CS1231S Notes

Tang Zhi Xiang

AY24/25 - Sem 1 (Prof Aaron)

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 $(b+c)a=ba+ca$

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

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 $a.(\frac{1}{a})=(\frac{1}{a}).a=1$

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

T7. Cancellation Law for Multiplication If $ab=ac$ and $a \neq 0$, then $b=c$. (In particular, this shows that the number 1 of 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 $b/a=b.a^{-1}$

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 $(-a)b=a(-b)=-(ab)$, $(-a)(-b)=ab$, 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 Fracions $\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}$, 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 $b \neq 0$ and $d \neq 0$

T17. Trichotomy Law For arbitrary real numbers a and b, exactly one of the 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. $a \leq b$ means $a<b$ or $a=b$. If $a<0$, we say that a is **negative**. $b>a$ means $a<b$. $b \geq a$ means $a \leq b$. If $a \geq 0$, we say that a is **nonnegative**

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.

Terminology

Definition	A precise and unambiguous description of the meaning of a mathematical term.
Axiom/Postulate	A statement assumed to be true without proof.
Theorem	A mathematical statement that is proved using rigorous mathematical reasoning. A theorem is usually a major or important result.
Lemma	A small theorem; a minor result whose purpose is to help in proving a theorem.
Corollary	A result that is a simple deduction from a theorem.
Conjecture	A statement believed to be true, but there is no proof (yet).

Definitions

Important Sets

$\mathbb{N}$**:** set of all natural numbers $\{0, 1, 2, 3, 4, ...\}$. Note: 0 is included in $\mathbb{N}$ for this course
$\mathbb{Z}$**:** set of all integers, e.g. 315, 3^5, $\sqrt{49}$
$\mathbb{Q}$**:** set of all rational numbers, e.g. $\frac{1}{2}$, 8.6
$\mathbb{R}$**:** set of all real numbers, e.g. π, $\sqrt{2}$
$\mathbb{C}$**:** set of all complex numbers, e.g. i. Note: not covered in this course
Note: Zero is neither positive nor negative

Properties of Integers

Closure: Integers are closed under addition and multiplication - $x + y \in \mathbb{Z}$ and $xy \in \mathbb{Z}$
Commutative: Addition and multiplication are commutative - $x + y = y + x$ and $xy = yx$
Associativity: Addition and multiplication are associative - $x+y+z = (x+y)+z = x+(y+z)$ and $xyz = (xy)z = x(yz)$
Distributive: Multiplication is distributive over addition (but not the other way around) - $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$
Trichotomy: Exactly one of the following is true: $x = y$, $x < y$, or $x < y$

Even integers: If n is an integer, then n is even $\leftrightarrow \exists$ an integer k such that $n = 2k$

Odd integers: If n is an integer, then n is odd $\leftrightarrow \exists$ an integer k such that $n = 2k + 1$
  Tutorial 1 Qn 11: Proof that n^2 is odd $\leftrightarrow$ n is odd

Assumption 1 (Lecture 1 Slide 27): For this course, can assume that every integer is even or odd, but not both

Divisibility: If $n, d \in \mathbb{Z}$ and $d \neq 0$, $d|n \leftrightarrow \exists\ k \in \mathbb{Z}$ such that $n = dk$. Note: $d|n$ means "d divides n"

Rational and irrational numbers: r is rational $\leftrightarrow \exists\ a, b \in \mathbb{Z}$ such that $r = \frac{a}{b}$ and $b \neq 0$. A real number that is not rational is irrational.

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

Assumption 2 (Lecture 1 Slide 37): Every rational can be reduced to a fraction in its lowest term

Colourful: An integer n is said to be colourful if there exist some integer k such that $n = 3k$, i.e. n is divisible by 3. Note: this terminology is only used in CS1231S.

Prime and Composite Numbers: 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. Symbolically: n is prime - $(n > 1) \wedge \forall\, r, s \in \mathbb{Z}^+,\ (n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$
An integer n is composite iff $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$. Symbolically: 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: Negation of statement variable p is "not p", denoted as $\sim p$

2.1.3 Conjunction: Conjunction of statement variables p and q is "p and q", denoted as $p \wedge q$

2.1.4 Disjunction: Disjunction of statement variables p and q is "p or q", denoted as $p \vee q$

2.1.5 Statement Form/Propositional Form: 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 logically equivalent if and only if they have identical truth values for every possible substitution of statements for their statement variables. Denoted by $\equiv$

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

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

Conditional Statements

2.2.1 Conditional: "if p then q" or "p implies q", denoted by $p \rightarrow q$. It is false when p is true and q is false, otherwise it is true. p is known as the *hypothesis* (or *antecedent*) of the conditional and q the *conclusion* (or *consequent*).
Note: A conditional statement is **vacuously true** or true by default if its hypothesis is false.

2.2.2 Contrapositive: Contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$ (flip and negate original statement)
Note: Contrapositive $\equiv$ conditional statement

2.2.3 Converse: Converse of $p \rightarrow q$ is $q \rightarrow p$ (flip original statement)
Note: Converse $\equiv$ inverse statement

2.2.4 Inverse: Inverse of $p \rightarrow q$ is $\sim p \rightarrow \sim q$ (negate original statement)

2.2.5 Only if: "p only if q" means "if not q then not p" (contrapositive), or equivalently, "if p then q" or "$p \rightarrow q$"

2.2.6 Biconditional: "p if, and only if, q", denoted by $p \leftrightarrow q$. It is true if both p and q have the same truth values and is false if p and q have opposite truth values. *if and only if* can be abbreviated as *iff.*
Note: p if $q \equiv q \rightarrow p \equiv$ if q, then p

2.2.7 Necessary and Sufficient Conditions:
"r is a sufficient condition for s" means "if r then s" or $r \rightarrow s$
"r is a necessary condition for s" means "if not r then not s" or "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, except for the final one, are called *premises* (or assumptions/hypothesis). The final statement is called the *conclusion.* The • symbol, read as "therefore", is normally placed just before the conclusion.
Note: **Valid argument** means that whenever the premises are true, the conclusion is also true. Testing for validity can be done by looking at the conclusion of critical rows; conclusion: false → invalid, conclusion: true → valid

Additional notes (**Tutorial 1**): given premises $p_1, p_2, \ldots, p_n$ and conclusion q, the argument is valid iff $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$ is a tautology.
Note: **Critical rows** are rows in truth table where all premises are true

2.3.2 Sound and Unsound Arguments: An argument is sound if and only if it is valid and all its premises are true; it is unsound otherwise
Note: Sound argument requires the argument to be both logically correct (validity) and the actual values of premises to be true

Order of Operations: From highest to lowest priority
$\sim$ - performed first
$\wedge$ and $\vee$ - coequal in order
$\rightarrow$ and $\leftrightarrow$ - coequal in order (performed last)

Quantified Statements

3.1.1 Predicate 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.
Note: "Domain" is also known as "domain of discourse", "universe of discourse", "universal set", "universe".

3.1.2 Truth set Truth set of $P(x)$ is denoted as $x \in D | P(x)$. This means that the truth set of $P(x)$ is the set of all elements of D that make $P(x)$ true when they are substituted for x.

3.1.3 Universal Statement 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.
Note: *Counterexample* is a value for x whereby $Q(x)$ is false.
Note: A statement of the form $\forall x \in D(P(x) \rightarrow Q(x))$ is **vacuously true** or true by default iff $P(x)$ is false for every x in D.

3.1.4 Existential Statement An existential statement is a statement of the form "$\exists\ x \in D$ such that $Q(x)$". It is defined to be true iff $Q(x)$ is **true for at least one** x in D. It is defined to be false iff $Q(x)$ is **false for all** x in D.
Note: $\exists!$ denotes "there exists a unique" or "there is one and only one"

3.2.1 Contrapositive, Converse, Inverse: Suppose $\forall x \in D(P(x) \rightarrow Q(x))$
Contrapositive - $\forall x \in D(\sim Q(x) \rightarrow \sim P(x))$
Converse - $\forall x \in D(Q(x) \rightarrow P(x))$
Inverse - $\forall x \in D(\sim P(x) \rightarrow \sim Q(x))$

3.2.2 Necessary and Sufficient conditions, Only if:
"$\forall x, r(x)$ is a **sufficient condition** for $s(x)$" means "$\forall x(r(x) \rightarrow s(x))$"
"$\forall x, r(x)$ is a **necessary condition** for $s(x)$" means "$\forall x(\sim r(x) \rightarrow \sim s(x))$" or "$\forall x(s(x) \rightarrow r(x))$"
"$\forall x, r(x)$ **only if** $s(x)$" means "$\forall x(\sim s(x) \rightarrow \sim r(x))$" or "$\forall x(r(x) \rightarrow s(x))$"

Universal Instantiation: If some property is true of everything in the set, then it is true of any particular thing in the set

Universal Modus Ponens: If x makes $P(x)$ true, then x makes $Q(x)$ true — a makes $P(x)$ true — • a makes $Q(x)$ true

Universal Modus Tollens: If x makes $P(x)$ true, then x makes $Q(x)$ true — a does not make $Q(x)$ true — • a does not make $P(x)$ true

3.4.1 Valid Argument Form: A valid argument form 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: If x makes $P(x)$ true, then x makes $Q(x)$ true — a makes $Q(x)$ true — • a makes $P(x)$ true

Inverse error: If x makes $P(x)$ true, then x makes $Q(x)$ true — a does not make $P(x)$ true — • a does not make $Q(x)$ true

Universal Transitivity: $\forall x(P(x) \to Q(x))$ — $\forall x(Q(x) \to R(x))$ — •$\forall x(P(x) \to R(x))$

Methods of Proofs

Disproof by Counterexample: To disprove $\forall x \in D(P(x) \to Q(x))$, find a value x in D for which the hypothesis $P(x)$ is true but the conclusion $Q(x)$ is false. Such an x is called a **counterexample**.
It is also the same as proving its negation is true - i.e. proving $\exists\ x \in D(P(x) \wedge \sim Q(x))$ is true.

Proof by exhaustion: Used when the domain D is finite or only a finite number of elements satisfy the predicate $P(x)$

Generalizing from the Generic Particular: To show that every element of a set satisfies a certain property, suppose x is a **particular** but **arbitrarily chosen** element of the set, and show that x satisfies the property.

Proof by Contradiction: Indirect proof. Suppose the statement to be proved, S, is false. That is, the negation of the statement, $\sim S$, is true. Show that this supposition leads logically to a contradiction (e.g. negation is false). Conclude that the statement S is true.

Proof by Contrapositive: Indirect proof. Since the contrapositive form of a statement is logically equivalent to the original conditional statement, proving that the contrapositive statement is true means that the original statement is true.

Sets

Set-roster notation: A set is an **unordered** collection of objects. Set-roster notation is one way of representing sets by writing all of its elements between braces - $\{1, 2, 3...\}$
Note: set and multiset (e.g. $\{a, b, c\}$ and $\{a, b, b, c\}$) are two different things. Multisets are not covered in this course.

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

Cardinality [$|S|$]: The cardinality of a set S, denoted as $|S|$, is the size of the set, that is, the number of **unique** elements in S. E.g. $|\{a, b, c\}| = 3$

Set-builder notation: The set of all x in U such that $P(x)$ is true - will be written as $\{x \in U \mid P(x)\}$ or $\{x \in U : P(x)\}$ in set-builder notation

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 $\{t(x) \mid x \in A\}$, which is read as "the set of all $t(x)$ where $x \in A$"

Subset and superset: A is a subset of B/A contained in B, written $A \subseteq B$, iff every element of A is also an element of B. Symbolically: $A \subseteq B$ iff $\forall x(x \in A \to x \in B)$. If $A \subseteq B$, we may also write $B \supseteq A$, which reads as "B contains A" or "B includes A" or "B is a superset of A".

Proper subset: Let A and B bet sets. A is a *proper subset* of B, denoted $A \subsetneq B$, iff $A \subseteq B$ and $A \neq B$. We can say that the inclusion of A in B is proper or strict. E.g. $\{1, 2\} \subsetneq \{1, 2, 3\}$

Not subset: If at least one element of A is not an element of B, then A is not a subset of B.
Symbolically: $A \nsubseteq B \leftrightarrow \exists\ x(x \in A \wedge x \notin B)$. E.g. $\{1, 2, 4\} \nsubseteq \{1, 2, 3, 5\}$

Ordered Pairs: An ordered pair is an expression in the form (x, y). Two ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$. Symbolically: $(a, b) = (c, d) \leftrightarrow (a = c) \wedge (b = d)$

Cartesian Product: The **cartesian product** of sets A and B, denoted $A \times B$ 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: $A \times B = \{(a, b) : a \in A \wedge b \in B\}$

Note: the term Cartesian Plane is often used to refer to a plane with this coordinate system
A more general term: $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n \wedge\}$

Set Equality: Set A equals set B, denoted as $A = B$, iff every element of A is in B and every element of B is in A. Symbolically: $A = B \leftrightarrow A \subseteq B \wedge B \subseteq A$, can also be represented as $A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$
General method for proving two sets are equal:

1. Let sets X and Y be given. To prove $X = Y$:
2. ($\subseteq$) Prove that $X \subseteq Y$
3. ($\supseteq$) Prove that $Y \subseteq X$ or $X \supseteq Y$
4. From (2) and (3), conclude that $X = Y$

Union: The union of sets A and B, denoted $A \cup B$, 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 sets A and B, denoted $A \cap B$, 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 $B - A$, or $B \setminus A$, is the set of all elements that are in B and not in 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: $\overline{A} = \{x \in U \mid x \notin A\}$
Note: X^c also represents the complement of X

Interval notation: Given real numbers a and b with $a \leq b$:
$(a, b) = \{x \in \mathbb{R} : a < x < b\}$, $(a, b\,] = \{x \in \mathbb{R} : a < x \leq b\}$, $[\,a, b\,] = \{x \in \mathbb{R} : a \leq x \leq b\}$, $[\,a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:
$(a, \infty) = \{x \in \mathbb{R} : x > a\}$, $[\,a, \infty) = \{x \in \mathbb{R} : x \geq a\}$, $(-\infty, b) = \{x \in \mathbb{R} : x < b\}$, $(-\infty, b\,] = \{x \in \mathbb{R} : x \leq b\}$

Unions and Intersections of an Indexed Collection of Sets:

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

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

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

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all non-negative integer } i\}$$

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

Mutally disjoint: Sets $A_1, A_2, A_3, \ldots$ are mutally disjoint (or *pairwise disjoint* or *nonoverlapping*) iff no two sets A_i and A_j with distinct subscripts have no elements in common. Symbolically: $A_i \cap A_j = \emptyset$ whenever $i \neq j$.
The set A is called a **union of mutually disjoint subsets** iff A_1, A_2, A_3, A_4 are mutually disjoint. The collection of sets $\{A_1, A_2, A_3, A_4\}$ is said to be a **partition** of A.

Power set: Given a set A, the power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.
E.g. $A = \{x, y\}$, $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$

Ordered n-tuple: 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 $(x_1, x_2, \ldots, x_n)$. An **ordered pair** is an ordered 2-tuple, an **ordered triple** is an ordered 3-tuple. Equality of two ordered n-tuples: $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \leftrightarrow x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$

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: If U is the **universal** set ($U \supseteq X$), $\overline{X}$ 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 $A \times B$. Given an ordered pair (x, y) in $A \times B$, x is related to y by R, or x is R-related to y, written xRy, iff $(x, y) \in R$. Symbolically: xRy means $(x, y) \in R$, $x \not R y$ means $(x, y) \notin R$

Domain: The **domain** of R, $Dom(R)$, is the set of $\{a \in A : aRb$ for some $b \in B\}$ (i.e. inputs to relation)

Co-domain: The **co-domain** of R, $coDom(R)$, is the set B (i.e. possible outputs of relation)

Range: The **range** of R, $Range(R)$, is the set of $\{b \in B : aRb$ for some $a \in A\}$ (i.e. actual outputs of relation)

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: $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$. Can also be written as: $\forall x \in A, \forall y \in B((y, x) \in R^{-1} \leftrightarrow (x, y) \in R)$

Relation on a Set: A **relation on a set A** is a relation from A to A. In other words, a relation on a set A is a subset of $A \times A$. We may write A^2 for $A \times A$, and A^n for $A \times \cdots \times A$ (n times)

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

Note: positions of R and S are swapped when represented in $S \circ R$ as you map the inner relation (R) first, before mapping the outer relation (S).

Proposition: Composition is Associative: $T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$ (Proof in **Tutorial 4 Qn 7**)

Proposition: Inverse of Composition: $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

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

Reflexivity, Symmetric, and Transitive:
R is **reflexive** iff $\forall x \in A(xRx)$
R is **symmetric** iff $\forall x, y \in A(xRy \rightarrow yRx)$
R is **transitive** iff $\forall x, y, x \in A(xRy \wedge yRz \rightarrow xRz)$
Note: Reflexivity, symmetry and transitivity are **properties of a relation**, not properties of members of a the set.
Tutorial 4 Qn 2: If R is symmetric, $R = R^{-1}$

Transitive Closure: Let A be a set and R be 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 $R^t \subseteq S$

* Transitive closure is adding the least number of ordered pairs to make the relation transitive
Note: As you add more arrows/relations, do check if the new relations lead to additional relations to be added

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

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

Tutorial 5 Qn 7: Proof on reflexive closure

Partition: $\mathcal{C}$ (read as curly 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. $\forall x \in A \forall S_1, S_2 \in \mathcal{C}(x \in S_1 \wedge x \in S_2 \rightarrow S_1 = S_2)$ and $\forall x \in A \exists\ S \in \mathcal{C}(x \in S)$

Elements of a partition are called components of the partition.
Shorter version: $\forall x \in A\ \exists\ !\ S \in \mathcal{C}(x \in S)$
E.g. $A = \{b, e, f, k, m, p\} \rightarrow \mathcal{C} = \{\{b, p\}, \{f, m\}, \{e\}, \{k\}\}$

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. $x, y \in S$
E.g. $A = \{0, 1, 2, 3, 4\}$, $\mathcal{C} of A : \{\{0, 3, 4\}, \{1\}, \{2\}\}$
$\{0, 3, 4\}$ is a component of the partition $\rightarrow 0R0, 0R3, 0R4, 3R0, 3R3, 3R4, 4R0, 4R3, 4R4$
$\{1\}$ is a component of the partition $\rightarrow 1R1$
$\{2\}$ is a component of the partition $\rightarrow 2R2$
• R (induced by this partition) $= \{(0, 0), (0, 3), (0, 4), (1, 1), (2, 2), (3, 0), (3, 3), (3, 4), (4, 0), (4, 3), (4, 4)\}$

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

Tutorial 4 Qn 10a: Proof of 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: $[a]_\sim = \{x \in A : a \sim x\}$

Congruence: Let $a, b \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $a - b = nk$ for some $k \in \mathbb{Z}$. In other words, $n|(a - b)$. In this case, we write $a \equiv b \pmod{n}$.
E.g. $-3 \equiv 12 (\text{mod } 5)$, $-3 - 12 = -15 = 5 \times (-3)$, $k = -3$

Proposition: Congruence-mod *n*: 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. $A/\sim$ denotes the set of all equivalence classes with respect to $\sim$, i.e., $A/\sim = \{[x]_\sim : x \in A\}$

Antisymmetry: Let R be a relation on a set A. R is **antisymmetric** iff $\forall x, y \in A(xRy \wedge yRx \rightarrow x = y)$
Note: Antisymmetric is not the same as not symmetric $(\exists\ x, y \in A(xRy \wedge y\not Rx))$

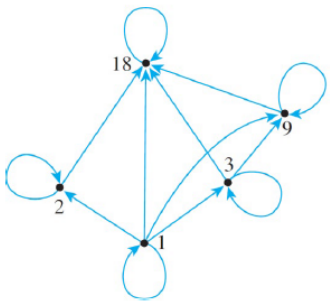
Partial Order Relation: Let R be a relation on a set A. Then R is a **partial order relation** iff R is reflexive, *antisymmetric* and transitive.
Note: examples include: "less than or equal to $(\leq)$" relation and "subset $(\subseteq)$" relation
Note: the symbol $\preccurlyeq$ is used to refer to a general partial order, and the notation $x \preccurlyeq y$ is read "x is curly less than or equals to y". Suppose $x, y \in A$. We write $x \preccurlyeq y$ iff task x must be done before or at the same time as task y.

Tutorial 5 Qn 5 & 6: Proving partial order relation

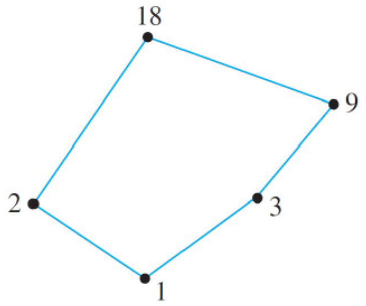
Partially Ordered Set: A set A is called a **partially ordered set** (or **poset**) with respect to a partial order relation R on A, denoted by (A, R)

Hasse diagram: Let $\preccurlyeq$ be a partial order on set A. A hasse diagram of $\preccurlyeq$ satisfies the following condition for all distinct $x, y, m \in A$:

If $x \preccurlyeq y$ and no $m \in A$ is such that $x \preccurlyeq m \preccurlyeq z$, then x is placed below y with a line joining them, else no line joins x and y.



Directed graph of the "divide" relation on {1,2,3,9,18}



Hasse diagram of the "divide" relation on {1,2,3,9,18}

Comparability: Suppose $\preccurlyeq$ is a partial order relation on a set A. Elements a and b of A are said to be **comparable** iff either $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, a and b are **noncomparable**. If all the elements in A are comparable, A is called a **total order** or **linear order**.
E.g. $A = \{a, b\}$ and $B = \{b, c\}$, $A \nsubseteq B$ and $B \nsubseteq A$, thus A and B are said to be *noncomparable.*
E.g. real numbers x and y are said to be *comparable* if either $x \leq y$ or $y \leq x$

Tutorial 5 Qn 2: example of comparability
Tutorial 5 Qn 11a: Proof that any 2 comparable elements are compatible

Compatibility: a, b are **compatible** iff there exists $c \in A$ such that $a \preccurlyeq c$ and $b \preccurlyeq c$.

Tutorial 5 Qn 9: Example on compatibility.

Maximal/Minimal/Largest/Smallest Element: Let set A be partially ordered with respect to a relation $\preccurlyeq$ and $c \in A$:

1. c is a **maximal element** of A iff $\forall x \in A(c \preccurlyeq x \rightarrow c = x)$ (e.g. if someone is *above* c, that person is c himself)
2. c is a **minimal element** of A iff $\forall x \in A(x \preccurlyeq c \rightarrow c = x)$ (e.g. if someone is *below* c, that person is c himself)
3. c is the **largest element** of A iff $\forall x \in A(x \preccurlyeq c)$ (e.g. c is above x)
4. c is the **smallest element** of A iff $\forall x \in A(c \preccurlyeq x)$ (e.g. x is above c)

Tutorial 5 Qn 3: example on min/max elements

Proposition: A smallest element is minimal: Consider a partial order $\preccurlyeq$ on a set A. Any smallest element is minimal. Likewise, any largest element is maximal.

smallest $\leftrightarrow$ everything is above $\equiv$ nothing is below $\leftrightarrow$ minimal

Total Order Relations: 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 $\preccurlyeq$ be a partial order on a set A. A linearization of $\preccurlyeq$ is a total order $\preccurlyeq^*$ on A such that $\forall x, y \in A(x \preccurlyeq y \rightarrow x \preccurlyeq^* y)$

Kahn's Algorithm: To linearize a partial order, pick a minimal element and place at bottom of a total order. Repeat until nothing left.

Well-ordered Set: Let $\preccurlyeq$ be a total order on a set A. A is **well-ordered** iff every non-empty subset of A contains a smallest element. Symbolically: $\forall S \in \mathcal{P}(A), S \neq \emptyset \rightarrow (\exists\, x \in S \forall y \in S(x \preccurlyeq y))$
E.g. $(\mathbb{N}, \leq)$ is well-ordered, $(\mathbb{Z}, \leq)$ is not well-ordered.

Asymmetry: Let R be a relation on a set A. R is **asymmetry** iff $\forall x, y \in A(xRy \rightarrow y \not R x)$
Note: Every asymmetric relation is antisymmetric.

Tutorial 5 Qn 8: Proof on asymmetry relation is also antisymmetric

Chain: A subset C of A is called a **chain** iff every pair of elements in C is comparable $(\forall a, b \in C(a \preccurlyeq b \vee b \preccurlyeq a))$.
E.g. In **tutorial 5 qn 10b**, one chain is $2, 6, 12$
Maximal Chain: A chain M such that $t \notin M \rightarrow M \wedge \{t\}$ is not a chain
E.g. In **tutorial 5 qn 10b**, $5, 35, 385$ is a maximal chain. If 35 is taken out, then it is not a chain anymore.

Theorems, Lemmas, and Corollaries

Implication law: $p \to q \equiv \sim p \vee q$

Theorem 2.1.1 Logical Equivalences

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**	$p \wedge \textbf{true} \equiv p$	$p \vee \textbf{false} \equiv p$
5	**Negation laws**	$p \wedge \sim p \equiv \textbf{false}$	$p \vee \sim p \equiv \textbf{true}$
6	**Double negative law**	$\sim (\sim p) \equiv p$	
7	**Idempotent laws**	$p \wedge p \equiv p$	$p \vee p \equiv p$
8	**Universal bound laws**	$p \wedge \textbf{false} \equiv \textbf{false}$	$p \vee \textbf{true} \equiv \textbf{true}$
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**	$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$
11	**Negation of true and false**	$\sim \textbf{true} \equiv \textbf{false}$	$\sim \textbf{false} \equiv \textbf{true}$

Variant absorption law (Assignment 1): $p \wedge (\sim p \vee q) \equiv p \wedge q$, $p \vee (\sim p \wedge q) \equiv p \vee q$

Table 2.3.1 Rules of Inference

Rule of Inference		
Modus Ponens	$p \to q$ p $\bullet\ q$	
Modus Tollens	$p \to q$ $\sim q$ $\bullet\ \sim p$	
Generalization	p $\bullet\ p \vee q$	q $\bullet\ p \vee q$
Specialization	$p \wedge q$ $\bullet\ p$	$p \wedge q$ $\bullet\ q$
Conjunction	p q $\bullet\ p \wedge q$	

Rule of Inference		
Elimination	$p \vee q$ $\sim q$ $\bullet\ p$	$p \vee q$ $\sim p$ $\bullet\ q$
Transitivity	$p \to q$ $q \to r$ $\bullet\ p \to r$	
Proof by Division into Cases	$p \vee q$ $p \to r$ $q \to r$ $\bullet\ r$	
Contradiction	$\sim p \to$ false $\bullet\ p$	

Rules of Inference for Quantified Statements

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

Theorem 3.2.1 Negation of a Universal Statement: $\sim (\forall x \in D, P(x)) \equiv \exists\ x \in D$ such that $\sim P(x)$. Negation of a universal statement ("all are") is logically equivalent to an existential statement ("some are not" or "there is at least

one that is not").

Theorem 3.2.2 Negation of an Existential Statement: $\sim (\exists\ x \in D$ such that $P(x)) \equiv \forall x \in D, \sim P(x)$. Negation of an existential statement ("some are") is logically equivalent to a universal statement ("none are" or "all are not").

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 and 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 positive integer d, there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$
P.S. Take q as quotient and r as remainder

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

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

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

Theorem 6.2.1 Some Subset Relations: For all sets A, B and C:

Inclusion of Intersection	$A \cap B \subseteq A$ $A \cap B \subseteq B$
Inclusion in Union	$A \subseteq A \cup B$ $B \subseteq A \cup B$
Transitive Property of Subsets	$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$

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

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 6.2.4: An empty set is a subset of every set, i.e $\emptyset \subseteq A$ for all sets A
Note: Empty set is a set with no elements, denoted by $\{\}$ or $\emptyset$

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

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

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 set A. The following are equivalent for all $x, y \in A$: (i) $x \sim y$ (ii) $[x] = [y]$ (iii) $[x] \cap [y] \neq \emptyset$
Note: can be proven by proving (i) → (ii), (ii) → (iii), (iii) → (i), **Proof** in Lect 6 slide 47-49

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.

Proof in Lect 6 slide 57-59

Proofs (for reference)

Prove that the sum of any two even integers is even

1. Let m and n be two particular but arbitrarily chosen even integers
   1.1. Then $m = 2r$ and $n = 2s$ for some integers r and s (by definition of even numbers)
   1.2. $m + n = 2r + 2s = 2(r + s)$ (by basic algebra)
   1.3. $2(r + s)$ is an integer (by closure of integers under + and x)
   1.4. Hence $m + n$ is an even number
2. Therefore, the sum of any two even integers is even

Proof by contraposition: For all integers n, if n^2 is even then n is even

1. Contrapositive Statement: For all integers n, if n is odd then n^2 is odd
2. Let n be an arbitrarily chosen odd number
   2.1 Then $n = 2k + 1$ for some integer k (by definition of odd number)
   2.2 Then $n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
   2.3 Let $m = 2k^2 + 2k$. Now, m is an integer (by closure property) and $n^2 = 2m + 1$
   2.4 So n^2 is odd
3. Therefore, for all integers n, if n^2 is even, then n is even

Proof that the congruence modulo 3 relation is an equivalence relation

$\forall x, y \in \mathbb{Z}(xRy \leftrightarrow 3|(x - y))$
1. Proof of Reflexivity
   1.1 Let a be an arbitrarily chosen integer
   1.2 Now $a - a = 0$
   1.3 But $3|0$ (since $0 = 3 \times 0$), hence, $3|(a - a)$
   1.4 Therefore aRa (by definition of R)
2. Proof of Symmetry
   2.1 Let a and b be arbitrarily chosen integers that satisfy aRb
   2.2 Then $3|(a - b)$ (by definition of R), hence $a - b = 3k$ for some integer k (by definition of divisibility)
   2.3 Multiplying both sides by -1 gives $b - a = 3(-k)$
   2.4 Since $-k$ is an integer, $3|(b - a)$ (by definition of divisibility)

2.5 Therefore bRa (by definition of R)

3. Proof of Transitivity

    3.1 Let a, b and c be arbitrarily chosen integers that satisfy aRb and bRc

    3.2 The $3|(a-b)$ and $3|(b-c)$ (by definition of R), hence $a-b=3r$ and $b-c=3s$ for some integers r and s (by definition of divisibility)

    3.3 Adding both equations give $a-c=3(r+s)$

    3.4 Since $r+s$ is an integer (by closure under $+$ and $\times$), $3|(a-c)$ (by definition of divisibility)

    3.5 Therefore aRc (by definition of R)

4. Hence, R is an equivalence relation

Extra
