UPSC Civil Services Main 1997 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Show that a necessary and sufficient condition for a subset H of a group G to be a subgroup is $HH^{-1} = H$.*

Solution. Let H be a subgroup. Clearly $H \subseteq HH^{-1}$ because $h \in H$ can be written as $h = he$ where $h \in H, e \in H^{-1} \Rightarrow h \in HH^{-1}$. If $x \in HH^{-1}$, then $x = hk^{-1}$ where $h, k \in H$. But H is a group, so $hk^{-1} \in H$, thus $HH^{-1} \subseteq H \Rightarrow HH^{-1} = H$.

Conversely, let $H = HH^{-1}$ and assume $H \neq \emptyset$.

1. $a \in H \Rightarrow a^{-1} \in H^{-1} \Rightarrow aa^{-1} \in HH^{-1} = H \Rightarrow e \in H$.
2. $x, y \in H \Rightarrow xy^{-1} \in H$. Thus $x \in H \Rightarrow x^{-1} = ex^{-1} \in H$. $x, y \in H \Rightarrow y^{-1} \in H \Rightarrow y \in H^{-1} \Rightarrow xyinH$.

Thus H is a subgroup of G. ∎

Question 1(b) *Show that the order of each subgroup of a finite group is a divisor of the order of the group.*

Solution. Lagrange's theorem, see Theorem 2.4.1 page 41 of Algebra by Herstein. ∎

Question 1(c) *In a group G, the commutator of $(a, b), a, b \in G$ is the element $aba^{-1}b^{-1}$ and the smallest subgroup containing all commutators is called the commutator subgroup of G. Show that a quotient group G/H is abelian $\Leftrightarrow H$ contains the commutator subgroup of G.*

Solution. Let G/H be abelian. Then $HaHb = HbHa \Rightarrow Hab = Hba \Rightarrow Haba^{-1}b^{-1} = H \Rightarrow aba^{-1}b^{-1} \in H$. This means H contains all the commutators, and therefore contains the group generated by them (i.e. the commutator subgroup).

Conversely, if H contains the commutator subgroup, then for any $a, b \in G, aba^{-1}b^{-1} \in H \Rightarrow Haba^{-1}b^{-1} = H \Rightarrow Hab = Hba \Rightarrow HaHb = HbHa \Rightarrow G/H$ is abelian. ∎

Question 2(a) *If $x^2 = x$ for all x in a ring R, show that R is commutative. Give an example to show that the converse is not true.*

Solution. $a + b = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b$. Thus $ab + ba = 0$. Setting $a = b$, we get $2b^2 = 0 \Rightarrow 2b = 0$. Thus $ab = -2ba + ba \Rightarrow ab = ba$. Thus R is commutative.

Converse is not true — $\mathbb{Z}$ is commutative but $n^2 \neq n$ for $n \neq 0, 1$. ∎

Question 2(b) *Show that an ideal S of the ring of integers $\mathbb{Z}$ is a maximal ideal $\Leftrightarrow$ S is generated by a prime integer.*

Solution. Let S be maximal. Since $\mathbb{Z}$ is a PID, we have $S = \langle q \rangle$ for some $q \in \mathbb{Z}, q \neq 0, 1, -1$. We will prove that if $q \mid ab, q \nmid a$ then $q \mid b$ showing that q is prime. Since $q \nmid a$, we have $a \notin S$. Consider the ideal generated by S and a. It is $\mathbb{Z}$, because S is maximal. $\langle S, a \rangle = \mathbb{Z} \;\Rightarrow\; 1 = \alpha + ta, \alpha \in S$. Thus $1 = xq + ta, \alpha = xq$. Hence $b = xbq + tab$. Clearly $q \mid$ RHS, so $q \mid b \Rightarrow q$ is a prime.

Conversely let $S = \langle p \rangle$ where p is a prime. We wish to show that S is maximal. Let A be an ideal, $A \supset S$ and $A \neq S$, then we shall show that $A = \mathbb{Z}$. Since $A \supset S, \exists a \in A, a \notin S$. Now $a \notin S \Leftrightarrow p \nmid a \Leftrightarrow (a, p) = 1 \Leftrightarrow xa + yp = 1$ for some $x, y \in \mathbb{Z} \Rightarrow 1 \in A (\because a \in A \Rightarrow xa \in A, p \in A \Rightarrow yp \in A)$. Hence $\mathbb{Z} = A$, so S is a maximal ideal. ∎

Question 2(c) *Show that in an integral domain every prime element is irreducible. Give an example to show that the converse is not true.*

Solution. Let R be an integral domain with unity. Let p be a prime element of R i.e. if $p \mid ab$ then $p \mid a$ or $p \mid b$. We have to show that if $a \mid p$ then either a is an associate of p or a is a unit. If $a \mid p$, then $p = ab$ for some $b \in R$. But p is a prime, therefore $p = ab \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$. If $p \mid a$, then p is an associate of a as $a \mid p$. If $p \mid b$, then $b = px$ for some $x \in R$. Thus $p = pax \Rightarrow ax = 1$ as R is an integral domain, thus a is a unit. Hence a prime element is irreducible.

The converse is not true. Let R be an integral domain which is not a unique factorization domain e.g. $R = \mathbb{Z}[\sqrt{-5}]$. For $\alpha = a + b\sqrt{-5}, N(\alpha) = a^2 + 5b^2$. 2 is an irreducible element of R — $2 = \alpha\beta \Rightarrow N(\alpha)N(\beta) = 4 \Rightarrow N(\alpha) = 1, 2, 4$. $N(\alpha) = 1 \Rightarrow \alpha$ is a unit, because if $\alpha = a + b\sqrt{-5}$ then $a^2 + 5b^2 = 1 \Rightarrow b = 0, a = \pm 1 \Rightarrow a$ is a unit. If $N(\alpha) = 4$, then $N(\beta) = 1$ so β is a unit. $N(\alpha) = 2$ is impossible as $a^2 + 5b^2 = 2$ is not possible.

Now 2 is not prime — $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$. But $2 \nmid 1 + \sqrt{-5}$ because $(1 + \sqrt{-5}) = 2\alpha = 2(a + b\sqrt{-5}) \Rightarrow 2a = 1$, which is not possible. Similarly $2 \nmid 1 - \sqrt{-5}$. So 2 is not prime. ∎