Honors Algebra **Spring 2025**
HW 1: Preliminary Topics **1/28/2025**

Abstract Algebra: An Integrated Approach by J.H. Silverman.
Page 26–34: 1.2, 1.5, 1.7, 1.11, 1.14, 1.16, 1.18

Problem 1 (1.2)**.** Use truth tables to prove the following logical equivalences:

(a) $P \iff \neg(\neg P)$

P	$\neg P$	$\neg(\neg P)$
T	F	T
T	F	T
F	T	F
F	T	F

(b) $\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$

P	Q	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$(\neg P) \wedge (\neg Q)$
T	T	F	F	F	F
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

(c) $(P \implies Q) \iff (\neg Q \implies \neg P)$

P	Q	$P \implies Q$	$\neg P$	$\neg Q$	$\neg Q \implies \neg P$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

(d) $(P \implies Q) \iff (\neg P) \vee Q$

P	Q	$P \implies Q$	$\neg P$	$(\neg P) \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

(e) $(P \iff Q) \iff \neg(P \veebar Q)$

P	Q	$P \iff Q$	$P \veebar Q$	$\neg(P \veebar Q)$
T	T	T	F	T
T	F	F	T	F
F	T	F	T	F
F	F	T	F	T

(f) $P \veebar Q \iff (P \wedge \neg Q) \vee (\neg P \wedge Q)$

P	Q	$P \veebar Q$	$\neg P$	$\neg Q$	$P \wedge \neg Q$	$\neg P \wedge Q$	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$
T	T	F	F	F	F	F	F
T	F	T	F	T	T	F	T
F	T	T	T	F	F	T	T
F	F	F	T	T	F	F	F

(g) $P \veebar Q \iff (P \vee Q) \wedge \neg(P \wedge Q)$

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge \neg(P \wedge Q)$	$P \veebar Q$
T	T	T	T	F	F	F
T	F	T	F	T	T	T
F	T	T	F	T	T	T
F	F	F	F	T	F	F

(h) $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

(i) $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	T	T	F	F
F	F	T	F	T	F	T	F
F	F	F	F	F	F	F	F

Problem 2. (1.5)

(a) Let $\mathbb{E}$ denote the set of even natural numbers. Give a mathematical description of the set $\mathbb{E}$, similar to our description of the set of primes $\mathbb{P}$.

The set $\mathbb{E}$, which consists of even natural numbers, can be described as:

$$\mathbb{E} = \{n \in \mathbb{N} \mid n = 2k \text{ for some } k \in \mathbb{N}\}.$$

In words, $\mathbb{E}$ is the set of all natural numbers that are divisible by 2.

(b) Goldbach's Conjecture says that every even natural number, except for 2, is equal to a sum of two prime numbers. Give a methematical description of Goldbach's conjecture. You may use $\mathbb{P}$ to denote the set of primes and $\mathbb{E}$ to denote the set of even numbers.

Goldbach's Conjecture states that every even natural number greater than 2 can be expressed as the sum of two prime numbers. Using the given notation, we can formally express this as:

$$\forall n \in \mathbb{E}, \quad n > 2 \implies \exists p_1, p_2 \in \mathbb{P} \text{ such that } n = p_1 + p_2.$$

Here, $\mathbb{E} = \{n \in \mathbb{N} \mid n \text{ is even}\}$ represents the set of even natural numbers, and $\mathbb{P}$ denotes the set of prime numbers. The conjecture asserts that for every even $n > 2$, there exist two primes p_1 and p_2 whose sum equals n.

Problem 3 (1.7)**.** Let S, T, and U be sets. Prove each of the following formulas:

(a) $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

Let x be an arbitrary element.

- ($\subseteq$) Suppose $x \in S \cap (T \cup U)$. Then, $x \in S$ and $x \in T \cup U$, meaning x is in at least one of T or U. This implies $x \in (S \cap T)$ or $x \in (S \cap U)$, so $x \in (S \cap T) \cup (S \cap U)$.
- ($\supseteq$) Suppose $x \in (S \cap T) \cup (S \cap U)$. Then, $x \in S \cap T$ or $x \in S \cap U$, meaning $x \in S$ and either $x \in T$ or $x \in U$. This implies $x \in S \cap (T \cup U)$.

Thus, the two sets are equal.

(b) $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$

Let x be arbitrary.

- ($\subseteq$) If $x \in S \cup (T \cap U)$, then either $x \in S$ or $x \in T \cap U$. If $x \in S$, then $x \in S \cup T$ and $x \in S \cup U$, so $x \in (S \cup T) \cap (S \cup U)$. If $x \in T \cap U$, then $x \in T$ and $x \in U$, so $x \in S \cup T$ and $x \in S \cup U$. Thus, $x \in (S \cup T) \cap (S \cup U)$.
- ($\supseteq$) If $x \in (S \cup T) \cap (S \cup U)$, then $x \in S \cup T$ and $x \in S \cup U$. If $x \in S$, then $x \in S \cup (T \cap U)$. Otherwise, $x \in T$ and $x \in U$, so $x \in T \cap U$, implying $x \in S \cup (T \cap U)$.

Thus, the two sets are equal.

(c) Suppose that S and T are subsets of U. Then

$$(S \cup T)^c = S^c \cap T^c \quad \text{and} \quad (S \cap T)^c = S^c \cup T^c$$

Using De Morgan's Laws:

- $(S \cup T)^c = S^c \cap T^c$ because $x \notin S \cup T$ means $x \notin S$ and $x \notin T$, which is exactly $x \in S^c \cap T^c$.
- $(S \cap T)^c = S^c \cup T^c$ because $x \notin S \cap T$ means $x \notin S$ or $x \notin T$, which defines $S^c \cup T^c$.

(d) The *symmetric difference of* S *and* T, denoted $S \Delta T$, is defined to be the set of elements that are in one of S and T, but not in both. Prove that

$$S \Delta T = (S \cup T) \backslash (S \cap T) = (S \backslash T) \cup (T \backslash S)$$

By definition, $S \Delta T$ is the set of elements in S or T, but not both.

- The set $(S \cup T) \setminus (S \cap T)$ consists of elements in $S \cup T$ that are not in $S \cap T$, meaning they are in exactly one of S or T, which matches $S \Delta T$.
- The set $(S \setminus T) \cup (T \setminus S)$ consists of elements in S but not T, or in T but not S, which again matches $S \Delta T$.

Thus, the given expressions for $S \Delta T$ are equal.

Problem 4 (1.11)**.** Which of the follwoing are equivalence relations on the set of integers $\mathbb{Z}$? For the equivalence relations, describe the distinct equivalence classes, and for the non-equivalence relations, explain which of the three properties of an equivalence relation fail.

(a) $a \sim b$ if $a - b$ is a multiple of 5

- *Reflexive:* For any $a \in \mathbb{Z}$, $a - a = 0$, which is a multiple of 5, so $a \sim a$.
- *Symmetric:* If $a \sim b$, then $a - b$ is a multiple of 5, meaning $b - a = -(a - b)$ is also a multiple of 5. Thus, $b \sim a$.
- *Transitive:* If $a \sim b$ and $b \sim c$, then $a - b$ and $b - c$ are multiples of 5. Adding these, $a - c = (a - b) + (b - c)$ is a multiple of 5, so $a \sim c$.

The equivalence classes are the sets of integers that leave the same remainder when divided by 5. For example:

$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}, \quad [1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}, \quad \text{and so on.}$$

(b) $a \sim b$ if $a + b$ is a multiple of 5

This is not an equivalence relation because it fails the transitive property. Let $a = 0$, $b = 3$, and $c = 2$:

- $a \sim b$ because $a + b = 0 + 3 = 3$, which is a multiple of 5.

- $b \sim c$ because $b + c = 3 + 2 = 5$, which is a multiple of 5.
- However, $a + c = 0 + 2 = 2$, which is not a multiple of 5, so $a \not\sim c$.

Thus, the relation is not transitive.

(c) $a \sim b$ if $a^2 - b^2$ is a multiple of 5

- *Reflexive:* For any $a \in \mathbb{Z}$, $a^2 - a^2 = 0$, which is a multiple of 5, so $a \sim a$.
- *Symmetric:* If $a \sim b$, then $a^2 - b^2$ is a multiple of 5. Since $a^2 - b^2 = -(b^2 - a^2)$, $b \sim a$.
- *Transitive:* If $a \sim b$ and $b \sim c$, then $a^2 - b^2$ and $b^2 - c^2$ are multiples of 5. Adding these, $a^2 - c^2 = (a^2 - b^2) + (b^2 - c^2)$, which is a multiple of 5, so $a \sim c$.

The equivalence classes correspond to the remainders of $a^2 \mod 5$. Since the possible remainders of $a^2 \mod 5$ are 0, 1, and 4, there are three equivalence classes:

$$[0], [1], [4].$$

(d) $a \sim b$ if $a - b^2$ is a multiple of 5

This is not an equivalence relation because it fails the symmetric property. For example, let $a = 6$ and $b = 1$:

- $a \sim b$ because $a - b^2 = 6 - 1^2 = 5$, which is a multiple of 5.
- However, $b \sim a$ would require $b - a^2$ to be a multiple of 5, but $1 - 6^2 = 1 - 36 = -35$ is not a multiple of 5.

Thus, the relation is not symmetric.

(e) $a \sim b$ if $a - b$ is purple

This is not an equivalence relation because the definition of the relation is not well-defined. The term "purple" has no mathematical meaning, so the relation cannot satisfy reflexivity, symmetry, or transitivity.

Problem 5 (1.14)**.** Which of the following binary relations are reflexive, symmetric, antisymmetric, and/or transitive? Which are equivalence relations? Which are partial orders?

(a) $S = \mathbb{R}$, and $(a, b)_{\mathcal{B}}$ iff $a \geq b$

- *Reflexive:* Yes, since for all $a \in \mathbb{R}$, we have $a \geq a$.
- *Symmetric:* No, because if $a \geq b$, it does not necessarily mean $b \geq a$ unless $a = b$.
- *Antisymmetric:* Yes, since if $a \geq b$ and $b \geq a$, then $a = b$.
- *Transitive:* Yes, because if $a \geq b$ and $b \geq c$, then $a \geq c$.

Since the relation is reflexive, antisymmetric, and transitive, it is a **partial order**. However, it is not an equivalence relation because it is not symmetric.

(b) $S = \mathbb{N}$, and $(a, b)_{\mathcal{B}}$ iff $\gcd(a, b) = 1$

- *Reflexive:* No, since $\gcd(a, a) = a$, which is not necessarily 1.
- *Symmetric:* Yes, because $\gcd(a, b) = \gcd(b, a)$.
- *Antisymmetric:* No, since there exist distinct a and b such that $\gcd(a, b) = 1$.
- *Transitive:* No, since $\gcd(a, b) = 1$ and $\gcd(b, c) = 1$ does not imply $\gcd(a, c) = 1$.

This relation is not an equivalence relation or a partial order.

(c) $S = \mathbb{N}$, and $(a, b)_{\mathcal{B}}$ iff $a|b$

- *Reflexive:* Yes, since $a|a$ for all $a \in \mathbb{N}$.
- *Symmetric:* No, since $a|b$ does not imply $b|a$ unless $a = b$.
- *Antisymmetric:* Yes, since if $a|b$ and $b|a$, then $a = b$.
- *Transitive:* Yes, since if $a|b$ and $b|c$, then $a|c$.

This relation is a partial order but not an equivalence relation.

(d) S is the set of students at your school, and $(a, b)_{\mathcal{B}}$ iff a and b have the same birthday.

- *Reflexive:* Yes, since everyone shares their own birthday.
- *Symmetric:* Yes, since if a has the same birthday as b, then b has the same birthday as a.
- *Antisymmetric:* No, since two distinct students can have the same birthday.
- *Transitive:* Yes, since if a shares a birthday with b and b shares a birthday with c, then a shares a birthday with c.

This relation is an equivalence relation but not a partial order.

(e) S is a graph, and $(a, b)_{\mathcal{B}}$ iff $a = b$ or there is an edge connecting a and b.

- *Reflexive:* Yes, since $a = a$.
- *Symmetric:* Yes, since if there is an edge from a to b, there is an edge from b to a in an undirected graph.
- *Antisymmetric:* No, unless the graph has no edges.
- *Transitive:* No, since a connected to b and b connected to c does not imply a is connected to c.

This is neither an equivalence relation nor a partial order.

(f) S is a graph, and $(a, b)_{\mathcal{B}}$ iff $a = b$ or a sequence of edges connects a to b.

- *Reflexive:* Yes.
- *Symmetric:* Yes, if the graph is undirected.

- *Antisymmetric:* No, unless the graph is trivial.
- *Transitive:* Yes, since if a is connected to b and b to c, then a is connected to c.

This relation is an equivalence relation for connected components.

(g) $S = \mathbb{R}$, and $f : S \to \mathbb{R}$ is a function, and $(a, b)_{\mathcal{B}}$ iff $f(a) = f(b)$.

Equivalence relation as it satisfies reflexivity, symmetry, and transitivity.

(h) S = (the collection of subsets of a set Σ), and $(A, B)_{\mathcal{B}}$ iff $A \subseteq B$.

Partial order

(i) S = (the collection of subsets of a set Σ), and $(A, B)_{\mathcal{B}}$ iff $A \cap B \neq \emptyset$.

This relation is symmetric but not transitive or reflexive.

(j) S = (the collection of subsets of a set Σ), and $(A, B)_{\mathcal{B}}$ iff $A \cap B = \emptyset$.

This relation is symmetric but neither reflexive nor transitive.

Problem 6 (1.16)**.** Let S and T be finite sets containing the same number of elements, and let $f : S \to T$ be a function from S to T. Prove that the following are equivalent:

(a) f is injective

Since S and T have the same finite number of elements, say $|S| = |T| = n$, an injective function f maps n distinct elements of S to n distinct elements of T. Since T also contains exactly n elements, no element in T can be left out. Thus, f must also be surjective.

(b) f is surjective

If f is surjective, then every element of T has at least one preimage in S. Since $|S| = |T| = n$, the surjectivity ensures that there are exactly n preimages. If f were not injective, then at least one element of T would have more than one preimage in S, contradicting the fact that S has only n elements. Hence, f must be injective.

(c) f is bijective

By definition, a function is bijective if and only if it is both injective and surjective. Since we have shown that injectivity implies surjectivity and vice versa, it follows that f is bijective.

Problem 7 (1.18)**.** Let S and T be finite sets, and let $f : S \to T$ be a function from S to T. Prove that

$$\#S = \sum_{t \in T} \#\{s \in S : f(s) = t\}$$

Each element $t \in T$ has a preimage set given by:

$$S_t = \{s \in S \mid f(s) = t\}.$$

The cardinality of this set is $\#S_t$, which represents the number of elements in S that map to t under f.

Since f is a function, every element $s \in S$ is mapped to exactly one element in T, meaning that the sets S_t for different t are disjoint. Moreover, their union covers all of S, i.e.,

$$S = \bigcup_{t \in T} S_t.$$

By the principle of counting for disjoint unions, we sum the sizes of these sets to obtain:

$$\#S = \sum_{t \in T} \#S_t.$$

Since $\#S_t = \#\{s \in S \mid f(s) = t\}$, we obtain the desired result:

$$\#S = \sum_{t \in T} \#\{s \in S \mid f(s) = t\}.$$