UPSC Civil Services Main 2006 - Mathematics Algebra

Sunder Lal
Retired Professor of Mathematics
Panjab University
Chandigarh

December 16, 2007

Question 1(a) *Let S be the set of all real numbers except -1. Define $*$ on S by*

$$a * b = a + b + ab$$

Is $(S, *)$ a group? Find the solution of the equation

$$2 * x * 3 = 7$$

in S.

Solution. Clearly $S \neq \emptyset$.

1. S is closed for the operation $(*)$. If $a+b+ab = -1$, then $a+b+ab+1 = (a+1)(b+1) = 0 \Rightarrow a = -1$ or $b = -1$. Thus $a, b \in S \Rightarrow a \neq -1, b \neq -1 \Rightarrow a+b+ab \neq -1 \Rightarrow a*b \in S$.

2. $a * 0 = 0 * a = a + 0 + a.0 = a$, showing that 0 is the identity for S.

3. $a \neq -1$, then $b = -\frac{a}{1+a} \neq -1$ and $a * b = b * a = a - \frac{a}{1+a} - \frac{a^2}{1+a} = 0$, thus S is closed with respect to inverses for the operation $(*)$.

4. $a * b = b * a$ for every $a, b \in S$.

5. $(a*b)*c = (a+b+ab)*c = a+b+ab+c+ac+bc+abc$ and $a*(b*c) = a*(b+c+bc) = a+b+c+bc+ab+ac+abc$. Thus $(a*b)*c = a*(b*c)$ thus the operation $(*)$ is associative.

Hence $(S, *)$ is an abelian group.

$2 * x * 3 = 2 + x + 3 + 2x + 3x + 6 + 6x$. Therefore we want $12x + 11 = 7$, so $x = -\frac{1}{3}$. ∎

Question 1(b) *If G is a group of real numbers under addition and $\mathbb{N}$ is the subgroup of G consisting of the integers, prove that $G/\mathbb{N}$ is isomorphic to the group H of all complex numbers of absolute value 1 under multiplication.*

Solution. Let $f : G \longrightarrow H$ be defined by $f(\alpha) = e^{2i\pi\alpha}$. Then f is an onto homomorphism.

1. $f(\alpha + \beta) = e^{2i\pi(\alpha+\beta)} = e^{2i\pi\alpha}e^{2i\pi\beta} = f(\alpha)f(\beta)$.

2. Let z be any complex number with $|z| = 1$, then $z \neq 0$. Let $\theta = \arg z$, then

$$f(\frac{\theta}{2\pi}) = e^{i\theta} = z$$

Moreover kernel $f = \mathbb{N}$, because $\alpha \in$ kernel f if and only if $e^{2i\pi\alpha} = 1 \Leftrightarrow \alpha \in \mathbb{N}$. Thus by the fundamental theorem of homomorphisms $G/\mathbb{N}$ is isomorphic to H.

Alternative solution. Let f be as defined above. Define $\phi : G/\mathbb{N} \longrightarrow H$ by $\phi(\overline{\alpha}) = \phi(\alpha + \mathbb{N}) = f(\alpha)$ for $\alpha \in G$. Then

1. ϕ *is well defined* i.e.. if $\overline{\alpha} = \overline{\beta}$ then $\phi(\overline{\alpha}) = \phi(\overline{\beta})$ i.e. ϕ does not depend on the choice of representative in the coset. Clearly $\overline{\alpha} = \overline{\beta} \Leftrightarrow \alpha - \beta \in \mathbb{N} \Rightarrow e^{2i\pi\alpha} = e^{2i\pi\beta} \Rightarrow f(\alpha) = f(\beta)$.

2. ϕ *is a homomorphism.* $\phi(\overline{\alpha} + \overline{\beta}) = \phi(\overline{\alpha + \beta}) = f(\alpha + \beta) = f(\alpha)f(\beta) = \phi(\overline{\alpha})\phi(\overline{\beta})$.

3. ϕ *is 1-1.* If $\overline{\alpha} \neq \overline{\beta}$, then $\alpha - \beta \notin \mathbb{N}$ and therefore $e^{2i\pi(\alpha-\beta)} \neq 1 \Rightarrow f(\alpha) \neq f(\beta) \Rightarrow \phi(\overline{\alpha}) \neq \phi(\overline{\beta})$.

4. ϕ *is onto.* If z is any complex number with $|z| = 1$ and $\alpha \in G$ is so determined that $f(\alpha) = z$ (as above) then $\phi(\overline{\alpha}) = f(\alpha) = z$.

Thus ϕ is an isomorphism from $G/\mathbb{N}$ onto H i.e. $G/\mathbb{N}$ is isomorphic to H. ∎

Question 2(a)

1. *Let $O(G) = 108$. Show that there exists a normal subgroup of order 27 or 9.*

2. *Let G be the set of all those ordered pairs (a, b) of real numbers for which $a \neq 0$ and define in G an operation $\otimes$ as follows:*

$$(a, b) \otimes (c, d) = (ac, bc + d)$$

Examine whether G is a group with respect to the operation $\otimes$. If it is a group, is G abelian?

Solution.

1. According to one of the Sylow theorems, the number of subgroups of G of order 27 is $\equiv 1$ (modulo 3) and is a divisor of 108 and therefore of 4, thus the number of such subgroups is 1 or 4. If G has a unique Sylow group H of order 27, then it has to be a normal subgroup because $O(a^{-1}Ha) = 27$ and therefore $a^{-1}Ha = H$ for every $a \in G$. Let us therefore assume that G has more than one subgroup of order 27. Then G has four subgroups of order 27, say H_1, H_2, H_3, H_4.

   We first of all observer that $H_i \cap H_j$ must have at least 9 elements, because if not, then $|H_iH_j|$, the number of elements in H_iH_j, would be at least 243 as $|H_iH_j| = \frac{|H_i||H_j|}{|H_i \cap H_j|}$, and this is not possible. Let $H = H_i \cap H_j, i \neq j$, then $O(H) = 9$, because $H_i \neq H_j$. Now $N_{H_i}(H)$, the normalizer of H in H_i, contains H properly (see 1995 question 1(b)), showing that $N_{H_i}(H) = H_i$ and similarly $N_{H_j}(H) = H_j$. Thus $N_G(H) \supseteq H_i$ as well as H_j and therefore $O(N_G(H)) \geq 81$ and is divisor of 108. Hence $N_G(H) = G$ and H is a normal subgroup of G. Thus G has a normal subgroup of order 27 or of order 9.

2. We observe that $G \neq \emptyset$ and

   (a) *G is closed with respect to the operation $\otimes$* i.e. $(a, b), (c, d) \in G \Rightarrow (a, b) \otimes (c, d) \in G$.

   (b) *(1, 0) is identity of G w.r.t.* $\otimes$ as $(a, b)(1, 0) = (a, b) = (1, 0) \otimes (a, b)$

   (c) If $(a, b) \in G$, then $(a^{-1}, -ba^{-1}) \in G$ as $a \neq 0$, and $(a, b) \otimes (a^{-1}, -ba^{-1}) = (1, 0) = (a^{-1}, -ba^{-1})(a, b)$. Thus every element of G has an inverse w.r.t. the operation $\otimes$ and it belongs to G.

   (d) $(a, b) \otimes ((c, d) \otimes (e, f)) = (a, b) \otimes (cd, de + f) = (ace, bce + de + f) = ((a, b) \otimes (c, d)) \otimes (e, f)$

   Thus G is a subgroup w.r.t. operation $\otimes$. G is not an abelian group, as $(a, b) \otimes (2, 0) = (2a, 2b)$ whereas $(2, 0) \otimes (a, b) = (2a, b)$ showing that $(2, 0) \otimes (a, b) \neq (a, b) \otimes (2, 0)$ when $b \neq 0$.

∎

Question 2(b) *Show that $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.*

Solution. Definition: An integral domain $R \neq \{0\}$ is called a Euclidean domain if there exists a function $g : R - \{0\} \longrightarrow \mathbb{Z}$ (ring of integers) such that

1. $g(a) \geq 0$ for every $a \in R^* = R - \{0\}$.

2. For every $a, b \in R^*, g(ab) \geq g(a)$.

3. Euclid's Algorithm: For every $a \in R, b \in R^*$, there exist $q, r \in R$ such that $a = bq + r$, where $r = 0$ or $g(r) < g(b)$.

For $\alpha \in \mathbb{Z}[\sqrt{2}], \alpha = a + b\sqrt{2}, a, b \in \mathbb{Z}$, we define $N(\alpha) = a^2 - 2b^2$ and $g(\alpha) = |N(\alpha)|$. Clearly

1. $g(\alpha) \geq 0$ for every $\alpha \in \mathbb{Z}[\sqrt{2}], \alpha \neq 0$.

2. For $\alpha, \beta \in \mathbb{Z}[\sqrt{2}], \alpha \neq 0, \beta \neq 0,\ g(\alpha\beta) = g(\alpha)g(\beta) \geq g(\alpha)$ because $g(\beta) \geq 1$.

   Note that if $\alpha = a + b\sqrt{2}, \beta = c + d\sqrt{2}$, then

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 - 2b^2)(c^2 - 2d^2) \\ &= a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2 \\ &= (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= N(ac + 2bd + \sqrt{2}(ad + bc)) \\ &= N(\alpha\beta) \end{aligned}$$

3. Let $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $\beta = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $\beta \neq 0$. Clearly

$$\frac{\alpha}{\beta} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = p + q\sqrt{2}$$

   where $p = \frac{ac-2bd}{c^2-2d^2}, q = \frac{bc-ad}{c^2-2d^2}$ are rational numbers. Let m, n be the integers nearest to p, q respectively i.e. $|p - m| \leq \frac{1}{2}, |q - n| \leq \frac{1}{2}$. Note that if $p = [p] + \theta$, where $0 \leq \theta < 1$ and $[p]$ is the integral part of p, then $m = [p]$ if $\theta \leq \frac{1}{2}$ and $m = [p] + 1$ if $\theta > \frac{1}{2}$.

   Let $p - m = r, q - n = s$, then $|r| \leq \frac{1}{2}, |s| \leq \frac{1}{2}$. Now

$$\begin{aligned} \alpha &= a + b\sqrt{2} = (c + d\sqrt{2})(p + q\sqrt{2}) \\ &= (c + d\sqrt{2})((m + r) + (n + s)\sqrt{2}) \\ &= (c + d\sqrt{2})(m + n\sqrt{2}) + (c + d\sqrt{2})(r + s\sqrt{2}) \end{aligned}$$

   Let $\gamma = m + n\sqrt{2}, \delta = (c + d\sqrt{2})(r + s\sqrt{2})$, then $\alpha = \beta\gamma + \delta$, where $\gamma \in \mathbb{Z}[\sqrt{2}]$ and $\delta = \alpha - \beta\gamma \in \mathbb{Z}[\sqrt{2}]$.

   Now either $\delta = 0$ or $g(\delta) = |N(\beta)||r^2 - 2s^2|$. But $|r^2 - 2s^2| \leq \frac{1}{4} + \frac{2}{4} < 1$, therefore $g(\delta) < g(\beta)$. Thus given $\alpha, \beta \in \mathbb{Z}[\sqrt{2}], \beta \neq 0$, we have found $\gamma, \delta \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha = \beta\gamma + \delta$ where $\delta = 0$ or $g(\delta) < g(\beta)$.

This shows that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain. ∎