UPSC Civil Services Main 2002 - Mathematics Algebra

Sunder Lal

Retired Professor of Mathematics

Panjab University

Chandigarh

December 16, 2007

Question 1(a) *Show that a group of order 35 is cyclic.*

Solution. Let G be a group of order 35. By Sylow's theorem, G has a subgroup of order 7 and the number of such groups is $\equiv 1 \mod 7$ and divides 35. If the number is $7t+1$, then $7t+1 \mid 35 \Rightarrow 7t+1 \mid 5 \Rightarrow t = 0$. Thus G has a unique Sylow subgroup H of order 7, which must be a normal subgroup of G. Similarly the number of 5-Sylow subgroups is $\equiv 1 \mod 5$ and divides 35. If this number is $5r+1$, then $5r+1 \mid 35 \Rightarrow 5r+1 \mid 7 \Rightarrow r = 0$. Thus G has a unique 5-Sylow group say K which is normal in G.

This means HK is a subgroup of G. $o(H) = 7, o(K) = 5 \Rightarrow H \cap K = \{e\}$. Let $x \in H, o(x) = 7, y \in K, o(y) = 5$. Now $xyx^{-1}y^{-1} = x \cdot yx^{-1}y^{-1} \in H, xyx^{-1} \cdot y^{-1} \in K \Rightarrow xyx^{-1}y^{-1} = e \Rightarrow xy = yx \Rightarrow o(xy) = 35$. Thus G is cyclic, xy being a generator.

More generally, $o(G) = pq, p < q, p \nmid q-1 \Rightarrow G$ is cyclic of order pq, using a similar argument. ■

Question 1(b) *Show that the polynomial* $25x^4 + 9x^3 + 3x + 3$ *is irreducible over the field of rational numbers.*

Solution. Eisenstein's irreducibility criterion states that if $f(x) = a_0 + a_1x + \ldots + a_nx^n$ is a polynomial with integer coefficients and if there is a prime p such that $p \mid a_i, 0 \leq i < n, p^2 \nmid a_0, p \nmid a_n$ then $f(x)$ is irreducible over the rationals. (Proof: see theorem 3.10.2 page 160 of Topics in Algebra by Herstein). In the present case $p = 3$ does the trick. ■

Question 2(a)

1. *Show that a group of order* p^2 *is abelian where* p *is a prime number.*
2. *Prove that a group of order 42 has a normal subgroup of order 7.*

Solution.

1. $o(G) = p^2$. Let C be the center of G. Then the center of G is nontrivial $\because$ $o(G)$ is a power of a prime. If $o(C) = p^2$, then $G = C \Rightarrow G$ is abelian. If $o(C) = p$, then G/C is cyclic of order p. Let G/C be generated by aC. Let $x, y \in G \Rightarrow xC = a^r C, yC = a^s C$ for some $r, s, 1 \leq r, s < p$. Then

$$\begin{aligned} &\Rightarrow \quad x = a^r c_1, y = a^s c_2 \quad \text{for some } c_1, c_2 \in C \\ &\Rightarrow \quad xy = a^r c_1 a^s c_2 \\ &\Rightarrow \quad xy = a^r a^s c_1 c_2 \quad \because c_1 a^s = a^s c_1 \\ &\Rightarrow \quad xy = a^s c_2 a^r c_1 = yx \end{aligned}$$

   Thus G is abelian.

2. By Sylow's theorem, G has a subgroup of order 7. The number of Sylow subgroups is $\equiv 1 \mod 7$ and divides 42. If this number is $7r+1$, then $7r+1 \mid 42 \Rightarrow 7r+1 \mid 6 \Rightarrow r = 0$. Thus this subgroup H is unique. Consider $aHa^{-1}, a \in G$. $o(aHa^{-1}) = o(H) = 7 \therefore aHa^{-1} = H$ as H is the unique subgroup of order 7. Thus H is a normal subgroup of order 7.

∎

Question 2(b) *Prove that in the ring $F[x]$ of polynomials over a field F, the ideal $I = [p(x)]$ is maximal $\Longleftrightarrow p(x)$ is irreducible over F.*

Solution. Let I be maximal. If $g(x)$ is any divisor of $p(x)$, then $[g(x)] \supseteq I \Rightarrow [g(x)] = F[x]$ or $[g(x)] = [p(x)]$. Thus $g(x)$ is a unit or $g(x)$ is an associate of $p(x)$. Thus $p(x)$ is irreducible.

Conversely let $p(x)$ be irreducible. Let M be an ideal, $M \supseteq [p(x)]$. Since $F[x]$ is Euclidean and therefore a Principal Ideal Domain, $M = [f(x)]$ say. Then $p(x) \in [f(x)] \Rightarrow f(x) \mid p(x)$. Thus $f(x)$ is a unit or $f(x)$ is an associate of $p(x) \Rightarrow M = F[x]$ or $M = [p(x)] \Rightarrow I$ is maximal. ∎

Question 2(c)

1. *Show that every finite Integral domain is a field.*

2. *Let F be a field with q elements and let E be an extension of F of degree n over F. Show that E has q^n elements.*

Solution.

1. See Lemma 3.2.2 page 127 of Algebra by Herstein.

2. E as a vector space over F has degree n. If $x_1, \ldots, x_n$ is a basis of E over F, then $\alpha \in E \Rightarrow \alpha = \alpha_1 x_1 + \ldots + \alpha_n x_n$ where $\alpha_1, \ldots, \alpha_n \in F$ are uniquely determined by α. Thus $E = \{\alpha_1 x_1 + \ldots + \alpha_n x_n \mid \alpha_i \in F\} \simeq F^n \Longrightarrow |E| = q^n$, as each α_i has q choices.

∎