UPSC Civil Services Main 1989 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let G be a finite group of order $2p$, p a prime. Show that G has a normal subgroup of order p.*

Solution. Assume that G has a subgroup H of p elements. We shall show that H is normal in G. Clearly $[G : H]$ i.e. the index of H in G is 2. Let $G = H \cup Hx$, where H and Hx are distinct right cosets i.e. $x \notin H$. Consider xH, $xH \neq H$ because $x \notin H \Rightarrow xH \cap H = \emptyset \Rightarrow xH \subseteq Hx$. Similarly, $Hx \subseteq xH$. Thus if $x \notin H$, then $Hx = xH$. If $x \in H$, then $xH = H = Hx$. Thus $xHx^{-1} = H$ for every $x \in G$, so H is normal in G.

Existence of H: State Cauchy's theorem, or better yet, prove it (See theorem 2.11.3 Page 87 of Algebra by Herstein). Let a be an element of G of order p, then H, the subgroup generated by a is of order p. ∎

Question 1(b) *Give an example of an infinite group in which every element is of finite order.*

Solution. Let Ω_n = group of n-th roots of unity.

Let $G = \cup_{n=1}^{\infty}\Omega_n = \{\alpha \mid \alpha \in \mathbb{C}, \alpha^n = 1 \text{ for some } n\}$. G is a subgroup of $\mathbb{C} - \{0\}$. If $\alpha \in G, \beta \in G$, then $\alpha^m = 1, \beta^n = 1$ for some $m, n \Rightarrow (\alpha\beta)^{mn} = 1 \Rightarrow \alpha\beta \in G$. $\alpha \in G \Rightarrow \alpha^{-1} \in G \because \alpha^n = 1 \Rightarrow \alpha^{-n} = 1$. Clearly every element of G is of finite order. If G were finite, say order M, then $\alpha^M = 1$ for every $\alpha \in G$. But $\beta = e^{\frac{2\pi i}{M+1}} \in G, \beta^M \neq 1$. Thus G is not finite.

Another example: Consider the set of all infinite sequences of bits, under the operation bitwise exclusive or: $0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$. The identity element is the all 0 sequence, every element is its own inverse, and the operation is associative and commutative. The group is clearly infinite, but every element has order 2. ∎

Question 1(c) *Let G be a group and let H be the smallest group containing elements of the form $x^{-1}y^{-1}xy, x, y \in G$. Show that H is normal in G and the factor group G/H is abelian.*

Solution. Let $x \in G, h \in H$, then $x^{-1}hx = x^{-1}hxh^{-1}h$. But $x^{-1}hxh^{-1} \in H$ by definition, therefore $x^{-1}hx = x^{-1}hxh^{-1}h \in H \Rightarrow x^{-1}Hx = H$ for every $x \in G$. Thus H is normal in G.

Now in the factor group G/H, $xH.yH = xyH$. Since $x^{-1}y^{-1}xyH = H$ as $x^{-1}y^{-1}xy \in H$, it follows that $xyH = yxH = yH.xH$, thus G/H is abelian. ■

Question 2(a) *If each element of a ring is idempotent, show that the ring is commutative.*

Solution. See question 2(a), 1997. ■

Question 2(b) *If a finite field F has q elements, then show that $q = p^n$, where p is the characteristic of F.*

Solution. Let e be the multiplicative identity of F. Consider the map $\phi : \mathbb{Z} \longrightarrow F$ defined by $\phi(n) = ne$. Then ϕ is a homomorphisms of rings as $\phi(m+n) = (m+n)e = me + ne = \phi(m) + \phi(n)$ and $\phi(mn) = mne = mne^2 = me.ne = \phi(m)\phi(n)$. Now $\ker \phi = \{n \mid \phi(n) = ne = 0 \Leftrightarrow p \mid n\} = \langle p \rangle$, the ideal generated by p. Thus the field $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to a subfield of F. In other words, F contains a subfield say Λ containing p elements. Now F is finite, therefore F as a vector space over Λ is of finite dimension. Let $(F : \Lambda) = n$, and let $\{v_1, \ldots, v_n\}$ be a basis of F over Λ. Then $F = \{a_1v_1 + \ldots + a_nv_n \mid a_1, \ldots a_n \in \Lambda\}$. Since each a_i has p values, F has p^n elements. Actually, F is isomorphic to Λ^n as a vector space. ■

Question 2(c) *Let A be a ring and I be a two-sided ideal generated by the subset of all elements of the form $ab - ba, a, b \in A$. Prove that the residue class ring A/I is commutative.*

Solution.

$$\begin{aligned} A/I \text{ is commutative} &\Leftrightarrow (a+I)(b+I) = (b+I)(a+I) \forall a, b \in A \\ &\Leftrightarrow ab + I = ba + I \\ &\Leftrightarrow ab - ba \in I \text{ which is true.} \end{aligned}$$

Hence A/I is commutative. ■