MATH1061
Discrete Mathematics I

Problem Set 4

Michael Kasumagic, sID#: 44302669

Due: 5pm, 25^{th} of October, 2024

Question 1: *(15 marks)*

Let T and F denote logical "true" and "false." Prove your answers to the following:

(a) Is $(\{T, F\}, \wedge)$ a group?

(b) Is $(\{T, F\}, \oplus)$ a group?

(c) Is $(\{T, F\}, \oplus, \wedge)$ a field?

Solution: (a)

$\wedge$	T	F
T	T	F
F	F	F

Table 1: The Cayley Table of $(\{T, F\}, \wedge)$

Claim. $(\{T, F\}, \wedge)$ is not a group.

Proof. To be a group, the given algebraic structure must be closed, associative, contain an identity element, and each element must have an inverse element. We'll test each of these conditions.

> **Closure:** The logical and takes two logical statements (which themselves evaluate to either T or F) and returns a T or a F. Further proof of closure lies in Table 1, the Cayley table for this algebraic structure. Therefore the set $\{T, F\}$ is closed under $\wedge$.
> **Associativity:** $\forall a, b, c \in \{T, F\},\ a \wedge (b \wedge c) = (a \wedge b) \wedge c$. This is law of logical equivilance, namely the law of associativity. Therefore $\{T, F\}$ is associative under $\wedge$.
> **Existence of an Identity:** Take $\iota :=$ True. Then, $\forall a \in \{T, F\},\ \iota \wedge a = a \wedge \iota = a$. Therefore, for the set $\{T, F\}$ under $\wedge$, there exists an identity element.
> **Existence of an Inverse:** $\nexists a \in \{T, F\} : a \wedge F = \iota$. Therefore, for the set $\{T, F\}$ under $\wedge$, there is at least one element without an inverse.

Therefore, $(\{T, F\}, \wedge)$ is not a group. □

Corollary. $(\{T, F\}, \wedge)$ is a monoid.

Solution: (b)

$\oplus$	T	F
T	F	T
F	T	F

Table 2: The Cayley Table of $(\{T, F\}, \oplus.)$

Claim. $(\{T, F\}, \oplus)$ is a group.

Proof. To be a group, the given algebraic structure must be closed, associative, contain an identity element, and each element must have an inverse element. We'll test each of these conditions.

> **Closure:** The logical exclusive-or takes two logical statements (which themselves evaluate to either T or F) and returns a T or a F. Further proof of closure lies in Table 2, the Cayley

table for this algebraic structure. Therefore the set $\{T, F\}$ is closed under $\oplus$.
Associativity: Let $a, b, c \in \{T, F\}$.
Case 1: $c = F$.

$$\begin{aligned} a \oplus (b \oplus c) &= a \oplus (b \oplus F) \\ &= a \oplus b \\ &= (a \oplus b) \oplus F \\ &= (a \oplus b) \oplus c \end{aligned}$$

Case 2: $c = T$.

$$\begin{aligned} a \oplus (b \oplus c) &= a \oplus (b \oplus T) \\ &= a \oplus {\sim} b \\ &= {\sim}(a \oplus b) \\ &= (a \oplus b) \oplus T \\ &= (a \oplus b) \oplus c \end{aligned}$$

Therefore, $\{T, F\}$ is associative under $\oplus$.
Existence of an Identity: Take $\iota = F$. Then $\forall a \in \{T, F\}\,,\ \iota \oplus a = F \oplus a = a$. Therefore, the algebraic structure $(\{T, F\}\,, \oplus)$ does possesses an identity element.
Existence of an Inverse: $\forall a \in \{T, F\}\,,$ take $a^{-1} = a$. Then $a \oplus a^{-1} = a \oplus a = F = \iota$. Therefore, every element of $(\{T, F\}\,, \oplus)$ possesses a corresponding inverse.

Therefore, $(\{T, F\}\,, \oplus)$ is a group. □

Solution: (c)
For the algebraic structure $(\{T, F\}\,, \oplus, \wedge)$ to form a field, $(\{T, F\}\,, \oplus)$ must be an Abelian group, $(\{T, F\} \setminus \{\iota\}\,, \wedge))$ must be an Abelian group, and the distributive property of $\wedge$ over $\oplus$ must hold.

Lemma. $(\{T, F\}\,, \oplus)$ is an Abelian group.

Proof. In question 1c, we proved that $(\{T, F\}\,, \oplus)$ is a group. To be Abelian, $(\{T, F\}\,, \oplus)$ must additionally satisfy commutativity.

Commutativity: $\forall a, b \in \{T, F\}\,,\ a \oplus b = b \oplus a$. Therefore the algebraic structure $(\{T, F\}\,, \oplus)$ is commutative.

Therefore, $(\{T, F\}\,, \oplus)$ is an Abelian group. □

Lemma. $(\{T, F\} \setminus \{\iota\}\,, \wedge)$ is an Abelian group.

Proof. Since, $\iota = F$, the set $\{T, F\} \setminus \{\iota\} = \{T\}$.

Closure: $\forall a \in \{T\}\,,\ a \wedge a = T \in \{T\}$ Therefore, $\{T\}$ is closed under $\wedge$.
Associativity: $\forall a, b, c \in \{T\}\,,\ a \wedge (b \wedge c) = T \wedge (T \wedge T) = T \wedge T = (T \wedge T) \wedge T = (a \wedge b) \wedge c$. Therefore $\{T\}$ is associative under $\wedge$.
Existence of an Identity: Take $i = T$. Then $\forall a \in \{T\}\,,\ a \wedge i = a \wedge T = T = i$. Therefore, under the multiplicative operation $\wedge$, $\{T\}$, has a multiplicative identity.
Existence of an Inverse: $\forall a \in \{T\}\,,$ take $a^{-1} = T$. Then $a \wedge a^{-1} = a \wedge T = T = i$. Therefore, for each element of the set $\{T\}$ under $\wedge$ has a corresponding inverse.
Commutativity: $\forall a, b \in \{T\}\,,\ a \wedge b = T \wedge T = b \wedge a$. Therefore this structure is commutative.

Therefore, $(\{T, F\} \setminus \{\iota\}\,, \wedge)$ is an Abelian group. □

Theorem. $(\{T, F\}\,, \oplus, \wedge)$ is a field.

Proof. We've proven that the additive and multiplicative structures of this algebraic structure are Abelian groups. Finally, we must prove that the multiplicative operation, $\wedge$ distributes over the additive operation $\oplus$.

The additive structure, $(\{T, F\}, \oplus)$ is an Abelian group.
The multiplicative structure, $(\{T, F\} \setminus \{\iota\}, \oplus)$, where ι is the additive identity, taking the value F, is an Abelian group.
Distributivity: $\forall a, b, c \in \{T, F\}$,

a	b	c	$a \wedge b$	$a \wedge c$	$b \oplus c$	$a \wedge (b \oplus c)$	$(a \wedge b) \oplus (a \wedge c)$
T	T	T	T	T	F	F	F
T	T	F	T	F	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	F	F	F	F
F	T	T	F	F	T	F	F
F	T	F	F	F	T	F	F
F	F	T	F	F	T	F	F
F	F	F	F	F	F	F	F

The leftmost columns are identical, which proves that $a \wedge (b \oplus c)$ is logically equivalent to $(a \wedge b) \oplus (a \wedge c)$.
Therefore, for the algebraic structure $(\{T, F\}, \oplus, \wedge)$, distributivity holds.

Therefore, the algebraic structure $(\{T, F\}, \oplus, \wedge)$ is a field. $\square$

Question 2: *(10 marks)*

(a) Prove that the group $(\mathbb{R}, +)$ is isomorphic to the group $(\mathbb{R}_+, \times)$.

(b) Prove that the group $(\mathbb{Z} \times \mathbb{Z}, +)$ is not isomorphic to the group $(\mathbb{Z}, +)$.

Solution: (a) $(\mathbb{R}, +) \cong (\mathbb{R}_+, \times) \iff \exists f : \mathbb{R} \to \mathbb{R}_+$ such that f is isomorphic (bijective [injective and surjective] and homomorphic [satisfies $f(g_1 + g_2) = f(g_1) \times f(g_2),\ \forall g_1, g_2 \in \mathbb{R}$]). We'll prove this by proposing an f, and proving that it is isomorphic.

Claim. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_+, \times)$.

Proof. Take $f : \mathbb{R} \to \mathbb{R}_+,\ x \mapsto \exp(x)$

Bijective:

Injective:
f is injective $\iff \forall a, b \in \mathbb{R},\ f(a) = f(b) \implies a = b$.
Let $a, b \in \mathbb{R}$ and $f(a) = f(b)$. Take the natural logarithm of both sides,
$\ln(f(a)) = \ln(f(b))$,
$\ln(\exp(a)) = \ln(\exp(b))$. This cancels out the exp on both sides, and simplifies to
$a = b$.
$\therefore f$ is injective.

Surjective:
f is surjective $\iff \forall y \in \mathbb{R}_+,\ \exists x \in \mathbb{R} : y = f(x)$.
Given $y \in \mathbb{R}_+$, we take $x = \ln(y)$.
Then, $f(x) = f(\ln(y)) = \exp(\ln(y)) = y$.
$\therefore f$ is surjective.

$\therefore f$ is bijective.

Homomorphic

f is homomorphic $\iff \forall a, b \in \mathbb{R},\ f(a + b) = f(a) \times f(b)$.
Let $a, b \in \mathbb{R}$.
Then $f(a + b) = \exp(a + b) = \exp(a) \times \exp(b) = f(a) \times f(b)$.
$\therefore f$ is homomorphic.

$\therefore f$ is an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}_+, \times)$.
$\therefore (\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_+, \times)$. $\square$

Solution: (b)

A group $(G, \cdot)$ is cyclic if there exists an element, called the generator, $g \in G$ such that every element of G can be expressed as $\mathbb{N} \ni n$ applications of $\cdot$ on g, denoted g^n. To show that $(\mathbb{Z} \times \mathbb{Z}, +)$ is not isomorphic to the group $(\mathbb{Z}, +)$, we can demonstrate that one group is cyclic, and one is not, thus there fundamental structure is incompatible, and isomorphism is impossible.

Claim. $(\mathbb{Z} \times \mathbb{Z}, +)$ is not isomorphic to $(\mathbb{Z}, +)$

Proof.

Is $(\mathbb{Z}, +)$ cyclic

Suppose $n \in \mathbb{Z}$. If $n \geq 0$, take the generator $g = 1$. If $n < 0$, take $g = -1$.

Case 1: $n \geq 0$

$$\begin{aligned} n &= 1 + 1 + \cdots + 1 \text{ (n times)} \\ &= g + g + \cdots + g \text{ (n times)} \\ &= g^n \end{aligned}$$

Case 2: $n < 0$

$$\begin{aligned} n &= -1 - 1 - \cdots - 1 \text{ (n times)} \\ &= g + g + \cdots + g \text{ (n times)} \\ &= g^n \end{aligned}$$

$\therefore$ all elements in $\mathbb{Z}$ can be expressed as g^n.

Therefore, $(\mathbb{Z}, +)$ is cyclic

Is $(\mathbb{Z} \times \mathbb{Z}, +)$ cyclic

Suppose $(\mathbb{Z} \times \mathbb{Z}, +)$ is cyclic.

Then, $\exists (g_1, g_2) \in \mathbb{Z} \times \mathbb{Z} : \forall (a, b) \in \mathbb{Z} \times \mathbb{Z}$,

$(a, b) = (g_1, g_2)^n = (g_1^n, g_2^n) = (g_1 + \cdots + g_1, g_2 + \cdots + g_2)$ (n times) $= (ng_1, ng_2)$.

Take $(a, b) = (1, 0)$.

Then, $a = 1 = ng_1$ and $b = 0 = ng_2$.

This forces us to fix $g_1 = 1$ and $g_2 = 0$.

Now take $(a, b) = (0, 1)$.

There does not exist an n such that $b = 0n$. ※

$\therefore$ there does not exist a generator (g_1, g_2)

which can generate all the other elements of $\mathbb{Z} \times \mathbb{Z}$.

Therefore, $(\mathbb{Z} \times \mathbb{Z}, +)$ is not cyclic.

Therefore, $(\mathbb{Z}, +)$ is cyclic but $(\mathbb{Z} \times \mathbb{Z}, +)$ is not.

Therefore, $(\mathbb{Z} \times \mathbb{Z}, +)$ is not isomorphic to $(\mathbb{Z}, +)$. $\square$

Question 3: (*5 marks*)

Your MATH1061 tutorial class contains 20 people, and together you have all decided to form a party for the coming election.

(a) How many ways could you choose five spokespeople for your party?

(b) How many ways could you choose people for the three leadership roles of president, vice-president, and treasurer?

Note: Give your answer as a single integer. (a) and (b) are independent questions.

Solution: (a)
We're choosing 5 subjects ($r = 5$), from a pool of 20 ($n = 20$). Order does not matter, so we can use nCr to solve this:

$$\begin{aligned}\binom{n}{r} &= \binom{20}{5} \\ &= \frac{20!}{5!(20-5)!} \\ &= \frac{20!}{5!15!} \\ &= \frac{20 \cdot 19 \cdot 18 \cdot 17 \cdot 16}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} \\ &= \frac{1.860.480}{120} \\ &= 15.504\end{aligned}$$

Therefore, there are 15.504 ways to choose 5 spokespeople for our political party.

Solution: (b)
We're choosing 1 subjects for 3 distinct roles ($r = 3$), from a pool of 20, without replacement ($n = 20$). The order matters, since a person could be either a president, a vice-president, or a treasurer, so we can use nPr here:

$$\begin{aligned}\mathrm{P}(n, r) &= \mathrm{P}(20, 3) \\ &= \frac{n!}{(n-r)!} \\ &= \frac{20!}{(20-3)!} \\ &= \frac{20!}{(17)!} \\ &= \frac{20 \cdot 19 \cdot 18}{1} \\ &= 6.840\end{aligned}$$

Therefore, there are 6.840 ways we could arrange the party leadership.

Question 4: *(10 marks)*

Your MATH1061 tutorial class contains 20 people, and together you have all decided to form a party for the coming election. These 20 students consist of 8 from the Science faculty, 9 from the ITEE faculty, and 3 from the Arts faculty (each student belongs to one faculty).

(a) How many ways could you choose people for the three leadership roles of president, vice-president, and treasurer, insisting that these three people come from three different faculties?

(b) How many ways could you choose 5 spokespeople for the party, insisting that there must be at least one spokesperson from each faculty.

Note: Give your answer as a single integer. (a) and (b) are independent questions.

Solution: (a)
We need to arrange 3 faculties into 3 leadership roles. Since the leadership roles are unique, order matters, hence, we'll use nPr for this.
We need to choose 1 student from each of the 3 faculties. Order doesn't matter, so we'll use nCr, but we'll need to do it three times, one of each faculty.
The faculty/leadership arrangements need to be multiiplied by the student/faculty choices. Then we'll arrive at the total number we seek.

$$\begin{aligned}
\mathrm{P}\,(3,3)\cdot\binom{8}{1}\cdot\binom{9}{1}\cdot\binom{3}{1} &= \frac{3!}{(3-3)!}\cdot\frac{8!}{1!(8-1)!}\cdot\frac{9!}{1!(9-1)!}\cdot\frac{3!}{1!(3-1)!}\\
&= \frac{3!}{0!}\cdot\frac{8!}{1!7!}\cdot\frac{9!}{1!8!}\cdot\frac{3!}{1!2!}\\
&= \frac{3!}{1}\cdot\frac{8!}{7!}\cdot\frac{9!}{8!}\cdot\frac{3!}{2!}\\
&= 3!\cdot 8\cdot 9\cdot 3\\
&= 3\cdot 2\cdot 8\cdot 9\cdot 3\\
&= 1.296
\end{aligned}$$

Therefore, there are 1.296 ways to select the party leadership, assuring that each of the 3 faculties are represented.

Solution: (b)
We'll start by calculating the total number of ways to choose 5 spokespeople from a pool of 20 party members. Since order doesn't matter,

$$\binom{20}{5} = \frac{20!}{5!(20-5!)} = \frac{20!}{5!15!} = \frac{20 \cdot 19 \cdot 18 \cdot 17 \cdot 16}{5 \cdot 4 \cdot 3 \cdot 2} = \frac{1.860.480}{120} = 15.504$$

We'll calculate the number of combinations where a whole faculty is completely missing. Science,

$$\binom{9+3=12}{5} = \frac{12!}{5!(12-5)!} = \frac{12!}{5!7!} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2} = \frac{95.040}{120} = 792$$

ITEE,

$$\binom{8+3=11}{5} = \frac{11!}{5!(11-5)!} = \frac{11!}{5!6!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{5 \cdot 4 \cdot 3 \cdot 2} = \frac{55.440}{120} = 462$$

Arts,

$$\binom{9+8=17}{5} = \frac{17!}{5!(17-5)!} = \frac{17!}{5!12!} = \frac{17 \cdot 16 \cdot 15 \cdot 14 \cdot 13}{5 \cdot 4 \cdot 3 \cdot 2} = \frac{742.560}{120} = 6.188$$

Next, we'll calculate the number of cominations where only a single faculty is represented among spokespeople. Science,

$$\binom{8}{5} = \frac{8!}{5!(8-5)!} = \frac{8!}{5!3!} = \frac{8 \cdot 7 \cdot 6}{3 \cdot 2} = \frac{336}{6} = 56$$

ITEE,

$$\binom{9}{5} = \frac{9!}{5!(9-5)!} = \frac{9!}{5!4!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} = \frac{3024}{24} = 126$$

Arts,

$$\binom{3}{5} = 0, \text{ We can't choose 5 from a pool of 3.}$$

We're applying the Inclusion-Exclusion principle here. We take the total number of combinations, remove from that total the combinations for which particular faculties are not chosen, and we add back combinations the number of combinations for which single faculties are represented, which undoes the double removal of some combinations originally removed.

$$15.504 - 792 - 462 - 6.188 + 56 + 126 + 0 = 8.244$$

Therefore, our final answer, the number of ways we can choose 5 spokespeople from a pool of 20 party members, assuring that each of 3 faculties is represented.

Question 5: *(10 marks)*

Consider points (x, y) on the 2-D plan $\mathbb{R} \times \mathbb{R}$. Let $S = \{(x, y) \mid 0 \le x, y \le 1\}$. That is, S represents a unit square including its boundary. Prove that S has the same cardinality as the entire $\mathbb{R} \times \mathbb{R}$ plane.

Solution: To prove that two sets have the same cardinality, we must prove that there exists a bijection between the two sets. This may be tricky, which is why we'll apply the Schröder-Bernstein theorem, which states that

$$\exists f : A \to B, g : B \to A \text{ such that } f \text{ and } g \text{ are injective} \implies \exists h : A \to B \text{ such that } h \text{ is bijective.}$$

This simplifies our problem because instead of needing to find a bijection, we can find two injections.

Claim. $|S| = |\mathbb{R} \times \mathbb{R}|$

Proof.
An injection from S to $\mathbb{R} \times \mathbb{R}$
Take $f : S \to \mathbb{R} \times \mathbb{R},\ (s_1, s_2) \mapsto (s_1, s_2)$.
Then, suppose $(a_1, a_1), (b_1, b_2) \in S$ and $f(a_1, a_2) = f(b_1, b_2)$.
Hence, $f(a_1, a_2) = (a_1, a_2) = (b_1, b_2) = f(b_1, b_2)$.
Therefore $(a_1, a_2) = (b_1, b_2)$
Therefore, the proposed $f : S \to \mathbb{R} \times \mathbb{R}$ is injective.

An injection from $\mathbb{R} \times \mathbb{R} \to S$
Take $g : \mathbb{R} \times \mathbb{R} \to S,\ (x, y) \mapsto \left(\frac{1}{2} + \frac{1}{\pi} \arctan(x),\ \frac{1}{2} + \frac{1}{\pi} \arctan(y)\right)$
The domain of $\arctan x$ is $\mathbb{R}$.
The codomain of $\arctan x$ is the open interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.
So, the codomain of $\frac{1}{\pi} \arctan x$ is the open interval $\left(-\frac{1}{2}, \frac{1}{2}\right)$.
Finally, the codomain of $\frac{1}{2} + \frac{2}{\pi} \arctan x$ is the open interval $(0, 1)$.
Therefore the codomain of our proposed injective function g is
$\{(x, y) \mid x \in (0, 1), y \in (0, 1)\} \subseteq S$.

Suppose $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$, and $f(x_1, y_1) = f(x_2, y_2)$.
Then $\frac{1}{2} + \frac{1}{\pi} \arctan(x_1) = \frac{1}{2} + \frac{1}{\pi} \arctan(x_2)$. Taking $\frac{1}{2}$ from both sides,
leaves $\frac{1}{\pi} \arctan(x_1) = \frac{1}{\pi} \arctan(x_2)$. Multiplying both sides by π,
leaves $\arctan(x_1) = \arctan(x_2)$. Finally, taking the tan of both sides,
leaves $\tan(\arctan(x_1)) = \tan(\arctan(x_1))$.
Since arctan is the inverse of tan, they cancel out one another, leading to the conclusion that $x_1 = x_2$.

We use the same argument and procedure to show that $y_1 = y_2$.

Therefore $(x_1, y_1) = (x_2, y_2)$.
Therefore the proposed function $g : \mathbb{R} \times \mathbb{R} \to S$ is injective.

Therefore, there exist injections from $S \to \mathbb{R} \times \mathbb{R}$ and $\mathbb{R} \times \mathbb{R} \to S$.
Therefore, by the Schröder-Bernstein theorem, there exists a bijection from $S \to \mathbb{R} \times \mathbb{R}$ to $\mathbb{R} \times \mathbb{R} \to S$
Therefore, because there exists a bijective function between the two sets, $|S| = |\mathbb{R} \times \mathbb{R}|$. $\square$