UPSC Civil Services Main 1983 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Show that the set $I \times I$ of integers is a commutative ring with unity with respect to addition and multiplication defined as under:*

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d)\\ (a, b)(c, d) &= (ac, bd)\end{aligned}$$

Solution. Let $(a, b), (c, d), (e, f)$ be any elements of $I \times I$.

1. Clearly $I \times I$ is closed with respect to the addition operation.
2. $(0, 0) + (a, b) = (a, b) + (0, 0) = (a, b)$. Thus $(0, 0)$ is the additive identity of $I \times I$.
3. $(a, b)+(-a, -b) = (0, 0) = (-a, -b)+(a, b)$, thus every element has an additive inverse.
4. $(a, b) + (c, d) = (a + c, b + d) = (c, d) + (a, b)$.
5. $[(a, b) + (c, d)] + (e, f) = (a + c + e, b + d + f) = (a, b) + [(c, d) + (e, f)]$. Thus $I \times I$ is an additive abelian group.
6. Clearly $I \times I$ is closed with respect to the multiplication operation.
7. $[(a, b) + (c, d)](e, f) = (ae + ce, bf + cf) = (a, b)(c, d) + (a, b)(e, f)$.
8. $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$.
9. $(1, 1)(a, b) = (a, b) = (a, b)(1, 1)$.

Thus $I \times I$ is a commutative ring with unity. ∎

Question 1(b) *Prove that the relation of isomorphism on the collection of groups is an equivalence relation.*

Solution. See 1985 Question 1(c)(4). ∎

Question 1(c) *Prove that a polynomial domain $K[x]$ over a field K is a principal ideal domain.*

Solution. Let A be an ideal of $K[x], A \neq \langle 0 \rangle, A \neq K[x]$. Let $f(x)$ be a polynomial of the smallest degree in $A - \{0\}$. Then $f(x)$ is a generator of A, proved as follows: if $g(x) \neq 0$ be any element of A. If $f(x)$ does not divide $g(x)$, then since $K[x]$ is a Euclidean domain (proof below), there exist polynomials $q(x)$ and $r(x)$ in $K[x]$ such that $g(x) = f(x)q(x) + r(x)$, where $\deg(r(x)) < \deg(f(x))$. Since $g(x), f(x) \in A$ and A is an ideal, it follows that $r(x) = g(x) - f(x)q(x) \in A$, which contradicts the fact that $f(x)$ has smallest degree in A. Thus any element of A is divisible by $f(x) \Rightarrow A = \langle f(x) \rangle$, the ideal generated by $f(x)$ (note that $0 = f(x)0$).

Proof of the fact that $K[x]$ is a Euclidean domain. The Euclidean function $d : K[x] - \{0\} \longrightarrow \mathbb{Z}$ is the degree of a polynomial.

1. $d(f(x)) \geq 0$ for every $f(x) \in K[x] - \{0\}$.

2. $d(f(x)) \leq d(f(x)g(x))$ for any $f(x) \neq 0, g(x) \neq 0$.

3. Given $g(x)$ and $f(x) \neq 0$, we show that there exist $q(x), r(x)$ such that $g(x) = q(x)f(x) + r(x)$ where $r(x) = 0$ or $d(r(x)) < d(f(x))$. The proof is by induction on the degree n of $g(x)$. If $n < d(f(x)) = m$, then $q(x) = 0, r(x) = g(x)$. Suppose the result holds for all polynomials of degree $< n$. Let $g(x) = \sum_{i=0}^{n} b_i x^i,\ b_n \neq 0$ and $f(x) = \sum_{i=0}^{m} a_i x^i$. Let $h(x) = g(x) - (b_n/a_m)x^{n-m}f(x)$. Then degree of $h(x) < n$, and therefore there exist $q_1(x)$ and $r(x)$ such that $h(x) = q_1(x)f(x) + r(x)$ where $r(x) = 0$ or $d(r(x)) < m$. Hence $g(x) = (q_1(x) + (b_n/a_m)x^{n-m})f(x) + r(x)$.

Thus $K[x]$ is a Euclidean domain. ∎