MTH101: Symmetry
Problem Set 2

Problem 1. Find the order of the subgroup $\langle \overline{20}, \overline{24}, \overline{30} \rangle$ of $\mathbb{Z}/40\mathbb{Z}$.

Solution. Let L denote the subgroup $\langle \overline{20}, \overline{24}, \overline{30} \rangle$ of $\mathbb{Z}/40\mathbb{Z}$. Let $\phi : \mathbb{Z} \to \mathbb{Z}/40\mathbb{Z}$ denote the quotient homomorphism. Let H be the the subgroup $\langle 20, 24, 30 \rangle$ of $\mathbb{Z}$. Then, $\phi(H) = L$. If d is a generator of H, the element $\phi(d) = \overline{d}$ will generate the subgroup $\phi(H)$.

The subgroup H is generated by the gcd of 20, 24 and 30. Thus, $H = \langle 2 \rangle$. (In such situations you may compute the gcd either by factorization or by using the Euclidean algorithm. Here, I have calculated it by just factorizing. However, if the problem explicitly asks you to use the Euclidean algorithm, you must do so.)

Thus, the element $\overline{2}$ generates the subgroup L of $\mathbb{Z}/40\mathbb{Z}$. The order of $\overline{2} = 2 \cdot \overline{1}$ is equal to

$$\frac{ord(\overline{1})}{gcd(2, ord(\overline{1}))} = \frac{40}{gcd(2, 40)} = 20.$$

Thus, $|L| = ord(\overline{2}) = 20$. □

Problem 2. Prove that $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ is not a cyclic group.

Solution. The group $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ is of order 240. We need to show that it has no element of order 240.

Let x be any element of $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z})$. Then x is of the form $(a + 12\mathbb{Z}, b + 20\mathbb{Z})$. Let m be any element such that $mx = 0$. Then $(ma + 12\mathbb{Z}, b + 20\mathbb{Z}) = (0 + 12\mathbb{Z}, 0 + 20\mathbb{Z})$. Thus, $12|ma$ and $20|mb$. Conversely, if $12|ma$ and $20|mb$, then $mx = 0$. If we take $m = 60$, then we see that these conditions are fulfilled (since $12|60$ and $20|60$). Thus, $60x = 0$ for any $x \in \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Thus, we see that the order of every element is less than or equal to 60. Thus, the group is not cyclic.

You could also use theorem 8.1 from Gallian's book, which says that $ord(x) = lcm(ord(a + 12\mathbb{Z}), ord(b + 20\mathbb{Z}))$. As $ord(a + 12\mathbb{Z})|12$ and $ord(b + 20\mathbb{Z})|20$, we see that $ord(x)|lcm(12, 20)$. (If m, n, p, q are integers such that $m|p$ and $n|q$, then $lcm(m, n)|cm(p, q)$.) Thus, $ord(x)|60$. This shows that the order is less than or equal to 60. □

Problem 3. Find an element of order 24 in S_{10}.

Solution. If a permutation has a cycle decomposition with cycles of length $m_1, m_2, \ldots, m_r$, then the order of the permutation is equal to $lcm(m_1, \ldots, m_r)$. Since the cycles in a cycle decomposition are disjoint, the sum of their lengths will be less than or equal to 10. So we need to find some integers such that their sum is less than 10 but their lcm is equal to 24. Clearly, $6 + 4 = 10$ and $lcm(6, 4) = 24$.

Thus, we may consider the permutation $(1, 2, 3, 4, 5, 6)(7, 8, 9, 10)$. The order of this permutation is equal to 24. □

Problem 4. Let G be a group. For any element $g \in G$, define a function $\lambda_g : G \to G$ by $\lambda_g(x) = gx$.

(a) Prove that λ_g is a permutation of G for any $g \in G$.

(b) Prove that the function $g \mapsto \lambda_g$ is a group homomorphism from G to $Perm(G)$.

Solution. First, let us see that λ_g is a one-to-one function. If $\lambda_g(g_1) = \lambda_g(g_2)$ for any elements $g_1, g_2 \in G$, then $gg_1 = gg_2$. Thus, $g^{-1}gg_1 = g^{-1}gg_2$, i.e. $g_1 = g_2$. Thus, we see that λ_g is a one-to-one function.

To see that λ_g is onto, we need to show that given any element $y \in G$, there exists an element x such that $\lambda_g(x) = y$. Thus, we need to find x such that $gx = y$. Clearly, if we take $x = g^{-1}y$, we see that $\lambda_g(x) = g(g^{-1}y) = y$. Thus, we see that λ_g is an onto function.

Thus, λ_g is a 1-1 correspondence. This completes the solution of (a).

Let $\phi : G \to Perm(G)$ denote the function $g \mapsto \lambda_g$. We want to show that $\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2)$. In other words, we want to show that $\lambda_{g_1g_2} = \lambda_{g_1} \circ \lambda_{g_2}$. Let x be any element of G. Then, $\lambda_{g_1g_2}(x) = (g_1g_2)x$. Also,

$$\lambda_{g_1} \circ \lambda_{g_2}(x) = \lambda_{g_1}(g_2x) = g_1(g_2x) = (g_1g_2)x.$$

This completes the solution of (b). □

Problem 5. Let G be a finite group and let H be a subgroup such that $|G| = 2|H|$. Prove that G is normal. (Hint: Try to prove that every left coset is a right coset.)

Proof. We will show that every left coset is a right coset. Since $|G| = 2|H|$, there are only two left cosets. One of the left cosets is H. This is also a right coset.

There is only one other left coset. Since the union of the two left cosets is equal to G, we see that this other coset is equal to $G \backslash H$. (In general, the set $G \backslash H$, i.e. the set of all elements of G which are not in H, is not a coset. It is the union of all cosets other than H. However, since there is only one such coset in this situation, we see that $G \backslash H$ is a left coset.)

By the same argument, the set $G \backslash H$ is also a right coset. Thus, we see that it is both a left coset as well as a right coset.

Thus, we see that G is normal. □

Problem 6. Let G be a finite group. Let $\phi : G \to \mathbb{Z}$ be a group homomorphism. Prove that $\phi(g) = 0$ for any $g \in G$.

Proof. Since G is a finite group, $|G|$ is equal to some positive integer n. Then, for any element $g \in G$, $g^n = 1_G$. Thus, if $\phi : G \to \mathbb{Z}$ is a homomorphism, $\phi(g^n) = \phi(1_G) = 0$. But $\phi(g^n) = n\phi(g)$. Thus, $n\phi(g) = 0$. As n is a positive integer, this implies that $\phi(g) = 0$. This proves the claim. □

Problem 7. Let $f : A \to B$ be a group homomorphism. Let C be a subgroup of B.

(a) Prove that $f^{-1}(C)$ is a subgroup of A.

(b) Prove that if C is a normal subgroup of B then $f^{-1}(C)$ is a normal subgroup of A.

Proof.
Part (a): We want to show that if C is a subgroup of B, then $f^{-1}(C)$ is a subgroup of A.

First, we observe that $f^{-1}(C)$ is non-empty. Since $f(1_A) = 1_B$ and since $1_B \in C$, we see that $1_A \in f^{-1}(C)$. Thus, $f^{-1}(C)$ is non-empty.

Now, it is enough to show that if $x, y \in f^{-1}(C)$, then $x^{-1}y \in f^{-1}(C)$. In other words, we want to show that $f(x^{-1}y) \in C$. But $f(x^{-1}y) = f(x)^{-1}f(y)$. As $x, y \in f^{-1}(C)$, $f(x)$ and $f(y)$ are in C. Thus, as C is a subgroup of B, $f(x)^{-1}f(y) \in C$. Thus, $f(x^{-1}y)$ is in C, i.e. $x^{-1}y$ is in $f^{-1}(C)$ are required.

(You could also prove this by checking that $f^{-1}(C)$ contains the identity and is closed under taking inverses and products.)

Part (b): Now, let us assume that C is a normal subgroup of B. We want to show that $f^{-1}(C)$ is a normal subgroup of A. Let $x \in f^{-1}(C)$ and let y be any element of A.

We want to prove that $yxy^{-1} \in f^{-1}(C)$. In other words, we want to show that $f(yxy^{-1}) \in C$. But $f(yxy^{-1} = f(y)f(x)f(y)^{-1}$. As $x \in f^{-1}(C)$, $f(x) \in C$. As C is a normal subgroup, $f(y)f(x)f(y)^{-1}$ is in C. Thus, $f(yxy^{-1} \in C$. This completes the proof. □

Problem 8. Let G be a group and, let $H \leqslant G$ and let $K \lhd G$.

(a) Prove that
$$HK := \{hk | h \in H, k \in K\}.$$
is a subgroup of G.

(b) Prove that $HK = \langle H \cup K \rangle$. (Thus, HK is the subgroup of G generated by H and K.)

(c) Prove that $HK = H$ if and only if $K \subset H$.

Proof.
Part (a): As $1 \in H$ and $1 \in K$, we see that $1 \in HK$.

Now, let $x \in HK$ be any element. Then $x = hk$ for some $h \in H$ and some $k \in K$. Then
$$x^{-1} = k^{-1}h^{-1} = hh^{-1}k^{-1}h = h(h^{-1}k^{-1}h).$$
As K is a subgroup of G, $k^{-1} \in K$. As K is a normal subgroup of G, $h^{-1}k^{-1}h \in K$. Thus, we see that $x^{-1} = h(h^{-1}kh) \in HK$.

Now, let x_1 and x_2 be elements of HK. Then, $x_1 = h_1k_1$ and $x_2 = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then,
$$x_1x_2 = h_1k_1h_2k_2 = h_1(h_2h_2^{-1})k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2.$$

As K is normal, $h_2^{-1}k_1h_2 \in K$ and so $h_2^{-1}k_1h_2k_2 \in K$. Thus, $x_1x_2 \in HK$.

Thus, we see that HK is a subgroup. This completes the solution of part (a).

Part (b): As K contains 1, $H = H \cdot 1 \subset HK$. Similarly, $K \subset HK$. Thus, $\langle H \cup K \rangle \subset HK$.

On the other hand, $\langle H \cup K \rangle$ contains both H and K and thus, must contain every element of the form hk where $h \in H$ and $K \in K$. Thus, $HK \subset \langle H \cup K \rangle$. Thus, we see that $HK = \langle H \cup K \rangle$.

Part (c): As $1 \in K$, it is always true that $H = H \cdot 1 \subset HK$. Now, suppose $K \subset H$. Then, every element of hk is also an element of H and so $HK \subset H$. Thus, $HK = H$.

Conversely, suppose that $HK = H$. Since $K = 1 \cdot K \subset HK$, it follows that $K \subset H$.

Thus, we see that $HK = H$ if and only if $K \subset H$. □

Problem 9. Let G be a group and let H and K be normal subgroups of G such that $K \subset H$.

(a) Prove that H/K is a normal subgroup of G/K.

(b) There exists an isomorphism $(G/K)/(H/K) \cong G/H$. (Third Isomorphism Theorem)

Solution.
Part (a): Let $h \in H$ and $g \in G$. We want to prove that the element $(gK)(hK)(gK)^{-1}$ is in H/K. By definition, $(hK)(gK)(hK)^{-1} = (hgh^{-1})K$. As H is a normal subgroup of G, $hgh^{-1} \in H$ and so $(hgh^{-1})K \in H/K$. This completes the proof of (a).

Part (b): We have quotient homomorphisms $\phi : G \to G/K$ and $\psi : G/K \to (G/K)/(H/K)$. We consider the composition $\psi \circ \phi$. A composition of homomorphisms is a homomorphisms. Thus, $\psi \circ \phi$ is a homomorphism.

Let $g \in ker(\psi \circ \phi)$. Then $\psi(gK) = 1_{(G/K)/(H/K)}$. In other words, $\psi(gK) \in ker(\psi)$. Thus, $gK \in H/K$. Thus, $g \in H$. Thus, $ker(\psi \circ \phi) \subset H$.

On the other hand, if $h \in H$, $\phi(h) \in H/K$. As $H/K = ker(\psi)$, we see that $\psi(\phi(h)) = 1_{(G/K)/(H/K)}$. In other words, $h \in ker(\psi \circ \phi)$.

Thus, we see that $H = \ker(\psi \circ \phi)$. Thus, by the First Isomorphism Theorem, G/H is isomorphic to the image of $\psi \circ \phi$. As ϕ and ψ are both onto, $\psi \circ \phi$ is also onto. Thus, the image of $\psi \circ \phi$ is equal to the group $(G/K)/(H/K)$. This completes the proof. □