## Question 1

Let $H$ and $K$ be subgroups of $G$. Prove that $H \cup K$ is a subgroup if and only if $H \subset K$ or $K \subset H$.

**Solution:** Notice that if $H \subset K$ then $H \cup K = K$ or if $K \subset H$ then $H \cup K = H$

($\Longrightarrow$) :

Assume that $H \not\subset K$ and $K \not\subset H$, where $H$ and $K$ are subgroup of $G$, Then, find an element $h \in H$ such that $h \notin K$ and $k \in K$ such that $k \notin H$. It is clear that the elements exists as both $H$ and $K$ are not a subset of the other one.

Consider $h \cdot k$, if $h \cdot k = \alpha$ for some $\alpha \in H$, then we get that $h \cdot k = \alpha = hh^{-1}\alpha = h(h^{-1}\alpha)$ which means that $k = h^{-1}\alpha \in H$. However, it contradicts with the assumption, so $h \cdot k \notin H$

Consider in the same manner that $h \cdot k = \beta$ for some $\beta \in K$, then we get that $h \cdot k = \beta = \beta k^{-1}k = (\beta k^{-1})k$ which means that $h^{\beta}k^{-1} \in K$. Which, again, contradicts with the assumption, so $h \cdot k \notin K$

Therefore, $h \cdot k \notin H \cup K$, which asserts that $H \cup K$ cannot be a subgroup of $G$ by contraposition.

($\Longleftarrow$) :

Since either of $K \cup H = K$ or $H \cup K = H$ holds and that $H$ and $K$ are both subgroup, then it follows that $K \cup H$ must be a subgroup of $G$

## Question 2

Prove that the subset $T_n(\mathbb{R}) = \{\, A \in GL_n(\mathbb{R}) \mid A_{ij} = 0 \text{ if } i < j \,\}$ of the group $GL_n(\mathbb{R})$ is a subgroup.

**Solution:** Firstly, $T_n(\mathbb{R})$ is not empty, as $I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & 0 \\ \vdots & & 1 & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \in T_n(\mathbb{R})$

### Claim 1

$\forall A, B \in T_n(\mathbb{R}),\ AB \in T_n(\mathbb{R})$

***Proof:*** Firstly, From the definition, for all $A, B \in T_n(\mathbb{R})$, $A_{ij} = B_{ij} = 0$ for $i < j$. And

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}$$

by the definition of matrix multiplication. So if $i < k$, then $A_{ik} = 0$ and if $k < j$, then $B_{kj} = 0$. But either $i < k$ or $k < j$ holds if $i < j$. Therefore,

$$\text{for } i < j,\ (AB)_{ij} = \sum_{k=1}^{n} 0$$

Which proves that $AB \in T_n(\mathbb{R})$ □

### Claim 2

$\forall A \in T_n(\mathbb{R}),\ A^{-1} \in T_n(\mathbb{R})$

***Proof:*** Let $M$ be an $n \times n$ matrix, and $M^{-1}$ be the inverse. Then,

$$(M^{-1}M)_{ij} = \sum_{k=1}^{n} M_{ik}^{-1}M_{kj} = I_{ij}$$

So for $j > i$,

$$0 = \sum_{k=1}^{n} M_{ik}^{-1} M_{kj} = \sum_{k=1}^{i} M_{ik}^{-1} M_{jk} + \sum_{k=i+1}^{n} M_{ik}^{-1} M_{jk} = \sum_{k=i+1}^{n} M_{ik}^{-1} M_{jk}$$

If an inverse of the matrix would exists, then it would have to be in the form that $\forall j > i \; M_{ij}^{-1} = 0$, which means that it must need to be an element of $T_n(\mathbb{R})$ □

Since $\forall A, B \in T_n(\mathbb{R})$, $A^{-1} \in T_n(\mathbb{R})$ and $AB \in T_n(\mathbb{R})$, then $T_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$

## Question 3

Let $D_{2n}$ denote the dihedral group of order $2n$. Show that $\{ g \in D_{2n} \mid g^2 = 1 \}$ is not a subgroup of $D_{2n}$.

**Solution:** Let $S(G)$ denotes the set $\{ g \in G \mid g^2 = 1 \}$ for simplicity.
Consider only for $n \geq 3$, then

$$S(D_{2n}) = \{ 1, f, fr, \ldots, fr^{n-1}, (r^{n/2} \text{ if n is even}) \} \subset D_{2n}$$

By the definition of the operator $(\cdot)$ of $D_{2n}$, $f \cdot fr = r \notin S(D_{2n})$. Therefore, $S(D_{2n})$ does not have closure over $\cdot$. Which means that $S(D_{2n})$ is not a subgroup of $D_{2n}$

## Question 4

Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any field $F$.

**Solution:** Notice that $GL_n(F)$ is a group, since it has closure, associative, has identity $I_n$ and has inverse.

**Claim 3**
$a \times 0 = 0$

***Proof:*** since $a \times 0 = a \times (0 + 0) = (a \times 0) + (a \times 0)$ □

For $n = 2$, let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ Then, $AB = \begin{bmatrix} 1+1 & 1 \\ 1 & 1 \end{bmatrix}$ but $BA = \begin{bmatrix} 1 & 1 \\ 1 & 1+1 \end{bmatrix}$. Therefore, $\cdot$ is commutative if and only if $1 + 1 = 1$, but $1 + 1 \neq 1$ since 1 cannot be the additive identity. So $GL_2(F)$ is non-abelian, since it is non-commutative.
Assume for induction, that $GL_n(F)$ is non-abelian, and that $AB \neq BA$. Then we can construct

$$A' = \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix} \text{ and } B' = \begin{bmatrix} B & 0 \\ 0 & 1 \end{bmatrix}$$

Then

$$A'B' = \begin{bmatrix} AB & 0 \\ 0 & 1 \end{bmatrix} \text{ but } B'A' = \begin{bmatrix} BA & 0 \\ 0 & 1 \end{bmatrix}$$

However, $AB \neq BA$, so $A'B' \neq B'A'$ certifies that $GL_n(F)$ is not commutative.
By induction, $GL_n(F)$ is non-commutative, hence, they are non-abelian groups.

## Question 5

Suppose that $G$ is a group such that $(gh)^2 = g^2h^2$ for all $g, h \in G$. Show that $G$ is abelian

**Solution:** For a group $G$ we get that $g^{-1} \in G$ for $g \in G$. Therefore, $\forall g, h$

$$hg = g^{-1}ghghh^{-1} = g^{-1}(gh)^2h^{-1} = g^{-1}(g^2h^2)h^{-1} = gh$$

So, $\forall g, h \in G, \; gh = hg$, which means that $G$ is an abelian group.

## Question 6

Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

**Solution:** Notice that $i = \sqrt{-1} \in \mathbb{C} - \{0\}$ and the order of $i$ is 4 since $i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$ and $i^4 = 1$

However, suppose that there is an element $g \in \mathbb{R} - 0$ such that $g^4 = 1$, then $g^2 = 1$, which will result in $g$ having the order 2, or $g^2 = -1$. However, there is no such $g \in \mathbb{R} - \{0\}$ such that $g^2 = -1$. Therefore, there cannot exists an isomorphism $\phi : \mathbb{C} - 0 \to \mathbb{R} - \{0\}$, since if there is such $\phi$, then $\phi(i)^2 = \phi(-1)$, which means that $\phi(i) \notin \mathbb{R} - \{0\}$.

Hence, there is no such isomorphism between $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$, so they are not isomorphic.

## Question 7

Let $G$ be a finite group and let $x$ and $y$ be distinct elements of order 2 in $G$ that generate $G$. Prove that $G \simeq D_{2n}$, where $n = |xy|$

**Solution:** For distinct $x$, $y$ of order 2 that generate $G$, notice that $x^{-1} = x$ and $y^{-1} = y$.

### Claim 4

All element $g \in G$ can be written as $x^p(xy)^k$ for some $k \in \mathbb{N}$ such that $0 \leq k \leq n-1$ and $p \in \{0, 1\}$.

***Proof:*** Consider if there is some element $g$ that contain consecutive $x$, say $g = axxb$ for certain $a, b \in G$, then $g = axxb = a1b = ab$. Similar argument is valid to show that there will be no consecutive $y$.

So an element $g \in G$ must be a string of alternating $x$ and $y$. If the string starts with $x$, then it is of the form $(xy)^k$, and if it starts with a $y$, then it is of the form $x(xy)^k$ since $x(xy) = y$. Note that it will be shown later on that the string will never terminate on $x$

Additionally, for an element that terminates with $x$, or is in the form of $g = x^p(xy)^k y$ for some $k \in \mathbb{N}$ and $p \in \{0, 1\}$, consider $y(xy)^{n-k}(xy)^k y = 1$, so $y(xy)^{n-k} = (xy)^k y$, which implies $x^p(xy)^k y = x^{1-p}(xy)^{n-k+1}$ shows the equivalent to the mentioned form □

So,

$$\forall g \in G \, \exists k \in \mathbb{N}, 0 \leq k \leq n-1, \quad g = x^p(xy)^k$$

where $p$ is either 1 or 0

### Claim 5

Furthermore, the representation mentioned above is unique for all element $g \in G$.

***Proof:*** Assume that for $g \in G$, $g = x^p(xy)^k = x^{p'}(xy)^{k'}$, then

$$x^{p-p'}(xy)^{k-k'} = 1$$

So, if $p \neq p'$, then $(xy)^{k-k'} = x$, which is impossible. Since $xy \neq x$ and $xy \neq y$, and $(xy)^2 = x(yxy) \neq x(1)$ since $y(xy) \neq y(y)$, and inductively for all integer $m$

Otherwise, if $p = p'$, then $(xy)^{k-k'} = 1$, but $0 \leq k - k' \leq n-1$, so $k - k' = 0$, otherwise, $n$ is not the order of $xy$. Therefore, $p = p'$ and $k = k'$. □

Then consider a homomorphism $\phi : G \to D_{2n}$ such that $\phi : x(xy)^n \mapsto fr^n$ and $\phi : (xy)^n \mapsto r^n$, for an $r$ and $f$ in $D_{2n}$

Since the representation of $g \in G$ as $x^p(xy)^k$ for $p \in \{0, 1\}, k \in \mathbb{N}$ is unique, then $\phi$ is well-defined and injective. And since a representation of $d \in D_{2n}$ as $f^p r^k$ for $p \in \{0, 1\}, k \in \mathbb{N}$ is also unique in similar manner, then $\phi$ is surjective.

Therefore, $\phi$ is an isomorphism that asserts $G \simeq D_{2n}$

## Question 8

Let $\sigma \in S_8$ be a permutation such that

$$\sigma(1) = 3, \sigma(2) = 6, \sigma(3) = 4, \sigma(4) = 1, \sigma(5) = 8, \sigma(6) = 2, \sigma(7) = 5, \sigma(8) = 7$$

Express this permutation as a product of disjoint cycles and a product of transpositions.

**Solution:** Consider $\sigma^* = (134) \circ (26) \circ (587)$, where $\circ$ denotes composition and $\phi = (a_1 a_2 \dots a_n)$ denotes a cyclic permutation of size $n$ such that

$$\phi(a_1) = a_2,\ \phi(a_2) = a_3,\ \dots,\ \phi(a_n) = a_1 \quad \text{and } \phi(x) = x \text{ for other } x \neq a_i$$

Therefore, it is trivial to check that $\sigma_*$ satisfies that condition of $\sigma$ in the statement. As

$$\begin{aligned}
\sigma^*(1) &= [(134) \circ (26) \circ (587)](1) = [(134) \circ (26)](1) = [(134)](1) = 3 \\
\sigma^*(2) &= [(134) \circ (26) \circ (587)](2) = [(134) \circ (26)](2) = [(134)](6) = 6 \\
\sigma^*(3) &= [(134) \circ (26) \circ (587)](3) = [(134) \circ (26)](3) = [(134)](3) = 4 \\
\sigma^*(4) &= [(134) \circ (26) \circ (587)](4) = [(134) \circ (26)](4) = [(134)](4) = 1 \\
\sigma^*(5) &= [(134) \circ (26) \circ (587)](5) = [(134) \circ (26)](8) = [(134)](8) = 8 \\
\sigma^*(6) &= [(134) \circ (26) \circ (587)](6) = [(134) \circ (26)](6) = [(134)](2) = 2 \\
\sigma^*(7) &= [(134) \circ (26) \circ (587)](7) = [(134) \circ (26)](5) = [(134)](5) = 5 \\
\sigma^*(8) &= [(134) \circ (26) \circ (587)](8) = [(134) \circ (26)](7) = [(134)](7) = 7
\end{aligned}$$

Notice that all of the cycles are disjoint. Furthermore, a cycle (134) is equivalent to a composition of transpositions $(14) \circ (13)$ and also (587) is equivalent to a composition of transpositions $(57) \circ (58)$. I shall prove the claim

### Claim 6

a cycle $(abc)$ is the same permutation as the composition $(ac) \circ (ab)$

***Proof:*** let $p$ be a permutation of $(ac) \circ (bc)$. Then the followings holds

$$\begin{aligned}
p(a) &= [(ac) \circ (ab)](a) = [(ac)](b) = b \\
p(b) &= [(ac) \circ (ab)](b) = [(ac)](a) = c \\
p(c) &= [(ac) \circ (ab)](c) = [(ac)](c) = a \\
\forall x \notin \{a, b, c\}\ p(x) &= [(ac) \circ (ab)](x) = [(ac)](x) = x
\end{aligned}$$

which agrees with the definition of $(abc)$, therefore $p = (abc)$. □

Thus, $(134) \circ (26) \circ (587) = (14) \circ (13) \circ (26) \circ (57) \circ (58)$. And it is possible to verify that $(14) \circ (13) \circ (26) \circ (57) \circ (58)$ satisfies the condition of $\sigma$ in the statement.

## Question 9

Write out multiplication tables for $D_6$ and $S_3$. Do they have the same structure?

**Solution:** Note that the multiplication table would be written so that the first column goes to the right hand side of the binary operator.

Notice that both table shows similar structure. Also, when applying the map $\phi$ as follows,

$$\begin{aligned}
\phi : r &\mapsto (123) \\
\phi : f &\mapsto (12)
\end{aligned}$$

and extends according to the multiplication rules. We can see that the multiplication table 1 over $\phi$ is exactly the same as table 2

| $\times$ | $e$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
| $r$ | $r$ | $r^2$ | $e$ | $fr^2$ | $f$ | $fr$ |
| $r^2$ | $r^2$ | $e$ | $r$ | $fr$ | $fr^2$ | $f$ |
| $f$ | $f$ | $fr$ | $fr^2$ | $e$ | $r$ | $r^2$ |
| $fr$ | $fr$ | $fr^2$ | $f$ | $r^2$ | $e$ | $r$ |
| $fr^2$ | $fr^2$ | $f$ | $fr$ | $r$ | $r^2$ | $e$ |

Table 1: the multiplication table of $D_6$

| $\times$ | $I$ | (123) | (132) | (12) | (23) | (13) |
|---|---|---|---|---|---|---|
| $I$ | $I$ | (123) | (132) | (12) | (23) | (13) |
| (123) | (123) | (132) | $I$ | (13) | (12) | (23) |
| (132) | (132) | $I$ | (123) | (23) | (13) | (12) |
| (12) | (12) | (23) | (13) | $I$ | (123) | (132) |
| (23) | (23) | (13) | (12) | (132) | $I$ | (123) |
| (13) | (13) | (12) | (23) | (123) | (132) | $I$ |

Table 2: the multiplication table of $S_3$

**Question 10**

Let $G$ be an abelian group. Prove that $\{\, g \in G \mid |g| < \infty \,\}$ is a subgroup of $G$ (called the torsion subgroup of $G$). Give an explicit example where this set is not a subgroup when $G$ is non-abelian.

**Solution:** Let denote the set $\{\, g \in G \mid |g| < \infty \,\}$ as $S$ Firstly, notice that for $g, h \in S$, $gh \in S$.

Consider $g, h \in S$, there exists $n, m \in \mathbb{N}$ such that $g^n = h^m = 1$ since the order of $g$ and $h$ is finite. Therefore,

$$(g^n)^m = (h^m)^n = 1 = g^{nm} = h^{nm}$$

Therefore $g^{nm}h^{nm} = 1$. Lastly, since $G$ is abelian, $gh = hg$, which asserts that

$$g^{nm}h^{nm} = (gh)^{nm} = 1$$

Hence, the fact that the order of $gh$ is bounded by $nm$ ensures that

$$gh \in \{\, g \in G \mid |g| < \infty \,\}$$

Morover, for $g \in S$, the inverse $g^{-1} \in S$ exists

Consider an element $g \in S$, then there exists some integer $n \in \mathbb{N}$ such that $g^n = 1$. From there, $g^{n-1}g = gg^{n-1} = 1$, which means that $g^{n-1} = g^{-1}$ by definition. Note that

$$g^{n-1^n} = g^{nn-1} = 1^{n-1} = 1$$

Since the order of $g^{-1}$ is bounded by $n$, then $g^{-1} \in S$.

Therefore, since $S$ has a closure over the operator, and the inverse of each element is contained within $S$, Then $S$ is a subgroup of $G$.

For a counterexample when $G$ is not abelian, consider $GL_2(\mathbb{R})$. There exist $A = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ such that $AB = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Then it is easy to verify that $A^2 = I = B^2$, but $(AB)^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$