UPSC Civil Services Main 1993 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let G be a cyclic group of order n and $p \mid n$. Prove that there exists a homomorphism of G onto a cyclic group of order p. What is the kernel of the homomorphism?*

Solution. Let $G = \langle a \rangle = \{a, a^2, \dots, a^n\}$ and $G' = \langle b \rangle = \{b, b^2, \dots, b^p\}$.

Define $\phi : G \longrightarrow G'$ by $\phi(a^r) = b^t$ where $r \equiv t \mod p$, $t = 1, 2, \dots p$.

$\phi(a^r \cdot a^s) = b^u$ where $r + s \equiv u \mod p$. If $\phi(a^r) = b^x$ where $r \equiv x \mod p$ and $\phi(a^s) = b^y$ where $s \equiv y \mod p$, then $x + y \equiv r + s \equiv u \mod p \Rightarrow b^{x+y} = b^u$. So $\phi(a^r \cdot a^s) = \phi(a^r)\phi(a^s)$, thus ϕ is a homomorphism.

$\ker \phi = \{a^r \mid \phi(a^r) = b^p \Leftrightarrow r \equiv p \mod p\}$. Thus the kernel of ϕ is $\{a^p, a^{2p}, \dots, a^{mp}, mp = n\}$. ∎

Question 1(b) *Show that a group G of order 56 cannot be simple.*

Solution. The number of 7-Sylow subgroups of $\equiv 1 \mod 7$ and divides 56, so can be 1 or 8. If 1, then the 7-Sylow group is normal in G. If the number is 8, then G has 48 elements of order 7, because if H, K are different Sylow subgroups of order 7, then $H \cap K = \{e\}$ because 7 is a prime.

Thus the Sylow subgroups of order 8 can come from the remaining elements which are only 8 in number (including e). Thus there is a unique Sylow subgroup of order 8, which has to be normal.

Thus any group of order 56 has a normal subgroup of order 7 or of order 8, so it cannot be simple. ∎

Question 1(c) *Let H and K be normal subgroups of G (finite), with H a normal subgroup of K. If $P = K/H, S = G/H$, show that $G/K \simeq S/P$.*

Solution. Define $\phi : G/H \longrightarrow G/K$ by $\phi(aH) = aK$.

- ϕ is well-defined: $aH = bH \Leftrightarrow b^{-1}a \in H \Rightarrow b^{-1}a \in K(\because H \subseteq K) \Rightarrow aK = bK \Rightarrow \phi(aH) = \phi(bH)$.
- ϕ is a homomorphism: $\phi(aH \cdot bH) = \phi(abH) = abK = aK \cdot bK = \phi(aH)\phi(bH)$.
- ϕ is onto: Given $xK \in G/K, \phi(xH) = xK, xH \in G/H$.

$\ker \phi = \{xH \mid xK = K\}$. But $xK = K \Leftrightarrow x \in K$. Thus $\ker \phi = K/H$. By the fundamental theorem of homomorphisms, $S/P = \frac{G/H}{K/H} \simeq G/K$. ■

Question 2(a) *If $\mathbb{Z}$ is the set of integers, then show that $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ is not a UFD.*

Solution. Let $\alpha = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$. Then α is a unit iff $N(\alpha) = a^2 + 3b^2 = 1$, because if $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1 \Rightarrow \alpha$ is a unit with $\overline{\alpha} = a - b\sqrt{-3}$ as its inverse. Conversely, if $\alpha\beta = 1$, then $N(\alpha\beta) = N(\alpha)N(\beta) = 1 \Rightarrow N(\alpha) = 1$. In fact $N(\alpha) = 1 \Rightarrow \alpha = \pm 1$, the only units of $\mathbb{Z}[\sqrt{-3}]$.

2 is irreducible. Let $2 = \alpha\beta$. We will prove that either α or β is a unit. $N(2) = 4 \Rightarrow N(\alpha) = 1, 2, 4$. But $N(\alpha) = a^2 + 3b^2 = 2$ is not possible for $a, b \in \mathbb{Z}$. If $N(\alpha) = 1$, then α is a unit, otherwise $N(\alpha) = 4 \Rightarrow N(\beta) = 1 \Rightarrow \beta$ is a unit. Thus 2 is irreducible.

Similarly it can be shown that $1 + \sqrt{-3}, 1 - \sqrt{-3}$ are irreducible $(N(1 + \sqrt{-3}) = 4)$. Moreover, $2, 1 + \sqrt{-3}, 1 - \sqrt{-3}$ are not associates of each other as the only units in $\mathbb{Z}[\sqrt{-3}]$ are ± 1. Now $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ are two different factorizations of 4 into irreducibles, hence $\mathbb{Z}[\sqrt{-3}]$ is not a UFD. ■

Question 2(b) *Construct the addition and mutiplication table for $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$, where $\mathbb{Z}_3$ is the set of integers modulo 3 and $\langle x^2 + 1\rangle$ is the ideal generated by $1 + x^2$.*

Solution. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ with $a_i \in \mathbb{Z}_3$. Since

$$x^r \equiv \left[\begin{array}{l} (-1)^{r/2} \\ (-1)^{\frac{r-1}{2}} x \end{array}\right. \mod x^2 + 1$$

it follows that

$$\begin{aligned} f(x) &\equiv a_0 + a_1 x - a_2 - a_3 x + a_4 + \ldots \mod x^2 + 1 \\ &= [b_o] + [b_1][x] \end{aligned}$$

where $[x]$ is the residue class of x modulo $x^2 + 1$ and $[b_0], [b_1]$ are residue classes in $\mathbb{Z}_3$. Conversely, $[b_o] + [b_1][x]$ always belongs to $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$.

Thus $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ has 9 elements, namely

$$\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

Note that we have listed representative elements of distinct residue classes modulo x^2+1.

Now addition is simply: $(a_0+a_1x)+(b_0+b_1x) = c_0+c_1x$ where $c_i \equiv a_i+b_i \mod 3$ for $i = 0, 1$.

Multiplication is defined by $(a_0+a_1x)(b_0+b_1x) = c_0+c_1x$ where $c_0 \equiv a_0b_0 - a_1b_1 \mod 3$ and $c_1 \equiv a_0b_1+a_1b_0 \mod 3$. The reader can now expand these into the appropriate addition and multiplication tables.

Notice the strong resemblance between the addition and multiplication rules derived above and the corresponding rules for complex numbers. This is a consequence of the fact that i is a root of x^2+1, in fact the ring of Gaussian integers is isomorphic to $\mathbb{Z}[x]/\langle x^2+1\rangle$. ∎

Question 2(c) *Let $\mathbb{Q}$ be the rational number field, and $\mathbb{Q}(2^{1/2}, 2^{1/3})$ by the smalled extension field containing $2^{1/2}, 2^{1/3}$. Find a basis of $\mathbb{Q}(2^{1/2}, 2^{1/3})$ over $\mathbb{Q}$.*

Solution. If $K \supseteq L \supseteq k$ are fields such that $(K : L) = m, (L : k) = n$ then $(K : k) = mn$. In fact if $\{v_1, \ldots, v_m\}$ is a basis of K over L, $\{w_1, \ldots, w_n\}$ is a basis of L over k, then $\{v_iw_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of K over k.

Proof: Let $\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}v_iw_j = 0$ with $a_{ij} \in k$. Then $\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}v_iw_j = \sum_{i=1}^{m}(\sum_{j=1}^{n} a_{ij}w_j)v_i = 0$. But $\sum_{j=1}^{n} a_{ij}w_j \in L$, and as $v_1, \ldots, v_m$ are linearly independent over L, $\sum_{j=1}^{n} a_{ij}w_j = 0$ for each $i, 1 \leq i \leq m$. However $w_1, \ldots, w_n$ are linearly independent over k, thus $a_{ij} = 0$ for $1 \leq i \leq m, 1 \leq j \leq n$.

Let $\alpha \in K$. Then $\alpha = \sum_{i=1}^{m} \alpha_iv_i, \alpha_i \in L$. Now let $\alpha_i = \sum_{j=1}^{n} a_{ij}w_j$ with $a_{ij} \in k$, then $\alpha = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}v_iw_j \Rightarrow \{v_iw_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ generate K over k. This completes the proof.

Now $\mathbb{Q}(2^{1/2})$ has $\{1, \sqrt{2}\}$ as a basis over $\mathbb{Q}$, and $(\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/2})) = 3$ with x^3-2 as the irreducible polynomial of $2^{1/3}$ over $\mathbb{Q}(2^{1/2})$. Thus $1, 2^{1/3}, 2^{2/3}$ is a basis of $(\mathbb{Q}(2^{1/2}, 2^{1/3})$ over $\mathbb{Q}(2^{1/2})$. Thus by the above result, $\{1, 2^{1/2}, 2^{1/3}, 2^{1/2+1/3}, 2^{2/3}, 2^{2/3+1/2}\}$ is a basis for $\mathbb{Q}(2^{1/2}, 2^{1/3})$ over $\mathbb{Q}$. ∎