UPSC Civil Services Main 1992 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *If H is a cyclic normal subgroup of a group G, then show that every subgroup of H is a normal subgroup of G.*

Solution. Let K be a normal subgroup of H. Let $H = \langle a \rangle$, and let $K = \langle a^r \rangle$, where r is the least positive integer such that $a^r \in K$.

Then $k \in K \Rightarrow k = (a^r)^m$ for some m.

$$gkg^{-1} = g(a^r)^m g = \underbrace{ga^m g \cdot ga^m g \dots ga^m g}_{r \text{ times}}$$

Now H is normal in G, so $ga^m g^{-1} \in H \Rightarrow ga^m g^{-1} = a^t$ for some t. Thus $gkg^{-1} = (a^r)^t = (a^r)^t \Rightarrow gkg^{-1} \in K$. Thus K is normal in G.

Note: Cyclic subgroups need not be normal. $G = S_3, H = \{I, (1, 2)\}$ is cyclic but not normal in S_3. ∎

Question 1(b) *Show that a group of order 30 is not simple.*

Solution. $o(G) = 3 \cdot 2 \cdot 5$.

n_5 = number of Sylow groups of order 5 is 1 or 6 because $n_5 \equiv 1 \mod 5$ and $n_5 \mid 30$.

n_3 = number of Sylow groups of order 3 is 1 or 10 because $n_3 \equiv 1 \mod 3$ and $n_3 \mid 30$.

If G has 6 Sylow groups of order 5, then G has 24 elements of order 5, because if H and K are two subgroups of order 5, then $H \cap K \ \{e\}$ when $H \neq K$. Thus each Sylow subgroup of order 5 gives rise to 4 distinct elements of order 5.

If G has 10 subgroups of order 3, then G has 20 elements of order 3. Thus either $n_3 = 1$ or $n_5 = 1$. So G has a unique Sylow subgroup of order 3 or 5, which has to be a normal subgroup of G. Thus G is not simple.

Note that $n_5 > 1, n_3 > 1$ means that G must have at least 45 elements. ∎

Question 1(c) *Let p be the smallest prime factor of the order of a group G, then prove that any subgroup of index p is normal in G.*

Solution. Let $G/H = \{x_1H, x_2H, \dots, x_pH\}$. For any $x \in G$ consider the mapping $\pi_x : G/H \longrightarrow G/H$ defined by $\pi_x(x_jH) = xx_jH = x_kH$ for some $k, 1 \leq k \leq p$. Clearly π_x is one-one and therefore gives rise to a permutation on p symbols. Let S_p denote the symmetric group on p symbold. Define $\phi : G \longrightarrow S_p$ by $\phi(x) = \pi_x$. Then ϕ is a homomorphism as

$$\pi_{xy}(x_jH) = xy(x_j(H)) = x(yx_jH) = \pi_x(\pi_y(x_jH) \;\Rightarrow\; \phi(xy) = \phi(x)\phi(y)$$

Thus by the fundamental theorem of homomorphisms G/K is isomorphic to a subgroup of S_p, where K is the kernel of ϕ.

$K \subseteq H$. Proof: Let $x \in K$. Then π_x is the identity permutation in S_p i.e. $\pi_x(x_jH) = xx_jH = x_jH$ for every $j, 1 \leq j \leq p$. Let x_r be such that $x_rH = H$, such an x_r exists then $xH = xx_rH = x_rH = H \Rightarrow x \in H$. Thus $K \subseteq H$.

$(G : K) = (G : H)(H : K)$ — This follows immediately from $(G : K) = o(G)/o(K)$. (Note that all groups are of finite order here. This statement also holds for groups of infinite order).

Let $(H : K) = r$. Then $(G : K) = pr$ and therefore $pr \mid p!$, because G/K is isomorphic to a subgroup of S_p, so order of $G/K = (G : K)$ divides $o(S_p) = p!$. Thus $r \mid (p-1)!$. But r divides $o(G)$ also, because K is a subgroup of H which is a subgroup of G. Consequently r divides $((p-1)!, o(G))$. But $((p-1)!, o(G)) = 1$ as p is the smallest prime factor of $o(G)$. Thus $r = 1 \Rightarrow K = H$. Hence H being a kernel of a homomorphism $\phi : G \longrightarrow S_p$ is a normal subgroup of G. ∎

Remark: We don't need it in the above proof, but it is worth noticing that

$$K = \cap_{a \in G} aHa^{-1}$$

$$\begin{aligned} \text{For} \quad x \in K \quad &\Leftrightarrow \quad xx_jH = x_jH \quad \forall j.1 \leq j \leq p \\ &\Leftrightarrow \quad x \in x_jHx_j^{-1} \quad \forall j.1 \leq j \leq p \\ &\Leftrightarrow \quad x \in aHa^{-1} \quad \forall a \in G \end{aligned}$$

(Note that $aHa^{-1} = x_jHx_j^{-1}$ if $a = x_jH$).

Proof of $(G : K) = (G : H)(H : K)$. Let $G/H = \{x_1H, x_2H, \dots, x_nH\}$ and $H/K = \{y_1K, \dots, y_mK\}$. Then we will show that $G/K = \{x_iy_jK \mid 1 \leq i \leq m, 1 \leq j \leq n\}$.

$$\begin{aligned} x_iy_j \equiv x_ky_l \mod K \quad &\Rightarrow \quad y_l^{-1}x_k^{-1}x_iy_j \in K \\ &\Rightarrow \quad y_l^{-1}x_k^{-1}x_iy_j \in H \\ &\Rightarrow \quad x_k^{-1}x_i \in H \quad (\because y_l, y_j \in H) \\ &\Rightarrow \quad x_kH = x_iH \Rightarrow k = i \\ &\Rightarrow \quad y_l^{-1}y_j \in K \\ &\Rightarrow \quad y_lK = y_jK \Rightarrow l = k \end{aligned}$$

Given $x \in G, xH = x_jH$ for some $j, 1 \leq j \leq n$. Since $x_j^{-1}x \in H, x_j^{-1}xK = y_kK$ for some $k, 1 \leq k \leq m$. Therefore $xK = x_jy_kK$, so $\{x_iy_jK \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a complete system of representation of cosets of G/K. This implies $(G : K) = mn = (G : H)(H : K)$.

Question 2(a) *If R is a unique factorization domain, then prove that any $f \in R[x]$ is an irreducible element of $R[x]$ if and only if either f is an irreducible element of R or f is an irreducible polynomial in $R[x]$.*

Solution. We first observe that units of R and $R[x]$ are the same — let $f, g \in R[x]$ be such that $fg = 1$ then $\deg f + \deg g = 0 \Rightarrow \deg f = 0, \deg g = 0 \Rightarrow f, g \in R$ and both are units in R.

If f is an irreducible element of R, then f is an irreducible element of $R[x]$ — if $f = gh$ then $\deg g + \deg h = 0 \Rightarrow \deg g = 0, \deg h = 0 \Rightarrow g, h \in R$, but since f is irreducible in R, either g is a unit in R or f is a unit in R, and therefore in $R[x]$.

Conversely, if f is an irreducible element in $R[x]$ and $f \in R$, then f has to be irreducible in R also, because if $f = gh$ is a proper factorization of $f \in R$, then this would be a proper factorization of f in $R[x]$ also, because units of R and $R[x]$ are the same, so g, h cannot be units in $R[x]$.

Now let $f \in R[x]$ be an irreducible element of $R[x]$ and $f \notin R$, then f is an irreducible polynomial. But an irreducible polynomial need not be an irreducible element of $R[x]$. For example, $2x^2+2$ is an irreducible polynomial in $\mathbb{Z}[x]$ but is not an irreducible element. Thus the correct question would be — $f \in R[x]$ is an irreducible element of $R[x]$ if and only if either f is an irreducible element of R or f is an irreducible *primitive* polynomial in $R[x]$. ∎

Question 2(b) *Prove that the polynomials x^2+1 and x^2+x+4 are irreducible over F, the field of integers modulo 11. Prove that $F[x]/\langle x^2+1\rangle$ and $F[x]/\langle x^2+x+4\rangle$ are isomorphic fields each having 121 elements.*

Solution. For irreducibility of the polynomial x^2+x+4 see question 2(c), 1996.

If possible let $x^2+1 \equiv (x+a)(x+b) \mod 11$ where a, b are integers. This implies that $a+b \equiv 0 \mod 11, ab \equiv 1 \mod 11 \Rightarrow a^2 \equiv -1 \mod 11$, which is not possible, since the only quadratic residues of 11 are 0, 1, 4, 9, 5 and 3. Thus x^2+1 has no linear factors modulo 11 i.e. x^2+1 is irreducible modulo 11.

Let $p(x)$ be an irreducible polynomial over a field F and α be a root of $p(x)$ in some extension of F. Then the field $F[x]/\langle p(x)\rangle$ is isomorphic to $F[\alpha]$. Proof: Consider the mapping $\rho : F[x] \longrightarrow F[\alpha]$ defined by $\rho(f(x)) = f(\alpha)$. It can be easily seen that ρ is a homomorphism, onto with kernel $\langle p(x)\rangle$. If $\deg p(x) = n$, then $(F[\alpha] : F) = n$. Clearly $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are independent over F, otherwise α will be the root of a polynomial of degree $< n$. Let $\beta \in F(\alpha) = F[\alpha]$, then $\beta = a_0 + a_1\alpha + \ldots a_r\alpha^r$, let $f(x) = a_0 + a_1x + \ldots + a_rx^r$, then there exist $q(x), s(x)$ such that $f(x) = q(x)p(x) + r(x)$ where $s(x) = 0$ or $\deg s(x) < \deg p(x)$. Thus $\beta = f(\alpha) = s(\alpha)$ as $p(\alpha) = 0$, showing that β is a linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

In case $p(x) = x^2+1, F =$ field of integers modulo 11, then $F[x]/\langle x^2+1\rangle \simeq F[\alpha]$ with $\alpha^2+1 = 0$. Now $(F[\alpha] = F(\alpha) : F) = 2$ with $1, \alpha$ as its basis. Thus $F(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in F\}$. Clearly $F(\alpha)$ has 121 elements. Similarly, $F[x]/\langle x^2+x+4\rangle$ has 121 elements.

Consider the mapping $\sigma : F[x] \longrightarrow F[x]$ defined by $\sigma(x) = x-5$ and $\sigma(a) = a$ for $a \in F$. It is obvious that σ is an isomorphism. Now $\sigma(x^2+1) = (x-5)^2+1 = x^2-10x+26 \equiv$

$x^2 + x + 4 \mod 11$. This shows that σ gives rise to a map from $K_1 = F[x]/\langle x^2+1\rangle$ to $K_2 = F[x]/\langle x^2+x+4\rangle$. Any typical element of K_1 is of the form $a_0 + a_1x + \langle x^2+1\rangle$ where $a_0, a_1 \in F$. Then $\sigma(a_0 + a_1x + \langle x^2+1\rangle) = a_0 + a_1(x-5) + \langle x^2+x+4\rangle$.

We now check that σ is an isomorphism. We write $\overline{\alpha x+\beta} = \alpha + \beta x + \langle x^2+1\rangle$. Then

$$\begin{aligned}\sigma(\overline{\alpha x+\beta} + \overline{\gamma x+\delta}) &= \sigma(\overline{(\alpha+\gamma)x+\beta+\delta}) \\ &= (\alpha+\gamma)x + \beta + \delta - 5((\alpha+\gamma) + \langle x^2+x+4\rangle \\ &= \sigma(\overline{\alpha x+\beta}) + \sigma(\overline{\gamma x+\delta})\end{aligned}$$

$$\begin{aligned}\sigma(\overline{(\alpha x+\beta)(\gamma x+\delta)}) &= \sigma(\overline{\alpha\gamma x^2 + (\alpha\delta+\beta\gamma)x + \beta\delta}) \\ &= \sigma(\overline{(\alpha\delta+\beta\gamma)x + \beta\delta - \alpha\gamma}) \text{ as } \alpha\gamma x^2 \equiv -\alpha\gamma \mod x^2+1 \\ &= (\alpha\delta+\beta\gamma)x - 5(\alpha\delta+\beta\gamma) + \beta\delta - \alpha\gamma + \langle x^2+x+4\rangle\end{aligned}$$

Now

$$\begin{aligned}&(\alpha x + \beta - 5\alpha + \langle x^2+x+4\rangle)(\gamma x + \delta - 5\gamma + \langle x^2+x+4\rangle) \\ =\ & \alpha\gamma x^2 + \alpha\delta x - 5\alpha\gamma x + \beta\gamma x + \beta\delta - 5\beta\gamma - 4\alpha\gamma x - 5\alpha\delta + 25\gamma\alpha + \langle x^2+x+4\rangle \\ =\ & \alpha\gamma(-x-4) + \alpha\delta x - 5\alpha\gamma x + \beta\gamma x + \beta\delta - 5\beta\gamma - 4\alpha\gamma x - 5\alpha\delta + 3\gamma\alpha + \langle x^2+x+4\rangle \\ =\ & x[-\alpha\gamma + \alpha\delta + \beta\gamma - 5\alpha\gamma - 5\alpha\gamma] + \beta\delta - 5\beta\gamma - 5\alpha\delta - \alpha\gamma + \langle x^2+x+4\rangle \\ \equiv\ & x[\alpha\delta + \beta\gamma] + \beta\delta - 5\beta\gamma - 5\alpha\delta - \alpha\gamma + \langle x^2+x+4\rangle \quad \mod 11\end{aligned}$$

Thus $\sigma(\overline{(\alpha x+\beta)(\gamma x+\delta)}) = \sigma(\overline{(\alpha x+\beta)})\sigma(\overline{(\gamma x+\delta)})$ showing that σ is a homomorphism.

σ is $1-1$: The kernel of σ is an ideal of K_1, but K_1 is a field, therefore the only ideals of K_1 are the trivial ideal $\langle 0\rangle$ and K_1. Since σ is not a zero map, it follows that the kernel of σ is $\langle 0\rangle$, thus σ is $1-1$.

σ is onto: Since K_1 and K_2 have 121 elements each, and *sigma* is one-one, $\sigma(K_1) = K_2$. Thus σ is an isomorphism from K_1 to K_2. ∎

Question 2(c) *Find the degree of the splitting field of $f(x) = x^5 - 3x^3 + x^2 - 3$ over $\mathbb{Q}$, the field of rationals.*

Solution. $f(x)$ has -1 as a root, so $f(x) = (x+1)(x^4 - x^3 - 2x^2 + 3x - 3)$. It does not have any other linear factors as $-1, 1, 3, -3$ are not roots of $x^4 - x^3 - 2x^2 + 3x + 3$.

Let $x^4 - x^3 - 2x^2 + 3x + 3 = (x^2 + bx + c)(x^2 + dx + e)$, where $b, c, d, e \in \mathbb{Z}$. Then $b + d = -1, c + e + bd = -2, be + dc = 3, ce = -3$. From $ce = -3$, we get $c = -1, e = 3$ or $c = 1, e = -3$ (the other choices are symmetric). Using $c = 1, e = -3$, we get $-3b + d = 3$, and now from $b + d = -1$, we get $b = -1, d = 0$. Thus we get

$$f(x) = (x+1)(x^2 - x + 1)(x^2 - 3)$$

Consequently, the splitting field of $f(x)$ over $\mathbb{Q}$ is the smallest field containing $\pm\sqrt{3}$, $\frac{1\pm i\sqrt{3}}{2}$, namely the roots of x^2-3 and x^2-x+1.

Thus $\mathbb{Q}(\sqrt{3},i)$ is the required splitting field. Since $\mathbb{Q}(\sqrt{3},i) \supseteq \mathbb{Q}(\sqrt{3}) \supseteq \mathbb{Q}$, and $(\mathbb{Q}(\sqrt{3}):\mathbb{Q}) = 2$ and $(\mathbb{Q}(\sqrt{3},i):\mathbb{Q}(\sqrt{3})) = 2$ it follows that the splitting field $\mathbb{Q}(\sqrt{3},i)$ of $f(x)$ has degree 4 over $\mathbb{Q}$. ∎