# Abstract algebra I

Homework 2

B13902024 張沂魁

Due: 24th September 2025

1. Let $G = \mathbb{Z}/30\mathbb{Z}$, which is an additive group as we have known. Among the following subsets of $G$, determine whether each of them is a subgroup. Prove or disprove them.

   (a) $G_1 = \{0, 1, 2, 3, \ldots, 14\}$

   (b) $G_2 = \{0, 2, 4, 6, \ldots, 28\}$

   (c) $G_3 = \{1, 7, 11, 13, 17, 19, 23, 29\}$

   **Solution:**

   (a) No. Since $14 + 3 = 17 \notin G_1$, so $G_1$ is not closed.

   (b) Note that $G_2 = \langle 2 \rangle$, so it is a subgroup of $G$.

   (c) Note that $0 \notin G_3$, so there does not exist an identity element in $G_3$ and thus $G_3$ can not be a subgroup.

2. Recall that a subgroup $H$ of a group $G$ is a subset $H \subset G$ that itself is a group, with the induced operation. We now introduce the criterion of a subset and we aim to prove this handful criterion and give an application.

   (i) **(Subgroup criterion)** Suppose $(G, *)$ is a group and $H \subset G$. Suppose that

   - $H$ is not empty,
   - (closedness of $*$) for any $a, b \in H$, we have $a * b \in H$, and
   - (closedness of inverse) for all $a \in H$, its inverse $a^{-1} \in H$.

   Prove that $H$ is a subgroup of $G$.

   (ii) Using the above criterion, check that the special linear group $SL_n(\mathbb{R})$ is a subgroup of the general linear group $GL_n(\mathbb{R})$. (Recall that $GL_n(\mathbb{R})$ is the set of all $n \times n$ matrices with real coefficients (entries) so that their determinants are not zero, while $SL_n(\mathbb{R})$ is the subset of $GL_n(\mathbb{R})$ containing those matrices with determinant 1.)

   **Solution:**

   (a) For all $a, b, c \in H$, since $a, b, c \in G$, so $(a * b) * c = a * (b * c)$, and this can be inherited to $H$. Also, since for all $a \in H$ we have $a^{-1} \in H$, and $*$ is closed under $H$, so $e = a * a^{-1} \in H$, so the identity element is in $H$. Also, we already know the closedness of inverse, so we know $H$ is a subgroup of $G$.

   (b) Note that $\mathrm{SL}_n(\mathbb{R})$ is not empty since $I_n \in SL_n(\mathbb{R})$, where $I_n$ is the matrix with all diagonal entries 1 and all the other entries 0. Also, if $a, b \in \mathrm{SL}_n(\mathbb{R})$, then $\det(a) = \det(b) = 1$, so we know $\det(ab) = \det(a)\det(b) = 1$, and thus $ab \in \mathrm{SL}_n(\mathbb{R})$. Besides, for any $a \in \mathrm{SL}_n(\mathbb{R})$, since $\det(a) = 1 > 0$, so it is invertible, and thus there exists $a^{-1}$ such that $aa^{-1} = a^{-1}a = I_n$, which implies $1 = \det(a)\det(a^{-1}) = 1 \cdot \det(a^{-1})$, and thus $a^{-1} \in \mathrm{SL}_n(\mathbb{R})$.

3. We define the order of a finite group $G$ to be $|G|$, i.e., the number of elements (or the cardinality) of $G$. Also, for any $g \in G$, the order of $g$, denoted by $|g|$ (or sometimes $o(g)$), is the smallest positive integer $m$ such that $g^m = e$.

   (a) For $n \geq 1$, show that the set of bijections $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, denoted by $S_n$, is a group of order $n!$.

   (b) Show that the subset given by $\{\sigma \in S_4 : \sigma(1) = 1\}$, i.e., the collection of bijections fixing 1, is a subgroup of $S_4$. Find its order.

   (c) Consider the multiplicative non-abelian group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = \pm 1 \right\}.$$

   Find the orders of

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

**Solution:**

(a) If $\pi : [n] \to [n]$ is a bijection, where $[n] = \{1, 2, \ldots, n\}$, then $\pi(1)$ has $n$ choices, $\pi(2)$ has $n - 1$ choices, and so on, so there are $n!$ possibilities for a bijection from $[n]$ to $[n]$, which means $S_n$ has $n!$ elements. Now we show that $S_n$ is a group. Since for $\pi, \psi \in S_n$, we know $\pi \circ \psi$ is still a bijection from $[n]$ to $[n]$ (the composition of two bijection is a bijeciton), so $\pi \circ \psi \in S_n$. Also, since every $\pi \in S_n$ is a bijeciton from $[n]$ to $[n]$, so the inverse of $\pi$ exists, say it is $\pi^{-1}$, and notice that $\pi^{-1}$ is still a bijection from $[n]$ to $[n]$, and thus $\pi^{-1} \in S_n$ and $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = e \in S_n$, where $e$ is the identity map, which is defined by $e(i) = i$ for all $i \in [n]$. Hence, we know $e \in S_n$, and $e$ is the identity element, so $S_n$ is a group of order $n!$.

(b) Suppose

$$H_4 = \{\sigma \in S_4 : \sigma(1) = 1\},$$

then for $a, b \in H_4$, we know $a(1) = b(1) = 1$, so $(a \circ b)(1) = a(1) = 1$, which means $a \circ b \in H_4$ since $S_4$ is a group and thus $a \circ b \in S_4$. Also, notice that the identity map $e \in H_4$ since $e(1) = 1$ and $e \in S_4$. Besides, for any $a \in H_4$, we can define $a^{-1}$ as $a^{-1}(1) = 1$ and $a^{-1}(a(i)) = i$ for all $i \in \{2, 3, 4\}$. Note that $a^{-1}$ is well-defined since $a$ is a bijection and $a(1) = 1$ , so $a^{-1}$ is also a bijection. Note that $a \circ a^{-1} = a^{-1} \circ a = e$, so $a^{-1}$ is the inverse of $a$ and $a^{-1} \in H_4$, so we know $H_4$ is a subgroup of $S_4$. Note that for any $\pi \in H_4$, since $\pi(1) = 1$, so just need to decide the value of $\pi(2), \pi(3), \pi(4)$ and make sure $\pi$ is a bijection, so we have 3 options for $\pi(2)$, 2 for $\pi(3)$, and 1 for $\pi(4)$, which means there are 6 elements in $H_4$, so the order of $H_4$ is 6.

(c) Since we know

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad a^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad a^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2,$$

so the order of $a$ is 4. Also, we know

$$b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

so the order of $b$ is 3.

4. For some positive integer $n$, let $G$ be a finite cyclic group of order $n$. (Recall that a cyclic group is a group generated by one of its elements, i.e., there exists some $g \in G$ of order $n$.)

   (a) Prove that if $g$ is a generator of $G$, then $g^k$ is a generator of $G$ if and only if $\gcd(k, n) = 1$.

   (b) For any $m \mid n$, prove that $G$ has exactly one subgroup of order $m$.

   (c) Show that $S_3$, the symmetric group on 3 letters, is not cyclic.

   **Solution:**

   (a)

   ( $\Longrightarrow$ ) If $g$ is a generator of $G$ and $g^k$ is a generator of $G$. If $\gcd(k, n) = d > 1$, then
   $$d \mid ak - bn \quad \forall a, b \in \mathbb{Z}.$$
   That is, if $c < d$ and $c \in \mathbb{N}$, then $g^c \notin \langle g^k \rangle = G$, which is a contradiction.

   ( $\Longleftarrow$ ) If $\gcd(k, n) = 1$, we claim that $\langle g^k \rangle = \langle g \rangle$. If not, then there exists $c \in \mathbb{N}$ s.t. $g^c \notin \langle g^k \rangle$, so there exists $i \neq j$ with $1 \leq i < j \leq n$ s.t. $g^{ik} = g^{jk}$ by Pigeonhole principle. However, this means $g^{(j-i)k} = e$, which means $n \mid (j - i)k$, but $j - i < n$ and $\gcd(k, n) = 1$, so this is impossible. Thus, we know $\langle g^k \rangle = \langle g \rangle$.

   (b) We first prove the existence, that is, there exists a subgroup of $G$ of order $m$. Suppose $n = md$, then
   $$\langle g^d \rangle = \left\{ g^d, g^{2d}, \ldots, g^{md} \right\}$$
   is a subgroup of order $m$ since $g^{md} = g^n = e$, and for every $g^{cd} \in \langle g^d \rangle$, we know $g^{md-cd} \in G$, so the inverse of every element of $\langle g^d \rangle$ is also in $\langle g^d \rangle$. Now we show that the uniqueness. We claim that the subgroup of a cyclic group must also be a cyclic group. If $H$ is a subgroup of $G$ and $G = \langle g \rangle$ is cyclic, then let $d = \min \left\{ k : g^k \in H \right\}$, then we know $\langle g^d \rangle \subseteq H$. Now we show that $H \subseteq \langle g^d \rangle$. Suppose $g^k \in H$ and $k = sd + r$ where $0 \leq r < d$ and $k, r \in \mathbb{N} \cup \{0\}$. If $r > 0$, then we know $g^{sd} * g^r = g^k \in H$, and $g^r = g^{-sd} * g^k \in H$ since $g^{-sd} \in \langle g^d \rangle \subseteq H$ and $g^k \in H$. However, $r < d = \min \left\{ k : g^k \in H \right\}$, so this is impossible. Now we know $r = 0$, so $H \subseteq \langle g^d \rangle$. Thus, the claim is true. Now go back to the original problem, we know $G$ is cyclic, and thus if $H$ is a subgroup of $G$, then $H$ is cyclic. Suppose $H = \langle g^k \rangle$, where $o\left(g^k\right) = m$, then we have
   $$md = n \mid km,$$
   and thus $d \mid k$, which means $k = dr$ for some $r \in \mathbb{N}$. Since $g^k$ is a generator of $H$. If $\gcd(r, m) = d'$, then $o\left(g^{rd}\right) = \frac{m}{d'}$. Hence, we know $d' = 1$ as a result of $o\left(g^{rd}\right) = m$. Now we know $g^d$ is a generator of $\langle g^d \rangle$ and $\gcd(r, m) = 1$, so $\left(g^d\right)^r$ is also a generator of $\langle g^d \rangle$ by (a). Hence, $H = \langle g^d \rangle$ since $g^{dr}$ is a generator of $H$ and $\langle g^d \rangle$.

   (c) Note that every cyclic group $G$ is Abelian since if $g$ is a generator of $G$, then $\forall a, b \in G$, we can write $a = g^p$ and $b = g^q$ for some $p, q \in \mathbb{N}$, and thus
   $$a * b = g^p * g^q = g^{p+q} = g^q * g^p = b * a.$$

However, notice that $S_3$ is not Abelian since $(12)(13) = (132)$ but $(13)(12) = (123)$.

5. For any subgroup $N$ of a group $(G, *)$, and any $g \in G$, we define

$$gN = \{g * n : n \in N\}, \quad Ng = \{n * g : n \in N\}.$$

We say that $N$ is a normal subgroup of $G$, denoted $N \trianglelefteq G$, if $gN = Ng$ for all $g \in G$.

(a) Show that if $N \trianglelefteq G$, then $(G/N, \cdot)$ is a group under the operation given by

$$g_1N \cdot g_2N = (g_1 * g_2)N.$$

(b) Consider the subgroup $H = \{(1), (12)\} \subset S_3$. Show that $H$ is not a normal subgroup of $S_3$.

(c) Show that every subgroup of an abelian group $G$ is normal.

(d) The converse is false; there exist non-abelian groups with all subgroups normal. Search for one, no justification required.

**Solution:**

(a)
- Well-defined: We need to show the operation $\cdot$ is well-defined. That is, if $g_1N = g_1'N$ and $g_2N = g_2'N$, then $(g_1 * g_2)N = (g_1' * g_2')N$. Since $N$ is a subgroup of $G$, so $e \in G$, and thus $g_1' = g_1' * e \in g_1'N = g_1N$, so $g_1' = g_1 * n_1$ for some $n_1 \in N$. Similarly, we know $g_2' = g_2 * n_2$ for some $n_2 \in N$. Note that for any $n \in N$, we have

$$g_1' * g_2' * n = (g_1 * n_1) * (g_2 * n_2) * n = g_1 * (n_1 * g_2) * n_2 * n.$$

Also, since $N$ is a normal subgroup of $G$, so

$$n_1 * g_2 \in Ng_2 = g_2N,$$

so we can write $n_1 * g_2 = g_2 * n_1'$ for some $n_1' \in G$. Hence, we have

$$g_1 * (n_1 * g_2) * n_2 * n = g_1 * (g_2 * n_1') * n_2 * n \in (g_1 * g_2)N.$$

Hence, $(g_1' * g_2')N \subseteq (g_1 * g_2)N$. Similarly, we can get $(g_1 * g_2)N \subseteq (g_1' * g_2')N$. Hence, we have $(g_1 * g_2)N = (g_1' * g_2')N$.
- Associativity: For any $g_1N, g_2N, g_3N \in G/N$, we have

$$(g_1N \cdot g_2N) \cdot g_3N = (g_1 * g_2)N \cdot g_3N = (g_1 * g_2 * g_3)N,$$

and

$$g_1N \cdot (g_2N \cdot g_3N) = g_1N \cdot (g_2 * g_3)N = (g_1 * g_2 * g_3)N.$$

Hence, we know $(g_1N \cdot g_2N) \cdot g_3N = g_1N \cdot (g_2N \cdot g_3N)$.
- Identity: $\forall gN \in G/N$, we know

$$gN \cdot eN = (g * e)N = gN \quad (e * g)N = eN * gN.$$

– Inverse: $\forall gN \in G/N$, we know

$$gN \cdot g^{-1}N = (g * g^{-1})N = eN \quad g^{-1}N \cdot gN = (g^{-1} * g)N = eN.$$

(b) Consider $(23) \in S_3$, then

$$(23)H = \{(23), (132)\} \quad H(23) = \{(23), (123)\},$$

so $(23)H \neq H(23)$, which means $H$ is not a normal subgroup of $G$.

(c) Suppose $H$ is a subgroup of an abelian group $G$, then for all $g * h \in gH$ with $g \in G$ and $h \in H$, we have $g * h = h * g \in Hg$, so $gH \subseteq Hg$, and similarly we can show $Hg \subseteq gH$, so $gH = Hg$ for all $g \in G$, and thus $H$ is normal.

(d) Consider $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, where the definition of multiplication operation of $Q_8$ is

| $*$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| $j$ | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| $-j$ | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| $k$ | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $i$ | $-1$ | $1$ |
| $-k$ | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-i$ | $1$ | $-1$ |