UPSC Civil Services Main 1988 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *If H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, show that $hk = kh$ for $h \in H, k \in K$.*

Solution. Consider $hkh^{-1}k^{-1}$. Since K is a normal subgroup of G, $hkh^{-1} \in K \Rightarrow hkh^{-1}k^{-1} \in K$. Similarly, H is normal in G, so $khk^{-1} \in H \Rightarrow hkh^{-1}k^{-1} \in H$. Thus $hkh^{-1}k^{-1} \in H \cap K \Rightarrow hkh^{-1}k^{-1} = e \Rightarrow hk = kh$ as required. ∎

Question 1(b) *Show that the set of even permutations on n symbols, $n > 1$, is a normal subgroup of the symmetric group S_n and has order $n!/2$.*

Solution. Let A_n be the set of all even permutations, then $A_n \neq \emptyset$ because the identity permutation is in A_n. If $\alpha, \beta \in A_n$, then $\alpha\beta \in A_n$ because α even, β even $\Rightarrow \alpha\beta$ is an even permutation. $\alpha \in A_n \Rightarrow \alpha^{-1} \in A_n$, because α even $\Rightarrow \alpha^{-1}$ even. Thus A_n is a subgroup of S_n.

A_n is a normal subgroup. Let $\beta \in A_n$, then $\alpha\beta\alpha^{-1}$ is even for all $\alpha \in S_n$, because if α is odd, then α^{-1} is odd, so $\alpha\beta\alpha^{-1}$ is even, and if α is even, then α^{-1} is even, so $\alpha\beta\alpha^{-1}$ is even. Thus $\alpha\beta\alpha^{-1} \in A_n$ for all $\alpha \in S_n, \beta \in A_n$, so A_n is normal in S_n.

Since $n > 1$, S_n has an odd permutation, for example $(1, 2)$. Then $S_n = A_n \cup A_n(1, 2)$ is the coset decomposition of S_n modulo A_n: Let $\alpha \in S_n$. If α is even, then $\alpha \in A_n$. If α is odd, then $\beta = \alpha(1, 2)$ is even, so $\beta \in A_n$. Now $\alpha = \beta(1, 2) \in A_n(1, 2)$, so $S_n = A_n \cup A_n(1, 2)$. It is obvious the $A_n \cap A_n(1, 2) = \emptyset$, so the index of A_n in S_n is 2, i.e. the order of $A_n = n!/2$ as required. ∎

Question 1(c) *Prove that the set of inner automorphisms of a group G is a normal subgroup of the group of automorphisms of G.*

Solution. Let A be the group of automorphisms of G and let I be the set of all inner automorphisms (which are automorphisms of the form $\alpha_a(x) = axa^{-1}$ for $a \in G$).

1. $I \neq \emptyset$ as the identity automorphism is in I, because if α is the identity automorphism, then $\alpha(x) = x = exe^{-1} = \alpha_e(x)$, so $\alpha \in I$.
2. If $\alpha_a, \alpha_b \in I$, then $\alpha_a \circ \alpha_b(x) = \alpha_a(\alpha_b(x)) = a(bxb^{-1})b^{-1} = \alpha_{ab}(x) \Rightarrow \alpha_a \circ \alpha_b = \alpha_{ab} \in I$.
3. $\alpha_a \in I \Rightarrow \alpha_{a^{-1}} \in I$ and $\alpha_a \alpha_{a^{-1}} = \alpha_{aa^{-1}} = \alpha_e$. Thus $\alpha_{a^{-1}}$ is the inverse of α_a in I.

Thus I is a subgroup of G.

Let $\sigma \in A$ be arbitrary. Then for any $\alpha_a \in I$,

$$\begin{aligned}
\sigma\alpha_a\sigma^{-1}(x) &= \sigma(a\sigma^{-1}(x)a^{-1}) \\
&= \sigma(a)\sigma(\sigma^{-1}(x))\sigma(a^{-1}) \\
&= \sigma(a)x\sigma(a)^{-1} = \alpha_{\sigma(a)}(x)
\end{aligned}$$

Thus $\sigma\alpha_a\sigma^{-1} \in I$. Hence I is a normal subgroup of A. ∎

Question 2(a) *Show that the numbers $0, 2, 4, 6, 8$ with addition and multiplication modulo 10 form a field isomorphic to J_5 the ring of integers modulo 5. Give the isomorphism explicitly.*

Solution. Let $F = \{0, 2, 4, 6, 8\}$.

1. F is closed w.r.t. addition modulo 10. The addition table is

+	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

2. Addition is commutative and associative, as it is so in J_{10} and $F \subset J_{10}$.
3. Clearly $2, 8$ and $4, 6$ are inverses of each other, so F is an abelian group under addition.

4. F is closed under multiplication. The multiplication table is

$\times$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

5. 6 is the multiplicative identity, and multiplication is commutative.

6. Every non-zero element has an inverse $2 \times 8 = 4 \times 4 = 6 \times 6 = 6$.

Thus $F^* = F - \{0\}$ is a multiplicative group. Thus F is a field.

Isomorphism. For $\alpha \in \mathbb{Z}$, let $[\alpha]$ be the residue class of α modulo 5. Let $\sigma : F \longrightarrow J_5$ be defined by $\sigma(0) = [0],\ \sigma(6) = [1],\ \sigma(2) = \sigma(6+6) = \sigma(6) + \sigma(6) = [1] + [1] = [2],\ \sigma(4) = \sigma(6+6+6+6) = 4\sigma(6) = [4],\ \sigma(8) = \sigma(6+6+6) = 3\sigma(6) = [3]$. It can be easily checked that σ is an isomorphism. ∎

Question 2(b) *If R is a commutative ring with identity and U is an ideal of R. Show that U is maximal if and only if R/U is a field.*

Solution. Let U be a maximal ideal. We already know that R/U is a commutative ring with identity given by $1 + U$. R/U will be a field if we show that every nonzero element $a + U \in R/U$ is invertible. Now $a + U \neq U \Rightarrow a \notin U$. Thus the ideal generated by a and U contains U properly $\Rightarrow \langle a, U \rangle = R$ as U is maximal. Thus $1 = ab + u$ for some $b \in R, u \in U \Rightarrow (a + U)(b + U) = 1 + U \Rightarrow a + U$ is invertible. Thus R/U is a field.

Conversely, let R/U be a field, and $M \supseteq U$ be an ideal. We shall show that if $M \neq U$, then $M = R \Rightarrow U$ is maximal. Now if $M \supsetneq U \Rightarrow \exists a \in M, a \neq U$. Thus $a + U$ is a non-zero element of R/U and therefore invertible i.e. there exists $b + U \in R/U$ such that $(a + U)(b + U) = 1 + U$, or $ab - 1 \in U \Rightarrow ab - 1 \in M$. But $ab \in M$ as $a \in M$, therefore $1 \in M \Rightarrow M = R \Rightarrow U$ is maximal.

See theorem 3.5.1 Page 138 of Algebra by Herstein for a different proof. ∎

Question 2(c) *Determine all the ideals U in J_{12}, the ring of integers modulo 12. In each case describe J_{12}/U by finding a familiar ring with which the quotient ring is isomorphic. Which of these ideals is maximal?*

Solution. Let $\langle [\alpha] \rangle$ denote the ideal generated by $[\alpha] \in J_{12} = \{[0], [1], \ldots [11]\}$. Since J_{12}

is a principal ideal domain, we have to determine the distinct principal ideals. These are

$$\begin{aligned}
\langle[0]\rangle &= \{[0]\} \\
\langle[1]\rangle &= J_{12} = \langle[11]\rangle = \langle[5]\rangle = \langle[7]\rangle \\
\langle[2]\rangle &= \{[0],[2],[4],[6],[8],[10]\} = \langle[10]\rangle \\
\langle[3]\rangle &= \{[0],[3],[6],[9]\} = \langle[9]\rangle \\
\langle[4]\rangle &= \{[0],[4],[8]\} = \langle[8]\rangle \\
\langle[6]\rangle &= \{[0],[6]\}
\end{aligned}$$

If $U = \langle[2]\rangle$, then $R/U = \{[0]+U,[1]+U\} \simeq \mathbb{Z}/2\mathbb{Z}$, the isomorphism being $\sigma([0]+U) = 0 \mod 2, \sigma([1]+U) = 1 \mod 2$.

If $U = \langle[3]\rangle$, then $R/U = \{[0]+U,[1]+U,[2]+U\} \simeq \mathbb{Z}/3\mathbb{Z}$, the isomorphism being $\sigma([0]+U) = 0 \mod 3,\ \sigma([1]+U) = 1 \mod 3,\ \sigma([2]+U) = 2 \mod 3$.

If $U = \langle[4]\rangle$, then $R/U = \{[0]+U,[1]+U,[2]+U,[3]+U\} \simeq \mathbb{Z}/4\mathbb{Z}$, the isomorphism being $\sigma([0]+U) = 0 \mod 4,\ \sigma([1]+U) = 1 \mod 4,\ \sigma([2]+U) = 2 \mod 4,\ \sigma([3]+U) = 3 \mod 4$.

If $U = \langle[6]\rangle$, then $R/U = \{[\alpha]+U \mid 0 \leq \alpha \leq 5\} \simeq \mathbb{Z}/6\mathbb{Z}$, the isomorphism being $\sigma([\alpha]+U) = \alpha \mod 6$.

Clearly ideals generated by $[2],[3]$ are maximal as $R/\langle[2]\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, and $R/\langle[3]\rangle \simeq \mathbb{Z}/3\mathbb{Z}$, which are fields.

Thus J_{12} has 6 ideals, namely $\langle[0]\rangle, \langle[1]\rangle, \langle[2]\rangle, \langle[3]\rangle, \langle[4]\rangle, \langle[4]\rangle$ of which $\langle[2]\rangle, \langle[3]\rangle$ are maximal. ∎