Group Theory Homework 2 Solutions

Karthik Boyareddygari
Professor Alexandru Suciu

Problem 1:

(i)

First of all, H as defined is nonempty because $e^3 = e$ always. Now suppose that $a, b \in H$ are arbitrary elements. Because G is Abelian, we find that

$$(ab^{-1})^3 = ab^{-1}ab^{-1}ab^{-1} = a^3b^{-3} = e(b^3)^{-1} = ee^{-1} = e \Longrightarrow ab^{-1} \in H.$$

Therefore, $\boxed{H \leq G.}$

(ii)

Consider the group $\mathrm{GL}_2(\mathbb{C})$, which is non-Abelian. In it, we find a pair of nonidentity elements of order 3, thereby making them elements of H.

$$\begin{bmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}} \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}^3$$

If H were a subgroup, it would be closed under multiplication of its elements, so we will compute the product of these elements as follows:

$$\begin{bmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}} \end{bmatrix} \cdot \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} e^{\frac{-\pi i}{3}} & e^{\frac{-\pi i}{3}} \\ e^{\frac{-2\pi i}{3}} & 0 \end{bmatrix}.$$

And now for the moment of truth, shall we find that this product belongs to H? That is to say, will its cube be the identity matrix? Taking the cube of the product, we find that

$$\begin{bmatrix} e^{\frac{-\pi i}{3}} & e^{\frac{-\pi i}{3}} \\ e^{\frac{-2\pi i}{3}} & 0 \end{bmatrix}^3 = \begin{bmatrix} -2 + \sqrt{3}i & \frac{-3}{2} + \frac{\sqrt{3}}{2}i \\ \sqrt{3}i & \frac{-1}{2} + \frac{\sqrt{3}}{2}i \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

which shows us that the product does not belong to H. Therefore, $\boxed{H \nleq \mathrm{GL}_2(\mathbb{C}).}$

Problem 2:

(i)

With $H, K \leq G$ subgroups, we find that $H \cap K \neq \varnothing$ because both contain the identity. Suppose that $a, b \in H \cap K$ are arbitrary elements. What this buys us is that the product $ab^{-1} \in H$ because H is a subgroup containing both a and b. Similarly, $ab^{-1} \in K \Longrightarrow ab^{-1} \in H \cap K$. Therefore, $\boxed{H \cap K \leq G.}$

(ii)

Let $G = \mathbb{Z}$, $H = 2\mathbb{Z}$, and $K = 3\mathbb{Z}$. The union $H \cup K$ consists of all multiples of 2 and 3. Then $2, 3 \in H \cup K$, yet $2 + 3 = 5 \notin H \cup K$ because 5 is neither a multiple of 2 nor 3. Therefore, $\boxed{H \cup K \not\leq G.}$ There are cases where it is true, but it is not true in general.

(iii)

Let S be an arbitrary collection of subgroups within G. Then the intersection of this collection is nonempty because e belongs to every subgroup and thereby belongs to the intersection as well. As in part (i), let

$$a, b \in \bigcap_{H \in S} H \iff \forall H \in S, a \in H \text{ and } b \in H$$

be arbitrary elements. Similarly to part (i), we find that

$$\forall H \in S, ab^{-1} \in H \iff ab^{-1} \in \bigcap_{H \in S} H \iff \boxed{\bigcap_{H \in S} H \leq G,}$$

where the first correspondence follows from all the H's being subgroups.

Problem 3:

(i)

Suppose that $o(a) = n \implies a^n = e$. Because a^n is the n-fold product of a with itself, and because f is a homomorphism, $f(a^n)$ can be expanded to the n-fold product of $f(a)$, notated as $f(a)^n$. That homomorphisms preserve the identity is a well-known fact, so $f(a)^n = f(a^n) = f(e) = e$. As proven in class, the order of an element in a group always divides all powers which annihilate that element, so

$$o(f(a))|n \implies \boxed{o(f(a)) \leq n.}$$

(ii)

There is an isomorphism between C_n and $\mathbb{Z}_n$ given by $a \mapsto 1$, so we will use the notation $\mathbb{Z}_n$ to mean the cyclic group of order n. It is obvious that $\mathbb{Z}_1$ is the trivial group; for any group G, there exists a unique homomorphism $e_G : \{e\} \to G$ (i.e. the trivial group is the initial object in the category of groups) given by $e \mapsto e$. Since $\mathbb{Z}$ is a group, there does exist a homomorphism $\mathbb{Z}_1 \to \mathbb{Z}$.

Now assume that the index $n \geq 2$. By part (i), any homomorphism $\mathbb{Z}_n \to \mathbb{Z}$ would need to send each element of $\mathbb{Z}_n$ to an element of finite order since $\mathbb{Z}_n$ is a finite group. However, the only element of finite order in $\mathbb{Z}$ is 0, so the $\underline{\text{only homomorphism } \mathbb{Z}_n \to \mathbb{Z} \text{ is the trivial map } k \mapsto 0 \text{ for any } 0 \leq k \leq n-1.}$

Problem 4:

(i)

Let $a, b \in G$ be arbitrary elements of an Abelian group. The coset product is defined as

$$(aH)(bH) := \{xy \mid x \in aH, y \in bH\}.$$

By the definitions of the left cosets aH and bH, any element of the coset product takes the form

$$ah_1bh_2 = abh_1h_2 \text{ for some } h_1, h_2 \in H.$$

Because H is a subgroup, $h_1h_2 \in H$ so that $ah_1bh_2 \in (ab)H$.

Conversely, let $abh \in (ab)H$ $(h \in H)$ be an arbitrary element. Note that $ab = aeb$ and that $e \in H$, so $abh = aebh \in (aH)(bH)$. Therefore, we have the set equality $\boxed{(aH)(bH) = (ab)H.}$

(ii)

Let $a, b \in G$ be such that

$$aH = bH \implies H = a^{-1}bH \implies a^{-1}b \in H.$$

Because H is a subgroup, it is closed under the operation in G, leading us to observe that the right coset

$$Ha^{-1}b = H \implies \boxed{Ha^{-1} = Hb^{-1} \iff f(aH) = f(bH).}$$

Because equivalent left cosets map to equivalent right cosets, $\underline{f \text{ is well-defined.}}$

To be clear, writing H on both sides of an equation amounts to stating that there exist $h_1, h_2 \in H$ which may separately take the places of H on either side, e.g. $aH = bH \iff ah_1 = bh_2$. This convention will be followed in the subsequent parts.

(iii)

This time let $a, b \in G$ be such that

$$f(aH) = f(bH) \iff Ha^{-1} = Hb^{-1} \implies Ha^{-1}b = H \implies a^{-1}b \in H.$$

Similar to part (ii), we find that

$$a^{-1}bH = H \implies bH = aH,$$

which asserts that $\underline{f \text{ is injective as desired.}}$

(iv)

Every right coset takes the form Ha for some $a \in G$. It is easy to find a left coset which maps to Ha; in particular, $f(a^{-1}H) = H(a^{-1})^{-1} = Ha$. Therefore, $\underline{f \text{ is surjective and altogether bijective.}}$

(v)

It is clear that g is well-defined because if $h_1 = h_2 \in H$, then $ah_1 = ah_2$. Surjectivity is also immediate because every element of aH is of the form ah for some $h \in H$, meaning that $g(h) = ah$. Injectivity is the only one which is not entirely immediate. Let $h_1, h_2 \in H$ be such that

$$g(h_1) = g(h_2) \iff ah_1 = ah_2 \implies h_1 = h_2,$$

where the equality follows from the cancellation property. Therefore, $\underline{g \text{ is a bijective function.}}$

Problem 5:

All subgroups of cyclic groups are again cyclic (stated in class), which can be shown by making use of the division algorithm. With this, the subgroups in the diagram will be completely determined up to isomorphism by their orders.

Arrows in the diagram indicate multiplication maps which surject onto the subgroups in the codomain position. And because these are functions, they may be composed; in other words, the arrows are transitive. The portrayal of these subgroup diagrams with maps instead of just dashes gives an example of a commutative diagram because all any paths from a domain to a codomain equal each other (the maps commute).

(i)

$$\begin{tikzcd}
\mathbb{Z}_{24} \arrow[d, "\cdot 2"'] \arrow[dr, "\cdot 3"] & \\
\mathbb{Z}_{12} \arrow[d, "\cdot 2"'] \arrow[dr, "\cdot 3"] & \mathbb{Z}_8 \arrow[d, "\cdot 2"] \\
\mathbb{Z}_6 \arrow[d, "\cdot 2"'] \arrow[dr, "\cdot 3"] & \mathbb{Z}_4 \arrow[d, "\cdot 2"] \\
\mathbb{Z}_3 & \mathbb{Z}_2
\end{tikzcd}$$

(ii)

$$\begin{tikzcd}
& \mathbb{Z}_{36} \arrow[dl, "\cdot 2"'] \arrow[dr, "\cdot 3"] & \\
\mathbb{Z}_{18} \arrow[d, "\cdot 2"'] \arrow[dr, "\cdot 3"] & & \mathbb{Z}_{12} \arrow[dl, "\cdot 2"'] \arrow[d, "\cdot 3"] \\
\mathbb{Z}_9 \arrow[d, "\cdot 3"'] & \mathbb{Z}_6 \arrow[dl, "\cdot 2"'] \arrow[dr, "\cdot 3"] & \mathbb{Z}_4 \arrow[d, "\cdot 2"] \\
\mathbb{Z}_3 & & \mathbb{Z}_2
\end{tikzcd}$$

Problem 6:

Because cyclic groups of the same order are isomorphic, a single representative of each isomorphism class will be given along with some generators existing within $\mathbb{Z}_6 \times \mathbb{Z}_3$. The largest order any element in $\mathbb{Z}_6 \times \mathbb{Z}_3$ can achieve is 6 because the largest orders of elements in $\mathbb{Z}_6$ and $\mathbb{Z}_3$ are 6 and 3, respectively, and the order of any element $([n]_6, [m]_3)$ is $\text{lcm}(n, m)$.

- The trivial group $\mathbb{Z}_1$ is a subgroup of all groups, here generated by $(0, 0)$.
- $\mathbb{Z}_2$ is generated by $(3, 0)$.
- $\mathbb{Z}_3$ is generated by $([2]_6, 0)$ and $(0, [1]_3)$.
- $\mathbb{Z}_6$ is generated by $([1]_6, 0)$ and $([1]_6, [1]_3)$.