.
- There are real numbers a, b such that S contains all elements c with $a < c < b$ and no elements with $a > c$ or $b < c$.

DEFINITION 383. Such a set is called an *interval*.

COROLLARY 384 (Intermediate Value Theorem). If the domain of f is connected and the codomain of f is $\mathbb{R}$, then the image of f is an interval.

PROPOSITION 385. For every uncountable subset A of $\mathbb{R}^n$, the set A' of its condensation points is nonempty and perfect. Further, $A \setminus A'$ is at most countable.

PROPOSITION 386. There exists a perfect set in $\mathbb{R}$ which contains no segment.

PROPOSITION 387. Every nonempty perfect set in $\mathbb{R}^n$ has cardinality $|\mathbb{R}|$.

THEOREM 388 (Baire). To each countable ordinal α, assign a closed set $S_\alpha \subseteq \mathbb{R}^n$, such that if $\alpha < \beta$ then $S_\beta \subseteq S_\alpha$. The intersection of all sets thus defined equals S_γ for some countable ordinal γ.

COROLLARY 389 (Cantor-Bendixson). Let S be a closed set, and define $S^{(\alpha)}$ for every ordinal α such that

- $S^{(0)} = S$
- $S^{(\alpha+1)}$ is the set of limit points of $S^{(\alpha)}$
- $S^{(\alpha)}$ is the intersection of all $S^{(\beta)}$ for $\beta < \alpha$, if α is a limit ordinal.

Then there is an ordinal γ which is at most countable such that $S^{(\gamma)}$ is the set of condensation points of S.

DEFINITION 390. A function f is *uniformly continuous* if for every $\varepsilon > 0$ there exists a $\delta > 0$ such that if $d(a, b) < \delta$ then $d(f(a), f(b)) < \varepsilon$.

THEOREM 391. Every continuous function on a compact metric space is uniformly continuous.

DEFINITION 392. It is *Lipschitz continuous* if for every there is a real constant K such that $d(f(a), f(b)) \leq Kd(a, b)$ for all a and b. If $K < 1$ then f is a *contraction*.

PROPOSITION 393 (Contraction Principle). A contraction on a complete metric space has a unique fixed point.

DEFINITION 394. Let $\{a_i\}$ be a sequence in A, where A is a normed vector space. If the limit on the right exists,

$$\sum_{i=1}^{\infty} a_i = \lim_{n\to\infty} \sum_{i=1}^{n} a_i.$$

Otherwise, the series *diverges*.

PROPOSITION 395. If $\sum a_n$ converges, then $\lim_{n\to\infty} a_n = 0$.

PROPOSITION 396. The series $\sum x^n$ converges iff $|x| < 1$, in which case its value is $\frac{1}{1-x}$.

PROPOSITION 397 (Comparison test). If $\|a_n\| \leq c_n$ for all sufficiently large n, and $\sum c_n$ converges, then so does $\sum a_n$.

COROLLARY 398. If $\sum \|a_n\|$ converges then so does $\sum a_n$.

DEFINITION 399. Such a sequence is said to *converge absolutely*.

PROPOSITION 400 (Cauchy condensation test). If $\{a_n\}$ is nonincreasing, then $\sum a_n$ converges iff $\sum 2^n a_{2^n}$ converges.

COROLLARY 401. $\sum n^{-s}$ converges iff $s > 1$.

PROPOSITION 402. $\sum \frac{1}{n!} = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$.

DEFINITION 403. We let this limit be e.

DEFINITION 404. We define the *extended real number system* as $\mathbb{R} \cup \{-\infty, \infty\}$ and extend the operations by $x + \infty = \infty, x - \infty = -\infty, \frac{x}{\infty} = 0$ and for $x > 0$, $x\infty = \infty, x(-\infty) = -\infty$.

If $S \subseteq \mathbb{R}$ is unbounded above, then $\sup S = \infty$. If it is unbounded below, then $\inf S = -\infty$.

We may regard the set $\{x \in \mathbb{R} : x > a\}$ as an open ball around ∞, and $\{x \in \mathbb{R} : x < -a\}$ as an open ball around $-\infty$. Clearly, the set of open balls still forms a basis for a topological vector space.

DEFINITION 405. We define

$$\limsup_{n\to\infty} s_n = \lim_{n\to\infty} \sup_{m\geq n} s_m.$$

We define $\liminf_{n\to\infty} s_n$ similarly.

PROPOSITION 406 (Root test). Let $\alpha = \limsup_{n\to\infty} \sqrt[n]{|a_n|}$. If $\alpha < 1$ then $\sum a_n$ converges; if α_1 then $\sum a_n$ diverges.

PROPOSITION 407. If $\{a_i\}$ is a sequence of positive reals,

$$\liminf_{n\to\infty} \frac{a_{n+1}}{a_n} \leq \liminf_{n\to\infty} \sqrt[n]{a_n}$$
$$\limsup_{n\to\infty} \frac{a_{n+1}}{a_n} \geq \limsup_{n\to\infty} \sqrt[n]{a_n}.$$

COROLLARY 408 (Ratio test). Let $b_n = \frac{\|a_{n+1}\|}{\|a_n\|}$. If $\limsup_{n\to\infty} b_n < 1$, then $\sum a_n$ converges. If $\sum a_n$ converges, then $b_n < 1$ for infinitely many n.

DEFINITION 409. Given a sequence $\{c_n\}$ of complex numbers, the series

$$\sum_{n=0}^{\infty} c_n z^n$$

is a *power series* in a complex number z.

PROPOSITION 410. Let $\alpha = \limsup_{n\to\infty} \sqrt[n]{|c_n|}$. Then $\sum c_n z^n$ converges if $|z| < \frac{1}{\alpha}$ and diverges if $|z| > \frac{1}{\alpha}$.

DEFINITION 411. We call α the *radius of convergence* for $\sum c_n z^n$.

PROPOSITION 412. Suppose the partial sums of $\sum a_n$ are bounded, $\{b_n\}$ is decreasing, and $\lim_{n\to\infty} b_n = 0$. Then $\sum a_n b_n$ converges.

COROLLARY 413. If $\{c_i\}$ is decreasing and converges to 0, $\sum c_n z^n$ has radius of convergence r, and $|z| = r \neq z$, then $\sum c_n z^n$ converges.

PROPOSITION 414. If $\sum a_n$ converges absolutely and $\sum b_n$ converges, then

$$\sum_n \sum_k a_k b_{n-k} = \left(\sum a_n\right)\left(\sum b_n\right).$$

PROPOSITION 415. If $\sum a_n$ converges absolutely then so does $\sum b_n$, where $\{b_n\}$ is any permutation of $\{a_n\}$.

PROPOSITION 416. If $\{a_n\}$ are real and $\sum a_n$ converges but does not converge absolutely, then $\sum b_n$ can be made to diverge or converge to any value, where $\{b_n\}$ is a permutation of a_n.

DEFINITION 417. Two norms on a vector space are said to be *equivalent* if they induce the same topology.

PROPOSITION 418. Any two norms on a finite-dimensional vector space are equivalent.

DEFINITION 419. Let L be a linear transformation on a normed vector space V. We say that L is *bounded* if there is some real K such that $\|Lx\| \leq K\|x\|$ for all $x \in V$. The greatest lower bound of all such K is denoted $\|L\|$.

PROPOSITION 420. Let V and W be finite-dimensional normed vector spaces. The function $\|\cdot\| : \mathcal{L}(V,W) \to \mathbb{R}$ is a norm on $\mathcal{L}(V,W)$; any two such norms are equivalent.

PROPOSITION 421. Let A be a self-adjoint linear map on a normed vector space V, and let $S = \{\langle Ax, x\rangle : \|x\| = 1\}$. Then, $\|A\| = \max\{|\inf S|, |\sup S|\}$.

PROPOSITION 422 (Min-Max Theorem). Let A be a self-adjoint linear map on an n-dimensional inner product space V. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of A according to multiplicity. Then for each k we have

$$\lambda_k = \inf\{\|A|_U\| : \dim U = n - k + 1\}.$$

THEOREM 423 (Ergodic Theorem). If U is an isometry on a finite-dimensional inner product space, and if M is the subspace of all solutions of $Ux = x$, then the sequence

$$\frac{1}{n}(1 + U + \cdots + U^{n-1})$$

converges to P_M.

PROPOSITION 424. Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series with radius of convergence r. If A is such that $\|A\| < r$, then $f(A)$ exists.

PROPOSITION 425. Let A be a contractive operator on a finite-dimensional normed vector space. Then, $(I - A)\sum_{n=0}^{\infty} A^n = I$.

DEFINITION 426. Let X and Y be metric spaces. We define Y^X as the space of functions $f : X \to Y$, and give it the *uniform metric* $\|f\| = \sup_x \max(1, f(x))$.

PROPOSITION 427. Under this definition, Y^X is a normed vector space.

PROPOSITION 428. If Y is complete, then so is Y^X.

DEFINITION 429. Suppose $\{f_n\}$ is a sequence in Y^X such that $\{f_n(x)\}$ converges for every x. We then say that $\{f_n\}$ *converges pointwise* to the function $f(x) = \lim f_n(x)$.

If $f = \lim f_n$, we say the sequence *converges uniformly* to f.

DEFINITION 430. Let $f : X \to Y$ be a function, where X and Y are metric spaces. Let p be a limit point of X. We say that

$$\lim_{x \to p} f(x) = q$$

if for every sequence $\{x_n\}$ which converges to p but does not contain p, $f(x_n)$ converges to q.

PROPOSITION 431. Assume $\{f_n\}$ converges uniformly and $\lim_{t\to x} f_n(t)$ is defined for all n. Then, $\lim_{t\to x}\lim_{n\to\infty} f_n(x) = \lim_{n\to\infty}\lim_{t\to x} f_n(x)$.

PROPOSITION 432. If X and Y are compact, then every sequence in Y^X has a subsequence that converges pointwise.

COROLLARY 433. The limit of a uniformly convergent sequence of continuous functions is continous.

DEFINITION 434. A sequence $\{f_n\} \in Y^X$ is said to be *equicontinuous* if for every $\varepsilon > 0$ there exists a $\delta > 0$ such that if $d(a,b) < \delta$ then $d(f_n(a), f_n(b)) < \varepsilon$ for all n.

PROPOSITION 435. If X is compact, all $\{f_n\}$ are continuous, and $\{f_n\}$ converges uniformly, then $\{f_n\}$ is equicontinuous.

PROPOSITION 436. If X and Y are compact, then every equicontinuous sequence in Y^X has a convergent subsequence.

DEFINITION 437. Let $A \subseteq \mathbb{R}^K$ be an algebra. If for each $x_1, x_2 \in K$ there is a function $f \in A$ such that $f(x_1) \neq f(x_2)$, then A is said to *separate points*. If for each $x \in K$ there is an $f \in A$ such that $f(x) \neq 0$, then A is said to *vanish at no point*.

THEOREM 438 (Stone-Weierstrass). Let $A \subseteq \mathbb{R}^K$ be an algebra of continuous functions on a compact set K which separates points and vanishes at no point. Then the closure of A is the set of real continuous functions on K.

COROLLARY 439. Let A be an algebra of complex continuous functions on a compact set K, such that A separates points and vanishes at no point. If A is closed under complex conjugation, the closure of A is the set of complex continuous functions on K.

COROLLARY 440 (Weierstrass). Every continuous function $f : D \to \mathbb{C}$, where D is a compact subset of $\mathbb{R}$, is a limit of a sequence of polynomials.

DEFINITION 441. An *analytic function* is a function of the form

$$f(x) = \sum c_n (x-a)^n,$$

where the radius of convergence is positive (and possibly infinite).

PROPOSITION 442. If $\varepsilon > 0$ and f is analytic with radius of convergence R, then $\sum c_n (x-a)^n$ converges uniformly for $x \in B_{R-\varepsilon}(a)$.

THEOREM 443 (Abel). An analytic function is continuous.

COROLLARY 444. Assuming all three sums converge,

$$\sum_n \sum_k a_k b_{n-k} = \left(\sum a_n\right)\left(\sum b_n\right).$$

THEOREM 445 (Taylor). If f is analytic with radius R around 0, and $a < R$, then f is analytic with radius at least $|R| - |a|$ around a.

PROPOSITION 446. If two analytic functions are equal on a set S which has a limit point, then they are equal.

DEFINITION 447. If A is a complete normed commutative algebra over $\mathbb{R}$, we define the *exponential*

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

PROPOSITION 448. We have $\exp(z+w) = \exp(z)\exp(w)$ and $\exp(a/b) = \sqrt[b]{e^a}$ for any integer a and positive integer b.

PROPOSITION 449. Let A be an operator on a complex finite-dimensional normed vector space. The eigenvalues of $\exp A$, together with their multiplicities, are equal to the exponentials of the eigenvalues of A.

PROPOSITION 450. Let A and B be operators on a finite-dimensional normed vector space such that $AB = BA$. Then, $\exp(A+B) = \exp A \exp B$.

PROPOSITION 451. The function $\exp|_{\mathbb{R}}$ has image $\mathbb{R}^+$ and is strictly increasing.

DEFINITION 452. We define the *natural logarithm* $\ln : \mathbb{R}^+ \to \mathbb{R}$ as the left-inverse of $\exp|_{\mathbb{R}}$.

PROPOSITION 453. The function $\exp(ix)|_{\mathbb{R}}$ attains exactly the values on the unit circle.

DEFINITION 454. We let π be the smallest positive real such that $\exp(i\pi) = -1$. We let $\cos(x) = \frac{\exp(ix)+\exp(-ix)}{2}$, $\sin(x) = \frac{\exp(ix)-\exp(-ix)}{2i}$, and $\tan(x) = \frac{\sin(x)}{\cos(x)}$.

PROPOSITION 455. The functions sin and cos have image $[-1,1]$; the function tan has image $\mathbb{R}$. The functions $\sin|_{[-\pi/2,\pi/2]}$, $\cos|_{[0,\pi]}$ and $\tan|_{(-\pi/4,\pi/4)}$ have the same images and are injective.

DEFINITION 456. The left-inverses of these three functions are denoted arcsin, arccos and arctan.

References.

- Rudin, *Principles of Mathematical Analysis*
- Tao, *Analysis II*

5. Calculus

DEFINITION 457. Let $f : E \to Y$ be a function. If there exists a linear map $A : X \to Y$ such that

$$\lim_{h\to 0} \frac{\|f(x+h) - f(x) - Ah\|}{\|h\|} = 0,$$

then f is said to be *differentiable at* x, A is said to be the *derivative* of f at x, and we write $f'(x) = A$ or $DF_x = A$. If f is differentiable at every $x \in E$, we say that f is *differentiable*.

PROPOSITION 458. If f is differentiable at x, then $f'(x)$ is uniquely defined.

PROPOSITION 459. If A is linear and $f(x) = Ax$, then $f'(x) = A$.

PROPOSITION 460 (Chain Rule). Let $f : E \to F$ and $g : F \to G$ be such that f is differentiable at x and g is differentiable at $f(x)$. Then

$$(g \circ f)'(x) = g'(f(x))f'(x).$$

PROPOSITION 461 (Sum Rule). $(f+g)' = f' + g'$.

PROPOSITION 462. If A is bilinear, then

$$A(f(x), g(x))'(x)h = A(f'(x)h, g(x)) + A(f(x), g'(x)h).$$

COROLLARY 463 (Product and Quotient Rule). If the codomain of g is $\mathbb{R}$, then

- $(fg)' = f'g + fg'$.
- $(f/g)' = \frac{f'g - fg'}{g^2}$ (if $g \neq 0$).

PROPOSITION 464. We have:

- $\exp' = \exp$

- $\ln'(x) = \frac{1}{x}$
- $\sin' = \cos$
- $\cos' = -\sin$
- $\tan'(x) = 1 + \tan^2(x)$
- $\arcsin'(x) = \frac{1}{\sqrt{1-x^2}}$
- $\arccos'(x) = \frac{-1}{\sqrt{1-x^2}}$
- $\arctan'(x) = \frac{1}{1+x^2}$

PROPOSITION 465. Suppose $\{f_n'\}$ converges uniformly and $\{f_n(x_0)\}$ converges. Then

$$\left(\lim_{n\to\infty} f_n\right)' = \lim_{n\to\infty} f_n'.$$

PROPOSITION 466. Let $f : [a, b] \to \mathbb{R}$ be differentiable. Then the image of f' contains $[f'(a), f'(b)]$.

DEFINITION 467. The *directional derivative* $D_u f$ is defined as

$$D_u f(x) = \lim_{t\to 0} \frac{f(x+tu) - f(x)}{t}.$$

PROPOSITION 468. The derivative Df exists and is continuous iff $D_u f$ exists and is continuous for every u. In this case we have $D_u f(x) = f'(x)u$.

PROPOSITION 469 (Mean Value Theorem). Let $f : X \to \mathbb{F}$, and let $x, y \in X$ such that the line segment joining x and y lies in X and $D_{y-x} f$ exists everywhere on that line. Then there exists a point c on this line segment such that $D_{y-x}(c) = \frac{f(y)-f(x)}{\|y-x\|}$.

PROPOSITION 470. Suppose X is convex and $\|f'(x)\| \le M$ for all $x \in X$. Then, for $a, b \in E$ we have $\|f(b) - f(a)\| \le M\|b - a\|$.

PROPOSITION 471 (L'Hôpital's Rule). Let a be a limit point of an open subset L of the extended real number system, let $f, g : L \to \mathbb{R}$ be differentiable, and suppose $g' \neq 0$ on L. If $\frac{f'(x)}{g'(x)} \to A$ as $x \to a$, and either

- $f(x), g(x) \to 0$ as $x \to a$, or
- $g(x) \to \pm\infty$ as $x \to a$,

then $\frac{f(x)}{g(x)} \to A$ as $x \to a$.

DEFINITION 472. A continuous function is C^0. If the derivative of a function exists and is C^n, then the function is C^{n+1}. If a function is C^n for all n, it is C^∞.

DEFINITION 473. We use the notation $d^n f_x$ for the nth order derivative of f at x, defining $d^0 f_x = x$.

PROPOSITION 474. If f and g are C^n, then so are $f+g$, $f \cdot g$ and f/g (assuming the codomains match).

PROPOSITION 475. If $D_v f$, $D_u f$ and $D_v D_u f$ exist in an open ball containing x, and if $D_v D_u f$ is continuous at x, then $D_u D_v f(x) = D_v D_u f(x)$.

COROLLARY 476. If f is C^n, then $f^{(n)}(x)$ (the nth derivative) is a symmetric multilinear map.

DEFINITION 477. An open set D is *star-shaped* with respect to $A \in D$ if for every $B \in D$ the segment AB is in D.

THEOREM 478 (Taylor). Let D be star-shaped with respect to A, and let $f : D \to V$ be n-times differentiable. Let

$$R_{n+1}(x) = f(a+x) - \sum_{i=0}^{n} \frac{d^i f_a(x, x, \ldots, x)}{i!}.$$

We have

$$\lim_{x \to a} \frac{R_{n+1}(x)}{\|x-a\|^n} = 0.$$

If f is $(n+1)$-times differentiable and its codomain is $\mathbb{R}$, we have the following expressions for the remainder:

- There is a $t \in [0,1]$ such that $R(x) = \frac{d^{n+1} f_a(tx)}{(n+1)!}$.
- If $g(t) = f(a + (x-a)t)$, then

$$R(x) = \frac{1}{n!} \int_0^1 (1-t)^n g^{(n+1)}(t) \mathrm{d}t.$$

PROPOSITION 479 (Second derivative test). Let $f : X \to \mathbb{R}$ be C^2, where $X \subseteq \mathbb{R}^n$. Let a be a point of f such that $f'(a) = 0$. We define the *Hessian matrix* $H_f(a)$ to be the matrix representation of $f''(a)$ using the standard bases for $\mathbb{R}^n$ and its dual space.

- If $H_f(a)$ is positive (resp. negative) definite, then f has a local minimum (resp. maximum) at a.
- If f has a local minimum (resp. maximum) at a, then $H_f(a)$ is positive (resp. negative) semidefinite.

DEFINITION 480. A collection $\{g_i : M \to [0,1]\}$ of C^∞ functions is a *partition of unity* if

- each g_i has compact support,
- each $x \in M$ has a neighbourhood V_x such that all but finitely many g_i are 0 on V_x, and
- $\sum g_i = 1$ everywhere on M.

A partition of unity $\{g_i\}$ is *subordinate* to an open cover $\{U_j\}$ of m if for every i the support of g_i is contained in some U_j.

THEOREM 481. Let $\{U_i\}$ be an open covering of M. There exists a partition of unity $\{g_i\}$ subordinate to $\{U_i\}$.

DEFINITION 482. A *k-cell* S is a product of k closed intervals. Its *volume* is $v(S)$, the product of the lengths of the intervals.

DEFINITION 483. A *partition* of a closed interval $[a,b]$ is a sequence $t_0, \ldots, t_k$, where $a = t_0 \leq t_1 \ldots \cdots \ldots t_k = b$.

A *partition* of a k-cell is a sequence of k partitions $\{P_i\}$, where each P_i is a partition of the corresponding $[a_i, b_i]$. This partition divides the k-cell into a collection of *subcells*.

DEFINITION 484. For a partition P and a bounded function f we define the *lower* and *upper sums* as

$$L(f,P) = \sum_S \left(v(S) \inf_{x \in S} f(S) \right), \; U(f,P) = \sum_S \left(v(S) \sup_{x \in S} f(S) \right).$$

PROPOSITION 485. If P_1 and P_2 are two partitions of the same k-cell, then $L(f, P_1) \leq U(f, P_2)$.

DEFINITION 486. Let A be a k-cell. A function $f : A \to \mathbb{R}$ is called *integrable* over A if f is bounded and $\sup\{L(f, P)\} = \inf\{U(f, P)\}$. In that case, their common value is the *integral* of f over A, denoted

$$\int_A f \mathrm{d}V.$$

PROPOSITION 487. A bounded function f is integrable over A iff for all $\varepsilon > 0$ there is a partition P of A such that $U(f, P) - L(f, P) \leq \varepsilon$.

DEFINITION 488. A subset A of $\mathbb{R}^k$ has *measure* 0 if for every $\varepsilon > 0$ there is a cover of A by k-cells with total volume less than ε.

THEOREM 489 (Sard). Let $g : A \to \mathbb{R}^n$ be continuously differentiable, where A is open. Then the subset of A on which $\det g' = 0$ has measure 0.

THEOREM 490. A bounded function is integrable over a k-cell iff its set of discontinuities in the k-cell has measure 0.

DEFINITION 491. The *support* of a function f is the closure of the set of points at which f is nonzero.

PROPOSITION 492. If f has compact support and is integrable over some k-cell containing its support, then for any k-cells A and B which contain its support we have $\int_A f(x)\mathrm{d}V = \int_B f(x)\mathrm{d}V$.

DEFINITION 493. We define the *characteristic function* $\chi_C(x)$ to be 1 for any $x \in C$, and 0 elsewhere.

COROLLARY 494. If A is a k-cell containing C, and if $\int_A \chi_C(x) f(x)\mathrm{d}V$ exists, then $\int_B \chi_C(x) f(x)\mathrm{d}V$ exists and equals this value for any k-cell B containing C.

DEFINITION 495. We define $\int_C f(x)\mathrm{d}V$, to be this value, if it exists. In the case where C is an interval $[a, b]$, we also write this as $\int_a^b f(x)\mathrm{d}V$.

PROPOSITION 496. If f is integrable over a k-cell A, C is a subset of A and the boundary of C has measure 0, then f is integrable over C.

PROPOSITION 497. Suppose $\{f_n\}$ converges uniformly and each f_n is integrable over C. Then,

$$\int_C \lim_{n\to\infty} f_n(x)\mathrm{d}x = \lim_{n\to\infty} \int_C f_n(x)\mathrm{d}x.$$

THEOREM 498 (Fundamental Theorem of Calculus). If $f : [a, b] \to \mathbb{R}$ is integrable, define

$$F(x) = \int_a^x f(t)\mathrm{d}t.$$

If f is continuous at $c \in [a, b]$, then F is differentiable at c, and $F'(c) = f(c)$.

If $F : [a, b] \to \mathbb{R}$ is differentiable, define $f(x) = F'(x)$. If f is integrable on $[a, b]$, then

$$F(x) = F(a) + \int_a^x f(t)\mathrm{d}t.$$

THEOREM 499 (Integration by Parts). Let F and G be differentiable on $[a,b]$ such that $F'=f$ and $G'=g$ are integrable. Then,

$$\int_a^b F(x)g(x)\mathrm{d}x = F(b)G(b) - F(a)G(a) - \int_a^b f(x)G(x)\mathrm{d}x.$$

THEOREM 500 (Fubini). Let A and B be k-cells, and let $f : A\times B \to \mathbb{R}$ be such that $f(x,b)$ is integrable for each $b\in B$ and $f(a,x)$ is integrable for each $a\in A$. Then, f is integrable over $A\times B$ and

$$\int_{A\times B} f\mathrm{d}V = \int_A \left(\int_B f\mathrm{d}V\right)\mathrm{d}V = \int_B \left(\int_A f\mathrm{d}V\right)\mathrm{d}V.$$

THEOREM 501 (Change of Variables). Let A be open in $\mathbb{R}^n$, and let $g : A\to\mathbb{R}^n$ be C^1 and bijective. If $f : g(A)\to\mathbb{R}$ is integrable, then

$$\int_{g(A)} f\mathrm{d}V = \int_A (f\circ g)|\det g'|.$$

THEOREM 502 (Differentiation under the Integral). Let $f : [a,b]\times[c,d]$ be such that $f(\cdot,t)$ is integrable for all t, and $D_{(0,1)}f$ is continuous. Then,

$$f'(s) = \int_a^b D_{(0,1)}f(x,s)\mathrm{d}x$$

for each $s\in(c,d)$.

PROPOSITION 503. We have:

- $\ln(1+x) = \sum(-1)^i \frac{x^{i+1}}{i+1}$ for $-1<x\le 1$
- $\frac{1}{2}\ln\left(\frac{1+x}{1-x}\right) = \sum \frac{x^{2i+1}}{2i+1}$ for $-1<x<1$
- $\arctan(x) = \sum \frac{(-1)^i x^{2i+1}}{2i+1}$ for $-1\le x\le 1$

DEFINITION 504. Let V be a normed vector space over $\mathbb{R}$. A *curve* is a map $f : [a,b]\to V$. We associate to each partition $P=\{x_i\}$ of $[a,b]$ the number $L(P) = \sum\|\gamma(x_i)-\gamma(x_{i-1})\|$. If these numbers have a supremum, then this supremum is the *length* of γ and γ is *rectifiable*. We say that γ is *piecewise* C^n if its domain can be divided into a finite number of intervals such that γ is C^n on each interval.

PROPOSITION 505. If γ is piecewise C^1, then γ is rectifiable. For each $x\in[a,b]$, the length of $\gamma([a,x])$ is

$$s(x) = \int_a^x \|\gamma'(t)\|\mathrm{d}t.$$

PROPOSITION 506. There is a function F such that $\gamma(x) = F(s(x))$ for each x. If F is differentiable, then $\|F'\|=1$ everywhere.

DEFINITION 507. The vector $F'(s)$ is called the *unit tangent vector* to γ.

DEFINITION 508. Let D be an open subset of an inner product space V, and let $F : D\to V$ be continuous. Let $C : [a,b]\to D$ be piecewise C^1. The *line integral* of F along C is

$$\int_C F\cdot\mathrm{d}s = \int_c^d F(C(t))\cdot C'(t)\mathrm{d}t.$$

PROPOSITION 509. The line integral is independent of parametrisation.

PROPOSITION 510. Let D be an open subset of V, where V is an inner product space over $\mathbb{R}$. If $f : D \to \mathbb{R}$ is differentiable, then for each x there is a vector $\nabla f(x)$ such that $f'(x)(y) = \nabla f \cdot y$ for all y.

DEFINITION 511. This vector ∇f is called the *gradient* of f.

PROPOSITION 512. Let E be open in X, and let $G : E \to Y$ be C^1. Let $A = G^{-1}(0)$. Assume $G'(a)$ is surjective for all $a \in A$. If $f : E \to \mathbb{R}$ is differentiable and the maximum of f on A occurs at a, then there is a functional $l \in Y^*$ such that $f'(a) = lG'(a)$.

COROLLARY 513 (Lagrange Multipliers). If the codomain of G is $\mathbb{R}$, then for some λ we have $\nabla f = \lambda \nabla g$.

THEOREM 514 (Fundamental Theorem of Line Integrals). Let $f : D \to \mathbb{R}$ be C^1, and let $\gamma : [a, b] \to D$ be a piecewise C^1 curve such that $\gamma(a) = X_0$ and $\gamma(b) = X_1$. Then,

$$\int_C \nabla f \cdot \mathrm{d}s = f(X_1) - f(X_0).$$

DEFINITION 515. A vector field $F : D \to V$ is *conservative* if $\int_C F \cdot \mathrm{d}s = 0$ whenever C is a closed rectifiable curve.

COROLLARY 516. A vector field over a connected open set is conservative iff it is the gradient of some function.

THEOREM 517 (Inverse Function). Let $f : X \to X$, and let a be such that f is C^k in an open ball containing a and $f'(a)$ is invertible. Then there is an open ball E containing a and such that f is injective on E, $F(E)$ is open, and $(F|_E)^{-1}$ is C^k.

DEFINITION 518. A *homeomorphism* between two topological spaces is a continuous function with continuous inverse.

COROLLARY 519. If $f : X \to X$ is differentiable and $|f'|$ is always nonzero, then f is a homeomorphism.

THEOREM 520 (Implicit Function). Let $\phi : X \times Y \to Y$ be C^k in an open set containing (x, y), and assume $\phi(x, y) = 0$. Let $\phi'(x, y) = A(x) + B(y)$, and assume B is invertible. Then there is an open set E containing x and an open set F containing y such that for each $e \in E$ there is a unique $f \in F$ such that $\phi(e, f) = 0$. The function $e \mapsto f$ is C^k.

DEFINITION 521. The *half-space* $\mathbb{H}^k$ is defined as $\mathbb{R}^{k-1} \times \mathbb{R}_{\geq 0}$.

DEFINITION 522. Let U and V be normed vector spaces. Let $f : S \to V$, where $S \subseteq U$. We say that f is C^r on S if there is an open set W containing U and a function $g : W \to V$ such that the restriction of g to S is f.

PROPOSITION 523. Let U be open in $\mathbb{H}^k$, and let $\alpha : U \to V$ be C^r. If β_1 and β_2 are extensions of α to open sets in $\mathbb{R}^k$ containing U, then $\beta_1' = \beta_2'$ on U.

DEFINITION 524. Thus, we define $\alpha' = \beta'$ on U for any such extension.

DEFINITION 525. A subset M of $\mathbb{R}^n$ is a k-dimensional *manifold with boundary* if for each $p \in M$, there is an open subset V of M containing p, a set U that is open in $\mathbb{H}^k$, and a C^∞ homeomorphism $\alpha : U \to V$ such that α' has rank k everywhere. Such an α is a *patch* around p. It is a *manifold* if these patches can be chosen such that each U is open in $\mathbb{R}^k$.

REMARK 526. In general, one may drop the smoothness condition for α and the full-rank condition for α'. However, these conditions make doing calculus on manifolds more convenient.

PROPOSITION 527. If (U_1, h_1), (U_2, h_2) and $(U_1 \cap U_2, h_3)$ are n-dimensional charts, then $h_1(U_1 \cap U_2)$ and $h_2(U_1 \cap U_2)$ are open in $\mathbb{H}^n$ and the function $h_1 \circ h_2^{-1}$ is continuous.

DEFINITION 528. A point p in a k-manifold with boundary M is said to lie on the *boundary* ∂M of M if no subset of M containing p is a k-manifold, and in the *interior* $M - \partial M$ otherwise.

PROPOSITION 529. If M is a k-manifold with boundary and ∂M is nonempty, then ∂M is a $(k-1)$-manifold.

THEOREM 530 (Rank Theorem). Let A be an open set in V, let $r < \dim W$ be an integer, and let $F : A \to W$ be C^∞ such that the rank of F' is r at every point in A. Then $F(A)$ is an r-dimensional smooth manifold in W.

DEFINITION 531. Given $x \in V$, we define a *tangent vector* at x to be a pair (x, v) where $v \in V$. The *tangent space* to V at x, denoted $\mathcal{T}_x(V)$, is the set of all tangent vectors, with the operations $(x, v_1) + (x, v_2) = (x, v_1 + v_2)$ and $a(x, v) = (x, av)$. Given an inner product and an orientation of V, we define an *induced* inner product and orientation on $\mathcal{T}_x(V)$ in the obvious way.

DEFINITION 532. Let A be open in W, and let $f : A \to V$ be differentiable. We define $f_* : \mathcal{T}_x(W) \to \mathcal{T}_{f(x)}(V)$ by $f_*(x, v) = (f(x), D_v f(x))$.

PROPOSITION 533. Let $M \subseteq W$ be a manifold with boundary, and let $p \in M$. Choose a chart (U, φ) around p, and let $f = \varphi^{-1}$. The set $f_*(\mathcal{T}_{\varphi(p)}(V))$ is a subspace of $T_p(W)$ independent of the choice of chart.

DEFINITION 534. This space is the *tangent space* to M at p, denoted $\mathcal{T}_p(M)$. The dual space $(T_x(M))^*$ is the *cotangent space* to M at x, denoted $T_x^*(M)$.

DEFINITION 535. A *k-tensor field* on a manifold with boundary M is a function assigning, to each $x \in M$, an element of $\otimes^k \mathcal{T}_x^*(M)$. A *differential form* of order k is a k-tensor field such that every element of its image is alternating. The *wedge product* of two differential forms is taken pointwise.

REMARK 536. Note that a function from M to $\mathbb{F}$ is a differential 0-form.

PROPOSITION 537. If f and g are C^n differential forms defined on an open set, then so is $f \wedge g$.

DEFINITION 538. Let M_1 and M_2 be manifolds with boundary, and let $\varphi : M_1 \to M_2$ be continuous. We say that two charts (U_1, α_1) and (U_2, α_2) are *compatible* under φ if $\varphi(U_1) \subseteq U_2$.

DEFINITION 539. A continuous function $\varphi : M_1 \to M_2$ is *differentiable* if for any compatible charts (U_1, α_1) and (U_2, α_2), the map $\alpha_2 \circ \varphi \circ \alpha_1^{-1}$ is differentiable.

PROPOSITION 540. If φ is differentiable, there is a unique function φ_* such that for any compatible charts (U_1, α_1) and (U_2, α_2) we have

$$\varphi_* \circ (\alpha_1^{-1})_* = (\alpha_2^{-1})_* \circ (\alpha_2 \circ \varphi \circ \alpha_1^{-1})_*.$$

DEFINITION 541. For a differential k-form ω on M_2 and a differentiable map $f : M_1 \to M_2$, we define the *pullback* $f^*\omega = (\wedge^k f_*)\omega$.

PROPOSITION 542. The function f^* commutes with the operations $+$, $\cdot$ and $\wedge$.

DEFINITION 543. If f is a differential k-form defined on an open set, we define the *exterior derivative* df as $df(p) = \mathrm{Alt}(f'(p))$.

PROPOSITION 544. Let p be a point on a manifold with boundary M, and let ω be a differential form defined on M. Let (U, φ) be a chart defined on a neighbourhood of p, and let $f = \varphi^{-1}$. Then,

$$\varphi^*(df^*(\omega))(p)$$

is independent of the choice of φ.

DEFINITION 545. We define this expression to be the *exterior derivative* $d\omega(p)$.

PROPOSITION 546. The exterior derivative has the following properties:

- If f is a 0-form, then $df = f'$.
- If f is a C^k differential n-form, then df is a C^{k-1} differential $(n+1)$-form.
- Let ω be a k-differential form. Then, $d(\omega \wedge \nu) = d\omega \wedge \nu + (-1)^k \omega \wedge d\nu$.
- $d(f^*\omega) = f^*(d\omega)$.

DEFINITION 547. A form ω is called *closed* if $d\omega = 0$ and *exact* if $\omega = d\nu$ for some ν. Let M be a manifold, and $\Omega^k(M)$ be the set of k-differential forms on M. Let $C^k(M)$ and $E^k(M)$ be the sets of closed and exact forms on M, respectively.

PROPOSITION 548. We have $E^k(M) \subseteq C^k(M) \subseteq \Omega^k(M)$, and each of these sets is a vector space.

DEFINITION 549. The *deRham cohomology group* $H^k(M)$ is the quotient space $C^k(M)/E^k(M)$.

THEOREM 550 (Poincaré Lemma). The deRham cohomology group of a star-shaped set is trivial for $k \geq 1$.

PROPOSITION 551. Let ω be a differential k-form in an open $D \subseteq V$, where V is k-dimensional, and let p be a point in D. Let O be an orientation on V. For any orthonormal basis $\{b_i\}$ of $\mathcal{T}_p(V)$, the expression

$$k!O(\{b_i\})\omega(\{b_i\})$$

is independent of b_i.

DEFINITION 552. We call the value of this expression $\rho^\omega(p)$, and define

$$\int_D \omega = \int_D \rho^\omega(p)\mathrm{d}V.$$

DEFINITION 553. Let M_1 and M_2 be two manifolds with boundary, and define $\mu_1(p)$ to be an orientation of $\mathcal{T}_p(M_1)$ for each $p \in M_1$. Define μ_2 similarly on M_2. Then a differentiable map $f : M_1 \to M_2$ is *orientation-preserving* if $\mu_2 \circ f_* = \mu_1$. A manifold M_1 is *oriented* if μ_1 is defined such that for each chart (U, φ), an orientation can be chosen on the codomain of φ such that φ is orientation-preserving.

PROPOSITION 554. Let ω be a k-form defined on an oriented k-manifold with boundary M which has support S. For any orientation-preserving chart φ defined on a superset of S,

$$\int_{\varphi(S)} \varphi^*(\omega)$$

is uniquely defined.

DEFINITION 555. We define this value, if it exists, to equal $\int_M \omega$.

PROPOSITION 556. Let ω be a k-form defined on a k-manifold with boundary M. Let $\{(U_i, \varphi_i)\}$ be an atlas of M, and let $\{g_j\}$ be a partition of unity subordinate to $\{U_i\}$. If

$$\sum_j \int_M g_j \omega$$

converges for some choice of $\{g_j\}$, then it converges to the same value for all choices.

DEFINITION 557. We define this value, if it exists, to be $\int_M \omega$.

PROPOSITION 558. At each point $p \in \partial M$, there are exactly two unit vectors n_1, n_2 in $\mathcal{T}_M(P)$ which are perpendicular to all vectors in $\mathcal{T}_{\partial M}(P)$. If $\varphi : M \to \mathbb{H}^k$ is a patch, then $\varphi_*(n_1)$ and $\varphi_*(n_2)$ differ only in the sign of the last component; one of them always has positive sign, and the other always has negative sign irrespective of the choice of φ.

DEFINITION 559. We let the *outward unit normal* at p be whichever of n_1 and n_2 has this sign negative.

PROPOSITION 560. Let M be an oriented manifold with boundary, and let $p \in \partial M$. Let $n(p)$ denote the outward unit normal at p, and let $\mu(p)$ be the orientation of M at p. The function $\nu(p)$ defined by

$$\nu(p)(v_2, \ldots, v_k) = \mu(n, v_2, \ldots, v_k)$$

orients ∂M.

DEFINITION 561. This is the *induced orientation* on ∂M.

THEOREM 562 (Stokes). If D is a C^∞ manifold with boundary of dimension n and ω is a C^1 differential $(n-1)$-form, then

$$\int_D d\omega = \int_{\partial D} \omega.$$

DEFINITION 563. Let $f : V \to V$. The *divergence* of f is $\nabla \cdot f = \operatorname{tr} f'$.

DEFINITION 564. Let $S \subseteq \mathbb{R}^n$ be an $(n-1)$-dimensional manifold. For any function $f : \mathbb{R}^n \to \mathbb{R}^n$, we define a differential $(n-1)$-form ω by letting $\omega(p)(V)$ be the determinant of the linear map which takes the standard basis to $(V, f(p))$. Then the *surface integral* of f over S is defined as

$$\int_S f \cdot \mathrm{d}A = \int_S \omega.$$

THEOREM 565 (Gauss' Divergence). Let $S \subseteq \mathbb{R}^n$ be an n-dimensional manifold with boundary. Then, for any C^1 function f, we have

$$\int_S \nabla \cdot f \mathrm{d}V = \int_{\partial S} f \cdot \mathrm{d}A.$$

PROPOSITION 566. Let $F : V \to V$ be C^1, where $V \subseteq \mathbb{R}^3$. At each point $(t, F(t))$ there exists a unique vector $\nabla \times F$ such that for all y we have

$$(F'(X) - F'(X)^T)y = (\nabla \times F) \times y.$$

DEFINITION 567. This vector $\nabla \times F$ is the *curl* of F.

THEOREM 568 (Stokes). Let $M \subseteq \mathbb{R}^3$ be an oriented 2-manifold with boundary, and let ∂M have the induced orientation. Let $F : \mathbb{R}^3 \to \mathbb{R}^3$ be C^1. Then,

$$\int_M (\nabla \times F) \cdot \mathrm{d}A = \int_{\partial M} f \cdot \mathrm{d}s.$$

References.

- Spivak, *Calculus on Manifolds*
- Munkres, *Analysis on Manifolds*
- Loomis and Sternberg, *Advanced Calculus*
- Nickerson, Spencer and Steenrod, *Advanced Calculus*

6. Complex Analysis

References.

- Ahlfors, *Complex Analysis*
- Conway, *Functions of One Complex Variable*
- Stein and Shakarchi, *Complex Analysis*

7. Differential Equations

References.

- Hurewicz, *Lectures on Ordinary Differential Equations*
- Arnol'd, *Ordinary Differential Equations*
- Simmons, *Differential Equations with Applications and Historical notes*
- Hirsch, Smale and Devaney, *Differential Equations, Dynamical Systems, and an Introduction to Chaos*

8. Algebra

PROPOSITION 569. If G is a group, then

- The identity element of G is unique.
- Every $a \in G$ has a unique inverse in G.
- For every $a \in G$, $(a^{-1})^{-1} = a$.
- For every $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- For any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 a_2 \cdots a_n$ is independent of how the expression is bracketed.

PROPOSITION 570. A nonempty subset H of G is a subgroup of G iff it is closed under multiplication and inverses.

PROPOSITION 571. If H is a nonempty finite subset of G which is closed under multiplication, then H is a subgroup of G.

PROPOSITION 572. Let $\phi : G \to H$ be a homomorphism, and let H' be a subgroup of G. Then $\phi(G)$ and $\phi^{-1}(H')$ are subgroups of H and G respectively.

DEFINITION 573. The *kernel* of a homomorphism is the inverse image of the identity.

DEFINITION 574. The *order* of a group G is $|G|$.

DEFINITION 575. Let H be a subgroup of G. For any $g \in G$, we let $gH = \{gh : h \in H\}$ and $Hg = \{hg : h \in H\}$, respectively called a *left coset* and *right coset* of H.

PROPOSITION 576. The sets of left and right cosets of H form partitions of G with equal cardinality.

DEFINITION 577. This cardinality is the *index* of H in G, denoted $[G : H]$.

PROPOSITION 578. Every left (resp. right) coset of H has the same cardinality as H.

COROLLARY 579 (Lagrange's Theorem). $|G| = [G : H]|H|$. In particular, if $|G|$ is finite then $|H| \mid |G|$.

COROLLARY 580. If G is a finite group, for any $x \in G$ we have $x^{|G|} = 1$.

PROPOSITION 581. Let $K \subseteq H \subseteq G$ be groups. Then, $[G : H][H : K] = [G : K]$.

DEFINITION 582. If H and K are subsets of G, let $HK = \bigcup\{hK : h \in H\}$.

PROPOSITION 583. If H and K are subgroups of G, then HK is a subgroup of G iff $HK = KH$.

PROPOSITION 584. If H and K are finite subgroups of G, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

PROPOSITION 585. The set of permutations of a set X is a group under composition.

DEFINITION 586. This group is denoted S_X, and any subgroup of it is a *permutation group*.

If $|X| = n$, then $S_n = A(\{1, 2, \ldots, n\})$ is called the *symmetric group* of degree n.

DEFINITION 587. A *cycle* is a nontrivial permutation φ of a set S such that for any two elements $a, b \in S$ such that $\varphi(a) \neq a$ and $\varphi(b) \neq b$, there is some k for which $\varphi^k(a) = b$.

PROPOSITION 588. Disjoint cycles commute.

PROPOSITION 589. Every permutation can be uniquely expressed as a product of disjoint cycles.

PROPOSITION 590. The function sign : $S_n \to \{1, -1\}$ is a homomorphism; further, the sign of any 2-cycle is -1.

DEFINITION 591. The kernel of this homomorphism is A_n, the *alternating group* of degree n.

DEFINITION 592. A *group action* of a group G on a set A is a map from $G \times A$ to A, written as $g \cdot a$, such that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ and $1 \cdot a = a$.

Definition 593. A *permutation representation* of G is a homomorphism of G into S_X for some X.

Proposition 594. For each g, the map $\sigma_g(a) = g \cdot a$ is a permutation on A. The map $g \mapsto \sigma_g$ from G to S_A is a homomorphism.

Definition 595. This homomorphism is the permutation representation *induced* by this group action.

Proposition 596. There is a bijection between the actions of G on A and the homomorphisms of G into S_A.

Definition 597. If G is a group acting on S and s is a fixed element of S, the *stabiliser* of s is the set $G_s = \{g \in G : gs = s\}$.

Proposition 598. The stabiliser of an element is a subgroup of G.

Definition 599. Let G act on $\mathcal{P}(G)$ by *conjugation*: that is, $g \cdot A = gAg^{-1}$. The *normaliser* $N_G(A)$ is the stabiliser of A under this action.

Proposition 600. If $H \subseteq N_G(K)$, $K \subseteq N_G(H)$, and $H \cap K = \{1\}$, then $HK \cong H \times K$.

Definition 601. In this case we call HK the *internal direct product* of H and K.

Definition 602. Let $N_G(A)$ act on A by conjugation. The *centraliser* $C_G(A)$ is the kernel of this action.

Definition 603. The *centre* of G is $Z(G) = C_G(G)$.

Definition 604. A subgroup N of G is *normal* if the normaliser of N is G.

Proposition 605. If K is a subgroup of G, then H is normal in K iff $K \subseteq N_G(H)$.

Proposition 606. The subgroup N of G is normal iff the set of left cosets of N equals the set of right cosets.

Proposition 607. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Then, G acts transitively on A, the stabiliser of $1H$ is H, and the kernel of the action is the largest normal subgroup of G contained in H.

Corollary 608 (Cayley). Every group is isomorphic to a permutation group.

Proposition 609. If G is a finite group and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Proposition 610. If N is normal in G, the set of cosets of N forms a group under multiplication.

Definition 611. This group is called the *quotient group* of G over N, denoted G/N.

Proposition 612. The mapping π from G to G/N defined by $\pi(x) = Nx$ is a surjective homomorphism with kernel N.

Definition 613. This mapping is called the *natural projection* of G onto G/N.

DEFINITION 614. Let A, B, C be groups, and let $f : A \to B$ be a homomorphism. Then, we say that $g : A \to C$ *factors through* f if there exists a homomorphism $h : B \to C$ such that $g = hf$.

PROPOSITION 615. Let H be a subset of G, let ϕ be a homomorphism such that its kernel contains H, and let N be the intersection of all normal subgroups containing H. Then, ϕ factors uniquely through the natural projection of G onto G/N.

THEOREM 616 (Isomorphism Theorems). In the following statements, all quotients are well-defined.

(1) If $\phi : G \to H$ is a homomorphism, then the image of ϕ is isomorphic to $\phi/\ker\phi$.
(2) Let G be a group and let A and B be subgroups of G such that $A \subseteq N_G(B)$. Then $AB/B \cong A/A \cap B$.
(3) Let G be a group and let H and K be normal subgroups of G with $H \subseteq K$. Then $(G/H)/(K/H) \cong G/K$.
(4) Let N be normal in A. Then the natural projection defines a bijection from the set of subgroups of G which contain N to the set of subgroups of G/N.

LEMMA 617 (Butterfly). Let G be a group with subgroups A, B, C, D such that B is a normal subgroup of A and D is a normal subgroup of C. Then we have

$$\frac{(A \cap C)B}{(A \cap D)B} \cong \frac{(A \cap C)D}{(B \cap C)D}.$$

PROPOSITION 618. For any set S there exists a group $F(S)$ containing S such that for any group G, any map $\varphi : S \to G$ can be extended to a unique homomorphism. This group is unique up to isomorphism.

DEFINITION 619. This group is the *free group* on S.

THEOREM 620 (Schreier). Subgroups of a free group are free.

DEFINITION 621. Let S be a subset of a group G. The subgroup of G *generated* by S, denoted $\langle S \rangle$, is the image of the homomorphism $F(S) \to G$ that fixes S.

DEFINITION 622. Let S be a subset of a group G that generates G. A *presentation* for G is a pair (S, R) such that the smallest normal subgroup containing R in $F(S)$ equals the kernel of the homomorphism $F(S) \to G$ that fixes S. The elements of S are called *generators* and those of R are called *relations* of G.

PROPOSITION 623. Let G and H be groups, let S be a set of generators for G, and let $\phi : F(S) \to G$ be the induced homomorphism. A set H is a homomorphic image of G iff there is a homomorphism $\pi : F(S) \to H$ such that $\ker\pi \subseteq \ker\phi$.

DEFINITION 624. A group G is *finitely generated* if there is a presentation (S, R) such that S is finite, and *finitely presented* if there is a presentation (S, R) such that both S and R are finite.

PROPOSITION 625. Every finite group is finitely presented.

DEFINITION 626. A group is *cyclic* if it is generated by a single element.

PROPOSITION 627. A group is cyclic iff it is isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}^+$.

PROPOSITION 628. Every group of prime order is cyclic.

THEOREM 629 (Cauchy). If p is a prime dividing $|G|$, then G has a subgroup of order p.

DEFINITION 630. Let G be a group acting on A. The set $Ga = \{g \cdot a : g \in G\}$ is called the *orbit* of a under G.

If there is only one orbit, then the action of G on A is called *transitive*.

PROPOSITION 631. The set of orbits of G partitions A.

PROPOSITION 632. $|Gs| = [G : G_s]$.

COROLLARY 633. The number of conjugates of a subset S in G is $[G : N_G(S)]$. In particular, the number of conjugates of an element s of G is $[G : C_G(s)]$.

COROLLARY 634 (Orbit decomposition formula). Let $\{s_i\}$ be a set containing one element from each of the orbits of G. If S is finite, then we have $|S| = \sum[G : G_{s_i}]$.

COROLLARY 635 (Class equation). Let $\{g_i\}$ be a set containing one element from each conjugacy class which is not in the centre of G. Then, $|G| = |Z(G)| + \sum[G : C_G(g_i)]$.

COROLLARY 636. A group of prime power order must have a nontrivial centre.

COROLLARY 637. If $|G| = p^2$ for some prime P, then either $p \cong \mathbb{Z}/p^2\mathbb{Z}$ or $p \cong (\mathbb{Z}/p\mathbb{Z})^2$.

DEFINITION 638. A *partition* of n is a set of positive integers whose sum is n.

PROPOSITION 639. The number of conjugacy classes of S_n equals the number of partitions of n.

DEFINITION 640. A group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and itself.

PROPOSITION 641. The alternating group A_n is simple for $n \geq 5$.

PROPOSITION 642. If G is a group, the set of automorphisms of G is also a group.

DEFINITION 643. We denote this group by $\mathrm{Aut}(G)$.

PROPOSITION 644. Let H be a normal subgroup of G. The permutation representation of the action of G on H by conjugation is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$.

COROLLARY 645. The permutation representation of the action of G on itself by conjugation is a homomorphism of G into $\mathrm{Aut}(G)$ with kernel $Z(G)$.

DEFINITION 646. The image of this homomorphism is called the group of *inner automorphisms* of G, denoted $\mathrm{Inn}(G)$.

DEFINITION 647. A subgroup H of a group G is *characteristic* in G if every automorphism of G maps H to itself.

PROPOSITION 648. If K is characteristic in H and H is normal in G, then K is normal in G.

PROPOSITION 649. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

PROPOSITION 650. For all $n \neq 6$ we have $\mathrm{Aut}(S_n) \cong S_n$.

DEFINITION 651. A group of order p^α for some $\alpha \geq 1$ is called a *p-group*. If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G.

THEOREM 652 (Sylow). Let $p^\alpha \| |G|$.

(1) Sylow p-subgroups of G exist.
(2) Any p-subgroup of G is contained in a conjugate of any Sylow p-subgroup of G.
(3) The number of Sylow p-subgroups is $1 \pmod p$ and divides $|G|$.

PROPOSITION 653 (Frattini's Argument). Let G be a finite group, let H be a normal subgroup of G and let P be a Sylow p-subgroup of H. Then $G = HN_G(P)$ and $[G : H] \mid |N_G(P)|$.

PROPOSITION 654. In a finite group G, if the number of Sylow p-subgroups is not $1 \pmod{p^2}$, then there are distinct Sylow p-subgroups P and R of G such that $P \cap R$ is of index p in both P and R.

PROPOSITION 655. Every proper subgroup of a p-group is a proper subgroup of its normaliser. Every maximal subgroup of a p-group is of index p and is normal.

COROLLARY 656. If H is a normal subgroup of G with order divisible by p^k, then H has a subgroup of order p^k that is normal in G.

THEOREM 657 (Fundamental Theorem of Finite Abelian Groups). Every finite abelian group is uniquely isomorphic to the direct product of cyclic groups, such that the order of each of them is a power of a distinct prime.

DEFINITION 658. In a group G, a sequence of subgroups

$$1 = N_0 \subseteq \cdots \subseteq N_k = G$$

is called a *composition series* if each N_i is normal in N_{i+1} and N_{i+1}/N_i is a simple group for all i. The quotient groups N_{i+1}/N_i are called *composition factors* of G.

THEOREM 659 (Jordan—Hölder). Let G be a nontrivial finite group. Then, G has a composition series and the composition factors are unique up to permutation and isomorphism.

DEFINITION 660. A group is *solvable* if its composition factors are abelian.

THEOREM 661 (Burnside). If $|G| = p^a q^b$ for some primes p and q, then G is solvable.

THEOREM 662 (Hall). If for all primes p, G has a subgroup whose index equals the order of a Sylow p-subgroup, then G is solvable.

DEFINITION 663. The *upper central series* of G is a sequence of subgroups of G such that $Z_0(G) = 1$ and $Z_{i+1}(G)$ is the preimage in G of the centre of $G/Z_i(G)$ under the natural projection. A group is *nilpotent of class n* if n is minimal such that $Z_n(G) = G$.

PROPOSITION 664. $Z_i(G)$ is characteristic in G for all i.

PROPOSITION 665. Every nilpotent group is solvable.

THEOREM 666. If G is finite, then the following are equivalent.

- G is nilpotent;
- Every proper subgroup of G is a proper subgroup of its normaliser in G;
- Every Sylow subgroup is normal in G;
- G the direct product of its Sylow subgroups;
- Every maximal proper subgroup is normal.

DEFINITION 667. An additive subgroup U of a ring R is a *left ideal* of R if $RU \subseteq U$, and a *right ideal* if $UR \subseteq U$. A subring which is both a left and right ideal is an *ideal*.

PROPOSITION 668. If U is an ideal of R, then U is normal in the additive group of R, and the multiplication of R is well-defined on each coset of U.

DEFINITION 669. The *quotient ring* R/U is the quotient group R/U under the induced multiplication.

PROPOSITION 670. Let S be a subset of R, let ϕ be a homomorphism such that its kernel contains S, and let N be the intersection of all ideals containing N. Then, ϕ factors uniquely through the natural projection of S onto S/N.

THEOREM 671 (Isomorphism Theorems). In the following statements, all quotients are well-defined.

(1) If $\phi : G \to H$ is a homomorphism, then the image of ϕ is isomorphic to $\phi/\ker\phi$.
(2) Let R be a ring. Let A be a subring of R and let B be an ideal of R. Then, $A/A \cap B \cong (A+B)/B$.
(3) Let R be a ring and let H and K be ideals of R with $H \subseteq K$. Then $(G/H)/(K/H) \cong G/K$.
(4) Let A be an ideal in R. Then the natural projection ϕ defines a bijection from the set of subrings of R which contain A to the set of subrings of G/A. Further, ϕ and ϕ^{-1} preserve ideals.

DEFINITION 672. An ideal M of R is *maximal* if the only ideals of R which contain M are M and R.

PROPOSITION 673. Every proper ideal is contained in a maximal ideal.

PROPOSITION 674. If R is a commutative ring and M is an ideal of R, then M is maximal iff R/M is a field.

DEFINITION 675. A nonzero element $a \in R$ is called a *zero divisor* if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.

DEFINITION 676. An element u of R is called a *unit* in R if it has a multiplicative inverse.

DEFINITION 677. A commutative nontrivial ring is called an *integral domain* if it has no zero divisors.

PROPOSITION 678. A finite integral domain is a field.

DEFINITION 679. The *characteristic* of a ring is the order of the additive subgroup generated by 1, and 0 if this subgroup is infinite.

Proposition 680. If an integral domain has finite characteristic, then its characteristic is a prime.

Definition 681. An ideal P of a commutative ring R is called a *prime ideal* if $P \neq R$ and whenever $ab \in P$, at least one of a, b is in P.

Proposition 682. If R is commutative, then every maximal ideal of R is prime.

Proposition 683. Let R be an integral domain and let $D = R \setminus \{0\}$. There is a field $Q(R)$ and a homomorphism $\pi : R \to Q(R)$ such that any injective homomorphism from ψ to a field factors through π.

Definition 684. This field $Q(R)$ is the *quotient field* of R.

Definition 685. Let a be an element of R. The smallest ideal of R containing a is the *principal ideal* generated by a.

Definition 686. A *principal ideal domain* (PID) is an integral domain R in which every ideal is principal.

Proposition 687. If R is a PID, then any nonzero prime ideal is maximal.

Definition 688. An integral domain R is *Euclidean* if for every $a \in R$ apart from 0 there is a nonnegative integer $|a|$ such that if $b \neq 0$, then for any a there exist $t, r \in R$ such that $a = tb + r$ and $|r| < |b|$.

Proposition 689. Every field is Euclidean. Every Euclidean domain is a PID.

Definition 690. If a and b are elements of a commutative ring R, then we say $a \mid b$ if there exists some c such that $b = ac$. If both $a \mid b$ and $b \mid a$, then a and b are *associates*.

Definition 691. If $a, b \in R$, then $d \in R$ is said to be a *greatest common divisor* of a and b if $d \mid a$, $d \mid b$, and whenever $c \mid a$ and $c \mid b$ we also have $c \mid d$.

Proposition 692. Let R be a PID. For any two elements $a, b \in R$ there exist $x, y \in R$ such that $ax + by = \gcd(a, b)$.

Theorem 693 (Chinese Remainder). If R is a PID and the elements $\{a_i\}$ are pairwise coprime, $R/\left(\prod a_i\right) \cong \prod R/(a_i)$.

Proposition 694. Let R be a commutative ring. If $R[x]$ is a PID, then R is a field. If R is a field, then $R[x]$ is Euclidean.

Definition 695. A nonzero nonunit element p is *prime* if (p) is prime, and *irreducible* if p is not the product of two nonunit elements.

Proposition 696. Every prime element of an integral domain is irreducible.

Definition 697. A *unique factorisation domain* (UFD) is an integral domain R in which every nonzero element can be written as a finite product of irreducibles, and the factorisation is unique up to associates.

Proposition 698. In a UFD, all irreducible elements are prime.

Proposition 699. If a UFD, all pairs of elements have a greatest common divisor.

THEOREM 700. Every PID is a UFD.

COROLLARY 701. If R is an integral domain, then a polynomial of degree n in $R[x]$ has at most n roots.

THEOREM 702. If R is a UFD, then so is $R[x]$.

DEFINITION 703. Let R be a subring of S, let $s \in S$, and let $f_s : R[x] \to S$ be the homomorphism which fixes R and sends x to s. We define $R[s] = R[x]/\ker f_i$.

PROPOSITION 704. The *Gaussian integers* $\mathbb{Z}[i]$ are Euclidean. The Gaussian integer $a + bi$ is prime in $\mathbb{Z}[i]$ iff either

- $a^2 + b^2$ is prime in $\mathbb{Z}$, or
- $\{a, b\} = \{0, p\}$, where p is prime in $\mathbb{Z}$ and $4 \mid p + 1$.

COROLLARY 705 (Fermat's Christmas Theorem). An integer $n = \prod p_i^{\alpha_i}$ can be written as a sum of two squares of integers iff whenever $4 \mid p_i + 1$, α_i is even. The number of such representations equals $4 \prod(\alpha_i + 1)$, where the product ranges over those i such that $4 \mid p_i - 1$.

DEFINITION 706. Let R be a ring. An *R-module* V is an additive abelian group together with a function $\cdot : R \times V \to V$ such that $a(bv) = (ab)v$, $1v = v$, $a(u + v) = au + av$ and $(a + b)v = av + bv$. A *morphism* of R-modules, also known as an *R-linear map*, must preserve scalar multiplication as well as addition.

PROPOSITION 707. For each R-module A the set of endomorphisms on A forms a ring under addition and composition.

DEFINITION 708. Let M be an R-module, and let $\{N_i\}$ be submodules of M. The *sum* of $\{N_i\}$ is the set of finite sums of elements from N_i.

DEFINITION 709. If $N = RA$ is a submodule of M, then N is *generated* by A. If A is finite then N is *finitely generated*; if $|A| = 1$ then N is *cyclic*.

DEFINITION 710. Let X be a subset of an R-module F. Then F is called a *free module* on X if for every R-module A, every function $f : X \to A$ extends uniquely to a morphism $X \to A$. The set X is called a *basis* for F.

THEOREM 711. If R is a PID, then any finitely generated R-module is isomorphic to a direct product of a finite number of cyclic submodules.

COROLLARY 712. Any finitely generated abelian group is the direct product of cyclic groups.

PROPOSITION 713. A finite subgroup of the multiplicative group of a field is cyclic.

DEFINITION 714. A ring is called a *division ring* if every nonzero element is a unit.

THEOREM 715 (Wedderburn). A finite division ring is a field.

THEOREM 716 (Jacobson). Let D be a ring such that every nonzero element is a root of identity. Then D is a field.

References.

- Herstein, *Topics in Algebra*
- Artin, *Algebra*
- Dummit and Foote, *Abstract Algebra*
- Mac Lane and Birkhoff, *Algebra*

9. Number Theory

References.

- Chandrasekharan, *Introduction to Analytic Number Theory*
- Serre, *A Course in Arithmetic*
- Ireland and Rosen, *A Classical Introduction to Modern Number Theory*
- Hardy and Wright, *An Introduction to the Theory of Numbers*

10. Geometry

References.

- Coxeter, *Introduction to Geometry*
- Hartshorne, *Geometry: Euclid and Beyond*
- Stillwell, *The Four Pillars of Geometry*

11. Topology

References.

- Munkres, *Topology*
- Willard, *General Topology*
- Kelley, *General Topology*
- Dugundji, *Topology*

12. Functional Analysis

References.

- Simmons, *Introduction to Topology and Modern Analysis*
- Strichartz, *A Guide to Distributions and Fourier Transforms*
- Stein and Shakarchi, *Fourier Analysis*
- Lax, *Functional Analysis*

13. Probability

References.

- Feller, *An Introduction to Probability Theory and its Applications*
- Billingsley, *Probability and Measure*
- Durrett, *Probability: Theory and Examples*
- Kallenberg, *Foundations of Modern Probability*

14. Statistics

References.

- Wasserman, *All of Statistics*
- Bickel and Doksum, *Mathematical Statistics*

15. Numerical Analysis

References.

- Acton, *Numerical Methods that Work*
- Strang, *Introduction to Computational Science and Engineering*
- Burden and Faires, *Numerical Analysis*
- Atkinson, *An Introduction to Numerical Analysis*

16. Logic

References.

- Johnstone, *Notes on Logic and Set Theory*
- Enderton, *An Introduction to Mathematical Logic*
- Hinman, *Fundamentals of Mathematical Logic*

17. Theory of Computation

DEFINITION 717. A *deterministic finite automaton (DFA)* is a 5-tuple

$$(Q, \Sigma, \delta, q_0, F),$$

where Q is a finite set called the *states*, Σ is a finite set called the *alphabet*, $\delta : Q \times \Sigma \to Q$ is the *transition function*, $q_0 \in Q$ is the *start state*, and $F \subseteq Q$ is the set of *accept states*. We say that machine M *accepts* string $s = s_0 s_1 \cdots s_n$ if $\delta(\delta(\cdots \delta(\delta(q_0, s_0), s_1) \cdots, s_{n-1}), s_n)$ is an accept state. The set A of all strings that machine M accepts is the *language of machine* M, notated $L(M)$. We also say that M *recognises* A.

DEFINITION 718. A language is a *regular language* if it is recognised by some finite automaton.

DEFINITION 719. Let A and B be languages. We define the *regular operations*

- *Union*: $A \cup B = \{x : x \in A \vee x \in B\}$.
- *Concatenation*: $A \circ B = \{xy : x \in A \wedge y \in B\}$.
- *Star*: $A^* = \{x_1 x_2 \cdots x_k : k \geq 0 \wedge \forall i,\ x_i \in A\}$.

DEFINITION 720. The *empty string* is notated ε.

DEFINITION 721. Let Σ be an alphabet. An *atomic regular expression* is one of

- a ($a \in \Sigma$),
- ε, and
- $\emptyset$.

Regular expressions are obtained by combining simpler regular expressions with the operations $\cup$, $\circ$, *.

A regular expression R *describes* a language $L(R)$ obtained by replacing each instance of a and ε with $\{a\}$ and $\{\varepsilon\}$, respectively, and then applying the regular operations.

THEOREM 722. A language is regular iff some regular expression describes it.

PROPOSITION 723 (Pumping Lemma). If A is a regular language, then there is a positive integer p such that if s is any string in A of length at least p, then s may be divided into three pieces, $s = xyz$, where y is nonempty, $|xy| \leq p$ and $x \circ y^* \circ z \subseteq A$.

References.

- Sipser, *Introduction to the Theory of Computation*
- Boolos, Burgess and Jeffrey, *Computability and Logic*
- Cormen, Leiserson, Rivest and Stein, *Introduction to Algorithms*

APPENDIX A

Proofs — Undergraduate