Question 1

Let m, n, a_i, and $1 \leq i \leq m$ be integers.
Prove that if $\gcd(a_i, n) = 1$ for all $1 \leq i \leq m$, then $\gcd(a_1 \cdots a_m, n) = 1$.

Solution: for m = 1, $\gcd(a_1, n) = 1$ then $\gcd(a_1, n) = 1$ obviously.

Claim 1

Ig $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ then $\gcd(ab, n) = 1$.

Proof: If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ then $\exists p, q, r, s \in \mathbb{N}$ such that $ap + nq = br + ns = 1$.

$$\begin{aligned} 1 &= (ap + nq)(br + ns) \\ &= (abpr + nbqr + nasp + nnqs) \\ &= ab(pr) + n(bqr + asp + nqs) \end{aligned}$$

Hence, $\gcd(ab, n) = 1$ □

From claim 1, the proposition holds at $m = 2$, by substituting a with a_1 and b with a_2. Then assuming that the argument holds for integer k. By assumption, $\gcd(a_1 \cdots a_k, n) = 1$. Therefore, it is possible to substitute a of claim 1 with $a_1 \cdots a_k$ and b with a_{k+1}.

Hence, the proposition holds true for all integer $m \geq 1$, for all integer n, by induction.

Question 2

Let $M_n(\mathbb{R}) = \{n \times n \text{ real matrices}\}$. Define a relation $\sim$ on $M_n(\mathbb{R})$ as follow:
$A \sim B$ if there exists an invertible $C \in M_n(\mathbb{R})$ such that $A = CBC^{-1}$. Show that this relation is an equivalence relation.

Solution: The relation $\sim$ would be an equivalence relation if it is symmetric, reflexive, and transitive.

- **Reflexive:** There exists the identity matrix $I \in M_n(\mathbb{R})$. Since
$$I^{-1} = I, \quad IA = AI = A$$
for all matrices A,
$$A = IAI^{-1}$$
Therefore, $A \sim A$.
- **Symmetric:** Assume that for some $A, B \in M_n(\mathbb{R})$, $A \sim B$. Then it follows that
$$\exists C,\ A = CBC^{-1}$$
By multiplying C and C^{-1},
$$C^{-1}AC = C^{-1}A(C^{-1})^{-1} = B$$
Since C^{-1} is also an $n \times n$ matrix, $C^{-1} \in M_n(\mathbb{R})$. Hence, $B \sim A$.
- **Transitive:** Assume for $X, Y, Z \in M_n(\mathbb{R})$, so that $X \sim Y$ and $Y \sim Z$. Then it follows that
$$\text{there exists } C, D \text{ such that } X = CYC^{-1},\ Y = DZD^{-1}$$
Then by substituting the second equation into the first,
$$X = CDZD^{-1}C^{-1}$$
Notice that CD is an $n \times n$ matrix since both C and D are an $n \times n$ matrix. Moreover,
$$\begin{aligned} CD \cdot D^{-1}C^{-1} &= C(DD^{-1})C^{-1} \\ &= CC^{-1} \\ &= I \end{aligned}$$

and

$$\begin{aligned} D^{-1}C^{-1} \cdot CD &= D^{-1}(C^{-1}C)D \\ &= D^{-1}D \\ &= I \end{aligned}$$

by the associativity of matrix multiplication. So $(CD)^{-1} = D^{-1}C^{-1}$ by definition. Therefore, $X \sim Z$.

As the relation is symmetric, reflexive, and transitive, it is an equivalence relation.

Question 3

Let H be a non-empty subset of a group G. We define a relation on G by $a \sim b$ if and only if $ab^{-1} \in H$. Prove that H is a subgroup of G if and only if the relation $\sim$ is an equivalence relation.

Solution: Let the operator of the group G be $(\cdot)$, write briefly by juxtaposition.

$(\Longrightarrow)$ Assume that H is a subgroup of G. Then

- **Reflexive:** Since $aa^{-1} = 1 \in H$, $a \sim a$ by definition.
- **Symmetric:** Assuming that $a \sim b$, then $ab^{-1} \in H$. But since $ab^{-1}ba^{-1} = 1$, then $ba^{-1} \in H$. Which means that $b \sim a$.
- **Transitive:** Assuming that $a \sim b$, and $b \sim c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$. Since H has closure over $(\cdot)$, then $ab^{-1} \cdot bc^{-1} = ac^{-1} \in H$. Thus, $a \sim c$ by definition.

Therefore, the relation $\sim$ is an equivalence relation.

$(\Longleftarrow)$ Assume that $\sim$ is an equivalence relation. Then

- **Closure:** Assuming that $a, b \in H$, then $1 \sim a$ and $1 \sim b^{-1}$. Hence, $a \sim b^{-1}$, which means that $ab \in H$.
- **Associativity:** Since the operator $(\cdot)$ is associative over G. The restriction of the operator over H must also be associative.
- **Identity:** Since $a \sim a$, then $aa^{-1} = 1 \in H$
- **Inverse:** Assuming that $ab^{-1} \in H$, then $a \sim b$. Then $b \sim a$ by reflexivity. Therefore, $ba^{-1} \in H$. Note that $ba^{-1}ab^{-1} = 1 = ab^{-1}ba^{-1}$. Hence, $(ab^{-1})^{-1} = ba^{-1}$ by the definition.

Therfore, as H is non-empty, H is a subgroup of G.

Question 4

Compute $(\mathbb{Z}/12\mathbb{Z})^{\times}$

Solution: $\mathbb{Z}/12\mathbb{Z} = \{\bar{0}, \dots, \bar{1}\bar{1}\}$ where $\bar{n}$ is the equivalence class of integer n modulo 12. $(\mathbb{Z}/12\mathbb{Z})^{\times}$ is the subset of elements with inverse. Consider that $\bar{1}$ is identity of multiplication since

$$\bar{1} \times \bar{n} = \bar{n} \times \bar{1} = \bar{n}$$

This is due to the fact that $\bar{n}$ is the equivalence class for $12m + n$ for some integer m, and that

$$(12m + 1)(12k + n) = 12(12mk + k + mn) + n$$

Claim 2

if $\gcd(n, 12) \neq 1$ then $\bar{n} \notin (\mathbb{Z}/12\mathbb{Z})^{\times}$

> ***Proof:*** let $d = \gcd(n, 12)$ and $\bar{n}$ is the equivalence class of $12m + n$. But
>
> $$d \mid 12m + n$$
>
> By assumption, $d \neq 1$. Now assume for contradiction that there exists $\bar{x}$ such that $\bar{x} \times \bar{n} = 1$. Then,
>
> $$(12m + n)(12k + x) = (12q + 1)$$
>
> contradicts that $d \mid 12m + n$ since $d \nmid 12m + 1$ Therefore, there exists no inverse of $\bar{n}$, thus $\bar{n} \notin (\mathbb{Z}/12\mathbb{Z})^{\times}$. $\square$

Therefore, $(\mathbb{Z}/12\mathbb{Z})^{\times} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$ as it is easy to see that $\bar{1}^2 = \bar{5}^2 = \bar{7}^2 = \bar{11}^2 = \bar{1}$

Question 5

(1) Let $G = \mathbb{R}\backslash\{-1\}$. Define an operation - by $a \cdot b = a + b + ab$. Show that $(G, \cdot)$ is a group.
(2) Let $G = \{a + b\sqrt{11} \mid a, b \in \mathbb{Q}\}$ be a subset of $\mathbb{R}$. Show that $(G\backslash\{0\}, \cdot)$ is a group, where $\cdot$ is the usual multiplication.

Solution:
(1)

let $u, v, w \in G$. Then,

- **Well-definedness:** Since addition and multiplication is well-defined in $\mathbb{R}$, then $(\cdot)$ is well-defined since it is a composition of well-defined operators.
- **Closure:** for $a, b \in \mathbb{R}$, $ab, a+b \in \mathbb{R}$ by the closure of addition and multiplication over real number. Assuming that $a + b + ab = -1$ yields that

$$\begin{aligned} 0 &= a + b + ab + 1 \\ &= a(1 + b) + (1 + b) \\ &= (a + 1)(b + 1) \end{aligned}$$

  Therefore, if $a \neq -1$ and $b \neq -1$, then $a \cdot b \neq -1$ Hence, $(\cdot)$ has a closure in G.
- **Associativity:** Consider $(u \cdot v) \cdot w$,

$$\begin{aligned} (u \cdot v) \cdot w &= (u + v + uv) \cdot w \\ &= u + v + uv + w + uw + vw + uvw \\ &= u + (v + w + vw) + (uw + vw + uvw) \\ &= u + (v + w + vw) + u(v + w + vw) \\ &= u \cdot (v + w + vw) \\ &= u \cdot (v \cdot w) \end{aligned}$$

  Hence, $(\cdot)$ is associative.
- **Identity:** Consider $0 \in G$, and $0 \cdot u = 0 + u + 0u = u$, and $u \cdot 0 = u + 0 + u0 = u$. So, $0 \in G$ is the identity.
- **Inverse:** Consider $u^{-1} = \frac{-u}{1+u}$. Then since $u \neq -1$, $u^{-1} \in G$. Morover,

$$\begin{aligned} u^{-1} \cdot u &= \frac{-u}{1+u} + u + \frac{-u}{1+u}u \\ &= \frac{u^2 - u^2 + u - u}{1+u} \\ &= 0 \end{aligned}$$

  And also,

$$\begin{aligned} u \cdot u^{-1} &= u + \frac{-u}{1+u} + u\frac{-u}{1+u} \\ &= \frac{u^2 - u^2 + u - u}{1+u} \\ &= 0 \end{aligned}$$

Therefore, u^{-1}, the inverse of u, exists in G.

Hence, $(G, \cdot)$ is a group.

(2)

Let $u, v, w \in G \backslash \{0\}$, and let $u = u_a + u_b\sqrt{11}$, $v = v_a + v_b\sqrt{11}$, and $w = w_a + w_b\sqrt{11}$ for $u_a, u_b, v_a, v_b, w_a, w_b \in \mathbb{Q}$.Then,

- **Well-definedness:** Since $G \subset \mathbb{R}$ and multiplication is well-defined under $\mathbb{R}$, the operation must also be well-defined under $G \backslash \{0\}$.
- **Closure:**

$$\begin{aligned} uv &= (u_a + \sqrt{11}u_b)(v_a + \sqrt{11}v_b) \\ &= u_a v_a + u_a v_b\sqrt{11} + u_b v_a\sqrt{11} + 11u_b v_b \\ &= (u_a v_a + 11u_b v_b) + (u_a v_b + u_b v_a)\sqrt{11} \end{aligned}$$

  Since $u_a v_a + 11u_b v_b \in \mathbb{Q}$ and $u_a v_b + u_b v_a \in \mathbb{Q}$. Moreover, both term cannot be 0 simultaneously. Thus, $G \backslash \{0\}$ has a closure.
- **Identity:** Consider $1 \in G \backslash \{0\}$ and that $1u = u1 = u_a + \sqrt{11}u_b = u$. So $1 \in G \backslash \{0\}$ is the identity.
- **Inverse:** Consider x for each fixed u, such that

$$x = \frac{-u_a}{-u_a^2 + 11u_b^2} + \frac{u_b}{-u_a^2 + 11u_b^2}\sqrt{11}$$

  It is easy to verify that $x \in G \backslash \{0\}$. Then, it will follow that

$$\begin{aligned} xu &= \left(\frac{-u_a}{-u_a^2 + 11u_b^2} + \frac{u_b}{-u_a^2 + 11u_b^2}\sqrt{11} \right)(u_a + u_b\sqrt{11}) \\ &= \left(\frac{-u_a^2 + 11u_b^2 + \sqrt{11}(u_a u_b - u_b u_a)}{-u_a^2 + 11u_b^2} \right) \\ &= 1 + 0\sqrt{11} = 1 \end{aligned}$$

  And since $(\cdot)$ is commutative $ux = xu = 1$, Therefore, $u^{-1} = x$ by definition.

Hence, $G \backslash \{0\}$ is a group under multiplication.

Question 6

Show that $\mathbb{Z}/n\mathbb{Z}$ with multiplication is not a group for $n \geq 2$.

Solution: for $n \geq 2$, notice that

$$\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{0} \times \bar{a} = \bar{a} \times \bar{0} = \bar{0}$$

Therefore, the inverse of $\bar{0}$ does not exists. Therefore, $(\mathbb{Z}/n\mathbb{Z}, \times)$ is not a group

Question 7

Let $G = \{g \in \mathbb{C} \mid g^n = 1 \text{ for some } n \in \mathbb{N}\}$. Show that G with multiplication is a group.

Solution: let $u, v, w \in G$ and $n, m, k \in \mathbb{N}$ such that $u^n = v^m = w^k = 1$. And let $\cdot$ denotes the multiplication operator. Firstly, G contains 1 as $1^1 = 1$. Therefore G is not empty. Note that the multiplication operation is well-defined on $\mathbb{C}$, therefore, it is well-defined on G.

- **Closure:** $(uv)^{nm} = u^{nm}v^{nm} = 1^m 1^n = 1$. Therefore, $uv \in G$.
- **Associative:** The multiplication of complex number is associative, Therefore, it is associative on the well-defined restriction of the operator.

- **Identity:** $\exists 1 \in G$ since $1 \in \mathbb{C}$, $1^1 = 1$. And by the multiplication of complex number, $1u = u1 = u$ for all $u \in G \subset \mathbb{C}$
- **Inverse:** $\forall u \in G$ let $n_u \in \mathbb{N}$ such that $u^{n_u} = 1$. If $n_u = 1$, then $u = 1$ is the identity. For $n_u > 1$, consider $u^{(n_u-1)(n_u)} = u^{(n_u)(n_u-1)} = 1^{n_u-1} = 1$, so $u^{n_u-1} \in G$. But also, $u^{n_u-1} \cdot u = u \cdot u^{n_u-1} = u^{n_u} = 1$. So $u^{-1} = u^{n_u-1}$ is the inverse of u.

Since G is a non-empty set and $(G, \cdot)$ has all the group properties. $(G, \cdot)$ is a group.

Question 8

Given two groups G and H, we denote their Cartesian product by $G \times H$ whose elements are of the form (g, h) for $g \in G$ and $h \in H$. Show that the product $G \times H$ with an operation given by $(g, h)(g', h') := (gg', hh')$ is a group.

Solution: Denote a well-defined operator $(\star)$ of group G, $(\times)$ of group H, and a new operator $(\cdot)$ of $G \times H$. However, the operator might be briefly written as juxtaposition.
For $G \times H$ to be a group, it must satisfies all the following properties.

- **Non-emptiness:** Since, G and H are both group, they are both non-empty. Therefore, the Cartesian product of G and H must contain at least one element: ie. (e_g, e_h), denoting the identity of G and H respectively.
- **Well-defined:** Note that $(g, h) \cdot (g', h') = (g \star g', h \times h')$. And if $(g, h) = (a, b)$ and $(g', h') = (a', b')$ then $(a, b) \cdot (a', b') = (a \star a', b \times b')$
  But then, $g = a, g' = a', h = b, h' = b'$, so by the well-definedness of $\star$ and $\times$, $g \star g' = a \star a'$ and $h \times h' = b \times b'$. Therefore, the operator $(\cdot)$ is well-defined.
- **Associativity:** For $(a, b), (g, h), (x, y) \in G \times H$,
$$\begin{aligned}
(a,b)((g,h)(x,y)) &= (a,b)(gx, hy) \\
&= (a(gx), b(hy)) \\
&= ((ag)x, (bh)y) \qquad \text{by associativity of group } G \text{ and } H \\
&= (ag, bh)(x,y) \\
&= ((a,b)(g,h))(x,y)
\end{aligned}$$
  Therefore, $(\cdot)$ is associative.
- **Identity:** Consider (e_g, e_h) where e_g is the identity element of group G and e_h is that of group H. Then for $(a, b) \in G \times H$,
$$(e_g, e_h) \cdot (a, b) = (e_g a, e_h b) = (a, b) = (ae_g, be_h) = (a, b) \cdot (e_g, e_h)$$
- **Inverse:** For $(g, h) \in G \times H$, $g \in G$ and $h \in H$. Therefore, there exists $g^{-1} \in G$ and $h^{-1} \in H$ such that $gg^{-1} = e_g$ and $hh^{-1} = e_h$. By that reason, $(g^{-1}, h^{-1}) \in G \times H$. Consider
$$(g,h) \cdot (g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_g, e_h)$$
$$(g^{-1}, h^{-1}) \cdot (g,h) = (g^{-1}g, h^{-1}h) = (e_g, e_h)$$
  Therefore, $(g^{-1}, h^{-1}) = (g, h)^{-1}$.

Hence, $G \times H$ is a group with the operation $(\cdot)$.

Question 9

Let G be a group. Show that $((ab)c)d = a(b(cd))$ for all $a, b, c, d \in G$.

Solution: Let $a, b, c, d \in G$. Then,
$$\begin{aligned}
ab &\in G && \text{by closure of } G \\
cd &\in G && \text{by closure of } G \\
((ab)c)d &= (ab)(cd) && \text{by associativity} \\
a(b(cd)) &= (ab)(cd) && \text{by associativity}
\end{aligned}$$

Therefore, $((ab)c)d = a(b(cd))$.

Question 10

Let G be the quaternion group Q_8. Find two subgroups H and K of G such that their union $H \cup K$ is not a subgroup of G.

Solution: Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group. Let $H = \{\pm 1, \pm i\}$ and $K = \{\pm 1, \pm j\}$. Then for H,

- **Well-definedness:** Since the operator is the restriction from a group operator, the operator must be well-defined.
- **Closure:** For all $x \in H$,
$$1x = x1 = x$$
$$i^2 = -1, \quad (-1)^2 = 1, \quad (-i)^2 = -1$$
$$(-1)(i) = i(-1) = -i, \quad (-1)(-i) = (-i)(-1) = i$$
$$(-i)i = i(-i) = 1$$
by the definition.
- **Associativity:** Since the operator is associative in G, the restriction must also be associative.
- **Identity:** $1 \in H$ is the identity element by definition.
- **Inverse:** The inverse of $1, -1, i, -i$ is $1, -1, -i, i$, respectively.

Therefore, H is a subgroup of G. With similar arguments, K is also a subgroup of G.
Consider $H \cup K = \{\pm 1, \pm i, \pm j\}$, The operator $(\cdot)$ of G does not have closure under $H \cup K$ since $i, j \in H \cup K$ but $i \cdot j = k \notin H \cup K$. Therefore, $H \cup K$ is not a subgroup of G.