Mid-Semestral Exam
Albegra I
B. Math - First year
2016-2017
Solutions

(1) State true or false. Justify your answers.

(a) Suppose a group G contains exactly eight elements of order 10. Then G has 3 cyclic subgroups of order 10.
Solution: False. In a cyclic subgroup of order 10 there are 4 elements of order 10, each of which generates the group. If the intersection of two cyclic subgroups of order 10 contains an element of order 10, then the subgroups are equal, since this element will generate both the groups. Therefore, if there were 3 cyclic subgroups of order 10, then there would be $3 \times 4 = 12$ distinct elements in the group of order 10. But given that there are exactly 8 such elements.

(b) There are 90 elements of order 4 in S_6.
Solution: False. Every element of S_6 can be written as a product of disjoint cycles. The order of an element is the l.c.m. of the orders of the factor cycles. Thus an element of order 4 must be either a product of a 4 cycles and a 2 cycle or a product of a 4 cycle and two 1 cycles. There are $\binom{6}{4} \times 3! = 90$ elements of both type. Hence there are 180 elements of order 4 in S_6.

(c) If G is a group having exactly one nontrivial proper subgroup, then G is cyclic, of order p^2 for some prime p.

Solution: True. If the order of a group is n whose prime decomposition is $n = p_1^{a_1} \cdots p_k^{a_k}$, then there exists a subgroup of order $p_i^{b_i}$, for all $1 \leq i \leq k$ and $b_i \leq a_i$. This and the fact that all non-trivial elements of a cyclic group of order p^2, except one, are generators and the exceptional element generates a subgroup of order p, implies the statement.

(d) There exist infinite groups in which every element has finite order.
Solution: True. Take for example a direct sum of infinitely many copies of $\mathbb{Z}/2\mathbb{Z}$.

(e) The set $\mathbb{R}_{>0}$ of all positive reals is the only subgroup of index 2 in the multiplicative group of nonzero reals $\mathbb{R}^\times$.
Solutions: True. Suppose H is a subgroup of index two. Then the quotient group is $\mathbb{Z}/2\mathbb{Z}$. Then for every $x \in \mathbb{R}$, $x^2 \in H$. If $x \in \mathbb{R}_{>0}$, then its positive square root $\sqrt{x} \in \mathbb{R}$. Thus $x = (\sqrt{x})^2 \in H$. Hence $\mathbb{R}_{>0} \subset H$. If $H \neq \mathbb{R}_{>0}$, then there exists $-y \in H$, where $y \in \mathbb{R}_{>0}$. Since $\frac{1}{y} \in \mathbb{R}_{>0}$, therefore $-y \cdot \frac{1}{y} = -1 \in H$ and hence $H = \mathbb{R}$. This is a contradiction since H is a proper subgroup. So we must have $H = \mathbb{R}_{>0}$.

(2) Let G be a cyclic group of order n.

(a) Show that every subgroup of G is cyclic.
Solution: Let x be a generator of G. Let H be a subgroup of G. Let d be the least non-zero integer such that $x^d \in H$. Then we claim that x^d generates H. Suppose $x^k \in H$. Let $k = qd + r$, where $r < d$. Then $x^k((x^d)^q)^{-1} = x^r \in H$. By definition of d we must have $r = 0$. Thus $x^k = (x^d)^q$, which implies that H is generated by x^d.

(b) Show that for each k dividing n, there exists a unique subgroup of order k in G.
Solution: Let $n = kq$ and let x be a generator of G. Then the subgroup generated by x^q is a subgroup of order k. By the previous problem, every subgroup of order k in G is cyclic. So any such subgroup will contain an element of order k. Let x^d be an element of order k. Then we must have $n \mid kd$. Since $n = kq$, this implies $q \mid d$ and hence x^d is contained in the subgroup generated by x^q. This proves the uniqueness.

(c) Show that for any divisor d of n, G contains exactly $\phi(d)$ elements of order d. Deduce the formula $\sum_{d|n} \phi(d) = n$.

Solution: By the previous problem, each element of order d is contained in a unique cyclic subgroup of order d. In a cyclic subgroup of order d there are exactly $\phi(d)$ many elements of order d.

The order of every element of a group G divides the order of G. Therefore G can be written as a disjoint union:

$$G = \cup_{d|n}\{g \in G : \text{ order of } g \text{ is } d\}.$$

Calculating the cardinality of both sides gives us the desired formula.

(3)(a) If K is a subgroup of G and N is a normal subgroup of G, prove that

(i) $KN = \{xy \in G : x \in K, y \in N\}$ is a subgroup of G.
Solution: We need to check that KN contains the identity element e, it is closed under multiplication and taking inverse. Both K and N, being subgroups, contain e. Therefore $e = e \cdot e \in KN$. Let $k_1, k_2 \in K$ and $n_1, n_2 \in N$. Then the product of the two elements k_1n_1 and k_2n_2 of KN can be written as $(k_1n_1)(k_2n_2) = (k_1k_2)((k_2^{-1}n_1k_2)n_2) \in KN$. Therefore KN is closed under multiplication. Let $k \in K$ and $n \in N$, then the inverse of the element kn of KN can be written as $(kn)^{-1} = n^{-1}k^{-1} = k^{-1}(kn^{-1}k^{-1}) \in KN$. Thus KN is closed under taking inverse. Hence KN is a subgroup.

(ii) $K \cap N$ is a normal subgroup of K.
Solution: Let $k \in K$ and $n \in K \cap N$. Since N is normal, therefore $knk^{-1} \in N$. On the other hand since k, n, k^{-1} belong to K, which is a subgroup, therefore $knk^{-1} \in K$. Thus $knk^{-1} \in K \cap N$ and so $K \cap N$ is normal in K.

(iii) KN/N is isomorphic to $K/(K \cap N)$.
Solution: Consider the composition

$$K \hookrightarrow KN \twoheadrightarrow KN/N,$$

where the first map is the inclusion and the second one is the quotient map. This composition is surjective since any element in KN/N is of the form $knN = kN$, where $k \in K$ and $n \in N$, and has the preimage k. The kernel of this composition is clearly $K \cap N$. Thus we get an isomorphism $K/(K \cap N) \to KN/N$.

(b) If M and N are normal subgroups of G and $N \subset M$, prove that $(G/N)/(M/N) \cong G/M$.

Solution: Consider the composition

$$G \twoheadrightarrow G/N \twoheadrightarrow (G/N)/(M/N),$$

where the both the maps are the relevant quotient maps. It is a surjective map and its kernel is clearly M. Thus we get an isomorphism $G/M \to (G/N)/(M/N)$.

(4) (a) Define conjugation action of a group G on itself.

Solution: Conjugation action of a group on itself is given by

$$\begin{aligned} G \times G &\to G \\ (h, g) &\mapsto hgh^{-1} \end{aligned}$$

(b) Show that the number of distinct conjugates of an element $g \in G$ is the index of the centraliser $C_G(g)$ in G.

Solution: This is just the orbit stabilizer theorem. Consider the conjugation action of the group on itself. Stabilizer of the element $g \in G$ under this action is $C_G(g)$. Hence the orbit must be in one to one correspondence with $G/C_G(g)$. Thus cardinality of the orbit, which is same as the number of distinct conjugates of g is equal to the index $[G : C_G(g)]$ of the centralizer $C_G(g)$ of g in G.

(c) Establish the Class Equation.

Solution: G is a disjoint union of orbits under the conjugacy action. Note that the orbits are the conjugacy classes in G. The elements of the centre $Z(G)$ of G are singleton orbits. Let us index the conjugacy classes of G, which are not in $Z(G)$, by the indexing set I. For each $i \in I$, choose a representative g_i of the corresponding conjugacy class. By the previous problem, cardinality of the conjugacy class represented by g_i is $[G : C_G(g_i)]$. Therefore we have

$$|G| = |Z(G)| + \sum_i [G : C_G(g_i)].$$

This is the class equation of G.

(5)(i) State and prove Cauchy's theorem for finite abelian groups.
Solution: *Cauchy's Theorem*: If the order of a group G is divisible by a prime p, then there exists an element of order p in G.
Proof in the abelian case: We will proceed by induction on the order of the group G. The base case is when $|G| = p$. In this case G is a cyclic group of order p and hence any generator is of order p. Now we carry out the induction step. Let g be a non-identity element of G. If the order of the group H generated by g is divisible by p, then the element $g^{|H|/p}$ is an element of order p. If the order of H is not divisible by p, then the order of the quotient group G/H must be divisible by p. By induction hypothesis, there exists an element $xH \in G/H$ of order p. Suppose order of x is m. Then $(xH)^m = x^m H = eH$ which implies that $p \mid m$. Thus $x^{m/p}$ is an element of order p. This finishes the induction step.

(ii) Using Class Equation, or otherwise, prove Cauchy's theorem for finite non-abelian groups.
Solutions: Again we will use induction. If p divides the centre $Z(G)$ of G, then by the abelian version, there is an element of order p in $Z(G)$ and hence in G. Otherwise by the Class equation there exits at least one conjugacy class represented by an element g_i such $p \nmid [G : C_G(g_i)] = |G|/|C_G(g_i)|$. Since $p \mid |G|$, this implies that $p \mid |C_G(g_i)|$. Since $g_i \notin Z(G)$, therefore $C_G(g_i)$ is a proper subgroup of G. Hence by induction hypothesis there exists an element of order p in $C_G(g_i)$ and hence G.

(6) (a) Show that $C_{S_n}((12)(34)) = 8 \times (n-4)!$ for all $n \geq 4$. Determine the elements of the centralizer explicitly.
Solution: Let $\sigma \in C_{S_n}((12)(34))$. Then we must have $\sigma((12)(34))\sigma^{-1} = (\sigma(1), \sigma(2))(\sigma(3), \sigma(4)) = (12)(34)$. We note that σ has to take the first four numbers to themselves and hence the last $n-4$ to themselves. Thus σ must belong to a subgroup isomorphic to the product $\{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\} \times S_{n-4}$. Thus the cardinality of the centralizer of $(12)(34)$ is $8 \times (n-4)!$.

(b) Show that if n is odd, the set of all n-cycles consists of two conjugacy classes of equal size in A_n.
Solution: Suppose a group G acts on a set X. Let $x \in X$ and let K be the stabilizer of x in G. Let H be a subgroup of G. Then stabilizer

of x in H is $K \cap H$. Let us denote the orbits of x under G and H actions by $\mathcal{O}_G(x)$ and $\mathcal{O}_H(x)$ repectively. By orbit stabilizer theorem we have bijections between $\mathcal{O}_G(x)$ and G/K, and between $\mathcal{O}_H(x)$ and $H/(H \cap K)$. By Problem (3)(a)(iii) $H/(H \cap K) \cong HK/K$ and by Problem (3)(b), $(G/K)/(HK/K) \cong G/HK$. Thus we have

$$\frac{|\mathcal{O}_G(x)|}{|\mathcal{O}_H(x)|} = \frac{|G|}{|HK|}.$$

In particular, for n odd, put $G = S_n, H = A_n$ and X to be the set of n-cycles in S_n. The action of S_n on X is transitive. Let x be any n-cycle. Then the stabilizer $K = C_{S_n}(x)$ of x in S_n is the subgroup generated by x. This subgroup belongs to A_n. Hence in this case we have $HK = H$. Thus $|\mathcal{O}_{S_n}(x)| = (|S_n|/|A_n|)|\mathcal{O}_{A_n}(x)| = 2|\mathcal{O}_{A_n}(x)|$. This proves that the set of all n-cycles consists of exactly two conjugacy classes of equal sizes in A_n.