UPSC Civil Services Main 1996 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let $\mathbb{R}$ be the set of all real numbers and $G = \{(a, b) \mid \ a, b \in \mathbb{R}, a \neq 0\}$. Let $x : G \times G \longrightarrow G$ be defined by $(a, b) * (c, d) = (ac, bc + d)$. Show that $(G, *)$ is a group. Is it abelian? Is $(H, *)$ a subgroup of $(G, *)$ where $H = \{(1, b) \mid \ b \in \mathbb{R}\}$?*

Solution.

1. $\alpha = (a, b) \in G, \beta = (c, d) \in G \Rightarrow \alpha * \beta \in G \because ac \neq 0$ when $a \neq 0, c \neq 0$.
2. $(a, b) * (1, 0) = (a, b.1 + 0) = (a, b)$. $(1, 0) * (a, b) = (a, 0.a + b) = (a, b)$. Hence $(1, 0)$ is identity of G.
3. $(a, b) * (1/a, -b/a) = (1, b/a - b/a) = (1, 0)$. $(1/a, -b/a) * (a, b) = (1, (-ab/a) + b) = (1, 0)$. Thus the inverse exists for every $(a, b) \in G$.
4. $(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, de + f) = (ace, bce + de + f)$. $[(a, b) * (c, d)] * (e, f) = (ac, bc + d) * (e, f) = (ace, bce + de + f)$. Thus $*$ is associative.

Hence G is a group.

G is not abelian: $(c, d) * (a, b) = (ac, da + b)$. Thus if $(a, b) * (c, d) = (c, d) * (a, b)$, then $bc + d = da + b$. This need not be true, for example if $a = d = 1, b = 0$.

If $(1, a), (1, b) \in H$, then $(1, a) * (1, b) = (1, a + b) \in H$. $(1, 0) \in H$. Finally $(1, a)^{-1} = (1, -a) \in H$, hence H is a subgroup of G. ∎

Question 1(b) *Let f be a homomorphism of a group G onto a group G' with kernel H. For each subgroup K' of G', define K as $K = \{x \mid x \in G, f(x) \in K'\}$. Prove that*

1. *K' is isomorphic to K/H.*
2. *G/K is isomorphic to G'/K'.*

Solution.

1. Let $f^* : K \longrightarrow K'$, f^* is a restriction of f. f^* is a homomorphism onto K' (onto because given $y \in K', y \in G' \Rightarrow \exists x \in G, f(x) = y$. This $x \in K$.). $\ker(f') = \{x \mid x \in K, f(x) = e'$, the identity of $G'\}$. $\ker(f^*) \subseteq H$, but $H \subseteq K$, therefore $f(x) = f^*(x) = e'$ for $x \in H$. Thus $H \subseteq \ker(f^*)$, that is $H = \ker(f^*)$. Thus $K/H \simeq K'$ by the fundamental theorem of homomorphisms.

2. Let $\phi : G \longrightarrow G'/K'$ defined by $\phi(x) = f(x)K'$. Now

   - ϕ is a homomorphism: $\phi(xy) = f(xy)K' = f(x)f(y)K' = f(x)K'f(y)K' = \phi(x)\phi(y)$.
   - ϕ is onto: Let $yK' \in G'/K'$. f is onto $\Rightarrow$ there exists $x \in G$ such that $f(x) = y$. Note that $y \in G'$. Then $\phi(x) = f(x)K' = yK'$. $\ker(\phi) = K \because x \in \ker(\phi) \Leftrightarrow f(x)K' = K' \Leftrightarrow f(x) \in K' \Leftrightarrow x \in K$. Thus $G/K \simeq G'/K'$.

∎

Question 1(c) *Prove that a normal subgroup H of a group G is maximal $\Leftrightarrow$ the quotient G/H is simple.*

Solution. Let G/H be simple. Let K be a normal subgroup of G such that $H \subseteq K$, $K \neq G$. Then K/H is a normal subgroup of G/H. G/H is simple so K/H is identity or $K/H = G/H$. If K/H is identity, then $K = H$. If $K/H = G/H$ then $K = G$. Hence H is maximal.

Conversely, let H be maximal. Let H' be a normal subgroup of G/H. Assume H' is different from the identity of G/H, i.e. H' contains at least one element different from the identity of G/H. We shall show that $H' = G/H$, showing that G/H is simple.

Let $\eta : G \longrightarrow G/H$ be the natural homomorphism. Then

$$\eta^{-1}(H') = \{x \mid x \in G, \eta(x) = Hx \in H'\}$$

is a normal subgroup of G. $\eta^{-1}(H') \supseteq H$. By assumption, there exists $x \in G, xH \neq H$ such that $xH \in H' \Rightarrow x \in \eta^{-1}(H')$ but $x \notin H$. Since H is maximal, $\eta^{-1}(H') = G \Rightarrow H' = G/H$. ∎

Question 2(a) *In a ring R, prove that the cancellation law holds in $R \Leftrightarrow R$ has no zero divisors.*

Solution. Let $ab = ac \Rightarrow b = c, a \neq 0$. Then R has no zero divisors because $ab = 0 = a0, a \neq 0 \Rightarrow b = 0$.

Conversely $ab = ac \Rightarrow a(b - c) = 0, a \neq 0 \Rightarrow b - c = 0 \Rightarrow b = c$. ∎

Question 2(b) *If S is an ideal of R and T any subring of R then prove that S is an ideal of $S + T = \{s + t \mid s \in S, t \in T\}$.*

Solution. The only thing we have to check is $\alpha \in S + T, a \in S \Rightarrow \alpha a \in S$ (the other condition $a, b \in S \Rightarrow a-b \in S$ is true). $\alpha = s+t, s \in S, t \in T$, thus $\alpha a = (s+t)a = sa+ta \in S$ because $s \in S, a \in S \Rightarrow sa \in S,\ t \in T \Rightarrow t \in R, a \in S \Rightarrow ta \in S \Rightarrow sa + ta \in S$. ∎

Question 2(c) *Prove that the polynomial $x^2 + x + 4$ is irreducible over the field of integers modulo 11.*

Solution. If $x^2 + x + 4$ were reducible modulo 11, then it would have a linear factor i.e. it would have a root in the field $\mathbb{Z}_{11}$. But

$$\begin{array}{lclcll}
x = 0 & \Rightarrow & 0 + 0 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 1 & \Rightarrow & 1 + 1 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 2 & \Rightarrow & 4 + 2 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 3 & \Rightarrow & 9 + 3 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 4 & \Rightarrow & 16 + 4 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 5 & \Rightarrow & 25 + 5 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 6 & \Rightarrow & 36 + 6 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 7 & \Rightarrow & 49 + 7 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 8 & \Rightarrow & 64 + 8 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 9 & \Rightarrow & 81 + 9 + 4 & \not\equiv & 0 & \text{mod } 11 \\
x = 10 & \Rightarrow & 100 + 10 + 4 & \not\equiv & 0 & \text{mod } 11
\end{array}$$

Therefore $x^2 + x + 4$ has no linear factor in $\mathbb{Z}_{11}[x]$ so it is irreducible in $\mathbb{Z}_{11}[x]$. ∎