Done by Marcus Pang in 2021

Statements

1. Universal (all, every, any): $\forall x \in D(Q(x))$ is **true** if and only if $Q(x)$ is **true** for every $x \in D$
2. Conditional (if...then): $\forall x \in D\ (P(x) \implies Q(x))$ is **true** if and only if $({\sim}P(x) \vee Q(x))$ is **true** for every $x \in D$
3. Existential (there exists, there is, some): $\exists x \in D$ such that $Q(x)$ is **true** for at least one $x \in D$

Definitions

1. Divisibility: if $n, d \in \mathbb{Z} \wedge n \neq 0$,
$$d \mid n \iff \exists k \in \mathbb{Z}(n = dk)$$
2. Congruence: if $a, b \in \mathbb{Z} \wedge n \in \mathbb{Z}^+$,
$$a \equiv b \pmod n \iff n \mid (a - b)$$
3. Rational:
$$n \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z}\left(n = \frac{a}{b} \wedge b \neq 0\right)$$
4. Even:
$$n \text{ is even} \iff \exists k \text{ such that } n = 2k$$
5. Odd:
$$n \text{ is odd} \iff \exists k \text{ such that } n = 2k + 1$$
6. Prime:
$$\forall r, s \in \mathbb{Z}^+(n = rs \implies (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$$
7. Composite:
$$\exists r, s \in \mathbb{Z}^+((n = rs) \wedge (1 < r < n) \wedge (1 < s < n))$$
8. Fraction in lowest term: largest integer that divides numerator and denominator is 1
9. Negation of p is ${\sim}p$
10. Conjuction of p and q is $p \wedge q$
11. Disjunction of p and q is $p \vee q$
12. Statement/Propositional form: expression made of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables
13. Logical equivalence: statements with identical truth values for each possible substitution of statements for their statement variables
14. Tautology/Contradiction: statement form that is always **true**/**false** regardless of the truth values of the individual statements substituted for its statement variables
15. Conditional (sufficient condition, only if) of q by p is "if p then q" or "p implies q" denoted as
$$p \implies q$$
p is the hypothesis/antecedent and q is the conclusion/consequent.
16. Contrapositive (sufficient condition, only if):
$${\sim}q \implies {\sim}p \equiv p \implies q$$
17. Converse (necessary condition, if):
$$q \implies p$$
18. Inverse (necessary condition, if):
$${\sim}p \implies {\sim}q \equiv q \implies p$$
19. Biconditional (if and only if):
$$p \iff q \equiv (p \implies q) \wedge (q \implies p)$$
20. Argument: sequence of statements, where all statements (except the last one) are called premises/assumptions/hypothesis. The final statement is called the conclusion.
   (a) Syllogism: argument with 2 premises and 1 conclusion
   (b) Critical Row: row in truth table where all premises are **true**
   (c) If there is a critical row in which the conclusion is **false**, then the argument form is invalid
   (d) If for all critical rows the conclusion is **true**, then the argument form is valid.
   (e) Sound if and only if it is valid and all its premises are true
21. Predicate: sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables, $P(x_1, x_2, \ldots)$
22. Domain of a predicate variable: set of all values that may be substituted in place of the variable
23. Truth set of $P(x)$: set of all elements of D that make $P(x)$ **true** when substituted for x, $\{x \in D \mid P(x)\}$
24. Set: unordered collection of objects
   (a) Sets of size 1 are called singletons
   (b) A set is finite if it has finitely many distinct elements
25. Set Equality: sets with all the same elements
$$A = B \iff \forall z(z \in A \iff z \in B)$$
26. Subset: set where all elements are contained by another set (set included by another set)
$$A \subseteq B \iff \forall z(z \in A \implies z \in B)$$
27. Power set: the set of all subsets, $\mathcal{P}(A)$
28. Cardinality: the number of (distinct) elements in a set, $|A|$
29. Ordered pairs: expressions of the form (x, y)
30. Ordered n-tuples: $(x_1, x_2, \ldots, x_n), n \geq 2$
$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \iff x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots x_n = y_n$$
31. Cartesian product of sets:
$$A \times B = \{x \in A \wedge x \in B\}$$
32. Union of sets:
$$A \cup B = \{x \mid x \in A \vee x \in B\}$$
33. Intersection of sets:
$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$
34. Complement of a set in another set:
$$A - B = A \backslash B = \{x \mid x \in A \wedge x \notin B\}$$
$$\overline{B} = U \backslash B$$
35. Disjoint sets: $A \cup B = \varnothing$
36. Pairwise/Mutually disjoint sets: for all distinct $i, j = \{1, 2, \ldots, n\}$,
$$A_i \cap A_j = \varnothing$$
37. Partition of set: $\mathscr{C}$ is a partition of a set A if it is a set of mutually disjoint nonempty subsets (components) of A whose union is A
   (a) $\forall S \in \mathscr{C}(\varnothing \neq S \subseteq A)$
   (b) $\forall x \in A\ \exists S \in \mathscr{C}(x \in S) \wedge$
$$\forall x \in A\ \forall S_1, S_2 \in \mathscr{C}\ (x \in S_1 \wedge x \in S_2 \implies S_1 = S_2)$$
$$\therefore \forall x \in A\ \exists! S \in \mathscr{C}(x \in S)$$
38. Relation:
   (a) $R \subseteq A \times B$
   (b) $x\ R\ y$ for $(x, y) \in R \wedge x \not R\ y$ for $(x, y) \notin R$
$$R = \{(x, y) \in A \times B \mid x\ R\ y\}$$
$$R^{-1} = \{(y, x) \in B \times A \mid y\ R^{-1}\ x\}$$
39. Binary relation on a set: relation from A to A
40. Reflexive: $\forall x \in A(x\ R\ x)$
41. Symmetric: $\forall x, y \in A(x\ R\ y \implies y\ R\ x)$
42. Transitive: $\forall x, y, z \in A(x\ R\ y \wedge y\ R\ z \implies x\ R\ z)$
43. Anti-symmetric:
$$\forall x, y \in A\,(x\ R\ y \wedge y\ R\ x \implies x = y)$$
44. Comparable: $x\ R\ y \vee y\ R\ x$
45. Equivalence relation: relation that is reflexive, symmetric, and transitive, usually $\sim$
46. Equivalence class of x w.r.t $\sim$: set of all elements that are $\sim$-related to x
$$[x]_\sim = \{y \in A \mid x{\sim}y\}$$
47. Set of all equivalence classes (quotient of set by relation):
$$A/{\sim} = \{[x]_\sim \mid x \in A\}$$
48. Representative of an equivalence class: element of the equivalence class
49. Quotient $\mathbb{Z}/{\sim_n}$ is denoted as $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$, and addition/multiplication is defined as follows
$$[x] + [y] = [x + y] \qquad [x] \cdot [y] = [x \cdot y]$$
50. (Non-strict) Partial Order: relation that is reflexive, anti-symmetric, and transitive, denoted with $\preccurlyeq$ and $x \prec y \equiv x \preccurlyeq y \wedge x \neq y$
51. (Non-strict) Total/Linear Order: partial order where every pair of elements is comparable
52. Partially Ordered Set (Poset) refers to the ordered pair (A, R) where R is a partial order on A
53. Hasse Diagram of $\preccurlyeq$: if $x \prec y$ and no $z \in A$ such that $x \prec z \prec y$, then x is placed below y and a line joins x to y, else no line
54. Minimal Element: $\forall x \in A(x \preccurlyeq c \implies c = x)$
55. Maximal Element: $\forall x \in A(c \preccurlyeq x \implies c = x)$
56. Smallest Element: $\forall x \in A(c \preccurlyeq x)$
57. Largest Element: $\forall x \in A(x \preccurlyeq c)$
58. Linearization of $\preccurlyeq$ is a total order $\preccurlyeq^*$ such that
$$\forall x, y \in A(x \preccurlyeq y \implies x \preccurlyeq^* y)$$
59. Function or a map from A to B: assignment to each element of A exactly one element of B, $f : A \to B$
   (a) If $x \in A$ then $f(x)$ is the image of x under f, if $y = f(x)$ then f maps x to y, denoted as $f : x \mapsto y$
   (b) A is the domain of f, B is the codomain of f
60. Identity function: id: $A \to A$, which satisfies
$$\forall x \in A\,(\mathrm{id}_A(x) = x)$$

Order of Operations

1. $\sim$
2. $\wedge$ and $\vee$
3. $\implies$ and $\iff$

Argument Forms

Rules of Inferences

$$\text{premise}_1 \wedge \ldots \wedge \text{premise}_n \implies \text{conclusion}$$

1. Modus Ponens and Universal Modus Ponens
$$\begin{gathered} p \implies q \\ p \\ \therefore q \end{gathered}$$
2. Modus Tollens and Universal Modus Tollens
$$\begin{gathered} p \implies q \\ \sim q \\ \therefore\ \sim p \end{gathered}$$
3. Generalization
$$\begin{gathered} p \\ \therefore p \vee q \end{gathered} \qquad \begin{gathered} q \\ \therefore p \vee q \end{gathered}$$
4. Specialization
$$\begin{gathered} p \wedge q \\ \therefore p \end{gathered} \qquad \begin{gathered} p \wedge q \\ \therefore q \end{gathered}$$
5. Conjunction
$$\begin{gathered} p \\ q \\ \therefore p \wedge q \end{gathered}$$
6. Elimination
$$\begin{gathered} p \vee q \\ \sim q \\ \therefore p \end{gathered} \qquad \begin{gathered} p \vee q \\ \sim p \\ \therefore q \end{gathered}$$
7. Transitivity
$$\begin{gathered} p \implies q \\ q \implies r \\ \therefore p \implies r \end{gathered}$$
8. Proof by division into cases
$$\begin{gathered} p \vee q \\ p \implies r \\ q \implies r \\ \therefore r \end{gathered}$$
9. Contradiction rule
$$\begin{gathered} \sim p \implies \textbf{false} \\ \therefore p \end{gathered}$$

Rules of Inference for Quantified Statements

1. Universal Modus Ponens
$$\begin{gathered} \forall x \in D(P(x) \implies Q(x)) \\ P(a) \text{ for a particular a} \in D \\ \therefore Q(a) \end{gathered}$$
2. Universal Modus Tollens
$$\begin{gathered} \forall x \in D(P(x) \implies Q(x)) \\ \sim Q(a) \text{ for a particular a} \in D \\ \therefore \sim P(a) \end{gathered}$$
3. Universal Transitivity
$$\begin{gathered} \forall x \in D(P(x) \implies Q(x)) \\ \forall x \in D(Q(x) \implies R(x)) \\ \therefore \forall x(P(x) \implies R(x)) \end{gathered}$$
4. Universal Instantiation
$$\begin{gathered} \forall x \in D(P(x)) \\ \therefore P(a) \text{ if } a \in D \end{gathered}$$
5. Universal Generalization
$$\begin{gathered} \forall P(a) \text{ for every } a \in D \\ \therefore \forall x \in D(P(x)) \end{gathered}$$
6. Existential Instantiation
$$\begin{gathered} \exists x \in D(P(x)) \\ \therefore P(a) \text{ for some } a \in D \end{gathered}$$
7. Existential Generalization
$$\begin{gathered} P(a) \text{ for some } a \in D \\ \therefore \exists x \in D(P(x)) \end{gathered}$$

Common Fallacies

1. Ambiguous premises
2. Circular reasoning
3. Jumping to a conclusion
4. Converse/Inverse error

Proof Types

1. Direct Proof: using algebra/definitions to construct an argument

2. By Construction: form of direct proof which comes up with a specific example to prove/disprove the statement

3. By Contradiction: assume the negation of the statement and arrive to the conclusion that the negation is false, and since every step is logically correct, the assumption must be false

4. By Exhaustion: list all possible scenarios (for finite cases)

(T2.1.1) Logical Equivalences

1. Commutative Law
$$p \wedge q \equiv q \wedge p \qquad p \vee q \equiv q \vee p$$
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
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (q \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (q \vee r)$$
4. Identity laws
$$p \wedge \textbf{true} \equiv p \qquad p \vee \textbf{false} \equiv p$$
5. Negation laws
$$p \vee \sim p \equiv \textbf{true} \qquad p \wedge \sim p \equiv \textbf{false}$$
6. Double negative law
$$\sim(\sim p) \equiv p$$
7. Idempotent laws
$$p \wedge p \equiv p \qquad p \vee p \equiv p$$
8. Universal bound laws
$$p \vee \textbf{true} \equiv \textbf{true} \qquad p \wedge \textbf{false} \equiv \textbf{false}$$
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
$$p \vee (p \wedge q) \equiv p \qquad p \wedge (p \vee q) \equiv p$$
11. Negation of true and false
$$\sim\textbf{true} \equiv \textbf{false} \qquad \sim\textbf{false} \equiv \textbf{true}$$

(T5.3.5) Set Identities

1. Identity Law
$$A \cup \varnothing = A \qquad A \cap U = A$$
2. Universal Bound Law
$$A \cup U = U \qquad A \cap \varnothing = \varnothing$$
3. Idempotent Law*
4. Double Complement Law
$$\overline{(\overline{A})} = A$$
5. Commutative Law*
6. Associative Law*
7. Distributive Law*
8. De Morgan's Law*
9. Absorption Law*
10. Complement Law
$$A \cup \overline{A} = U \qquad A \cap \overline{A} = \varnothing$$
11. Set Difference Law
$$A \backslash B = A \cap \overline{B}$$
12. Top and Bottom Law
$$\overline{\varnothing} = U \qquad \overline{U} = \varnothing$$

Theorems (5^{th} edition)

1. (T4.8.1) $\sqrt{2}$ is irrational

2. (P4.7.4) $\forall n \in \mathbb{Z}(n^2 \text{ is even} \implies n \text{ is even})$

3. (T3.2.1) $\sim(\forall x \in D, P(x)) \equiv \exists x \in D$ such that $P(x)$

4. (T3.2.2) $\sim(\exists x \in D$ such that $P(x)) \equiv \forall x \in D, P(x)$

5. (T4.3.1) Every integer is a rational number

6. (T4.3.2) Sum of any two rational number is rational

7. (C4.2.3) Double of a rational number is rational

8. (T4.4.1) $\forall a, b \in \mathbb{Z}^+(a \mid b \implies a \leq b)$

9. (T4.4.2) The only divisors of 1 are 1 and -1

10. (T4.4.3) $\forall a, b, c \in \mathbb{Z}(a \mid b \wedge b \mid c \implies a \mid c)$

11. (T4.7.1) There is no greatest integer

12. (T5.1.1.7) Empty set is a unique set with no element

13. (T5.2.4) For finite sets, $|\mathcal{P}(A)| = 2^{|A|}$

14. (T5.3.12) For (pairwise) disjoint sets,
$$|A \cup B| = |A| + |B|$$
$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$$

15. (T5.3.13) Inclusion-Exclusion Principle: for finite sets, $|A \cup B| = |A| + |B| - |A \cap B|$

16. (L6.4.4) Let $\sim$ be an equivalence relation, then
$$\begin{tikzcd} & x \sim y \arrow[dr, Rightarrow] & \\ {[x]_\sim = [y]_\sim} \arrow[ur, Rightarrow] & & {[x] \cap [y] \neq \varnothing} \arrow[ll, Rightarrow] \end{tikzcd}$$

17. (T6.4.9) $A/\sim$ is a partition of A

18. (P7.1.5) Addition/Multiplication is well-defined on $\mathbb{Z}_n$. $\forall n \in \mathbb{Z}^+$,
$$[x_1] = [x_2] \wedge [y_1] = [y_2] \implies$$
$$[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$$
$$\wedge [x_1] \cdot [y_1] = [x_1 \cdot y_1] = [x_2 \cdot y_2] = [x_2] \cdot [y_2]$$

19. (P7.4.4) For posets, a smallest element is minimal and there is at most one smallest element

20. (P7.4.6) For a nonempty finite poset, a minimal element can be found

21. (T7.4.10) For any partial order on a set, there exists a total order on that set

22. (Tutorial 4) Division Theorem:
$\forall n \in \mathbb{Z}, d \in \mathbb{Z}^{+} \exists! q, r \in \mathbb{Z}$ s.t.

$$n = dq + r \wedge 0 \leq r < d$$

23. (P6.2.16) $\sim_{\mathscr{C}}$ the same-component relation is an equivalence relation

24. (P6.3.4) $\sim_{n}$ the congruence-mod-n relation is an equivalence relation

Set Notations

1. Roster notation: $\{x_1, x_2, ..., x_n\}$
2. Set builder notation: $\{x \in U \mid P(x)\}$
3. Replacement notation: $\{f(x) \mid x \in U\}$

Useful

1. $(p \vee q) \wedge \sim(p \wedge q) \equiv p \oplus q$
2. $(A \cap B) \cup (A \backslash B) = A$
3. $A \cap B \subseteq A$
4. (Tutorial 4) The following are equivalent:
   (a) $\forall x, y \in A(x \ R \ y \implies y \ R \ x)$
   (b) $R = R^{-1}$
   (c) $\forall x, y \in A(x \ R \ y \iff y \ R \ x)$
5. (Tutorial 4) Relation on $\mathbb{Q}$:
   (a) $xy \geq 0$ is reflexive and symmetric
   (b) $xy \geq 0$ is symmetric and transitive
6. (Quiz 3)
   (a) Order of quantifiers can be freely arranged if all quantifiers are of the same type
   (b) $\forall(P(x) \wedge Q(x)) \iff \forall x P(x) \wedge \forall x Q(x)$
   (c) $\exists(P(x) \vee Q(x)) \iff \exists x P(x) \vee \exists x Q(x)$
7. (Quiz 5)
   (a) $\mathcal{P}(\varnothing) = \{\varnothing\}$ has 1 element and 2 subsets
   (b) For all sets, $B \times A \neq A \times B$
8. (Quiz 6)
   (a) non-symmetric relations which are reflexive $\not\Rightarrow$ they are antisymmetric
   (b) non-symmetric relation which are antisymmetric $\not\Rightarrow$ they are reflexive
   (c) symmetric relations may be antisymmetric or not
   (d) antisymmetric relations may be symmetric or not
   (e) $\min(|R|) = n$ if R is an equivalence relation on A where $|A| = n$
9. (Quiz 7.3/7.4)
   (a) not symmetric may not be antisymmetric
   (b) for finite posets,
      i. any minimal element is not necessarily smallest
      ii. any smallest is minimal
      iii. the smallest element is unique
      iv. $\exists$ smallest *implies* exactly 1 minimal
      v. exactly 1 minimal $\not\Rightarrow$ $\exists$ smallest

Assumptions

1. every integer is even or odd, but not both
2. every rational can be reduced to a fraction in its lowest term