Solutions to Exam I

Problem 1. A1) A group is a set G with a binary operation $* : G \times G \longrightarrow G$ such that

1. $a * (b * c) = (a * b) * c$ for any $a, b, c \in G$ ($*$ is associative).
2. There is $e \in G$ such that $g * e = g = e * g$ for every $g \in G$.
3. For every $a \in G$ there is $b \in G$ such that $a * b = e = b * a$.

The element e in 2. is unique and called the identity of G. The element b in 3. is unique. It is called the inverse of a and denoted by a^{-1}.

A2) A subgroup of a group G is a subset H of G such that $e \in H$ and for any $a, b \in H$ the elements ab and a^{-1} are also in H. The subgroup H is called normal if any of the following equivalent conditions holds:

- For any $g \in G$ we have $gH = Hg$.
- For any $g \in G$ we have $gHg^{-1} \subseteq H$.
- For any $g \in G$ and any $h \in H$ we have $ghg^{-1} \in H$.
- any left (right) coset of H in G is also a right (left) coset.

A3) A homomorphism from a group G to a group H is a function $f : G \longrightarrow H$ such that $f(ab) = f(a)f(b)$ for any $a, b \in G$. The kernel of a homomorphism $f : G \longrightarrow H$ is the set $\ker f = \{a \in G : f(a) = e\}$. It is always a normal subgroup of G.

A4) Let N be a normal subgroup of a group G. Then G/N is the set of all left cosets of N in G (which is the same as the set of all right cosets as $gN = Ng$ for every $g \in G$). The multiplication of subsets of G defined by $ST = \{st : s \in S, t \in T\}$ is a binary operation on G/N which makes G/N a group, called the quotient group of G by N. The coset $eN = N$ is the identity element and for any 2 cosets aN, bN we have $(aN)(bN) = (ab)N$. The function $\pi : G \longrightarrow G/N$ defined by $\pi(a) = A = aN$ is a surjective group homomorphism and $\ker \pi = N$.

A5) **Fundamental Homomorphism Theorem (FHT).** Let $\phi : G \longrightarrow H$ be a **surjective** homomorphism and let $f : G \longrightarrow K$ be any homomorphism such that $\ker \phi \subseteq \ker f$. Then there is unique homomorphism $\overline{f} : H \longrightarrow K$ such that $\overline{f}\phi = f$. It is defined as follows: for $h \in H$ take any $g \in G$ such that $\phi(g) = h$ and set $\overline{f}(h) = f(g)$. In addition, $\ker \overline{f} = \phi(\ker f)$ and $\overline{f}(H) = f(G)$.
In particular, if f is surjective and $\ker \phi = \ker f$ then $\overline{f}$ is an isomorphism.

A6) Let G be a group and H a subgroup of G. The number of left cosets of H in G is the same as the number of right cosets of H in G and it is denoted by $[G : H]$ and called the **index** of H in G.

Lagrange's Theorem. Let G be a finite group and H a subgroup of G. Then

$$|G| = |H|[G : H].$$

In particular, the order of a subgroup always divides the order of the group and the order of every element in a group divides the order of the group.

A7) **Fundamental Theorem of Finite Abelian Groups.**
1) If G is a finite abelian group of order $n = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$, where $p_1 < \dots < p_t$ are prime numbers, then G has unique subgroup P_i of order $p_i^{s_i}$, $i = 1, \dots, t$ and

$$G \cong P_1 \times P_2 \times \dots \times P_t.$$

2) If P is a finite abelian group of order p^m, p a prime, then

$$P \cong \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_k}}$$

for some $m_1 \geq m_2 \geq \dots \geq m_k \geq 1$ such that $m_1 + \dots + m_k = m$. Moreover, the numbers $m_1, m_2, \dots, m_k$ are unique for P.

A8) If G is a group and $g \in G$ has oder n then g^k has order $\dfrac{n}{\gcd(n,k)}$ for every integer k.

Problem 2. a) Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 8 & 1 & 7 & 3 & 2 & 6 & 5 \end{pmatrix}$ in S_9.

i) $\sigma = (1,4)(2,9,5,7)(3,8,6)$ and $\sigma^{-1} = (1,4)(2,7,5,9)(3,6,8)$

ii) The order of a permutation is equal to the lest common multiple of the lengths of the cycles appearing in the disjoin cycles decomposition. Thus the order of σ is $\operatorname{lcm}(2,3,4) = 12$.

iii) A k-cycle is even if and only if k is odd. Thus a permutation is even if and only if the number of cycles of even length appearing in the disjoint cycles decomposition is even. The permutation σ has two cycles of even length, so σ is even.

iv) Recall that $\tau(a_1, \dots, a_k)\tau^{-1} = (\tau(a_1), \dots, \tau(a_k))$. Take $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 8 & 9 & 6 & 7 \end{pmatrix} = (6,8)(7,9)$. Then

$$\tau\sigma\tau^{-1} = \tau(1,4)(2,9,5,7)(3,8,6)\tau^{-1} = \tau(1,4)\tau^{-1}\tau(2,9,5,7)\tau^{-1}\tau(3,8,6)\tau^{-1} =$$

$$(\tau(1)\tau(4))(\tau(2),\tau(9),\tau(5),\tau(7))(\tau(3),\tau(8),\tau(6)) = (1,4)(2,7,5,9)(3,6,8) = \sigma^{-1}.$$

b) Suppose that a subgroup H of S_6 contains $\sigma = (1,6)$ and $\tau = (2,3,4,5,6)$. We will show that H contains every transposition. Since every permutation is a product of transpositions, this will imply that $H = S_6$.

Note that $\tau\sigma\tau^{-1} = (\tau(1), \tau(6)) = (1,2)$. Since H is a subgroup and $\sigma, \tau \in H$, we have $(1,2) \in H$. Similarly $\tau(1,2)\tau^{-1} = (1,3) \in H$, and $\tau(1,3)\tau^{-1} = (1,4) \in H$, and $\tau(1,4)\tau^{-1} = (1,5) \in H$. Note that for any $i \neq j$ we have $(1,i)(1,j)(1,i) = (i,j)$. Since H contains $(1,2), (1,3), (1,4), (1,5), (1,6)$, it contains (i,j) for all $1 \leq i < j \leq 6$. Thus H contains all transpositions and therefore $H = S_6$.

Problem 3. Note that $100 = 2^2 \cdot 5^2$. By the Fundamental Theorem of Finite Abelian Groups, any group of order 100 is of the form $P \times Q$ for unique abelian groups P, Q of order 4 and 25 respectively. Part b) of the Fundamental Theorem of Finite Abelian Groups tells us that there are 2 possibilities for P: $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Similarly, that there are 2 possibilities for Q: $\mathbb{Z}_{25}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5$. Thus there are 4 abelian groups of order 100, up to isomorphism:

$$\mathbb{Z}_4 \times \mathbb{Z}_{25}, \quad \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5.$$

Problem 4. a) $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic because it has order 8 but no element has order 8 (the 4-th power of every element in $\mathbb{Z}_2 \times \mathbb{Z}_4$ is the identity).

b) $\mathbb{Z}_3 \times \mathbb{Z}_5$ is cyclic because it has order 15 and the element $(1,1)$ has order 15.

Problem 5. Let K and N be normal subgroups of a group G and let $k \in K$ and $n \in N$. We have $knk^{-1}n^{-1} = (knk^{-1})n^{-1}$. Since N is normal, $knk^{-1} \in N$ and $n^{-1} \in N$ so $knk^{-1}n^{-1} \in N$.

Similarly, $knk^{-1}n^{-1} = k(nk^{-1}n^{-1})$. Since K is normal and $k^{-1} \in K$, we have $nk^{-1}n^{-1} \in K$, so $knk^{-1}n^{-1} \in K$.
Thus $knk^{-1}n^{-1} \in N \cap K$.

Problem 6. The function $p(x) = x^n$ is a homomorphism $p : A \longrightarrow A$ for any abelian group A, since $p(ab) = (ab)^n = a^n b^n = p(a)p(b)$ for any $a, b \in A$.

Let $G =< a >$ be a cyclic group of order 12 generated by a and let $f : G \longrightarrow G$ be a function defined by $f(x) = x^8$. Since G is abelian, f is a homomorphism. Note that $a^i \in \ker f$ if and only if $(a^i)^8 = a^{8i} = e$ which holds if and only if $12|8i$, i.e. $3|2i$. The last condition is equivalent to $3|i$. Thus $\ker f = \{e, a^3, a^6, a^9\}$. Since G has 12 elements and $\ker f$ has 4 elements, the image of f has $12/4 = 3$ elements.

Problem 7. Let $G =< a >$ be a cyclic group and $f : G \longrightarrow G$ a homomorphism. Since $f(a) \in G$ we have $f(a) = a^n$ for some integer n. Any element $g \in G$ is of the form a^i for some i, so

$$f(g) = f(a^i) = f(a)^i = (a^n)^i = a^{ni} = (a^i)^n = g^n.$$

Thus $f(g) = g^n$ for all $g \in G$.

Problem 8. Let G be a group, $a, b \in G$ two elements such that $aba^{-1} = b^{-1}$ and a has odd order. Note that

$$a^2ba^{-2} = a(aba^{-1})a^{-1} = ab^{-1}a^{-1} = (aba^{-1})^{-1} = b.$$

In other words, a^2 commutes with b. Thus any even power of a commutes with b. In m is the order of a then m is odd so $m+1$ is even and therefore $a^{m+1} = a^m a = a$ commutes with b. Thus $b = aba^{-1} = b^{-1}$.

Problem 9. Let G be a group and let $AutG$ be the group of all automorphisms of G. Define on the set $G \times AutG$ a binary operation $*$ as follows: $(g, \phi) * (h, \psi) = (g\phi(h), \phi\psi)$. First we check that $*$ is associative:

$$((g,\phi)*(h,\psi))*(k,\eta) = (g\phi(h), \phi\psi)*(k,\eta) = (g\phi(h)(\phi\psi)(k), (\phi\psi)\eta) = (g\psi(h)\phi(\psi(k)), \phi\psi\eta)$$

and

$$(g,\phi)*((h,\psi)*(k,\eta)) = (g,\phi)*(h\psi(k), \psi\eta) = (g\phi(h\psi(k)), \phi(\psi\eta)) = (g\psi(h)\phi(\psi(k)), \phi\psi\eta).$$

This shows that $*$ is associative.

Is there an identity element for $*$? Let us try (e, id), where e is the identity in G and id is the identity automorphism (i.e. identity in $AutG$):

$$(g,\phi) * (e, id) = (g\phi(e), \phi id) = (g, \phi) \text{ and } (e, id) * (g, \phi) = (eid(g), id\phi) = (g, \phi).$$

Thus (e, id) is the identity element for $*$. To get the inverse we follow the hint:

$$(g,\phi) * (\phi^{-1}(g^{-1}), \phi^{-1}) = (g\phi(\phi^{-1}(g^{-1})), \phi\phi^{-1}) = (gg^{-1}, id) = (e, id)$$

and

$$(\phi^{-1}(g^{-1}), \phi^{-1})*(g,\phi) = (\phi^{-1}(g^{-1})\phi^{-1}(g), \phi^{-1}\phi) = (\phi^{-1}(g^{-1}g), id) = (\phi^{-1}(e), id) = (e, id).$$

This shows that any element (g, ϕ) invertible. This completes our verification that $G \times Aut(G)$ is a group under the operation $*$.

Remark. The construction in this problem is a special case of a **semi-direct product** of groups.

Problem 10. Let G be a group of odd order and let H be a normal subgroup of G of order 3. We have $H = \{e, a, a^{-1}\}$ for some a such that $a^3 = e$. Let $g \in G$. Then g has odd order. Since H is normal, $gag^{-1} = a$ or $gag^{-1} = a^{-1}$. If we had $gag^{-1} = a^{-1}$ then by problem 8 we would have $a^{-1} = a$, which is not possible. Thus we must have $gag^{-1} = a$. Since g was arbitrary, this proves that a is in the center of G. Thus $H \subseteq Z(G)$.

Problem 11. Let G be a group, N a normal subgroup of G and H a subgroup of G. Consider the quotient homomorphism $\pi : G \longrightarrow G/N$. We have $\ker \pi = N$.

a) Suppose that $\gcd(|H|, [G : N]) = 1$. Note that the image $\pi(H)$ is a subgroup of G/N and $|\pi(H)|||H|$. On the other hand, $|G/N| = [G : N]$ so $|\pi(H)|||[G : N]$ by Lagrange's Theorem. Since $|\pi(H)|$ divides both $|H|$ and $[G : N]$ and $\gcd(|H|, [G : N]) = 1$, we conclude that $|\pi(H)| = 1$, i.e $\pi(H) = \{e\}$. This means that $H \subseteq \ker \pi = N$.

b) Suppose that $H \cap N = \{e\}$. Then $\pi : H \longrightarrow \pi(H)$ is injective (as $\ker \pi = N$). Thus H and $\pi(H)$ are isomorphic, so $|H| = |\pi(H)|$. Since $\pi(H)$ is a subgroup of G/N, we have

$$|\pi(H)| = |H|||G/N| = [G : N].$$

Problem 12. Let G be a group and let $a, b, u \in G$ be such that $ba = uab$ and u commutes with both a and b. We prove by induction on n that for every natural number n we have $b^n a = u^n ab^n$ and $(ab)^n = u^{(n-1)n/2} a^n b^n$. For $n = 1$ this is clear. Suppose that the result is true for some n. Then

$$b^{n+1}a = bb^n a = bu^n ab^n = u^n bab^n = u^n uabb^n = u^{n+1}ab^{n+1}$$

and

$$(ab)^{n+1} = (ab)^n ab = u^{(n-1)n/2} a^n b^n ab = u^{(n-1)n/2} a^n u^n ab^n b =$$

$$u^{(n-1)n/2} u^n a^n ab^{n+1} = u^{n(n+1)/2} a^{n+1} b^{n+1}$$

(we used here the equality $(n-1)n/2 + n = n(n+1)/2$). Thus the result holds for $n+1$. By the method of induction, the result is true for all positive integers n.

Problem 13. Let G be a finite group such that $3 \nmid |G|$. Suppose that the function $f(g) = g^3$ from G to G is a homomorphism. The condition that $3 \nmid |G|$ means that f is injective: if $u \in \ker f$ then $u^3 = e$ so u has order 1 or 3. Since $3 \nmid |G|$, u can not have order 3, so it has order 1,i.e. $u = e$. This shows that $\ker f = \{e\}$, i.e. f is injective. Since $f : G \longrightarrow G$ is injective and G is finite, f is a bijection. This means that every element in G is a cube of some other element.

Since f is a homomorphism, for any $a, b \in G$ we have $(ab)^3 = a^3 b^3$, so $(ba)^2 = a^2 b^2$. Multiplying by ba on the left we get $(ba)^3 = ba^3 b^2$. Since $(ba)^3 = b^3 a^3$ we have $b^3 a^3 = ba^3 b^2$,

i.e. $b^2a^3 = a^3b^2$. This proves that in G any square commutes with any cube. Since every element in G is a cube, we see that any square commutes with all elements in G. So

$$(ba)^2 = a^2b^2 = b^2a^2 \quad \text{and therefore} \quad ab = ba.$$

Thus G is abelian.