UPSC Civil Services Main 1995 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let G be a finite set closed under an associative binary operation such that $ab = ac \Rightarrow b = c, ba = ca \Rightarrow b = c$ for all $a, b, c \in G$. Prove that G is a group.*

Solution. Let $G = \{a_1, a_2, \ldots, a_n\}$. Consider $\{a_1a_1, a_2a_1, \ldots, a_na_1\}$ and $\{a_1a_1, a_1a_2, \ldots, a_1a_n\}$. These sets have distinct elements because $a_ja_i = a_ka_i \Rightarrow a_j = a_k$, and $a_ia_j = a_ia_k \Rightarrow a_j = a_k$. Thus $G = \{a_1, a_2, \ldots, a_n\} = \{a_1a_1, a_2a_1, \ldots, a_na_1\} = \{a_1a_1, a_1a_2, \ldots, a_1a_n\}$. Thus there exists $r, 1 \leq r \leq n$ such that $a_1 = a_1a_r$. Now for any $a_j \in G$, $a_j = a_sa_1$ for some s, therefore $a_ja_r = a_sa_1a_r = a_sa_1 = a_j$. Hence we have proved that G has a right identity. As seen above, for any $a_j \in G$, the set $\{a_ja_1, a_ja_2, \ldots, a_ja_n\} = G$, hence therefore there exists $k, 1 \leq k \leq n$ such that $a_ja_k = a_r$, thus every element has a right inverse.

Similarly, we can show that G has a left identity and every element in G has a left inverse. Let a_s be the left identity. Then $a_r = a_sa_r = a_s$, so the left identity is the same as the right identity. If $a_ia_j = a_r$ and $a_ka_i = a_r$, then $a_k = a_ka_r = a_ka_ia_j = a_ra_j = a_j$ (using associativity), hence the left inverse is the same as the right inverse. Thus G has an identity, every element of G has an inverse, and the operation is associative, so G is a group.

Alternatively, let $x \in G$ and let $xy = e$, where e is the right identity. Then $exy = ee = e = xy \Rightarrow ex = x$, so e is also the left identity. Now $yxy = ye = ey \Rightarrow yx = e$, thus the right inverse is the same as the left inverse. ∎

Question 1(b) *Let G be a subgroup of order p^n, where p is a prime number and $n > 0$. Let H be a proper subgroup of G and $N(H) = \{x \in G \mid x^{-1}hx \in H \text{ for every } h \in H\} = \{x \in G \mid x^{-1}Hx = H\}$. Prove that $N(H) \neq H$.*

Solution. The proof is by induction over n. If $n = 1$, then $H = \{e\}$ is the only possibility for a proper subgroup, since G is cyclic. $N(H) = G \neq H$. If $n = 2$, it is well known that G is abelian, and therefore for any proper subgroup H of G, $N(H) = G \neq H$.

Assume as induction hypothesis that the result is true for all groups of order p^m where $m < n$.

Let G be a group of order p^n and let H be a proper subgroup of G. We consider the following two possible cases

Case (i): H does not contain C, the center of G, then there exists an element $z \in C - H$. Clearly $z \in N(H)$ and therefore $N(H) \supset H$ properly.

Case (ii): $H \supseteq C$. In this case $\overline{H} = H/C$ is a proper subgroup of $\overline{G} = G/C$. Since G is a prime power group, it is known that the center C of G is nontrivial, therefore $|\overline{G}| =$ order of $\overline{G} = p^m$ where $m < n$. Thus by the induction hypothesis the normalizer of $\overline{H}$ in $\overline{G}$ contains $\overline{H}$ properly, i.e. there exists an element $b \in G$ such that $\overline{b} \notin \overline{H}$ and $\overline{b} \in N(\overline{H})$ i.e. $\overline{b}^{-1}\overline{H}\overline{b} = \overline{H}$. It is now obvious that $b \notin H$ and $b^{-1}Hb \subseteq HC = H$ i.e. $b \in N(H)$. Hence $N(H) \neq H$.

Alternative presentation: Let $C_o = \{e\}$, $C_1 =$ center of G. If $C_1 \neq G$, let Z_1 be the center of G/C_1. Let $C_2 = \eta^{-1}(Z_1)$, where $\eta : G \longrightarrow G/C_1$ is the natural map. Thus $C_2/C_1 = Z_1$. If $C_2 \neq G$, we define $C_3 = \eta^{-1}(\text{center of } G/C_2)$, where η is now the natural map from G ont G/C_2.

Clearly $C_0 \subsetneq C_1 \subsetneq C_2 \subsetneq \dots$ because the center of a prime power group is non-trivial. Since G is finite, we have $C_r = G$ for some r. Thus $C_0 \subsetneq C_1 \subsetneq C_2 \subsetneq \dots \subsetneq C_r = G$. Now each C_i is normal in G, because Z_1 is normal in $G/C_1 \Rightarrow \eta^{-1}(Z_1) = C_2$ is normal in G and so on.

Since $C_0 \subseteq H$, and $C_r \not\subseteq H$, there is a $k, 0 \leq k < r$ such that $C_k \subseteq H$, $C_{k+1} \not\subseteq H$. Let $x \in C_{k+1}, x \notin H$. For any $g \in G, x^{-1}g^{-1}xg \in C_k$, because $xC_k \in$ center of $G/C_k, x \in C_{k+1}$, which means that $xgC_k = xC_kgC_k = gC_kxC_k = gxC_k$. Thus $x^{-1}g^{-1}xg \in C_k$.

In particular $x^{-1}h^{-1}xh \in C_k \forall h \in H$. Thus $x^{-1}h^{-1}xh \in H$ because $C_k \subseteq H$, or $x^{-1}h^{-1}x \in H$ for all $h \in H$. Thus $x \in N(H)$. But $x \notin H$, so $N(H) \neq H$. ∎

Question 1(c) *Show that a group of order 112 is not simple.*

Solution. Let G be a group of order 112.

If the Sylow 2-subgroup, which is of order 16, is unique, then it is automatically a normal subgroup of G and we have nothing to prove.

Let us therefore assume that G has more than one Sylow 2-subgroups. By one of Sylow theorems, the number of such subgroups is $\equiv 1 \mod 2$, and is a divisor of 112 and therefore of 7. Thus G has 7 subgroups say $H_1, H_2, \dots, H_7$ such that $|H_i| = 16, 1 \leq i \leq 7$.

Observe that $H_i \cap H_j$ for $i \neq j$ must have at least 4 elements because if not $|H_iH_j| \geq 128$ as $|H_iH_j| = \frac{|H_i||H_j|}{|H_i \cap H_j|}$, which is not possible.

We now consider the following two cases.

Case 1: Suppose (without loss of generality) that $|H| = |H_1 \cap H_2| = 8$. This means that H is a normal subgroup of H_1 as well as H_2 and therefore $N(H)$ contains H_1H_2. But $|H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = 32$, therefore $|N(H)| \geq 32$ and 16 divides $|N(H)|$ as $N(H) \supset H$. Consequently $|N(H)| = 112$ i.e. $N(H) = G$. Thus H is a normal subgroup of G showing that G is not simple.

Case 2: Let $|H_i \cap H_j| = 4$ for $i \neq j$. Let $H = H_1 \cap H_2$, then $|H| = 4$. We have proved in question 1(b) that $N_{H_1}(H)$ (the normalizer of H in H_1) contains H properly and also $N_{H_2}(H)$ contains H properly. Thus each of $N_{H_1}(H)$ and $N_{H_2}(H)$ have 8 or 16 elements.

Case 2(a): One of the normalizers has 16 elements — suppose without loss of generality that $N_{H_1}(H) = H_1$, then $N_G(H)$ contains H_1 and $N_{H_2}(H)$ and therefore $N_G(H)$ contains at least $16 \times 8/4$ elements, and 16 divides $|N_G(H)|$ as $H_1 \subset N_G(H)$ — note that $|H_i| = 16, |N_{H_2}(H)| \geq 8$ and $H_1 \cap N_{H_2}(H)$ being a subgroup of $H_1 \cap H_2$ has at most 4 elements. Thus as in case 1, we get $N_G(H) = G$, so H is a normal subgroup of G, showing that G is not simple.

Case 2(b): $N_{H_1}(H) \neq H_1$ and $N_{H_2}(H) \neq H_2$, then $|N_{H_1}(H)| = |N_{H_2}(H)| = 8$. In this case $N_G(H)$ contains at least $8 \times 8/4$ elements and 8 divides $|N_G(H)|$. Thus $|N_G(H)| = 16$ or 56. If $|N_G(H)| = 16$, then it is one of the H_i, say $N_G(H) = H_3$, in this case $|H_1 \cap H_3| = 8$, which contradicts the precondition for case 2 i.e. $|H_i \cap H_j| = 4$ for $i \neq j$. Thus $|N_G(H)| = 56$, and in this case G is not simple as $N_G(H)$ is a proper normal subgroup of G.

This completes the proof.

Alternative Presentation. $o(G) = 2^4 \cdot 7$. The number of 7-Sylow subgroups $\equiv 1 \mod 7$ and divides $o(G)$. Thus the number of 7-Sylow subgroups is 1 or 8. If 1, then the 7-Sylow subgroup of G is normal in G, and G is not simple. Otherwise we will show that G has a unique 16-Sylow subgroup, which will be normal in G and hence G will not be simple.

Let the number of 7-Sylow subgroups be 8. This accounts for 49 elements, 48 of order 7, and the identity. Note that if H and K are Sylow subgroups of order 7, then $H \cap K = \{e\}$ if $H \neq K$ because order of H is prime.

We are now left with 63 elements + identity. The number of 2-Sylow groups is $\equiv 1 \mod 2$ and divides 7. Thus out of these 64 elements we should get 7 16-Sylow subgroups (because if there is only one 16-Sylow subgroup, it is normal, hence G is not simple). These 7 subgroups of order 16 will have a unique subgroup of order 8, which would be normal in G.

Thus in all cases, G is not simple. ∎

Question 2(a) *Let R be a ring with identity. If an element of R has more than one right inverse, show that it has infinitely many right inverses.*

Solution. Let $ax = e, ay = e, x \neq y$, then $xa \neq e$ (because $xa = e \Rightarrow xay = x \Rightarrow ey = x \Rightarrow y = x$). Consider $x, (xa - e) + x, (ya - e) + x$. Then

$$ax = a((xa-e)+x) = axa-a+ax = a-a+ax = ea((ya-e)+x) = aya-a+ax = a-a+ax = e$$

Thus we get three distinct right inverses (if $xa - e + x = ya - e + x$ then $xax = yax \Rightarrow x = y$). So given n inverses $a_1, a_2, \ldots, a_n$ of a, by considering $a_1, a_1a - e + a_1, a_2a - e + a_1, \ldots, a_na - e + a_1$ we can get $n + 1$ distinct right inverses. Hence there must be infinitely many right inverses. ∎

Question 2(b) *Let $\langle p(x)\rangle$ be an ideal generated by an irreducible polynomial in $F[x]$, F a field. Prove that it is a maximal ideal.*

Solution. Let $\langle p(x)\rangle \subsetneq M \subseteq F[x]$. We will show that $M = F[x]$.

Let $g(x) \in M, g(x) \notin \langle p(x)\rangle \Rightarrow p(x) \not| g(x)$. Thus $(g(x), p(x)) = 1$ i.e. $g(x)$ and $p(x)$ are coprime. Then there exist $a(x), b(x) \in F[x]$ such that $a(x)g(x) + p(x)b(x) = 1 \Rightarrow 1 \in M \Rightarrow M = F[x]$.

Note that $F[x]$ is a principal ideal domain. Therefore $\langle p(x), g(x)\rangle$ is a principal ideal and it has to be generated by 1, because $p(x)$ has no other divisors. ∎

Question 2(c) *Let F be a field of characteristic $p > 0$. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$. Define $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$. If $f'(x) = 0$, then prove that there exists $g(x) = F[x]$ such that $f(x) = g(x^p) = g(x)^p$.*

Solution. $f'(x) = 0 \Leftrightarrow ra_r = 0 \Leftrightarrow a_r = 0$ when $r \not\equiv 0 \mod p$. Thus $f(x) = \sum_{m=0}^{t} a_{mp}x^{mp}$ where $t = [n/p]$. Let $g(y) = a_0 + a_py + \ldots a_{tp}y^t$. Then $g(x^p) = f(x) = (g(x))^p$. ∎