Solutions for Problem Set 5.

A. Let $G = A \times B$, where A and B are groups. Define a map $\varphi : G \to B$ by

$$\varphi\big(\ (a,\ b)\ \big) \ = \ b$$

for all elements $(a,\ b) \in G$. Prove that φ is a surjective group homomorphism. Determine the kernel of φ.

Solution. Let e denote the identity element of A and let f denote the identity element of B. To show that φ is a homomorphism, suppose that $g_1,\ g_2 \in G$. Then $g_1 = (a_1,\ b_1)$ and $g_2 = (a_2,\ b_2)$, where $a_1,\ a_2 \in A$ and $b_1,\ b_2 \in B$. Then $\varphi(g_1) = b_1$ and $\varphi(g_2) = b_2$. We have

$$\varphi(g_1g_2) \ = \ \varphi\big((a_1,\ b_1)(a_2,\ b_2)\big) \ = \ \varphi\big((a_1a_2,\ b_1b_2)\big) \ = \ b_1b_2 \ = \ \varphi(g_1)\varphi(g_2) \ .$$

Therefore, φ is a homomorphism from G to B. The fact that φ is surjective follows by noticing that, for any $b \in B$, if we let $g = (e,\ b)$, then $g \in G$ and $\varphi(g) = b$.

The kernel of φ has the following description

$$Ker(\varphi) \ = \ \{\ (a,\ b) \in G \bigm| \varphi\big((a,\ b)\big) = f\} \ = \ \{\ (a,\ b) \in G \bigm| b = f\} \ = \ \{\ (a,\ f) \bigm| a \in A\} \ .$$

B. Let $G = A \times A$, where A is a nonabelian group. Consider

$$H \ = \ \{\ (a,\ a) \bigm| a \in A\} \ .$$

Prove that H is a subgroup of G, but that H is not a normal subgroup of G. Prove that H is isomorphic to A. Does G have any normal subgroups which are isomorphic to A?

Solution. Let e denote the identity element of A. Since A is nonabelian, there exists elements $b,\ c \in A$ such that $bc \neq cb$. It then follows that $cbc^{-1} \neq b$. (Reason: We have the implication $cbc^{-1} = b \Longrightarrow cb = bc$.). Let $d = cbc^{-1}$. Then $d \neq b$. Consider the element $h = (b,\ b)$. By definition, $h \in H$. Let $g = (c,\ e)$. Then $g \in G$ and $g^{-1} = (c^{-1},\ e)$. Furthermore, we have

$$ghg^{-1} \ = \ (c,\ e)(b,\ b)(c^{-1},\ e) \ = \ (cbc^{-1},\ ebe) \ = \ (d,\ b) \ .$$

Since $d \neq b$, it follows that $(d,\ b) \notin H$. Thus, $h \in H$, but $ghg^{-1} \notin H$. As discussed in class, a normal subgroup N of a group G must have the following property:

If $n \in N$ and $g \in G$, then $gng^{-1} \in N$. More succinctly, $gNg^{-1} \subseteq N$ for all $g \in G$.

However, with the above choice of g and h, we have $h \in H$, but $ghg^{-1} \notin H$. Therefore H is not a normal subgroup of G.

The fact that $H \cong A$ can be verified by considering the homomorphism $\psi : H \to A$ defined by

$$\psi\big((a,\ a)\big) \;=\; a$$

for all elements $(a,\ a)$ in H. The fact that ψ is a homomorphism is easily verified. In fact, if one uses the result from problem **A**, and one takes $B = A$, then $\psi = \varphi|_H$. The fact that φ is a homomorphism implies that ψ is a homomorphism. The fact that ψ is a bijection from H to A is clear. Therefore, ψ is an isomorphism from H to A.

Finally, G does have a normal subgroup which is isomorphic to A. The following is such a subgroup:

$$K \;=\; \{\ (a,\ e) \bigm| a \in A\ \}\ .$$

One can verify directly that K is a normal subgroup of G. Alternatively, one can also notice that if one takes $B = A$ in problem **A**, then $K = Ker(\varphi)$ and therefore K must be a normal subgroup of G. The fact that K is isomorphic to A can be seen by considering the map $\rho : A \to K$ defined by $\rho(a) = (a,\ e)$.

C. Suppose that G is a finite group and that M and N are normal subgroups of G. Suppose also $M \cap N = \{e\}$, where e is the identity element of G. Suppose also that $|G| = |N| \cdot |M|$. Consider the map $\varphi : G \to (G/M) \times (G/N)$ defined as follows:

$$\varphi(g) \;=\; \big(gM,\ gN\big)$$

for all $g \in G$. Prove that φ is an isomorphism from the group G to the group $(G/M)\times(G/N)$.

Solution. First of all, we verify that φ is a homomorphism. To see this, let $g_1,\ g_2 \in G$. Then

$$\varphi(g_1g_2) \;=\; (g_1g_2M,\ g_1g_2N) \;=\; (g_1Mg_2M,\ g_1Ng_2N) \;=\; (g_1M,\ g_1N)(g_2M,\ g_2N) \;=\; \varphi(g_1)\varphi(g_2)\ .$$

This shows that φ is a homomorphism.

The identity element in $(G/M) \times (G/N)$ is $(M,\ N)$. If $g \in Ker(\varphi)$, then

$$\varphi(g) \ = \ (gM,\ gN) \ = \ (M,\ N)$$

and hence $gM = M$ and $gN = N$. It follows that $g \in M$ and $g \in N$. Therefore, $g \in M \cap N$. Since we are assuming that $M \cap N = \{e\}$, it follows that $g = e$. Thus, $Ker(\varphi) = \{e\}$. Therefore, φ is injective.

Finally, we will use the assumption that $|G| = |N| \cdot |M|$. Thus,

$$|G/M| \ = \ [G : M] \ = \ \frac{|G|}{|M|} \ = \ |N| \qquad \textit{and} \qquad |G/N| \ = \ [G : N] \ = \ \frac{|G|}{|N|} \ = \ |M|$$

and hence the group $(G/M) \times (G/N)$ has order

$$|G/M| \cdot |G/N| \ = \ |N| \cdot |M| \ = \ |G|$$

The map $\varphi : G \to (G/M) \times (G/N)$ is an injective map and the sets G and $(G/M) \times (G/N)$ have the same cardinality. It follows that φ is surjective.

We have proved that φ is a bijective homomorphism and hence φ is an isomorphism.

D. Let σ be the following element in S_9:

$$\sigma \ = \ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 8 & 9 & 7 & 6 \end{pmatrix} \quad .$$

(a) Find the cycle decomposition of σ.

Solution. We notice the following orbits under the action of powers of σ:

$$1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1, \qquad\qquad 6 \mapsto 8 \mapsto 7 \mapsto 9 \mapsto 6$$

and hence the cycle decomposition of σ is

$$\sigma \ = \ (1\ 2\ 3\ 4\ 5)(6\ 8\ 7\ 9) \quad .$$

(b) Let $H = \langle \sigma \rangle$, the cyclic subgroup of S_9 generated by σ. Determine $|H|$ and $[S_9 : H]$.

Solution. We know that $|H| = |\sigma|$. The cycle decomposition for σ tells us that the order of σ is the least common multiple of the cycle lengths 5 and 4. Thus, $|\sigma| = lcm(5,\ 4) = 20$. Therefore, $|H| = 20$. The index of H in S_9 is given by

$$[S_9 : H] \ = \ \frac{|S_9|}{|H|} \ = \ \frac{9!}{20} \ .$$

(c) Does there exist an element $\tau \in S_9$ such that $\tau\sigma\tau^{-1} = \tau^3$? If so, find such a τ. If not, explain why.

Solution. Multiplying the stated equation by tau^{-1} on the left and by τ on the right, we obtain the equation $\sigma = \tau^3$. The group H is a cyclic group of order 20. Suppose that r is an integer such that $gcd(r, 20) = 1$. As explained in class, the map $\varphi : H \to H$ defined by $\varphi(h) = h^r$ is an automorphism of H. In particular, φ is a bijection of H to itself. Take $r = 3$. Obviously, $gcd(3, 20) = 1$. Thus, there must exist an element $\tau \in H$ such that $\varphi(\tau) = \sigma$. Since H is a subgroup of S_9, we have $\tau \in S_9$.

Alternatively, and explicitly, we can simply notice that $\tau = \sigma^7$ works. Indeed, for that choice of τ, we have

$$\sigma \ = \ \sigma^{21} \ = \ (\sigma^7)^3 \ = \ \tau^3 \ .$$

(d) Does there exist an element $\tau \in S_9$ such that $\tau\sigma\tau^{-1} = \tau^2$? If so, find such a τ. If not, explain why.

Solution. As in part (c), the stated equation is equivalent to $\sigma = \tau^2$. If such a $\tau \in S_9$ exists, then we claim that $|\tau| = 40$. To see this, let $m = |\tau|$. It is clear that

$$\tau^{40} \ = \ (\tau^2)^{20} \ = \ \sigma^{20} \ = \ e$$

and hence m divides 40. However,

$$\sigma^m \ = \ \tau^{2m} \ = \ (\tau^m)^2 \ = \ e^2 \ = \ e \ .$$

Since $|\sigma| = 20$, it follows that m is divisible by 20. It follows that $m \in \{20,\ 40\}$. On the other hand,

$$\tau^{20} \ = \ (\tau^2)^{10} \ = \ \sigma^{10} \ \neq \ e$$

since $10 < 20$ and $|\sigma| = 20$. Thus, $m \neq 20$. Therefore, $m = 40$, as claimed.

Thus, $\tau \in S_9$ and $|\tau| = 40$. But no such τ exists. To verify that, consider the cycle decomposition of τ. There are many possibilities. The length of each k-cycle in the cycle decomposition of τ must divide 40 and the sum of the lengths is 9. If there is no 8-cycle in that decomposition, then the lengths will not be divisible by 8. The lcm of the lengths will not be divisible by 8 and cannot equal 40. However, if there is a cycle of length 8, then τ is a product of an 8-cycle and a 1-cycle, and will have order 8 instead of order 40. We have proved that S_9 has no elements of order 40. It follows that the equation $\sigma = \tau^2$ cannot hold for any $\tau \in S_9$.

(e) Determine the cardinality of the conjugacy class of σ in S_9.

Solution. The conjugacy class of σ in S_9 consists of all elements of S_9 of the form

$$(a\ b\ c\ d\ e)(f\ \ g\ \ h\ \ i) \ \ .$$

Here $a,\ b,\ c, ..., h,\ i$ is any permutation of $1,\ 2,\ 3, ..., 8,\ 9$. There are 9! such permutations. But the 5-cycle can be expressed in 5 different ways and the 4-cycle can be expressed in 4 different ways. Thus, the number of conjugates of σ in S_9 is $9!/20$.

There is a reason why this answer is the same as the index $[S_9 : H]$ given in part (b) of this problem. In fact, it turns out that H is the centralizer of σ in S_9. Proposition 5 on the Conjugacy handout states that the cardinality of a conjugacy class of an element a in a group G is equal to the index $[G : C(a)]$.

E: Suppose that G is a group of order 35. We will prove in class that G must have at least one normal subgroup N of order 7. You may use that fact in this problem. Prove that if H is any subgroup of G such that $|H| = 7$, then $H = N$. (Thus, it follows that G has exactly one subgroup of order 7.)

Solution: We will assume that G has a normal subgroup N of order 7. Consider the quotient group G/N. Then

$$\big|G/N\big| \ = \ [G : N] \ = \ |G|\big/|N| \ = \ 35/7 \ = \ 5 \ \ .$$

Thus, G/N is a group of order 5. Every element of G/N must have order 1 or 5.

Suppose that H is a subgroup of G and that $|H| = 7$. Since 7 is a prime, we know that H must be cyclic. That is, $H = \langle h \rangle$ for some $h \in H$. Thus, $h^7 = e$, the identity element in G. Consider the element hN in the group G/N. We have

$$(hN)^7 \ = \ h^7N \ = \ eN \ = \ N$$

which is the identity element in G/N. Therefore, the order of the element hN must divide 7. Thus, the order of hN is 1 or 7. However, every element of G/N has order 1 or 5. Therefore, hN must have order 1 or 5. It follows that hN has order 1. This means that $hN = N$. Hence $h \in N$. Since N is a subgroup of G, any power of h is also in N. Therefore,

$$H = \langle h \rangle \subseteq N \ .$$

Finally, since both H and N have the same cardinality (namely, 7), it follows that $H = N$, as claimed.

F. Suppose that G is a finite, abelian group. Let $n = |G|$. Suppose that $k \in \mathbb{Z}$ and that $gcd(k,\ n) = 1$. Consider the map $\varphi : G \to G$ defined by

$$\varphi(g) = g^k$$

for all $g \in G$. Prove that φ is an automorphism of the group G.

Solution. If $a,\ b \in G$, then

$$\varphi(ab) = (ab)^k = a^k b^k = \varphi(a)\varphi(b) \ .$$

The second equality follows from the assumption that G is an abelian group. Hence φ is a homomorphism from G to G.

Let $N = Ker(\varphi)$. Suppose that $a \in N$. Then $\varphi(a) = e$, where e is the identity element in G. Thus, $a^k = e$. It follows that $|a|$ divides k. However, we also know that $|a|$ divides $n = |G|$. Therefore, $|a|$ is a common divisor of k and n. Since $gcd(k,\ n) = 1$, it follows that $|a| = 1$. Hence, $a = e$. Therefore, $Ker(\varphi) = \{e\}$. It follows that φ is injective.

Finally, we use the fact that G is finite. Since $\varphi : G \to G$ is an injective map and G is a finite set, it follows that φ is also surjective. Thus, φ is a bijective homomorphism and therefore an isomorphism of G to itself. That means that φ is an automorphism of G.