# UPSC Civil Services Main 1980 - Mathematics Algebra 

Brij Bhooshan<br>Asst. Professor<br>B.S.A. College of Engg \& Technology<br>Mathura

Question 1(a) Let $R$ be a relation on a non-empty set $A$ and for every $y \in A$ let

$$
B_{y}=\{x \mid(x, y) \in R\}
$$

Show that the collection $\left\{B_{y} \mid y \in A\right\}$ is a partition if and only if $R$ is an equivalence relation.

Solution. Let $R$ be an equivalence relation. We need to show that $\left\{B_{y} \mid y \in A\right\}$ is a partition of $A$. Let $a, b \in A$. It is enough to show that if $x \in B_{a} \cap B_{b}$, then $B_{a}=B_{b}$. Let $y \in B_{a}$, then $(y, a) \in R$. As $x \in B_{a},(x, a) \in R$, and $x \in B_{b},(x, b) \in R$. Now by symmetry and transitivity of $R,(x, a) \in R \Rightarrow(a, x) \in R$, and $(y, a) \in R,(a, x) \in R \Rightarrow(y, x) \in R$, and now $(x, b) \in R \Rightarrow(y, b) \in R \Rightarrow y \in B_{b}$ so $B_{a} \subseteq B_{b}$. Similarly $B_{b} \subseteq B_{a} \Rightarrow B_{a}=B_{b}$. So $B_{a} \cap B_{b}=\emptyset$ or $B_{a}=B_{b}$ for all $a, b \in A$. Since $A=\bigcup_{a \in A} B_{a}$, the set $\left\{B_{y} \mid y \in A\right\}$ is a partition of $A$.

The converse is false. Let $A=\{a, b\}$ and let $R=\{(a, b),(b, a)\}$. Then $B_{a}=\{b\}, B_{b}=$ $\{a\}$, which is a partition of $A$, but $R$ is not an equivalence relation, as it is not reflexive or transitive.

Question 1(b) Let $I$ be the set of integers and let $R$ be a relation on $I \times I$ defined by $(m, n) R(p, q)$ if and and only if $m q=n p$. Show that $R$ is an equivalence relation and identify the partition generated by $R$.

Solution. The question as stated is not correct. $(2,3) R(0,0)$ and $(0,0) R(1,2)$, but $(2,3) R(1,2)$ is false, as $2 \times 2 \neq 3 \times 1$. However if we define $I^{*}=I-\{0\}$, and $R$ is defined as a relation over $I \times I^{*}$ with the above definition, then we can show that it is an equivalence relation.

Reflexive: Clearly $(m, n) R(m, n)$, as $m n=n m$. Symmetric: $(m, n) R(p, q) \Rightarrow(p, q) R(m, n)$ because $m q=n p \Rightarrow q m=p n$. Transitive: If $(m, n) R(p, q)$, then $m q=n p$. If $(p, q) R(r, s)$ then $p s=q r$. Thus $m q s=n p s=n q r \Rightarrow m s=n r$ because $q \neq 0$. Thus $(m, n) R(r, s)$.

Clearly $B_{(m, n)}=\{(a, b) \mid m b / n \in I, a=m b / n\}$. In fact this is isomorphic to the set of all rational numbers.

Question 1(c) Let $A$ and $B$ be any two non-empty sets. Show that the collections of all mappings from $A$ to $B$ is a proper subset of the collection of all relations from $A$ to $B$.

Solution. Let $f$ be a function from $A$ to $B$. Then the set $\{(a, f(a)) \mid a \in A\}$ is a relation from $A$ to $B$. Thus the set of all functions is a subset of the set of all relations. It is a proper subset if $B$ has more than one element - the $R=A \times B$ is a relation from $A$ to $B$, but is not a function.

Question 2(a) Show that the set of all transformations $x \longrightarrow \frac{a x+b}{c x+d}, a, b, c, d \in \mathbb{R}, a d-b c=1$ is a group. Examine whether the restricted set of transformations where $a, b, c, d$ are integers subject to the same constraint will form a group.

Solution. Let $G$ be the set of all transformations, and $H$ be the set of all transformations where $a, b, c, d$ are integers.

- $G$ is nonempty. $I: x \longrightarrow x$ is in $G$, with $a=d=1, b=c=0$.
- If $T_{1}(x)=\frac{a_{1} x+b_{1}}{c_{1} x+d_{1}}, T_{2}(x)=\frac{a_{2} x+b_{2}}{c_{2} x+d_{2}}$, then $\left(T_{2} \circ T_{1}\right)(x)=\frac{a_{2} \frac{a_{1} x+b_{1}}{c_{1} x+b_{1}}+b_{2}}{c_{2} \frac{1}{1} x+b_{1}} \frac{c_{1}+d_{2}}{c_{1} x+d_{1}}=\frac{\left(a_{1} a_{2}+b_{2} c_{1}\right) x+a_{2} b_{1}+b_{2} d_{1}}{\left(c_{2} a_{1}+d_{2} c_{1}\right) x+c_{2} b_{1}+d_{1} d_{2}}$ is an element of $G$ because $\left(a_{1} a_{2}+b_{2} c_{1}\right)\left(c_{2} b_{1}+d_{1} d_{2}\right)-\left(a_{2} b_{1}+b_{2} d_{1}\right)\left(c_{2} a_{1}+d_{2} c_{1}\right)=$ $\left(a_{1} d_{1}-b_{1} c_{1}\right)\left(a_{2} d_{2}-b_{2} c_{2}\right)=1$.
- $T \circ I=I \circ T=T$ for every $T \in G$.
- Given $T(x)=\frac{a x+b}{c x+d}, T^{-1}(x)=\frac{d x-b}{-c x+a}$ is the inverse of $T$. In fact $T \circ T^{-1}=I=T^{-1} \circ T$, this can be checked by substituting in the above formula and setting $a d-b c=1$.
- The operation is clearly associative.

Thus $G$ is a group. $H$ is clearly closed, and $T \in H \Rightarrow T^{-1} \in H$, so $H$ is a group.
In fact $G$ is isomorphic to $\left\{\left.\left(\begin{array}{ll}a & b \\ c & d\end{array}\right) \right\rvert\, a d-b c=1, a, b, c, d \in \mathbb{R}\right\}$ and $H$ is isomorphic to $\left\{\left.\left(\begin{array}{ll}a & b \\ c & d\end{array}\right) \right\rvert\, a d-b c=1, a, b, c, d \in \mathbb{Z}\right\}$.

Question 2(b) Show that a group of order 15 is cyclic.
Solution. By Cauchy's theorem, a group of order 15 has an element $a$ such that the order of $a=o(a)=5$ and $G$ has an element $b$ such that $o(b)=3$. Let $H=\langle a\rangle$, the group generated by $a$, and $K=\langle b\rangle$, the group generated by $b$. Then $H \cap K=\{e\}$, because $x \in H \Rightarrow x=e$ or $o(x)=5$, and $x \in K \Rightarrow x=e$ or $o(x)=3$.

Since $G$ has a unique subgroup of order 5 , and a unique subgroup of order 3 , by Sylow's theorems, $H, K$ are normal subgroups of $G$. Then $a b=b a$ because $a b a^{-1} \in H, b a^{-1} b^{-1} \in$ $K \Rightarrow a b a^{-1} b^{-1} \in H \cap K \Rightarrow a b=b a$. Hence $o(a b)=15 \Rightarrow G$ is cyclic.

Here we have used the fact that if in a group $G, o(x)=l, o(y)=m,(l, m)=1, x y=$ $y x \Rightarrow o(x y)=l m$.

Question 2(c) Let $G$ be a finite group and $F=\{f: G \longrightarrow \mathbb{C}\}$ be the set of all complex valued functions on $G$. If addition and multiplication in $F$ are defined for $f, g \in F$ by

$$
\begin{aligned}
(f+g)(x) & =f(x)+g(x) \\
(f g)(x) & =\sum_{y \in G} f\left(x y^{-1}\right) g(y)
\end{aligned}
$$

for every $x \in G$, show that $F$ is a ring with identity.
Solution. $F$ is a commutative group for addition is obvious, as the 0 function is the additive identity, $-f$ is the inverse of $f$, and + is commutative and associative in $\mathbb{C}$.

Let $e^{*}: F \longrightarrow \mathbb{C}$ be defined by $e^{*}(x)=1$ if $x=e, 0$ otherwise. Then

$$
\left(f . e^{*}\right)(x)=\sum_{y \in G} f\left(x y^{-1}\right) e^{*}(y)=f\left(x e^{-1}\right)=f(x)
$$

and

$$
\left(e^{*} . f\right)(x)=\sum_{y \in G} e^{*}\left(x y^{-1}\right) f(y)=f(x)
$$

because $e^{*}\left(x y^{-1}\right)=1 \Leftrightarrow x y^{-1}=e \Leftrightarrow x=y$, and all other terms vanish.

1. Thus $e^{*}$ is the multiplicative identity of $F$.
2. $f(g+h)=\sum_{y \in G} f\left(x y^{-1}\right)(g+h)(y)=f g+f h$
3. $(f+g) h=f h+g h$

Thus $F$ is a ring with identity element.

