Important Definitions for CS1231S

Michael Yang

Semester 1, AY23/24 (Prof Aaron Tan)

Appendix A (Properties of Real Numbers)

F1. Commutative Laws For all real numbers a and b, $a+b = b+a$ and $ab = ba$.

F2. Associative Laws For all real numbers a, b and c, $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.

F3. Distributive Laws For all real numbers a, b and c, $a(b+c) = ab+ac$ and $(b+c)a = ba+bc$.

F4. Existence of Identity Elements There exists two distinct real numbers, denoted 0 and 1, such that for every real number a, $0+a = a+0$ and $1 \cdot a = a \cdot 1$.

F5. Existence of Additive Inverses For every real number a, there is a real number, denoted $-a$ and called the **additive inverse** of a, such that $a+(-a) = (-a)+a = 0$.

F6. Existence of Reciprocals For every real number $a \neq 0$, there is a real number, denoted $1/a$ or a^{-1}, called the **reciprocal** of a, such that $a \cdot (\frac{1}{a}) = (\frac{1}{a}) \cdot a = 1$.

T1. Cancellation Law for Addition If $a+b = a+c$, then $b = c$. (In particular, this shows that the number 0 of Axiom F4 is unique.)

T2. Possibility of Subtraction Given a and b, there is exactly one x such that $a+x = b$. This x is denoted by $b-a$. In particular, $0-a$ is the additive inverse of a, $-a$.

T3. $b-a = b+(-a)$.

T4. $-(-a) = a$.

T5. $a(b-c) = ab-ac$.

T6. $0 \cdot a = a \cdot 0 = 0$.

T7. Cancellation Law for Multiplication If $ab = bc$ and $a \neq 0$, then $b = c$. (In particular, this shows that the number 1 of Axiom F4 is unique.)

T8. Possibility of Division Given a and b with $a \neq 0$, there is exactly one x such that $ax = b$. This x is denoted by b/a and is called the **quotient** of b and a. In particular, $1/a$ is the reciprocal of a.

T9. If $a \neq 0$, then $b/a = b \cdot a^{-1}$.

T10. If $a \neq 0$, then $(a^{-1})^{-1} = a$.

T11. Zero Product Property If $ab = 0$, then $a = 0$ or $b = 0$.

T12. Rule for Multiplication with Negative Signs $(-a)b = a(-b) = -(ab)$, and $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$.

T13. Equivalent Fractions Property $\frac{a}{b} = \frac{ac}{bc}$, if $b \neq 0$ and $c \neq 0$.

T14. Rule for Addition of Fractions $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, if $b \neq 0$ and $d \neq 0$.

T15. Rule for Multiplication of Fractions $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, if $b \neq 0$ and $d \neq 0$.

T16. Rule for Division of Fractions $\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$, if $b \neq 0$, $c \neq 0$ and $d \neq 0$.

T17. Trichotomy Law For arbitrary real numbers a and b, exactly one of these three relations $a < b$, $b > a$ or $a = b$ holds.

T18. Transitive Law If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a+c < b+c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a+b < c+d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

Ord1. For any real numbers a and b, if a and b are positive, so are $a+b$ and ab.

Ord2. For every real number $a \neq 0$, either a is positive or $-a$ is positive but not both.

Ord3. The number 0 is not positive.

Definition Given real numbers a and b, $a < b$ means $b+(-a)$ is positive. $b > a$ means $a < b$. $a \leq b$ means $a < b$ or $a = b$. $b \geq a$ means $a \leq b$. If $a < 0$, we say that a is **negative**. If $a \geq 0$, we say that a is **non-negative**.

Note: Whenever you are proving a universal statement using an arbitrary particular, you should quote **WLOG** (Without Loss Of Generality). This means that the proof for the special case can be easily applied to all other cases.

Definitions

Divisibility If $n, d \in \mathbb{Z}$ and $d \neq 0$, $d|n \Leftrightarrow \exists k \in \mathbb{Z}$ such that $n = dk$.

Rational Numbers r is rational $\leftrightarrow \exists a, b \in \mathbb{Z}$ s.t. $r = \frac{a}{b}$ and $b \neq 0$.

Fraction in lowest term A fraction $\frac{a}{b}$ where $b \neq 0$ is said to be in **lowest terms** if the largest integer that divides both a and b is 1.

Prime and Composite An integer n is **prime** iff $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** iff $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$. In symbols,

n **is prime:** $(n > 1) \wedge \forall r, s \in \mathbb{Z}^+, (n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$.

n **is composite:** $\exists r, s \in \mathbb{Z}^+ (n = rs \wedge (1 < r < n) \wedge (1 < s < n))$.

Compound Statements

2.1.1 Statement A **statement** (or **proposition**) is a sentence that is true or false, but not both.

2.1.2 Negation If p is a variable, the **negation** of p is "not p" or it is not the case that p" and is denoted $\sim p$.

2.1.3 Conjunction If p and q are statement variables, the conjunction of p and q is "p and q", denoted $p \wedge q$.

2.1.4 Disjunction If p and q are statement variables, the disjunction of p and q is "p or q", denoted $p \vee q$.

2.1.5 Statement Form A statement form (or propositional form) is an expression made up of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables.

2.1.6 Logical Equivalence Two statement forms are called logically equivalent if, and only if, they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted by $P \equiv Q$.

2.1.7 Tautology A tautology is a statement form that is **always true** regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement**.

2.1.8 Contradiction A contradiction is a statement form that is **always false** regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradiction is a **contradictory statement**.

2.2.1 Conditional If p and q are statement variables, the conditional of q by p is "if p then q" or "p implies q", denoted $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We called p the **hypothesis** (or **antecedent**) of the conditional and q the **conclusion** (or **consequent**).

2.2.2 Contrapositive The contrapositive of a conditional statement of the form "if p then q" is "if $\sim q$ then $\sim p$". Symbolically, the contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.

2.2.3 Converse The **converse** of a conditional statement "if p then q" is "if q then p". Symbolically, the converse of $p \rightarrow q$ is $q \rightarrow p$.

2.2.4 Inverse The **inverse** of a conditional statement "if p then q" is "if $\sim p$ then $\sim q$". Symbolically, the inverse of $p \rightarrow q$ is $\sim p \rightarrow \sim q$.

Note that $p \rightarrow q \not\equiv q \rightarrow p$.

2.2.5 Only If If p and q are statements, "p only if q" means "if not q then not p" or $\sim q \rightarrow \sim p$. Or, equivalently, "if p then q" or "$p \rightarrow q$".

2.2.6 Biconditional Given statement variables p and q, the **biconditional** of p and q is "p if, and only if, q" and is denoted $p \leftrightarrow q$. It is true if both p and q have the same truth values and is false if p and q have opposite truth values. The words *if and only if* are sometimes abbreviated as *iff*.

2.2.7 Necessary and Sufficient Conditions If r and s are statements, r is a sufficient condition for s means "if r then s" or $r \rightarrow s$, and "r is a necessary condition for s" means "if s then r" or $s \rightarrow r$. r is a necessary and sufficient condition for s means "r if and only if s" or $r \leftrightarrow s$.

2.3.1 Argument An **argument** (**argument form**) is a sequence of statements (statement forms). All statements in an argument (argument form), except for the final one, are called **premises** (or **assumptions** or **hypothesis**). The final statement (statement form) is called the **conclusion**. The symbol $\bullet$, which is read "therefore", is normally placed just before the conclusion. To say that an argument form is valid means that no matter what particular statements are substituted for the statement variables in its premises, if the resulting premises are all true, then the conclusion is also true.

2.3.2 Sound and Unsound Argument An argument is called **sound** if, and only if, it is valid and all its premises are true. An argument that is not sound is called **unsound**.

Quantified Statements

3.1.1 Predicate A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable.

"Domain" may also be known as "domain of discourse", "universe of discourse", "universal set", or simply "universe".

3.1.2 Truth Set If $P(x)$ is a predicate and x has a domain D, the **truth set** is the set of all elements of D that make $P(x)$ true when they are substituted for x. The truth set for $P(x)$ is denoted as $\{x \in D | P(x)\}$.

3.1.3 Universal Statement Let $Q(x)$ be a predicate and D the domain of x. A **universal statement** is a statement of the form "$\forall x \in D, Q(x)$". It is defined to be true iff $Q(x)$ is **true for every** x in D. It is defined false iff $Q(x)$ is **false for at least one** x in D. A value for x for which $Q(x)$ is false is called a **counterexample**.

3.1.4 Existential Statement Let $Q(x)$ be a predicate and D the domain of x. An **existential statement** is a statement of the form "$\exists x \in D, Q(x)$". It is defined to be true iff $Q(x)$ is **true for at least one** x in D. It is defined false iff $Q(x)$ is **false for all** x in D.

The $\exists!$ is used to denote "there exists a unique" or "there is one and only one".

3.2.1 Contrapositive, converse, inverse Consider a statement of the form: $\forall x \in D(P(x) \to Q(x))$.

1. It's **contrapositive** is: $\forall x \in D(\sim Q(x) \to \sim P(x))$.
2. It's **converse** is: $\forall x \in D(Q(x) \to P(x))$.
3. It's **inverse** is: $\forall x \in D(\sim P(x) \to \sim Q(x))$.

3.2.2 Necessary and Sufficient conditions, Only if "$\forall x, r(x)$ is a **sufficient condition** for $s(x)$" means $\forall x(r(x) \to s(x))$.

"$\forall x, r(x)$ is a **necessary condition** for $s(x)$" means $\forall x(\sim r(x) \to \sim s(x))$ or equivalently, "$\forall x(s(x) \to r(x))$".

"$\forall x, r(x)$ **only if** $s(x)$" means $\forall x(\sim s(x) \to \sim r(x))$ or equivalently, "$\forall x(r(x) \to s(x))$".

Universal Modus Ponens $\forall x(P(x) \to Q(x))$. $P(a)$ for a particular a. $\bullet\ Q(a)$.

Universal Modus Tollens $\forall x(P(x) \to Q(x))$. $\sim Q(a)$ for a particular a. $\bullet\ \sim P(a)$.

3.4.1 Valid Argument Form To say that **an argument form is valid** means the following: No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true. An argument is called **valid** if, and only if, its form is valid.

Converse Error (Quantified Form) $\forall x(P(x) \to Q(x))$. $Q(a)$ for a particular a. $\bullet\ P(a)$.

Inverse Error (Quantified Form) $\forall x(P(x) \to Q(x))$. $\sim P(a)$ for a particular a. $\bullet\ \sim Q(a)$.

Universal Transitivity $\forall x(P(x) \to Q(x))$. $\forall x(Q(x) \to R(x))$. $\bullet\ \forall x(P(x) \to R(x))$.

Additional Notes (from Tutorial 2)

Equivalent expressions: $\forall x \in D, P(X) \equiv \forall x((x \in D) \wedge P(X))$.

Well-formed formulas (wff): **true** and **false** are wffs. A propositional variable (e.g. x, p) is a wff. A predicate name followed by a list of variables (e.g. $P(x), Q(x, y)$), which is called an *atomic formula*, is a wff. If A, B and C are wffs, then so are $\sim A$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ and $(A \leftrightarrow B)$. If x is a propositional variable and A is a wff, then so are $\forall x A$ and $\exists x A$.

Scope of quantifiers / bound variables / use of parentheses:

The *scope* of a quantifier is the range in the formula where the quantifier "engages in". It is put right after the quantifier and is usually in parentheses.

Example: $\forall x\ \exists y\ P(x, y)$ - both x and y are bound. However,

$\forall x(\exists y\ P(x, y) \vee Q(x, y))$ - in $Q(x, y)$, x is bound but y is free as the $\exists y$ quantifier applies only to $P(x, y)$.

If you want the y in $Q(x, y)$ to be bound as well, you have to put parentheses over the entire formula, i.e. $\exists y(P(x, y) \vee Q(x, y))$, in which case you can just remove the outermost parentheses and it just becomes $\forall x\ \exists y(P(x, y) \vee Q(x, y))$.

Tip for negating quantified statements: if you need to negate nested quantifiers, just flip each of the quantifier symbols ($\forall$ to $\exists$ and vice versa) and apply the negation to the inner predicate, then apply De Morgan's laws from there

Sets

Set-Roster Notation A set may be specified by writing all of its elements between braces. Examples: {1, 2, 3}, {1, 2, 3, ..., 100}, {1, 2, 3, ...}. (The symbol ... is called an ellipsis and is read "and so forth".)

Membership of a Set (Notation: $\in$) If S is a set, the notation $x \in S$ means that s is an element of S. ($x \notin S$ means x is not an element of S.)

Cardinality of a Set (Notation: $|S|$) The cardinality of a set S, denoted as $|S|$, is the size of the set, that is, the number of elements in S.

Set Builder Notation Let U be a set and $P(x)$ be a predicate over U. Then the set of all elements $x \in U$ such that $P(x)$ is true is denoted as $\{x \in U : P(x)\}$ or $\{x \in U | P(x)\}$ which reads as "the set of all x in U such that $P(x)$ is true".

Replacement Notation Let A be a set and $t(x)$ be a term in a variable x. Then the set of all objects of the form $t(x)$ where x ranges over the elements of A is denoted $\{t(x) : x \in A\}$ or $\{t(x) | x \in A\}$ which is read as "the set of all $t(x)$" where $x \in A$.

Subset and superset Let A and B be sets. A is a **subset** of B, written $A \subseteq B$, iff every element of A is also an element of B. Symbolically, $A \subseteq B$ iff $\forall x(x \in A \Rightarrow x \in B)$. Another way of saying "A is a subset of B" is "A is contained in B". If $A \subseteq B$, we may also write $B \supseteq A$ which reads as "B is contained in A" or "B includes A" or "B is a superset of A".

Proper Subset Let A and B be sets. A is a **proper subset** of B, denoted $A \subset B$, iff $A \subseteq B$ and $A \neq B$. In this case, we may say that the inclusion of A in B is proper or strict.

Ordered Pair An **ordered pair** is an expression of the form (x, y). Two ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$. Symbolically, $(a, b) = (c, d) \Rightarrow (a = c) \wedge (b = d)$.

Cartesian Product Given sets A and B, the **Cartesian product** of A and B, denoted $\mathbf{A \times B}$ and read "A cross B", is the set of all ordered pairs (a, b) where a is in A and b is in B. Symbolically, $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

Set Equality Given sets A and B, A equals B, written $A = B$ iff every element of A is in B and every element of B is in A. Symbolically, $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$. (Alternative definition: $A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$).

Universal set / Universe of Discourse The context or domain of the problem.

Union The **union** of A and B, denoted $\mathbf{A \cup B}$, is the set of all elements that are in at least one of A or B. Symbolically, $A \cup B = \{x \in U : x \in A \vee x \in B\}$.

Intersection The **intersection** of A and B, denoted $\mathbf{A \cap B}$, is the set of all elements that are common to both A and B. Symbolically, $A \cap B = \{x \in U : x \in A \wedge x \in B\}$.

Difference The **difference** of B minus A (or **relative complement** of A in B), denoted $\mathbf{B - A}$, or $\mathbf{B \setminus A}$, is the set of all elements that are in B and not A. Symbolically, $B \setminus A = \{x \in U : x \in B \wedge x \notin A\}$.

Complement The complement of A, denoted $\overline{A}$, is the set of all elements in U that are not in A. Symbolically, $\overline{A} = \{x \in U \mid x \notin A\}$.

Unions and Intersections of an Indexed Collection of Sets Given sets A_0, A_1, A_2... that are subsets of a universal set U and a given nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i\}$$

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for all } i = 0, 1, 2, \ldots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all nonnegative integers } i\}$$

Disjoint Two sets are **disjoint** iff they have no elements in common. Symbolically: A and B are disjoint iff $A \cap B = \emptyset$.

Mutually disjoint Sets $A1, A2, A3 \ldots$ are **mutually disjoint** (or **pairwise disjoint** or **nonoverlapping**) iff no two sets A_i and A_j with distinct subscripts have any elements in common, i.e. for all $i, j = 1, 2, 3, \ldots$ $A_i \cap A_j = \emptyset$ wherever $i \neq j$.

Power Set Given a set A, the **power set** of A, denoted $P(A)$, is the set of all subsets of A. (symbol for power set is $\wp$)

Ordered n-tuples Let $n \in \mathbb{Z}^+$ and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elements. An **ordered n-tuple** is an expression of the form $(x_1, x_2, \ldots, x_n)$. Equality of two ordered n-tuples: $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \Leftrightarrow x_1 = y_1, x_2 = y_2, \ldots x_n = y_n$.

Cartesian product Given sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $x_1, x_2, \ldots, x_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$.

$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$. If A is a set, then $A^n = A \times A \times \cdots \times A$.

Procedural Versions of Set Definitions Let X and Y be subsets of a universal set U and suppose a and b are elements of U.

1. $a \in X \cup Y \Leftrightarrow a \in X \vee a \in Y$.
2. $a \in X \cap Y \Leftrightarrow a \in X \wedge a \in Y$.
3. $a \in X - Y \Leftrightarrow a \in X \wedge a \notin Y$.
4. $a \in \overline{X} \Leftrightarrow a \notin X$.
5. $(a, b) \in X \times Y \Leftrightarrow a \in X \wedge b \in Y$.

Note: In a context where where U is the universal set (so that implicitly means $U \supseteq X$), the complement of X, denoted $\overline{X}$ or X^c, is defined by $\overline{X} = U \setminus X$.

Relations

Relation Let A and B be sets. A (binary) **relation from A to B** is a subset of $\mathbf{A} \times \mathbf{B}$. Given an ordered pair (x, y) in $A \times B$, **x is related to y** by **R**, or **x is related to y**, written **x R y**, iff $(\mathbf{x}, \mathbf{y}) \in \mathbf{R}$.

Domain, Co-Domain, Range Let A and B be sets and R be a relation from A to B. The **domain of** R, $Dom(R)$, is the set $\{a \in A : a\ R\ b \text{ for some } b \in B\}$. The **co-domain** of R, $coDom(R)$, is the set B. The **range** of R, $Range(R)$, is the set $\{b \in B : a\ R\ b \text{ for some } a \in A\}$.

Inverse of a Relation Let R be a relation from A to B. Define the **inverse relation** R^{-1} from B to A as follows: $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$.

Relation on a Set A **relation on a set** A is a relation from A to A. In other words, a relation on set A is a subset of $A \times A$. (The arrow diagram can be modified such that it becomes a **directed graph**).

Composition of Relations Let A, B and C be sets. Let $R \subseteq A \times B$ be a relation. Let $S \subseteq B \times C$ be a relation. The **composition of** R **with** S, denoted $S \circ R$, is the relation from A to C such that: $\forall x \in A, \forall z \in C(x\ S \circ R\ z \Leftrightarrow (\exists y \in B(x\ R\ y \wedge y\ S\ z)))$.

Proposition: Composition is Associative (Lecture 6 Slide 18) Let A, B, C, D be sets. Let $R \subseteq A \times B$, $S \subseteq B \times C$ and $T \subseteq C \times D$ be relations. $T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$.

Proposition: Inverse of Composition (Lecture 6 Slide 18) Let A, B and C be sets. Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations. Then $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

n-ary Relation Given n sets $A_1, A_2, \ldots, A_n$, an **n-ary relation** R on $A_1 \times A_2 \times \ldots, A_n$ is a subset of $A_1 \times A_2 \times \ldots \times A_n$. The special cases of 2-ary, 3-ary, and 4-ary relations are called **binary**, **ternary** and **quaternary relations** respectively.

Reflexivity, Symmetry, Transitivity Let R be a relation on a set A.

1. R is **reflexive** iff $\forall x \in A(xRx)$.
2. R is **symmetric** iff $\forall x, y \in A(xRy \rightarrow yRx)$.
3. R is **transitive** iff $\forall x, y, z \in A(xRy \wedge yRz \rightarrow xRz)$.

Note: for transitivity, if either of the premises are false, R is transitive as the argument is vacuously true. Reflexivity, symmetry and transitivity are **properties of a relation**, not properties of members of the set. You say that a relation is reflexive or not reflexive, while an element is related or not related to itself.

Transitive Closure Let A be a set and R a relation on A. The transitive closure of R is the relation R^t on A that satisfies the following three properties:

1. R^t is transitive.
2. $R \subseteq R^t$.
3. If S is any other transitive relation that contains R then $R^t \subseteq S$.

Reflexive Closure (Tutorial 5 Q5) The reflexive closure S of a relation R on a set A is obtained by adding (a, a) to R for each $a \in A$. Symbolically, $S = R \cup \{(x, x) : x \in X\}$.

Partition $\mathcal{C}$ is a **partition** of a set A if the following hold:

1. $\mathcal{C}$ is a set of which all elements are non-empty subsets of A, i.e., $\emptyset \neq S \subseteq A$ for all $S \in \mathcal{C}$.
2. Every element of A is in exactly one element of $\mathcal{C}$, i.e., $\forall x \in A \exists S \in \mathcal{C}(x \in S)$ and $\forall x \in A \exists S_1, S_2, \in \mathcal{C}(x \in S_1 \wedge x \in S_2 \rightarrow S_1 = S_2)$.

(In simpler terms: $\mathcal{C}$ is a partition of set A if $\mathcal{C}$ is a set of all elements which are nonempty subsets of A, and every element of A is in exactly one component of $\mathcal{C}$).

Elements of a partition are called **components** of the partition.

Partition (shorter definition) A **partition** of set A is a set $\mathcal{C}$ of non-empty subsets of A such that $\forall x \in A \; \exists! \; S \in \mathcal{C}(x \in S)$.

Relation Induced by a Partition Given a partition $\mathcal{C}$ of a set A, the relation R **induced by the partition** is defined on A as follows: $\forall x, y \in A$, $xRy \Leftrightarrow \exists$ a component S of $\mathcal{C}$ s.t. $x, y \in S$.

Equivalence Relation Let A be a set and R a relation on A. R is an **equivalence relation** iff R is reflexive, symmetric and transitive. Note: the symbol $\sim$ is commonly used to denote an equivalence relation.

Equivalence Class Suppose A is a set and $\sim$ is an equivalence relation on A. For each $a \in A$, the **equivalence class** of a, denoted $[a]$ and called the **class of a** for short, is the set of all elements $x \in A$ s.t. a is $\sim$-related to x. Symbolically, $[a]_\sim = \{x \in A : a \sim x\}$. The procedural definition is: $\forall x \in A(x \in [a]_\sim \Leftrightarrow a \sim x)$.

Proof (Tutorial 4 Q9(a)): If $x \in S \in \mathcal{C}$, then $[x] = S$. (If x is an element of a component S which is an element of a partition, then the equivalence class of x is S.)

Tip: think of classes as "school buses" - two students are in the same equivalence class if they are in the same "school bus".

Congruence Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $a - b = nk$ for some $k \in Z$. In other words, $n|(a - b)$. In this case, we write $a \equiv b \pmod{n}$.

Proposition (Lecture 6 Slide 54) Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$.

Set of equivalence classes Let A be a set and $\sim$ be an equivalence relation on A. Denote by $A/\sim$ the set of all equivalence classes with respect to $\sim$, i.e., $A/\sim = \{x_\sim : x \in A\}$. We may read $A/\sim$ as "the quotient of A by $\sim$".

Proof (Tutorial 4 Q9(b)): $A/\sim = \mathcal{C}$ (The set of equivalence classes of A is a partition of A.)

Antisymmetry Let R be a relation on a set A. R is **antisymmetric** iff $\forall x, y \in A(x \; R \; y \wedge y \; R \; x \rightarrow x = y)$.

Asymmetry (Tutorial 5 Q6) Let R be a binary relation on a set A. R is **asymmetric** iff $\forall x, y \in A(x \; R \; y \rightarrow y \not R \; x)$.

Tutorial 5 Q6(c) All asymmetric relations are antisymmetric.

Partial Order Relations Let R be a relation on a set A. Then R is a **partial order relation** (or simply **partial order**) iff R is reflexive, antisymmetric and transitive.

Note: the symbol $\preceq$ is often used to refer to a general partial order, and the notation $x \preceq y$ is read as "x is curly less than or equal to y".

Proof (Tutorial 5 Q3): Binary relation $\subseteq$ on $P(A)$ is a partial order.

Partially Ordered Sets A set A is called a **partially ordered set** (or **poset**) with respect to a partial order relation R on A, denoted by (A, R).

Hasse Diagram Let $\preceq$ be a partial order on a set A. A **Hasse diagram** of $\preceq$ satisfies the following condition for all distinct $x, y, m \in A$: If $x \preceq y$ and no $m \in A$ is such that $x \preceq m \preceq y$, then x is placed below y with a line joining them, else no line joins x and y.

(Tip: to obtain a Hasse Diagram, start with a directed graph of the relation, placing vertices on the page so that all arrows point upwards. Then **eliminate** 1. the loops at all the vertices, 2. all arrows whose existence is implied by the transitive property, and 3. the direction indicators on the arrows.)

Comparability Suppose $\preceq$ is a partial order relation on a set A. Elements a and b of A are said to be **comparable** iff either $a \preceq b$ or $b \preceq a$. Otherwise, a and b are **noncomparable**.

Compatible (Tutorial 5 Q7) Elements a, b are **compatible** iff there exists $c \in A$ such that $a \preceq c$ and $b \preceq c$.

Maximal/Minimal/Largest/Smallest Element

1. c is a **maximal element** of A iff $\forall x \in A$, either $x \preceq c$, or x and c are not comparable. Alternatively, c is a maximal element of A iff $\forall x \in A(c \preceq x \rightarrow c = x)$.
2. c is a **minimal element** of A iff $\forall x \in A$, either $c \preceq x$, or x and c are not comparable. Alternatively, c is a minimal element of A iff $\forall x \in A(x \preceq c \rightarrow c = x)$.
3. c is the **largest element** of A iff $\forall x \in A(x \preceq c)$.
4. c is the **smallest element** of A iff $\forall x \in A(c \preceq x)$.

Note: Alternative terms: Largest element = greatest element = maximum; smallest element = least element = minimum.

Proposition (Lecture 6 Slide 83) Consider a partial order $\preceq$ on a set A. Any smallest element is minimal. (Likewise, any largest element is maximal.)

Total Order Relations If R is a partial order relation on a set A, and for any two elements x and y in A, either xRy or yRx, then R is a **total order relation** (or simply **total order**) on A. In other words, R is a total order iff R is a partial order and $\forall x, y \in A(xRy \vee yRx)$.

Linearization of a partial order Let $\preceq$ be a partial order on a set A. A **linearization** of $\preceq$ is a total order $\preceq^*$ on A such that $\forall x, y \in A(x \preceq y \rightarrow x \preceq^* y)$.

Well-Ordered Set Let $\preceq$ be a total order on a set A. A is **well-ordered** iff every non-empty subset of A contains a smallest element. Symbolically, $\forall S \in P(A), S \neq 0 \rightarrow (\exists x \in S\ \forall y \in S(x \preceq y))$.

Tutorial 5 Discussion Q1 Let R be a binary relation on a non-empty set A. If $R = \emptyset$, then R is not reflexive, but it is symmetric and transitive (vacuously true).

Functions

Function A function f from a set X to a set Y, denoted $f : X \rightarrow Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X\ \exists y \in Y(x, y) \in f$

(F2) $\forall x \in X\ \forall y_1, y_2 \in Y(((x, y_1) \in f \wedge (x, y_2) \in f) \rightarrow y_1 = y_2)$

(F3) $\forall x_1, x_2 \in X(x_1 = x_2 \rightarrow f(x_1) = f(x_2))$

Function (alternative definition) Let f be a relation on sets X and Y, i.e. $f \subseteq X \times Y$. Then f is a function from X to Y, denoted $f : X \rightarrow Y$, iff $\forall x \in X\ \exists!\ y \in Y(x, y) \in f$. Informally, a function from X and Y is an assignment of each element of X to **exactly one element** of Y.

Another view of function Let $f : X \rightarrow Y$ be the type signature of function. $\forall x \in X\ \exists y \in Y, \{y\} = \{b \mid (x, b) \in f\}$.

Argument, image, preimage, input, output Let $f : X \to Y$ be a function. We write $f(x) = y$ iff $(x, y) \in f$. We say that "f sends/maps x to y" and we may also write $x \to y$ or $f : x \longmapsto y$. Also, x is called the **argument** of f. $f(x)$ is read "f of x" or "the **output** of f for the **input** x", or "the value of f at x", or "the **image** of x under f". If $f(x) = y$, then x is a **preimage** of y.

Setwise image and preimage Let $f : X \to Y$ be a function from set X and set Y and $f : P(X) \to P(Y)$

- If $A \subseteq X$, then let $f(A) = \{f(x) : x \in A\}$.
- If $B \subseteq Y$, then let $f^{-1}(B) = \{x \in X : f(X) \in B\}$.

We call $f(A)$ the **(setwise) image** of A, and $f^{-1}(B)$ the **(setwise) preimage** of B under f.

Domain, Co-domain, Range Let $f : X \to Y$ be a function from set A to set B.

- A is the **domain** of f and B the **co-domain** of f.
- The **range** of f is the (setwise) image of A under f: $\{b \in B : b = f(x) \text{ for some } a \in A\}$.

Sequence (of infinite length) A sequence $a_0, a_1, a_2 \dots$ can be represented by a function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$.

Fibonacci Sequence The **Fibonacci Sequence** $F_0, F_1, F_2, \dots$ is defined by setting, for each $n \in \mathbb{Z}_{\geq 0}, F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$.

String (of finite length) Let A be a set. A **string** or word over A is an expression of the form $a_0a_1a_2 \dots a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$ and $a_0a_1a_2 \dots a_{l-1} \in A$. Here l is called the **length** of the string. The **empty string** ε is the string of length 0.

Equality of Sequences Given two sequences $a_0, a_1, a_2, \dots$ and $b_0, b_1, b_2, \dots$ defined by the functions $a(n) = a_n$ and $b(n) = b_n$ respectively for every $n \in \mathbb{Z}_{\geq 0}$, we say that the two sequences are equal if and only if $a(n) = b(n)$ for every $n \in \mathbb{Z}_{\geq 0}$.

Equality of Strings Given two strings $s_1 = a_0a_1a_2 \dots a_{l-1}$ and $s_2 = b_0b_1b_2 \dots b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, we say that $s_1 = s_2$ if and only if $a_i = b_i$ for all $i \in \{0, 1, 2, \dots, l-1\}$.

Injection (one-to-one function) A function $f : X \to Y$ is **injective** (or **one-to-one**) iff $\forall x_1, x_2 \in X(f(x_1) = f(x_2) \to x_1 = x_2)$, or equivalently (contrapositive), $x_1 \neq x_2 \to f(x_1) \neq f(x_2)$. An injective function is called an **injection**. Informally, every element in the codomain must have **at most one arrow** going into it.

Surjective (onto function) A function $f : X \to Y$ is **surjective** (or **onto**) iff $\forall y \in Y \ \exists x \in X(y = f(x))$. Every element in the co-domain has at least one preimage. So, range = co-domain. A surjective function is called a **surjection**. Informally, every element in the codomain must have **at least one arrow** going into it.

Bijection (one-to-one correspondence) A function $f : X \to Y$ is **bijective** iff f is injective and surjective, i.e. $\forall y \in Y \ \exists x \in X(y = f(x))$. A bijective function is called a **bijection** or **one-to-one correspondence**. Informally, every element in the codomain must have **exactly one arrow** going into it.

Inverse Function Let $f : X \to Y$. Then $g : Y \to X$ is an **inverse** of f iff $\forall x \in X \ \forall y \in Y(y = f(x) \Leftrightarrow x = g(y))$.

Proposition (Lecture 7 Slide 39) If g_1 and g_2 are inverses of $f : X \to Y$, then $g_1 = g_2$.

Composition of Functions Let $f : X \to Y$ and $g : Y \to Z$ be functions. Define a new function $g \circ f : X \to Z$ as follows: $(g \circ f)(x) = g(f(x)) \ \forall x \in X$, where $g \circ f$ is read "g circle f" and $g(f(x))$ is read "g of f of x". The function $g \circ f$ is called the **composition** of f and g.

Addition and Multiplication on $\mathbb{Z}_n$ Define addition $+$ and multiplication $\cdot$ on $\mathbb{Z}_n$ as follows: whenever $[x], [y] \in \mathbb{Z}_n$, $[x]+[y] = [x + y]$ and $[x] \cdot [y] = [x \cdot y]$.

Proposition: Addition on $\mathbb{Z}_n$ is well defined (Lecture 7 Slide 63) For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n, ([x_1], [y_1]) = ([x_2], [y_2]) \to [x_1] + [y_1] = [x_2] + [y_2]$.

General Well-Defined Function Property $\forall x_1, x_2 \in X, \ \forall f : X \to Y, x_1 = x_2 \to f(x_1) = f(x_2)$.

Well-Defined Property w.r.t Equiv Relation $\sim$ $\forall x_1, x_2 \in X, \ \forall f : X \to Y, x_1 \sim x_2 \to f(x_1) \sim f(x_2)$.

Well-Defined Property w.r.t Equiv Class [x] $\forall x_1, x_2 \in X, \ \forall f : X \to Y, [x_1] = [x_2] \to [f(x_1)] = [f(x_2)]$.

Mathematical Induction

Sequences and Terms A **sequence** is an ordered set with members called **terms**. Usually, the terms are numbers. A sequence may have infinite terms. General form: $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$ where $m \leq n$. The k in a_k is called a **subscript** or **index**. Infinite sequence: $a_m, a_{m+1}, a_{m+2}, \ldots$.

An **explicit** formula for a sequence is a rule that shows how the values of a_k depend on k. E.g. $a_k = \frac{k}{k+1}$ for all integers $k \geq 1$. $a_1.a_2.a_3 \ldots$ Dots are element separators.

Sequence Comprehension

$\{f(k) : k \in S\} : P(B) \quad f : S \to B$	Order not important, duplicates discarded
$[f(k) : k \in [n..m]\ ] : Seq(B) \quad f : Z \to B$	Order important, duplicates are kept
$[f(k) : k \in [n..]\ ] : Seq(B)$	Infinite sequences

Summation If m and n are integers, $m \leq n$, the symbol

$$\sum_{k=m}^{n} a_k$$

is the **sum** of all the terms $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$ (a.k.a summation notation). We say that $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ is the **expanded** form of the sum, and we write $\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$. We call k the **index** of the summation, m the **lower limit** of the summation and n the **upper limit** of the summation.

Recursive definition of summation: If m is any integer, then

$$\sum_{k=m}^{m} a_k = a_m \text{ and } \sum_{k=m}^{n} a_k = (\sum_{k=m}^{n-1} a_k) + a_n$$

By convention, an **empty** sum (e.g. $\sum_{k=m}^{n} a_k$ where $m > n$) is equal to the additive identity **0**.

Telescoping sums are finite sums in which pairs of consecutive terms **cancel each other out**, leaving only the **initial** and **final terms**. E.g. $\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$. (Note that $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$)

Product Notation If m and n are integers, $m \leq n$, the symbol

$$\prod_{k=m}^{n} a_k$$

is the **product** of all the terms $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$. We write $\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \cdots \cdot a_n$.

Recursive definition for product notation: If m is any integer, then

$$\prod_{k=m}^{m} a_k = a_m \text{ and } \prod_{k=m}^{n} a_k = (\prod_{k=m}^{n-1} a_k) \cdot a_n$$

Arithmetic Sequence A sequence $a_0, a_1, a_2, \ldots$ is called an **arithmetic sequence** (or **arithmetic progression**) iff there is a constant d such that $a_k = a_{k-1} + d$ for all integers $k \geq 1$. It follows that $a_n = a_0 + dn$ for all integers $n \geq 0$. d is the **common difference**, a_0 is the **initial value**.

Summing an arithmetic sequence of n terms:

$$\sum_{k=0}^{n-1} a_k = \frac{n}{2}(2a_0 + (n-1)d)$$

Geometric Sequence A sequence $a_0, a_1, a_2, \ldots$ is called a **geometric sequence** (or **geometric progression**) iff there is a constant r such that $a_k = ra_{k-1}$ for all integers $k \geq 1$. It follows that $a_n = a_0 r^n$ for all integers $n \geq 0$. r is the **common ratio**, a_0 is the **initial value**.

Summing a geometric sequence of n terms:

$$\sum_{k=0}^{n-1} a_k = a_0(\frac{1-r^n}{1-r})$$

Principal of Mathematical Induction (PMI) Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following 2 statements are true:

1. (basis step) $P(a)$ is true.
2. (inductive step) For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement "for all integers $n \geq a, P(n)$" is true.

Note: the basis step need not be $P(1)$; it can be $P(a)$ where a is a fixed integer.

Closed Form If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis (...) or a summation symbol ($\sum$), we say that it is written in **closed form**.

Well-Ordering Principle for the Integers Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Well-Ordering Principle for Non-Negative Integers Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Take note that the well-ordering principle applies only to **integers** and **non-empty subsets**. That means it does not apply for (and is not violated by) **real numbers** or **non-empty sets**.

Recurrence Relation A **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$, where i is an integer with $k - i \geq 0$. If i is a fixed integer, the **initial conditions** for such a recurrent relation specify the values of $a_0, a_1, a_2, \ldots, a_{i-1}$. If i depends on k, the initial conditions specify the values of $a_0, a_1, a_2, \ldots, a_m$, where m is an integer with $m \geq 0$.

Recursive definition of Fibonacci: $F_n = F_{n-1} + F_{n-2}$ for $n > 1$.

Recursive defintion of factorial: $n! = n \cdot (n-1)!$ for $n \geq 1$.

Recursive definition of power: $a^n = a^{n-1} \cdot a$ for $n \geq 1$.

Recursively Defined Sets Let S be a finite set with at least one element. A **string over** S is a finite sequence of elements from S. The elements of S are called **characters** of the string, and the **length** of a string is the number of characters it contains. The **null string over** S is defined to be the "string" with no characters. It is usually denoted ϵ and is said to have length 0.

$S = \{c_1, \ldots, c_n\}$

$Str(S) ::= \epsilon \mid c.Str(S)$ s.t. $c \in S$

Recursive Definition of a set S

Base clause:	Specify that certain elements, called **founders**, are in S: if c is a founder, then $c \in S$.
Recursion clause:	Specify certain functions, called **constructors**, under which the set S is closed: if f is a constructor and $x \in S$, then $f(x) \in S$.
Minimality Clause:	Membership for S can always be demonstrated by (infinitely many) successive applications of the clauses above.

Structural Induction over S To prove that $\forall x \in S\ P(x)$ is true, where $P(x)$ is a proposition, it suffices to:

Base clause:	Show that $P(c)$ is true for every founder c; and
Induction step:	Show that $\forall x \in S(P(x) \rightarrow P(f(x)))$ is true for every constructor f. In words, if all the founders satisfy a property P, and P is preserved by all constructors, then all elements of S satisfy P.

Induction vs Co-Induction Inductive proofs are proof based on how data are *constructed*. Co-inductive proofs are proofs based on how data are *decomposed*. Think: A property holds by *induction* if there is **good reason** for it to hold. A property holds by *co-induction* if there is **no good reason** for it not to hold.

Theorems, Lemmas & Corollaries

Theorem 2.1.1 Logical Equivalences Given any statement variables p, q and r, a tautology is **true** and a contradiction is **false**:

1	Commutative Laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2	Associative Laws	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$
3	Distributive Laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4	Identity Laws	$p \wedge \mathbf{true} \equiv p$	$p \vee \mathbf{false} \equiv p$
5	Negation Laws	$p \vee \sim p \equiv \mathbf{true}$	$p \wedge \sim p \equiv \mathbf{false}$
6	Double Negation Law	$\sim(\sim p) \equiv p$	
7	Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
8	Universal bound laws	$p \vee \mathbf{true} \equiv \mathbf{true}$	$p \wedge \mathbf{false} \equiv \mathbf{false}$
9	De Morgan's laws	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10	Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11	Negation of **true** and **false**	$\sim\mathbf{true} \equiv \mathbf{false}$	$\sim\mathbf{false} \equiv \mathbf{true}$

Implication Law $p \to q \equiv \sim p \vee q$

Table 2.3.1 Rules of Inference (Quote the rules if you use them in proofs)

Rule of Inference		Rule of Inference	
Modus Ponens	$p \to q \quad p \quad \bullet$q	Elimination	$p \vee q \quad \sim q \quad \bullet p$
Modus Tollens	$p \to q \quad \sim q \quad \bullet \sim p$	Transitivity	$p \to q \quad q \to r \quad \bullet p \to r$
Generalization	$p \quad \bullet p \vee q$	Proof by Division into Cases	$p \vee q \quad p \to r \quad q \to r \quad \bullet r$
Specialization	$p \wedge q \quad \bullet p$	Contradiction Rule	$\sim p \to \mathbf{false} \quad \bullet p$
Conjuction	$p \quad q \quad \bullet p \wedge q$		

Theorem 3.2.1 Negation of Universal Statement The **negation** of a statement of the form $\forall x \in D, P(x)$ is logically equivalent to a statement of the form $\exists x \in D$ such that $\sim P(x)$. Symbolically, $\sim(\forall x \in D, P(x)) \equiv \exists x \in D$ such that $\sim P(x)$.

Theorem 3.2.2 Negation of an Existential Statement The **negation** of a statement of the form $\exists x \in D, P(x)$ is logically equivalent to a statement of the form $\forall x \in D$ such that $\sim P(x)$. Symbolically, $\sim(\exists x \in D, P(x)) \equiv \forall x \in D$ such that $\sim P(x)$.

Rules of Inference (Quantified Statements)

Rule of Inference	Name
$\forall x \in DP(x) \quad \therefore P(a)$ if $a \in D$	Universal instantiation
$P(a)$ for every $a \in D \quad \therefore \forall x \in DP(x)$	Universal generalization
$\exists x \in DP(x) \quad \therefore P(a)$ for some $a \in D$	Existential instantiation
$P(a)$ for some $a \in D \quad \therefore \exists x \in DP(x)$	Existential generalization

Theorem 4.2.1 (5th: 4.3.1) Every integer is a rational number.

Theorem 4.2.2 (5th: 4.3.2) The sum of any two rational numbers is rational.

Corollary 4.2.3 (5th: 4.2.3) The double of a rational number is rational.

Theorem 4.3.1 (5th: 4.4.1) A Positive Divisor of a Positive Integer: For all positive integers a and b, if $a|b$, then $a \leq b$.

Theorem 4.3.2 (5th: 4.4.2) Divisors of 1: The only divisors of 1 are 1 and -1.

Theorem 4.3.3 (5th: 4.4.3) Transitivity of Divisibility: For all integers a, b and c, if $a|b$ and $b|c$, then $a|c$.

Theorem 4.4.1 The Quotient-Remainder Theorem Given any integer n and a positive integer d, there exists unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.

Theorem 4.6.1 (5th: 4.7.1) There is no greatest integer.

Theorem 4.6.4 (5th: 4.7.4) For all integers n, if n^2 is even then n is even.

Proof (Tutorial 1 Q10) The product of any two odd integers is an odd integer.

Proof (Tutorial 1 Q11) n^2 is odd if and only if n is odd.

Proof (Tutorial 2 Q4(a)) Integers are not closed under division.

Proof (Tutorial 2 Q4(b)) Rational numbers are closed under addition.

Proof (Tutorial 2 Q4(c)) Rational numbers are not closed under division.

Proof (Tutorial 2 Q8) $\forall x \in \mathbb{R}((x^2 > x) \to (x < 0) \vee (x > 1))$.

Proof (Tutorial 2 Q11) If n is a product of two positive integers a and b, then $a \leq n^{1/2}$ or $b \leq n^{1/2}$.

Theorem 4.7.1 (5th: 4.8.1) $\sqrt{2}$ is irrational.

Theorem 5.1.1 If $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ are sequences of real numbers and c is any real number, then the following equations hold for any integer $n \geq m$:

1. $\displaystyle\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$
2. $\displaystyle c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$
3. $\displaystyle (\prod_{k=m}^{n} a_k) \cdot (\prod_{k=m}^{n} b_k) = (\prod_{k=m}^{n} (a_k \cdot b_k))$

Theorem 5.2.2 (5th: 5.2.1) Sum of first n Integers For all integers $n \geq 1$, $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$.

Theorem 5.2.3 (5th: 5.2.2) Sum of a Geometric Sequence For any real number $r \neq 1$, and any integers $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Proposition 5.3.1 (5th: 5.3.2) For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proposition 5.3.2 (5th: 5.3.3) For all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof (Lecture 8 Slide 39) For $n \in \mathbb{Z}^+$, any $2^n \times 2^n$ board with one square removed can be tiled by L-trominoes.

Proof (Lecture 8 Slide 45) Any integer > 1 is divisible by a prime number.

Theorem 6.2.1 Subset Relations

1. **Inclusion of Intersection:** For all sets A and B, (a) $A \cap B \subseteq A$ (b) $A \cap B \subseteq B$.
2. **Inclusion in Union:** For all sets A and B, (a) $A \subseteq A \cup B$ (b) $B \subseteq A \cup B$.
3. **Transitive Property Of Subsets:** For all sets A, B and C, $A \subseteq B \wedge B \subseteq C \to A \subseteq C$.

Theorem 6.2.2 Set Identities Let all sets referred to below be subsets of a universal set U.

Theorem 6.2.4 An empty set is a **subset** of every set, i.e. $\emptyset \subseteq A$ for all sets A.

Note: a set with exactly one element is called a **singleton**.

Theorem: Cardinality of a Power Set of a Finite Set Let A be a finite set where $|A| = n$, then $|P(A)| = 2^n$.

Theorem 6.3.1 Suppose A is a finite set with n elements, then $P(A)$ has 2^n elements. In other words, $|P(A)| = 2^{|A|}$.

Theorem 8.3.1 Relation Induced by a Partition Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.

Lemma Rel.1 Equivalence Classes Let $\sim$ be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$.
(i)$x \sim y$ (ii) $[x] = [y]$ (iii) $[x] \cap [y] \neq \emptyset$.

1	Commutative Laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
2	Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
3	Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4	Identity Laws	$A \cup \emptyset = A$	$A \cap U = A$
5	Complement Laws	$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$
6	Double Complement Law	$\overline{\overline{A}} = A$	
7	Idempotent Laws	$A \cup A = A$	$A \cap A = A$
8	Universal Bound Laws	$A \cup U = U$	$A \cap \emptyset = \emptyset$
9	De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
10	Absorption Laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
11	Complements of U and $\emptyset$	$\overline{U} = \emptyset$	$\overline{\emptyset} = U$
12	Set Difference Law	$A \setminus B = A \cap \overline{B}$	

Theorem 8.3.4 The Partition Induced by an Equivalence Relation If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any two distinct classes is empty.

Theorem Rel.2 Equivalence classes form a partition Let $\sim$ be an equivalence relation on a set A. Then $A/\sim$ is a partition of A.

Theorem 7.1.1 Function Equality Two functions $f : A \to B$ and $g : C \to D$ are equal, i.e. $f = g$, iff (i)$A = C$, and (ii) $f(x) = g(x)\ \forall x \in A$.

Theorem 7.2.3 If $f : X \to Y$ is a bijection, then $f^{-1} : Y \to X$ is also a bijection. In other words, $f : X \to Y$ is bijective iff f has an inverse.

Theorem 7.3.1 Composition with an Identity Function If f is a function from set X to set Y, and id_x is the identity function on X, and id_y is the identity function on Y, then $f \circ id_x = f$ and $id_y \circ f = f$.

Theorem 7.3.2 Composition of a Function with its Inverse If $f : X \to Y$ is a bijection with the inverse function $f^{-1} : Y \to X$, then $f^{-1} \circ f = id_x$ and $f \circ f^{-1} = id_y$.

Theorem: Associativity of Function Composition Let $f : A \to B$, $g : B \to C$ and $h : C \to D$. Then $(h \circ g) \circ f = h \circ (g \circ f)$. Function composition is associative.

Theorem 7.3.3 If $f : X \to Y$ and $g : Y \to Z$ are both injective, then $g \circ f$ is injective.

Theorem 7.3.4 If $f : X \to Y$ and $g : Y \to Z$ are both surjective, then $g \circ f$ is surjective.

Examples of Proofs (For reference)

Prove that the product of two consecutive odd numbers is always odd.

1. Let a and b be the two consecutive odd numbers.
   - 1.1 WLOG, assume that $a < b$, hence $b = a + 2$.
   - 1.2 Now, $a = 2k + 1$ for some integer k (by definition of odd numbers).
   - 1.3 Similarly, $b = a + 2 = 2k + 3$.
   - 1.4 Therefore, $ab = (2k + 1)(2k + 3) = (4k^2 + 6k) + (2k + 3) = 4k^2 + 8k + 3 = 2(2k^2 + 4k + 1) + 1$ (by basic algebra).
   - 1.5 Let $m = (2k^2 + 4k + 1)$, which is an integer (by closure of integers under $\times$ and $+$.
   - 1.6 Then $ab = 2m + 1$, which is odd (by definition of odd numbers).
2. Therefore, the product of two consecutive odd numbers is always odd.

Prove that the following statement is false: The product of two irrational numbers is always irrational.

1. Let them two irrational numbers be $\sqrt{2}$ and $\sqrt{8}$.
   - 1.1 Then $\sqrt{2} \times \sqrt{8} = \sqrt{16} = 4$, which is a rational number (by basic algebra).
2. Therefore, the statement "the product of two irrational numbers is always irrational" is false.

Note: One counter-example is sufficient.

Prove that the difference of two consecutive squares between 30 and 100 is odd. (Proof by exhaustion / brute force)

1. The squares between 30 and 100 are 36, 49, 64 and 81.
   - 1.1 Case 1: 49 – 36 = 13 which is odd.
   - 1.2 Case 2: 64 – 49 = 15 which is odd.
   - 1.3 Case 3: 81 – 64 = 17 which is odd.
2. Therefore, the difference of two consecutive squares between 30 and 100 is odd.

Prove that the difference of two consecutive squares is always odd. (Proof by deduction / direct proof)

1. Let the numbers be n and $n + 1$.
   - 1.1 $(n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1$ (by basic algebra).
   - 1.2 $2n + 1$ is odd (by definition of odd numbers).
2. Therefore, the difference of two consecutive squares is odd.

Prove Theorem 4.7.1(5th: 4.8.1) $\sqrt{2}$ is irrational. (Proof by contradiction)

Proposition 4.6.4(5th: 4.7.4) For all integers n, if n^2 is even then n is even.

1. Suppose not, that is, $\sqrt{2}$ is rational.
   - 1.1 Then $\exists a, b \in \mathbb{Z}, b \neq 0$ s.t. $\sqrt{2} = \frac{a}{b}$ (by definition of rational numbers).
   - 1.2 Convert $\frac{a}{b}$ into its lowest term $\frac{m}{n}$.
   - 1.3 $m^2 = 2n^2$ (by basic algebra).
   - 1.4 Hence m^2 is even (by definition of even number, as n^2 is an integer by closure).
   - 1.5 Hence m is even (by Proposition 4.6.4).
   - 1.6 Let $m = 2k$; substituting into 1.3: $4k^2 = 2n^2$, or $n^2 = 2k^2$.
   - 1.7 Hence n^2 is even (by definition of even number).
   - 1.8 Hence n is even (by Proposition 4.6.4).
   - 1.9 So both m and n are even, but this contradicts that $\frac{m}{n}$ is in its lowest term.
2. Therefore, the assumption that $\sqrt{2}$ is rational is false.
3. Hence $\sqrt{2}$ is irrational.

Note: To prove a statement S by contradiction, you first assume that $\sim S$ is true. Based on this, you use known facts and theorems to arrive at a logical contradiction. Since every step of your argument thus far is logically correct, the problem must lie in your initial assumption (that $\sim S$ is true). Thus you conclude that $\sim S$ is false, that is, S is true.

Prove that there exist irrational numbers p and q such that p^q is rational.

1. From Theorem 4.7.1, $\sqrt{2}$ is irrational.
2. Consider $\sqrt{2}^{\sqrt{2}}$. It is either rational or irrational.
3. Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational.
   - 3.1 Let $p = q = \sqrt{2}$, and we are done.
4. Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.
   - 4.1 Let $p = \sqrt{2}^{\sqrt{2}}$, and $q = \sqrt{2}$.
   - 4.2 Now p is irrational (by assumption), so is q (by Theorem 4.7.1).
   - 4.3 Consider $p^q = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\times\sqrt{2}} = (\sqrt{2})^2 = 2$ (by basic algebra).
   - 4.4 Clearly 2 is rational.
5. In either case, we have found the required p and q.

Mathematical Induction Proofs

Prove that the sum of the first n integers is $\frac{n(n+1)}{2}$

1. Let $P(n) \equiv (1 + 2 + \cdots + n = \frac{n(n+1)}{2})$, $\forall n \in \mathbb{Z}^+$.
2. **Basis step**: $1 = \frac{1(1+1)}{2}$, therefore $P(1)$ is true.
3. Assume $P(k)$ is true for some $k \geq 1$. That is, $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$
4. **Inductive Step**: (to show $P(k+1)$ is true)
   - 4.1 $1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)((k+1)+1)}{2}$
   - 4.2 Therefore $P(k+1)$ is true.
5. Therefore, $P(n)$ is true for $n \in \mathbb{Z}^+$.