Advanced Algebra.

MA180-4.

Prof. Götz Pfeiffer
http://schmidt.nuigalway.ie/ma180-4

School of Mathematics, Statistics and Applied Mathematics
NUI Galway

Semester 2 (2017/2018)

Outline

1. The Language of Mathematics: Logic and Sets.
   - Propositional Logic.
   - Valid Arguments.
   - Sets and Boolean Algebra.
   - Functions and Relations.
2. Examples of Algebraic Objects: Permutations and Polynomials.
   - Composition of Functions.
   - Permutations.
   - Polynomials.
   - Factorisation of Polynomials.
3. Mathematical Tools: Induction and Matrix Algebra.
   - Mathematical Induction.
   - Examples and Applications of Induction.
   - Determinants.
   - Eigenvalues and Eigenvectors.

References.

Norman L. Biggs.
Discrete Mathematics.
Oxford UP 2003.

Lindsay Childs.
A Concrete Introduction to Higher Algebra.
Springer 2000.

Douglas E. Ensley and J.Winston Crawley
Discrete Mathematics.
Wiley 2006.

Mark V. Lawson
Algebra & Geometry: An Introduction to University Mathematics
Taylor & Francis 2016

Introduction: The Language of Mathematics

Mathematics . . .

- . . . is about solving **problems**.
- . . . explains **patterns**.
- . . . is a set of statements deduced **logically** from axioms and definitions.
- . . . uses **abstraction** to model the real world.
- . . . employs a precise and powerful **language** to organize, communicate, and manipulate ideas.

As with any language, in order to participate in a conversation, it helps to be able to **read** and **write**.
In this section, we introduce basic elements of the mathematical language and study their meaning:

- **logic**: the language of mathematical arguments;
- **sets**: the language of relationships between mathematical objects.

Links: The Language of Mathematics.

- http://en.wikipedia.org/wiki/Mathematics_as_a_language
- http://en.wikipedia.org/wiki/Knights_and_Knaves
- http://www.raymondsmullyan.com
- http://www.iep.utm.edu/prop-log/
- http://en.wikipedia.org/wiki/Mathematical_proof
- http://plato.stanford.edu/entries/boolalg-math/
- http://en.wikipedia.org/wiki/Power_set
- http://en.wikipedia.org/wiki/Equivalence_relation
- http://en.wikipedia.org/wiki/Injective_function
- http://en.wikipedia.org/wiki/Surjective_function
- http://www-history.mcs.st-andrews.ac.uk/Biographies/Smullyan.html is a biography of the American mathematician, logician and magician **Raymond Merrill Smullyan** (1919–).
- http://www-history.mcs.st-andrews.ac.uk/Biographies/Boole.html is a biography of the British mathematician **George Boole** (1815–1864).
- http://www-history.mcs.st-andrews.ac.uk/Biographies/De_Morgan.html is a biography of the British mathematician **Augustus De Morgan** (1806–1871).

Logic Puzzles.

- A **logic puzzle** is a riddle that can be solved by **logical thinking**.

Example (The Island of Knights and Knaves.)

- A certain island has **two types** of inhabitants: knights and knaves.
- **Knights** always tell the truth.
- **Knaves** always lie.
- Every inhabitant is either a knave or a knight.
- You visit the island, and talk to two of its inhabitants, called A and B.
- A says: “Exactly one of us is a knave”.
- B says: “At least one of us is a knight.”
- **Who** (if any) **is telling the truth?**

Systematical Solution: Table Method.

- For a systematical solution, use a **truth table**.
- On the **left**, **list** all possible truth values of the claims 'X is a knight' (T for 'true', F for 'false').

A is a knight	B is a knight	Exactly one is a knave	At least one is a knight
T	T	F	T
T	F	T	T
F	T	T	T
F	F	F	F

- On the **right**, **compute** the corresponding truth values of each of the statements.
- X is a knight if and only if X speaks the truth. Therefore the entry in the **left** column 'X is a knight' **must be equal** to the **right** entry for X's statement.
- Here, row 4 contains the **only match**, hence the **unique solution** of the puzzle.

Further Examples.

- You meet 2 inhabitants of the island.

  A: Exactly one of us is a knight.

  B: All of us are knaves.

  Who (if anyone) is telling the truth?

The following examples illustrate important points.

- You meet 1 inhabitant of the island.

  A: I am a knight.

A	A: ...	
T	T	*
F	F	*

(There can be more than one solution.)

- You meet 1 inhabitant of the island.

  A: I am a knave.

A	A: ...
T	F
F	T

(No solution? This cannot happen.)

A Puzzle With More Than Two Inhabitants.

- You meet 3 inhabitants of the island.

  A: Exactly one of us is a knight.
  B: All of us are knaves.
  C: The other two are lying.

  Who (if anyone) is lying?

Solution

A	B	C	$A: \ldots$	$B: \ldots$	$C: \ldots$	
T	T	T	F	F	F	
T	T	F	F	F	F	
T	F	T	F	F	F	
T	F	F	T	F	F	$*$
F	T	T	F	F	F	
F	T	F	T	F	F	
F	F	T	T	F	T	
F	F	F	F	T	T	

Symbols.

Truth Values

T : **true**

F : **false**

Logical Operations

$\wedge$: **and** (conjunction)

$\vee$: **or** (disjunction)

$\neg$: **not** (negation)

Variables

$a, b, c, \ldots, p, q, r, \ldots$: any statement

- Let a stand for 'A is a knight' and b for 'B is a knight.
- Then $\neg a$ means: A is a knave.
- B's statement: 'At least one of us is a knight' (i.e., 'A is a knight' or 'B is a knight') becomes: $a \vee b$.

Note: $\vee$ is an inclusive 'or'.

The disjunction $p \vee q$ allows for **both** p and q to be true.

Propositional Logic.

- Informally, a **proposition** is a statement that is **unambiguously** either **true** or **false**.
- A **propositional variable** is a symbolic name (like p, q, r, ...) that stands for an arbitrary proposition.
- Formally, a proposition is defined recursively:

Definition (Formal Proposition)

1. Any **propositional variable** is a **formal proposition**.

Moreover, if p and q are formal propositions, the following **compound statements** are **formal propositions**:

2. the **conjunction** $p \wedge q$ (read: "p and q"), stating that "both p and q are true";
3. the **disjunction** $p \vee q$ (read: "p or q"), stating that "either p or q are true";
4. the **negation** $\neg p$ (read: "not p"), stating that "it is not the case that p is true".

Truth Tables.

- A **truth table** shows the truth value of a compound statement for every possible combination of truth values of its simple components.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	$\neg p$
T	F
F	T

Example (The truth table for $(p \vee q) \wedge \neg(p \wedge q)$.)

p	q	$p \wedge q$	$\neg(p \wedge q)$	$p \vee q$	$(p \vee q) \wedge \neg(p \wedge q)$
T	T	T	F	T	F
T	F	F	T	T	T
F	T	F	T	T	T
F	F	F	T	F	F

A truth table built from the tables of $p \wedge q$, $p \vee q$ and $\neg p$.

Simplifying Negations.

- In mathematics, propositions often involve formulas.
- The negation of such a proposition can usually be reformulated in simpler terms with different symbols.

Example

- The negation of the statement "$x < 18$" is "$\neg(x < 18)$", or simply "$x \geqslant 18$".

- The negation of a **conjunction** is a **disjunction**(!)

Example (Truth tables for $\neg(p \wedge q)$ and $(\neg p \vee \neg q)$.)

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Logical Equivalence.

- Two statements p and q are **logically equivalent** if they have the **same truth value** for every row of the truth table: We then write $p \equiv q$.

Theorem (DeMorgan's Laws)

Let p and q be propositions. Then

1. $\neg(p \vee q) \equiv \neg p \wedge \neg q$;
2. $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

- A proposition p is a **tautology**, if its truth value is T, for all possible combinations of the truth values of its propositional variables: $p \equiv T$.
- A proposition p is a **contradiction**, if its truth value is F, for all possible combinations of the truth values of its propositional variables: $p \equiv F$.
- Every logical equivalence is a tautology.

Logical Equivalences.

Theorem (for propositional variables p, q, r.)

All of the following are valid logical equivalences.

- *Commutative Laws:* $p \wedge q \equiv q \wedge p$, *and* $p \vee q \equiv q \vee p$.
- *Associative Laws:* $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$, *and* $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
- *Distributive Laws:* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$, *and* $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
- *Absorption Laws:* $p \wedge (p \vee q) \equiv p$, *and* $p \vee (p \wedge q) \equiv p$.
- *Idempotent Laws:* $p \wedge p \equiv p$, *and* $p \vee p \equiv p$.
- *Complementary Laws:* $p \wedge \neg p \equiv F$, *and* $p \vee \neg p \equiv T$.
- *Identity Laws:* $p \wedge T \equiv p$, *and* $p \vee F \equiv p$.
- *Universal Bound:* $p \wedge F \equiv F$, *and* $p \vee T \equiv T$.
- *DeMorgan:* $\neg(p \wedge q) \equiv \neg p \vee \neg q$, *and* $\neg(p \vee q) \equiv \neg p \wedge \neg q$.
- *Negation:* $\neg T \equiv F$, *and* $\neg F \equiv T$.
- *Double Negation:* $\neg(\neg p) \equiv p$.

Proof: truth tables. □

Sets.

- A **set** is a collection of objects, its **elements**.

Notation.

$a \in S$ means: object a is an element of the set S. And $a \notin S$ means: object a is **not** an element of the set S.

- Two sets A and B are **equal** ($A = B$) if they have the same elements:
  $a \in B$ for all $a \in A$ **and** $b \in A$ for all $b \in B$.

Examples

$\{0, 1\}$,
$\mathbb{N} = \{1, 2, 3, \dots\}$ (the **natural numbers**),
$\{x \in \mathbb{N} \mid x$ is a multiple of $5\}$,
$\varnothing = \{\,\}$ (the **empty set**).

Predicates.

Definition

A **predicate** $P(x)$ is a statement that incorporates a **variable** x, such that whenever x is **replaced by a value**, the resulting statement becomes a **proposition**.

Example

- Suppose $P(n)$ is the **predicate** "n is even".
- Then $P(14)$ is the **proposition** "14 is even".
- The proposition $P(13)$ is false.
- $P(22)$ is true.

- Predicates can be combined using the **logical operators** $\wedge$ (and), $\vee$ (or), $\neg$ (not) to create **compound predicates**.
- A predicate can have more than one variable, e.g., $P(x, y)$ can stand for the predicate "$x \leqslant y$".

Quantified Predicates.

Notation.

- Suppose that $P(x)$ is a predicate and that S is a set.
- "$\forall a \in S, P(a)$" is the proposition:
  "**for all** elements a of S the statement $P(a)$ is true".
- "$\exists a \in S, P(a)$" is the proposition:
  "**there exists** (at least) one element a in the set S such that the statement $P(a)$ is true".

Suppose $S = \{x_1, x_2, \dots\}$.

- "$\forall a \in S, P(a)$" abbreviates "$P(x_1) \wedge P(x_2) \wedge \cdots$".
- "$\exists a \in S, P(a)$" abbreviates "$P(x_1) \vee P(x_2) \vee \cdots$".

Negating Quantified Predicates.

- The negation of "$\forall x \in S, P(x)$" is "$\exists x \in S, \neg P(x)$";
- the negation of "$\exists x \in S, P(x)$" is "$\forall x \in S, \neg P(x)$".

Implications.

Definition

An **implication** is a statement of the form "if p then q". In symbols, we write this as $p \rightarrow q$ (read: "p implies q"). We call proposition p the **hypothesis** and proposition q the **conclusion** of the implication $p \rightarrow q$.

- The **truth table** of $p \rightarrow q$ has the form

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Remark.

The **only way** for an implication $p \rightarrow q$ to be false is when the **hypothesis** p is **true**, but the **conclusion** q is **false**.

Converse, Inverse, Contrapositive.

Various variations of the implication $p \to q$ are of sufficient interest:

- $q \to p$ is the **converse** of $p \to q$.
- $\neg p \to \neg q$ is the **inverse** of $p \to q$.
- $\neg q \to \neg p$ is the **contrapositive** of $p \to q$.

Remark.

1. An implication is logically equivalent to its contrapositive: $p \to q \equiv \neg q \to \neg p$.
2. The converse and the inverse of an implication are logically equivalent: $q \to p \equiv \neg p \to \neg q$.
3. But an implication is not logically equivalent to its converse (and hence not to its inverse).

Proof: Truth tables. □

Biconditional.

- Write $p \leftrightarrow q$ if both $p \to q$ and $q \to p$ are true.
- Then $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$.
- The **truth table** of $p \leftrightarrow q$ has the form

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

- Usually, to prove a statement of the form $p \leftrightarrow q$, one proves the two statements $p \to q$ and $q \to p$ separately.

Examples

- n is even if and only of n^2 is even.
- The integer n is a multiple of 10 if and only if it is even.

Validating Arguments.

- An **argument** is a list of **statements**, ending in a **conclusion**.
- The logical **form** of an argument can be abstracted from its **content**.

Definition

Formally, an **argument structure** is a list of statements $p_1, p_2, \dots, p_n, \therefore c$ starting with **premises** $p_1, \dots, p_n$ and ending in a **conclusion** c.

- An argument is **valid** if the conclusion follows **necessarily** from the premises.
- Validity of arguments depends only on the form, not on the content.
- The argument structure '$p_1, \dots, p_n, \therefore c$' is **valid** if the proposition $(p_1 \wedge \cdots \wedge p_n) \to c$ is a **tautology**, otherwise it is **invalid**.

How to Test Argument Validity.

1. Identify the **premises** and the **conclusion** of the argument.
2. Construct a **truth table** showing the truth values of all premises and the conclusion.
3. A **critical row** is a row of the truth table in which **all** the **premises** are **true**. Check the critical rows as follows.
4. If the **conclusion is true in every critical row** then the **argument structure is valid**.
5. If there is a critical row in which the conclusion is false, then it is possible for an argument of the given form to have a **false conclusion despite true premises** and so the **argument structure is invalid**.

Example of an Invalid Argument Structure.

Example

- Premises: $p_1 = (p \to q \vee \neg r)$, $p_2 = (q \to p \wedge r)$.
- Conclusion: $c = (p \to r)$.
- The argument structure $p_1, p_2, \therefore c$ is **invalid**:

p	q	r	$\neg r$	$q \vee \neg r$	$p \wedge r$	p_1	p_2	c
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	
T	F	T	F	F	T	F	T	
T	F	F	T	T	F	T	T	F(!)
F	T	T	F	T	F	T	F	
F	T	F	T	T	F	T	F	
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

Valid Arguments vs Invalid Arguments.

Some Valid Argument Forms.

- Modus ponens: $p \to q$, p, $\therefore q$.
- Modus tollens: $p \to q$, $\neg q$, $\therefore \neg p$.
- Generalization: p, $\therefore p \vee q$.
- Specialization: $p \wedge q$, $\therefore p$.
- Conjunction: p, q, $\therefore p \wedge q$.
- Elimination: $p \vee q$, $\neg q$, $\therefore p$.
- Transitivity: $p \to q$, $q \to r$, $\therefore p \to r$.
- Division into cases: $p \vee q$, $p \to r$, $q \to r$, $\therefore r$.
- Contradiction Rule: $\neg p \to F$, $\therefore p$.

Some Common Fallacies.

- Converse fallacy: $p \to q$, q, $\therefore p$.
- Inverse fallacy: $p \to q$, $\neg p$, $\therefore \neg q$.

"All Humans Are Mortal."

- **Modus Ponens:**
  $p \to q,\ p,\ \therefore\ q.$

Example

- If Socrates is human then he is mortal.
- Socrates is human.
- $\therefore$ Socrates is mortal.

- Proof by truth table:

p	q	$p \to q$	p	q
T	T	T	T	T
T	F	F	T	
F	T	T	F	
F	F	T	F	

- **Modus Tollens:**
  $p \to q,\ \neg q,\ \therefore\ \neg p.$

Example

- If Zeus is human then he is mortal.
- Zeus is not mortal.
- $\therefore$ Zeus is not human.

- Proof by truth table:

p	q	$p \to q$	$\neg q$	$\neg p$
T	T	T	F	
T	F	F	T	
F	T	T	F	
F	F	T	T	T

Fallacies.

- **Converse Fallacy:**
  $p \to q,\ q,\ \therefore p.$

Example (WRONG!)

- If Socrates is human then he is mortal.
- Socrates is mortal
- $\therefore$ Socrates is human.

- Truth table:

p	q	$p \to q$	q	p
T	T	T	T	T
T	F	F	F	
F	T	T	T	F(!)
F	F	T	F	

- **Inverse Fallacy:**
  $p \to q,\ \neg p,\ \therefore \neg q.$

Example (WRONG!)

- If Zeus is human then he is mortal.
- Zeus is not human.
- $\therefore$ Zeus is not mortal.

- Truth table:

p	q	$p \to q$	$\neg p$	$\neg q$
T	T	T	F	
T	F	F	F	
F	T	T	T	F(!)
F	F	T	T	T

Knights and Knaves Revisited.

- $a =$ 'A is a knight'.
- $b =$ 'B is a knight'.

Example

- You visit the island of knights and knaves and find that:

$$
\begin{aligned}
a &\to \neg b \\
\neg a &\to \neg b \\
b &\to a \vee b \\
\neg b &\to \neg a \wedge \neg b
\end{aligned}
$$

(a 'formal version' of the original puzzle).

- Who (if any) is telling the truth?

Solution

- Start with the tautology $a \vee \neg a$.
- Division into cases:

$$
\begin{array}{l}
a \vee \neg a, \\
a \to \neg b, \\
\underline{\neg a \to \neg b,} \\
\therefore \neg b.
\end{array}
$$

- Modus ponens:

$$
\begin{array}{l}
\neg b \to \neg a \wedge \neg b, \\
\underline{\neg b, \qquad\qquad\qquad} \\
\therefore \neg a \wedge \neg b.
\end{array}
$$

- Both are knaves!

- This solution is a 'formal version' of the original solution.

Subsets and Set Operations.

- A set B is a **subset** of a set A if each element of B is also an element of A:
  $B \subseteq A$ if $b \in A$ for all $b \in B$.
- $A = B$ if and only if $B \subseteq A$ and $A \subseteq B$.
- We assume that all our sets are subsets of a (big) **universal set**, or **universe** U.

Definition

Let $A, B \subseteq U$.

- The **union** of A and B is the set
  $A \cup B = \{x \in U : x \in A \text{ or } x \in B\}$.
- The **intersection** of A and B is the set
  $A \cap B = \{x \in U : x \in A \text{ and } x \in B\}$.
- The **(set) difference** of A and B is the set
  $A \setminus B = \{x \in U : x \in A \text{ and } x \notin B\}$.
- The **complement** of A (in U) is the set
  $A' = \{x \in U : x \notin A\}$.

Set Equations.

Theorem

Let A, B, C *be subsets of a universal set* U*. Then all of*

$$
\begin{aligned}
A \cap B &= B \cap A, & A \cup B &= B \cup A,\\
(A \cap B) \cap C &= A \cap (B \cap C), & (A \cup B) \cup C &= A \cup (B \cup C),\\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), & A \cup (B \cap C) &= (A \cup B) \cap (A \cup C),\\
A \cap (A \cup B) &= A, & A \cup (A \cap B) &= A,\\
A \cap A &= A, & A \cup A &= A,\\
A \cap A' &= \varnothing, & A \cup A' &= U,\\
A \cap U &= A, & A \cup \varnothing &= A,\\
A \cap \varnothing &= \varnothing, & A \cup U &= U,\\
(A \cap B)' &= A' \cup B', & (A \cup B)' &= A' \cap B',\\
U' &= \varnothing, & \varnothing' &= U,\\
(A')' &= A
\end{aligned}
$$

are valid properties of set operations.

Proof: element-wise. $\square$

Boolean Algebra.

- An example of **abstraction** in mathematics ...

- **Sets** (together with the operations $\cap$, $\cup$, $'$, and the constants $\varnothing$, $\mathcal{U}$) behave similar to **Propositions** (together with the operations $\wedge$, $\vee$, $\neg$, and the constants F, T)
- Both are examples of an **abstract structure** (with $\cdot$, $+$, $'$, and 0, 1) called a **Boolean algebra**

- For any **logical equivalence**, there is a corresponding **set equality**, and vice versa.

Duality

- The **dual** of a set equality is obtained by swapping $\cap$ with $\cup$ and swapping $\varnothing$ with $\mathcal{U}$.
- The dual of a valid set equality is also a valid set equality ...

Sets of Sets.

Definition

Let A be a set. The **power set** of A is the set
$P(A) = \{B : B \subseteq A\}$
of **all** subsets B of A.

Example

The power set of $A = \{1, 3, 5\}$ is the set
$P(A) = \{\varnothing, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{1, 3, 5\}\}$

Definition

A **partition** of a set A is a set $P = \{P_1, P_2, \ldots\}$ of **parts** $P_1, P_2, \ldots \subseteq A$ such that

1. no part is empty: $P_i \neq \varnothing$ for all i;
2. distinct parts are disjoint: $P_i \cap P_j = \varnothing$ for all $i \neq j$;
3. every point is in some part: $A = P_1 \cup P_2 \cup \cdots$.

Products of Sets.

Definition

The **Cartesian product** of sets A and B is the set
$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$
of all **(ordered) pairs** (a, b).

Examples

- $A = \{1, 2, 3\}$, $B = \{X, Y\}$.
  $A \times B = \{(1, X), (1, Y), (2, X), (2, Y), (3, X), (3, Y)\}$.
- $A = \{1, 3\}$. $A^2 = A \times A = \{(1, 1), (1, 3), (3, 1), (3, 3)\}$

- More generally, for $n \in \mathbb{N}$, the Cartesian product of n sets $S_1, S_2, \dots, S_n$ is the set
  $S_1 \times S_2 \times \cdots \times S_n = \{(x_1, x_2, \dots, x_n) : x_i \in S_i\}$
  of all n**-tuples** $(x_1, x_2, \dots, x_n)$.
- $A^n = A \times A \times \cdots \times A$ (n factors).

Relations are Sets.

- A **relation** from a **domain** X to a **codomain** Y is a subset $R \subseteq X \times Y$.

Notation.

Write xRy (and say "x is related to y") for $(x, y) \in R$.

- Let R be a relation on X, i.e, $R \subseteq X \times X$.
- R is **reflexive** if xRx for all $x \in X$.
- R is **symmetric** if xRy then yRx for all $x, y \in X$.
- R is **transitive** if xRy and yRz then xRz, for all $x, y, z \in X$.
- A relation $R \subseteq X \times X$ that is reflexive, symmetric and transitive is called an **equivalence relation**.

Equivalence Relations are Partitions.

- Suppose R is an **equivalence relation** on a set X.
  For $x \in X$, denote by $[x] = \{y : xRy\}$ the **equivalence class** of x, i.e., the set of all $y \in X$ that x is R-related to.
  Also denote by $X/R = \{[x] : x \in X\}$ the **quotient set**, i.e., the set of all equivalence classes.
- Suppose that P is a **partition** of X.
  For $x \in X$, denote by $P(x)$ the **unique part** of P that contains x.

Theorem

1. *If R is an **equivalence relation** on the set X, then the quotient set X/R is a **partition** of X.*
2. *Conversely, if P is a **partition** of a set X, then the relation $R = \{(x, y) \in X^2 : P(x) = P(y)\}$ is an **equivalence relation**.*

Functions are Relations are Sets.

- A **function** f from a **domain** X to a **codomain** Y is a **relation** $f \subseteq X \times Y$, with the property that,

  for every $x \in X$,
  there is a **unique** $y \in Y$ such that $(x, y) \in f$.

- (This is often called the **Vertical Line Test**.)

Notation.

Write $f \colon X \to Y$ for a function f from X to Y
and $f(x) = y$ for the unique $y \in Y$ such that if $(x, y) \in f$.

- A **function** thus consists of three things: a **domain** X and a **codomain** Y together with a **rule** $f \subseteq X \times Y$ that associates to each point $x \in X$ a **unique value** $f(x) = y \in Y$.

Injective and Surjective Functions.

- A function $f\colon X \to Y$ is called **surjective** (or **onto**) if,

  for every $y \in Y$,
  there is **at least** one $x \in X$ such that $f(x) = y$.

- A function $f\colon X \to Y$ is called **injective** (or **one-to-one**) if,

  for every $y \in Y$,
  there is **at most** one $x \in X$ such that $f(x) = y$.

- A function $f\colon X \to Y$ is called **bijective** (or a **one-to-one correspondence** if it is both **injective** and **surjective**, i.e., if,

  for every $y \in Y$,
  there is a **unique** $x \in X$ such that $f(x) = y$.

- A function is injective/surjective/bijective if it passes a suitable **Horizontal Line Test**.

Bijections of Partitions and Subsets.

- Consider a **function** $f\colon X \to Y$.
- The **image** $f(X) = \{f(x) : x \in X\}$ is a **subset** of Y.
- The **relation** $\sim_f$ on X by $x \sim_f x'$ if $f(x) = f(x')$ is an **equivalence** relation and the equivalence classes $[x] = \{x' \in X : f(x) = f(x')\}$ form **partition** $X/\sim_f$ of X, called the **kernel** of f.

Theorem

1. *Let $f\colon X \to Y$. Then the function $F\colon X/\sim_f \to f(X)$ defined by $F([x]) = f(x)$ for $x \in X$ is a well-defined bijection between the kernel $X/\sim_f$ of f and the image $f(X)$ of f.*
2. *Conversely, if $Y' \subseteq Y$ is any subset of Y, if $\sim$ is any equivalence relation on X and $F\colon X/\sim \to Y'$ is a bijection then the rule $f(x) = F([x])$ defines a function f from X to Y.*

Summary: The Language of Mathematics.

- **Formal propositions** consist of **propositional variables**, combined by the **logical connectives** $\wedge$ (and), $\vee$ (or), and $\neg$ (not).
- A **truth table** determines the truth value of a proposition depending on the truth values of its propositional variables.
- Truth tables can **validate** and invalidate **argument structures**.
- Sets, with the operations $\cap$ (intersection), $\cup$ (union), and $'$ (complement in a universal set $\mathcal{U}$) form a **Boolean algebra**, like the formal propositions with their logical operations.
- Claims about sets are **proved** by valid arguments.
- **Functions** and **relations** are sets (of pairs).
- A function is a one-to-one **correspondence** between a **partition** of its **domain** and a **subset** of its **codomain**.

Introduction: Permutations and Polynomials.

- Certain **types of functions** occur frequently in **applications** and form examples of important **algebraic structures**.
- **Permutations** of a set correspond to **rearrangements** of its elements.
- In Computer Science, permutations are used in the study of **sorting** algorithms.
- The **product** of two permutations is a **composition** of functions.
- **Polynomials** are linear combinations of powers of an **indeterminate** x.
- Solving **polynomial equations** is a central problem in algebra.
- **Addition**, **multiplication** and **division** of polynomials share many properties with the corresponding operations on the **integers**.

Links: Permutations and Polynomials.

- http://en.wikipedia.org/wiki/Fifteen_puzzle
- http://en.wikipedia.org/wiki/Rubik's_Cube
- http://en.wikipedia.org/wiki/Function_composition
- http://en.wikipedia.org/wiki/Permutation
- http://en.wikipedia.org/wiki/Symmetric_group
- http://en.wikipedia.org/wiki/Cycle_(mathematics)
- http://www.cut-the-knot.org/Curriculum/Combinatorics/PermByTrans.shtml
- http://en.wikipedia.org/wiki/Group_(mathematics)
- http://en.wikipedia.org/wiki/Ring_(mathematics)
- http://en.wikipedia.org/wiki/Field_(mathematics)
- http://en.wikipedia.org/wiki/Polynomial
- http://en.wikipedia.org/wiki/Polynomial_long_division
- http://en.wikipedia.org/wiki/Irreducible_polynomial
- http://mathworld.wolfram.com/IrreduciblePolynomial.html
- http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra

Composition of Functions.

- The **composition** of relations $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ is the relation $S \circ R$ from X to Z defined by $x(S \circ R)z$ if xRy and ySz for some $y \in Y$.
- The **composition** of functions $f\colon X \to Y$ and $g\colon Y \to Z$ is the function $g \circ f\colon X \to Z$ defined by $(g \circ f)(x) = g(f(x))$ for $x \in X$.

Theorem

Composition of functions is ***associative****:* $(f \circ g) \circ h = f \circ (g \circ h)$.

Proof.

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$
$$= f((g \circ h)(x)) = (f \circ (g \circ h))(x). \qquad \square$$

- The composition of functions $f\colon X \to X$ and $g\colon X \to X$ is a function $g \circ f$ from the set X to itself.

Bijections and Inverse functions.

Example

Let X be a set. The **identity function** $\mathrm{id}_X \colon X \to X$, defined by $\mathrm{id}_X(x) = x$ for all $x \in X$, is a bijection.

- If $f \colon X \to Y$ is a bijection there is a function $g \colon Y \to X$ defined by $g(y) = x$ if $f(x) = y$ (i.e., g maps $y \in Y$ to the unique $x \in X$ that f maps to y.)
- The function g is bijective as well and has the property that $g \circ f = \mathrm{id}_X$ (i.e., $g(f(x)) = x$ for all $x \in X$) and $f \circ g = \mathrm{id}_Y$ (i.e. $f(g(y)) = y$ for all $y \in Y$).
- This function g is **uniquely determined** by f and called the **inverse** of f.

Theorem

A function has an ***inverse*** *if and only if it is a* ***bijection****.*

Permutations.

- A **permutation** of a set X is a **bijection** from X to **itself**.
- Frequently, $X = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.

Example ($X = \{1, 2, 3, 4, 5, 6\}$.)

The **relation** $\pi = \{(1,2), (2,5), (3,3), (4,6), (5,1), (6,4)\}$ on X is a **bijection**, which is written in **two-line-notation** as the **permutation** $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix}$.

- There are $n! = 1 \cdot 2 \cdots n$ permutations of X if $|X| = n$.
- The set S_n of all permutations of $X = \{1, 2, \ldots, n\}$ is called the **symmetric group** of degree n.

Example ($n = 3$.)

$S_3 = \{\binom{1\,2\,3}{1\,2\,3}, \binom{1\,2\,3}{2\,1\,3}, \binom{1\,2\,3}{3\,2\,1}, \binom{1\,2\,3}{1\,3\,2}, \binom{1\,2\,3}{2\,3\,1}, \binom{1\,2\,3}{3\,1\,2}\}$. $|S_3| = 3! = 6$.

Products of Permutations.

- The **product** $\sigma \circ \pi$ of $\pi, \sigma \in S_n$, defined by $(\sigma \circ \pi)(x) = \sigma(\pi(x))$, for $x \in X$, is a permutation.
- The **inverse** of $\pi = \binom{1 \ \cdots \ n}{\pi(1) \ \cdots \ \pi(n)}$ is the permutation $\pi^{-1} = \binom{\pi(1) \ \cdots \ \pi(n)}{1 \ \cdots \ n}$, since $\pi^{-1} \circ \pi = \mathrm{id}_X$.
- An m**-cycle** $(x_1, x_2, \dots, x_m)$ permutes the m points $x_1, x_2, \dots, x_m \in X$ cyclically.
- Each permutation is a product of **disjoint cycles**.

Example

$\pi = \binom{123456}{253614} = (1,2,5)(3)(4,6) = (1,2,5)(4,6)$.

- The **order** of a permutation π is the smallest $k \in \mathbb{N}$ such that $\pi^k = \pi \circ \pi \circ \cdots \circ \pi = \mathrm{id}_X$.
- An m-cycle has order m.
- The order of $\pi \in S_n$ is the lcm of its cycle lengths.

Write a Permutation as Disjoint Cycles.

Algorithm: Disjoint Cycles.

0. Consider all points $x \in \{1, 2, \ldots, n\}$ as "**unmarked**".
1. If all points are marked: STOP
   Otherwise, let x be the **smallest unmarked point**.
2. Determine its **cycle**

   $$(x, \pi(x), \pi^2(x), \ldots)$$

   and mark all the points in the cycle.
3. **Go back** to step 1.

- Here $\pi^2 = \pi \circ \pi$, $\pi^k = \pi \circ \pi^{k-1}$.
- Given $\pi \in S_n$, what is the smallest $k \in \mathbb{N}$, such that $\pi^k = \mathrm{id}_X$?
- This k is called the **order** of π.

Products of Transpositions.

Examples

$(1,2)^{-1} = (1,2)$ and $(1,2)(2,3) = (1,2,3)$.

- A 2-cycle is called a **transposition**.
- Each n-cycle is a product of transpositions: $(x_1, x_2, \ldots, x_n) = (x_1, x_2)(x_2, x_3)\cdots(x_{n-1}, x_n)$.

Theorem (Librarian's Nightmare.)

Each permutation $\pi \in S_n$ is a product of transpositions

- $\pi \in S_n$ is called **even** (resp. **odd**) if it is a product of an even (resp. odd) number of transpositions.

Fact.

A permutation $\pi \in S_n$ is either even or odd, **but not both**.

Groups.

- The symmetric group S_n is an example of a **group**.
- In general, a group is defined by **axioms**.

Definition

A **group** is a set G, together with a **binary operation** $\star \colon G \times G \to G$ such that:

(G1) **Associative:** $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.

(G2) **Identity:** There exists an element $e \in G$ such that $a \star e = a$ and $e \star a = a$ for all $a \in G$.

(G3) **Inverse:** For each $a \in G$ there exists an element $a' \in G$ such that $a \star a' = e$ and $a' \star a = e$.

Examples

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \cdot)$, $(\{\pm 1\}, \cdot)$, ...
- The set of invertible 2×2-matrices over $\mathbb{Q}$.
- $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$, $(P(S), \cup)$, $(P(S), \cap)$ are **not groups**.

Rings.

- A group $(G, \star)$ is **abelian** (or **commutative**) if $a \star b = b \star a$ for all $a, b \in G$.

Definition

A **ring** is a set R together with binary operations $+$ **and** $\star$: $R \times R \to R$ such that $(R, +)$ is an abelian group and:

(R1) $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in R$.

(R2) There exists an element $e \in R$ such that $a \star e = a$ and $e \star a = a$ for all $a \in R$.

(R3) $a \star (b + c) = a \star b + a \star c$ and $(a + b) \star c = a \star c + b \star c$ for all $a, b, c \in R$.

- A ring $(R, +, \star)$ is called **commutative** if $a \star b = b \star a$ for all $a, b \in R$.

Examples

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_m$, ..., the set of **all** 2×2-matrices over $\mathbb{Q}$.

Polynomials are like Numbers.

Definition

Suppose R is a commutative ring. A **polynomial** over R is an expression of the form

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$= a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n = \sum_{i=0}^{n} a_i x^i.$$

for some integer $n \geqslant 0$, with **coefficients** $a_0, a_1, \ldots, a_n \in R$ (e.g. $R = \mathbb{R}$ or $R = \mathbb{Z}_m$)

- Two polynomials are **equal** if they have the **same coefficent** at every power of x.
- A polynomial $p(x)$ defines a **polynomial function** $R \to R$ by the rule $a \mapsto p(a)$.

Distinct polynomials can define the same function.

Rings of Polynomials.

- The set of all polynomials over R is denoted by $R[x]$.
- Polynomials can be **added**:

$$\left(\sum a_i x^i\right) + \left(\sum b_i x^i\right) = \sum (a_i + b_i) x^i.$$

- Polynomials can be **multiplied**:

$$\begin{aligned}\left(\sum a_i x^i\right)\left(\sum b_i x^i\right) &= \sum_j \sum_k a_j b_k x^{j+k} \\ &= \sum_i \Big(\sum_{j+k=i} a_j b_k \Big) x^i.\end{aligned}$$

- $R[x]$ is a **commutative ring**.

Quotients and Roots of Polynomials.

- A **field** is a commutative ring F, where each $a \in F \setminus \{0\}$ has an inverse.

Examples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, $\mathbb{Z}$ is not. $\mathbb{Z}_m$ is a field if m is a prime.

Theorem

Suppose that F is a field.

- (**Division Theorem.**) *Let $f, g \in F[x]$ be polynomials with $g \neq 0$. Then there exist unique polynomials $q \in F[x]$ (the **quotient**) and $r \in F[x]$ (the **remainder**) with $\deg r < \deg g$ such that $f = gq + r$.*
- (**Remainder Theorem.**) *For any polynomial $f(x) \in F[x]$ and $a \in F$, the value $f(a)$ is the remainder of $f(x)$ upon division by $(x - a)$.*
- (**Root Theorem.**) *$a \in F$ is a **root** of $f(x) \in F[x]$ if and only if $x - a$ is a **factor** of $f(x)$.*

Greatest Common Divisors.

- **Euclid's Algorithm** can be used to compute the **gcd** of two polynomials f and g.

Example

- $f = x^5 + 1 \in \mathbb{Z}_3[x]$, $g = x^2 + 1 \in \mathbb{Z}_3[x]$.
- $x^5 + 1 = (x^2 + 1)(x^3 + 2x) + (x + 1)$.
- $x^2 + 1 = (x + 1)(x + 2) + 2$.
- $\gcd(f, g) = 2 = -1 \cdot 1$.

Example

- $f = x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$, $g = x^2 + 2x + 1 \in \mathbb{Z}_3[x]$.
- $x^3 + 2x^2 + 2 = (x^2 + 2x + 1)x + (2x + 2)$.
- $x^2 + 2x + 1 = (2x + 2)(2x + 2) + 0$.
- $\gcd(f, g) = 2x + 2 = -1 \cdot (x + 1)$.

- $\gcd(f, g)$ can be computed without factoring f or g.

Irreducible Polynomials.

- Recall that, if $f \in F[x]$ then $\deg f \leqslant 0$ if and only if f is a constant polynomial, i.e. $f \in F$.
- A polynomial $p \in F[x]$ is **irreducible** if $\deg p > 0$ and if $p = fg$ for polynomials $f, g \in F[x]$ implies that either $\deg f = 0$ or $\deg g = 0$.
- Any nonzero polynomial $f \in F[x]$ is either irreducible or it is a **product** of **irreducible polynomials**.

Theorem

Let $f \in F[x]$. If $f = p_1 p_2 \cdots p_s$ and $f = q_1 q_2 \cdots q_t$ are two factorizations of f into a product of irreducible polynomials, then $s = t$, and up to rearranging the factors, $q_i = r_i p_i$ for some $r_i \in F$, $i = 1, \ldots, s$.

- Thus the factorization of a polynomial f into a product of irreducible polynomials is essentially **unique**.

Examples of Irreducible Polynomials.

- $f(x) = x - r \in F[x]$ for any $r \in F$ is irreducible.
- $f(x) = x^2 + bx + c \in \mathbb{R}[x]$ is irreducible if $b^2 - 4c < 0$.

Theorem (Fundamental Theorem of Algebra)

If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n > 0$ then $f(x)$ has a root in $\mathbb{C}$.

- Consequently, no polynomial $f \in \mathbb{C}[x]$ with $\deg f > 1$ is irreducible.
- No polynomial $f \in \mathbb{R}[x]$ with $\deg f > 2$ is irreducible.

Proof.

Suppose $\deg f > 2$. By the Fundamental Theorem, $f(x)$ has a complex root $\alpha \in \mathbb{C}$. Note that $\overline{f(x)} = f(\overline{x})$. $f(\alpha) = 0$ implies $f(\overline{\alpha}) = \overline{f(\alpha)} = \overline{0} = 0$. Hence both $(x - \alpha)$ and $(x - \overline{\alpha})$ are factors of $f(x)$. Suppose $\alpha = a + b\,i$. Then $(x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$ is an irreducible factor of $f(x)$. □

Summary: Permutations and Polynomials.

- **Composition** of functions is **associative**.
- A **permutation** is a bijection from a set to itself.
- A permutation is a product of **disjoint cycles**.
- The cycle lengths determine the **order** of a permutation.
- A permutation has **sign** $(-1)^\ell$ if it is a product of ℓ **transpositions**.
- The permutations of the set $\{1, \dots, n\}$ form the **symmetric group** S_n with **composition** as product.
- The **polynomials** over a **commutative ring** R form a **commutative ring** $R[x]$.
- **Quotients** and **remainders** of polynomials are computed by **long division**.
- A polynomial over a **field** is a product of **irreducible** polynomials in an essentially **unique** way.
- Every irreducible polynomial $f \in \mathbb{C}[x]$ has degree 1.
- An irreducible polynomial $f \in \mathbb{R}[x]$ has $\deg f \leqslant 2$.

Introduction: Induction and Matrix Algebra

- Induction, in the **experimental sciences**, is a type of reasoning used to infer an event from the observation of past events.
- Mathematics is an **exact science**, where this type of reasoning is not considered valid.
- **Mathematical Induction** is a technique used to prove statements about natural numbers.
- Here, properties of the numbers $1, \ldots, n-1$ are used to **prove** a property of the number n.
- The technique **applies** to theorems about **numbers**, about **polynomials**, about **matrices**, ...
- Insights into properties of **square matrices** are obtained by computing their **determinants** and **eigenvalues**.
- Eigenvalues can be found as **roots** of the **characteristic polynomial** of a matrix.

Links: Induction and Matrix Algebra.

- http://oeis.org/search?q=2,4,8,16,31
- http://en.wikipedia.org/wiki/Mathematical_induction
- http://www.cut-the-knot.org/induction.shtml
- http://en.wikipedia.org/wiki/Determinant
- http://mathworld.wolfram.com/Determinant.html
- http://en.wikipedia.org/wiki/Adjugate_matrix
- http://en.wikipedia.org/wiki/Minor_(linear_algebra)
- http://en.wikipedia.org/wiki/Eigenvalues_and_eigenvectors
- http://mathworld.wolfram.com/Eigenvalue.html
- http://en.wikipedia.org/wiki/Characteristic_polynomial
- http://en.wikipedia.org/wiki/Cayley-Hamilton_theorem
- http://www-history.mcs.st-andrews.ac.uk/Biographies/Cayley.html is a biography of the British mathematician **Arthur Cayley** (1821–1895).
- http://www-history.mcs.st-andrews.ac.uk/Biographies/Hamilton.html is a biography of the Irish mathematician **William Rowan Hamilton** (1805–1865).

The Principle of Induction.

- A **statement about the natural numbers** is a **predicate** $P(n)$ with **domain** $\mathbb{N}$.
- That is, when any natural number is substituted for n then $P(n)$ becomes a **proposition**, a statement that is unambiguously true or false.

Principle of Mathematical Induction

Let $P(n)$ be a statement about the natural numbers. If

1. $P(1)$ is true, and
2. $P(k)$ implies $P(k+1)$, for every integer $k > 0$,

then we can conclude that $P(n)$ is true for every $n \in \mathbb{N}$.

- $P(1)$ is called the **base case**.
- A proof that $P(k)$ implies $P(k+1)$ for all $k > 0$ is called the **induction step**.

An Example of Mathematical Induction.

- Suppose that $a_n = \begin{cases} 1, & \text{if } n = 1, \\ a_{n-1} + (2n-1), & \text{if } n > 1. \end{cases}$

- **Claim:** $a_n = n^2$ for all $n > 0$.

Proof.

Let $P(n)$ be the statement "$a_n = n^2$".

Base Case. $P(1)$ is the statement "$a_1 = 1^2$".
$P(1)$ is true since both $a_1 = 1$ and $1^2 = 1$.

Induction Step. Let $k > 0$.
Assume that $P(k)$ is true, i.e., that $a_k = k^2$.
$P(k+1)$ is the statement "$a_{k+1} = (k+1)^2$".
By definition $a_{k+1} = a_k + 2k + 1$.
Using $P(k)$, conclude that $a_{k+1} = k^2 + 2k + 1$.
Now $P(k+1)$ is true since $(k+1)^2 = k^2 + 2k + 1$.

Consequently, $P(n)$ is true for all $n > 0$. $\square$

Variations of the Induction Theme.

- Sometimes the base case is different from $k = 1$.

Let $P(n)$ be a statement about the integers. If

1. $P(l)$ is true for some $l \in \mathbb{Z}$, and
2. $P(k)$ implies $P(k+1)$, for every integer $k \geqslant l$,

then $P(n)$ is true for every integer $n \geqslant l$.

- Sometimes it is necessary to assume $P(m)$ for **all** $m \leqslant k$ in order to derive $P(k+1)$.

Let $P(n)$ be a statement about the integers. If

1. $P(1)$ is true, and
2. for every integer $k \geqslant 1$, the truth of $P(m)$ for all $1 \leqslant m \leqslant k$ implies $P(k+1)$,

then $P(n)$ is true for every integer $n \geqslant m$.

Applications of Mathematical Induction.

Counting Subsets.

- A set X of size n has exactly 2^n subsets: $|X| = n \implies |P(X)| = 2^n$.

Sums of Integers, Squares, Cubes, ...

- $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$ for all $n \in \mathbb{N}$.
- $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ for all $n \in \mathbb{N}$.
- $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$ for all $n \in \mathbb{N}$.

Each Permutation is a Product of Transpositions.

- $(x_1, x_2, \ldots, x_n) = (x_1, x_2)(x_2, x_3) \cdots (x_{n-1}, x_n)$.

The Roots of a Complex Polynomial.

- If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree d, then $f(x)$ has exactly d (not necessarily distinct) roots.

Determinants.

- Recall $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$.
- And $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - afh - bdi - ceg$.

- In general, if $A = (a_{ij})$ is an $n \times n$-matrix then the **determinant** of A is the **number**

$$\det(A) = |A| = \sum_{\pi \in S_n} \operatorname{sign}(\pi)\, a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)},$$

  a sum of $n!$ terms.

- This formula is used for **theoretical** purposes.

Properties of the Determinant.

- $\det(A^T) = \det(A)$, where A^T is the **transpose** of A.
- $\det(AB) = \det(A)\det(B)$, if A and B are both $n \times n$,
- $\det(A) \neq 0$ if and only if A is invertible.

More about Determinants.

Further Properties of the Determinant.

- $\det(I_n) = 1$, where I_n is the $n \times n$ **identity** matrix.
- $\det(A) = 0$ if two rows of A are the **same**.
- $\det(A)$ is **linear** in the ith row of A, for each i.

The Determinant under Row Operations.

- If B is obtained from A by adding a multiple of row i to row j, $(j \neq i)$ then $\det B = \det A$.
- If B is obtained from A by multiplying row i with a scalar c then $\det B = c \det A$.
- If B is obtained from A by swapping rows i and j $(j \neq i)$ then $\det B = -\det A$.

Cofactors.

- The **minor matrix** A_{ij} is obtained from $A = (a_{ij})$ by deleting its ith row and its jth column:

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \vdots & & & & \vdots \\ a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & & & & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{pmatrix}$$

- The **cofactor** a'_{ij} of a_{ij} in A is the number $a'_{ij} = (-1)^{i+j} \left|A_{ij}\right|$.

- $|A| = a_{11}a'_{11} + a_{12}a'_{12} + \cdots + a_{1n}a'_{1n}$.

Example Determinant Calculation.

- $A = \begin{bmatrix} 5 & -2 & 4 & -1 \\ 0 & 1 & 5 & 2 \\ 1 & 2 & 0 & 1 \\ -3 & 1 & -1 & 1 \end{bmatrix}$.
- $|A| = 5\,|A_{11}| - (-2)\,|A_{12}| + 4\,|A_{13}| - (-1)\,|A_{14}|$, where
- $|A_{11}| = \begin{vmatrix} 1 & 5 & 2 \\ 2 & 0 & 1 \\ 1 & -1 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ -1 & 1 \end{vmatrix} - 5\begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} + 2\begin{vmatrix} 2 & 0 \\ 1 & -1 \end{vmatrix} = 1-5-4 = -8$,
- $|A_{12}| = \begin{vmatrix} 0 & 5 & 2 \\ 1 & 0 & 1 \\ -3 & -1 & 1 \end{vmatrix} = 0 - 5\begin{vmatrix} 1 & 1 \\ -3 & 1 \end{vmatrix} + 2\begin{vmatrix} 1 & 0 \\ -3 & -1 \end{vmatrix} = -20-2 = -22$,
- $|A_{13}| = \begin{vmatrix} 0 & 1 & 2 \\ 1 & 2 & 1 \\ -3 & 1 & 1 \end{vmatrix} = 0 - 1\begin{vmatrix} 1 & 1 \\ -3 & 1 \end{vmatrix} + 2\begin{vmatrix} 1 & 2 \\ -3 & 1 \end{vmatrix} = -4 + 14 = 10$,
- $|A_{14}| = \begin{vmatrix} 0 & 1 & 5 \\ 1 & 2 & 0 \\ -3 & 1 & -1 \end{vmatrix} = 0 - 1\begin{vmatrix} 1 & 0 \\ -3 & -1 \end{vmatrix} + 5\begin{vmatrix} 1 & 2 \\ -3 & 1 \end{vmatrix} = 1 + 35 = 36$.
- So $|A| = 5\cdot(-8) + 2\cdot(-22) + 4\cdot 10 + 36 = \underline{-8}$.

The Adjoint of a Matrix.

- For a square matrix $A = (a_{ij})$ let $A' = (a'_{ij})$ be the **matrix of cofactors** $a'_{ij} = (-1)^{i+j} \left|A_{ij}\right|$ of A.
- The **adjoint matrix** A^* of A is the **transpose** of A':
$$A^* = (A')^\top.$$

Properties

- $A^* \cdot A = A \cdot A^* = |A| \cdot I_n$,
  where I_n is the $n \times n$ identity matrix.
- **Expansion** by the rth **row**:
  $|A| = a_{r1}a'_{r1} + a_{r2}a'_{r2} + \cdots + a_{rn}a'_{rn}$
  for each row index r
- **Expansion** by the sth **column**:
  $|A| = a_{1s}a'_{1s} + a_{2s}a'_{2s} + \cdots + a_{ns}a'_{ns}$
  for each column index s

Upper Triangular Matrices.

- A square matrix $U = (u_{ij})$ is called an **upper triangular matrix** if $u_{ij} = 0$ whenever $i < j$, i.e., if it has the form

$$U = \begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & u_{nn} \end{pmatrix}$$

- The **determinant** of an upper triangular matrix U is the **product** of its **diagonal entries**:

$$|U| = u_{11}u_{22}\cdots u_{nn}.$$

Proof.

by induction on n. □

- A similar result holds for **lower triangular matrices**.

Eigenvalues and Eigenvectors.

- Any $n \times n$-matrix A can be regarded as a **linear transformation** on the vector space $\mathbb{R}^n$ which maps a (column) vector $v \in \mathbb{R}^n$ to the (column) vector $Av \in \mathbb{R}^n$.

- A number λ is an **eigenvalue** of A if there is a **nonzero** vector $v \in \mathbb{R}^n$ such that $Av = \lambda v$.
- The vector v is then called an **eigenvector** of A for the eigenvalue λ.

Example

- $$\begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \end{bmatrix} = 4 \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$
- Here the eigenvalue is $\lambda = 4$ and $v = \binom{1}{1}$ is an eigenvector.

Computing Eigenvalues.

- Write $Av = \lambda v$ as $Av - \lambda v = 0$, or $(A - \lambda I_n)v = 0$, where I_n is the **identity matrix**.
- A number λ is an eigenvalue of A if and only if the system $(A - \lambda I_n)v = 0$ of linear equations has a **nontrivial solution** v.
- $(A - \lambda I_n)v = 0$ has a nontrivial solution v if and only if $\det(A - \lambda I_n) = 0$.

Definition

The **polynomial** $f_A(x) = \det(A - xI_n)$ is the **characteristic polynomial** of the matrix A.

Theorem

*A number λ is an **eigenvalue** of the matrix A if and only if λ is a **root of the characteristic polynomial** $f_A(x)$, i.e., $f_A(\lambda) = 0$.*

Computing Eigenvectors; Diagonalization.

- To **find an eigenvector** v for an eigenvalue λ solve the system of linear equations $(A - \lambda I_n)v = 0$ for v and find a **nontrivial solution**.
- Let E be the matrix which has as its **columns** eigenvectors $v_1, \dots, v_n$ corresponding to the eigenvalues $\lambda_1, \dots, \lambda_n$ of A.
- Let D be the **diagonal matrix** with the eigenvalues $\lambda_1, \dots, \lambda_n$ on its diagonal (and all other entries 0).
- Then $AE = ED$.
- If the eigenvalues are **distinct** then E is **invertible** and $A = EDE^{-1}$.

Example

$$\begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & -3 \end{bmatrix} \begin{bmatrix} 4 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & -3 \end{bmatrix}^{-1}.$$

Properties of Eigenvalues and Eigenvectors.

Suppose A is an $n \times n$ matrix.

- $\det A$ equals the **product** of the eigenvalues; and $\operatorname{trace} A = a_{11} + a_{22} + \cdots + a_{nn}$ equals their **sum**.

If λ is an eigenvalue of A with eigenvector v then

- λ^k is an eigenvalue of the kth **power** A^k with the same eigenvector v.
- if the **inverse** A^{-1} exists, λ^{-1} is an eigenvalue of A^{-1} with the same eigenvector v.
- $\lambda + \mu$ is an eigenvalue of $A + \mu I_n$ with the same eigenvector v.

Moreover,

- A and its **transpose** $A^\top$ have the same eigenvalues;
- if P is an invertible matrix then $P^{-1}AP$ and A have the same eigenvalues.

Summary: Induction and Matrix Algebra.

- Mathematical **induction** is a powerful tool to prove statements about the natural numbers.
- A proof by mathematical induction constists of 1. the explicit verification of a **base case**, 2. an **induction step** that derives the next case from previous cases.
- An **eigenvalue** of a square matrix A is a number λ such that $Av = \lambda v$ for some vector $v \neq 0$.
- An **eigenvector** of a square matrix A is a vector $v \neq 0$ such that $Av = \lambda v$ for some number λ.
- The eigenvalues of A are the **roots** of the **characteristic polynomial** $\det(A - \lambda I_n)$ of A.
- An eigenvector for the eigenvalue λ is a **nontrivial solution** x of the system $(A - \lambda I_n)x = 0$.
- If the eigenvalues of A are **distinct**, the corresponding eigenvectors form an invertible matrix E which **diagonalizes** A as $A = EDE^{-1}$.

Course Summary and Outlook.

- **Logic** and **Set Theory** form the basis of the language of mathematics.
- Properties of **functions** and **relations** are studied in **Discrete Mathematics** (**MA284**).
- **Permutations** are examples of **group elements**.
- **Groups** are studied in **Group Theory**: (**MA3343**, **MA4344**).
- **Polynomials** (with coefficients from a **field**) and **matrices** are examples of **ring elements**.
- **Rings** and **Fields** are studied in **Abstract Algebra**: (**MA416**, **MA3491**).
- Matrices act as **linear transformations** on vectors.
- **Linear transformations** on **vector spaces** are studied in **Linear Algebra** (**MA283**).