UPSC Civil Services Main 1994 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *If G is a group such that $(ab)^n = a^n b^n$ for three consecutive integers for all $a, b \in G$, then show that G is abelian.*

Solution. We are given that $(ab)^i = a^i b^i, (ab)^{i+1} = a^{i+1}b^{i+1}, (ab)^{i+2} = a^{i+2}b^{i+2}$.

Now $(ab)^{i+1} = aba^ib^i = aba^ib^i = a^{i+1}b^{i+1}$. Thus $a^ib = ba^i$.

Also, $(ab)^2(ab)^i = a^{i+2}b^{i+2} = a^2a^ib^2b^i = a^2a^ibbb^i = a^2ba^ibb^i = a^2b^2a^ib^i$, because $a^ib = ba^i$. But $(ab)^i = a^ib^i$, hence $(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2 \Rightarrow ba = ab$. Thus G is abelian.

Note that the result is false if we only have two consecutive integers e.g. $G = S_3$ has $(ab)^6 = e = a^6b^6$, and $(ab)^7 = (ab)^6ab = ab = a^7b^7$. ∎

Question 1(b) *Can a group of order 42 be simple? Justify your claim.*

Solution. By Sylow theorems, the number of 7-Sylow groups is $\equiv 1 \mod 7$, and divides 42, and therefore divides 6 $\Rightarrow$ there is only 1 Sylow group of order 7, which has to be normal, thus a group of order 42 cannot be simple. ∎

Question 1(c) *Show that the additive group of integers modulo 4 is isomorphic to the multiplicative group of the non-zero elements of integers modulo 5. State the two isomorphisms.*

Solution.

$$\begin{aligned}
\mathbb{Z}/(4) &= \{[0],[1],[2],[3]\} = \langle[1]\rangle \\
\mathbb{Z}/\langle 5\rangle &= \{[1],[2],[3],[4]\} = \langle[2]\rangle \\
&= \{[2],[2]^2 = [4],[2]^3 = [3],[2]^4 = [1]\}
\end{aligned}$$

Two cyclic groups of the same order are isomorphic. $\phi : \mathbb{Z}/(4) \longrightarrow \mathbb{Z}/\langle 5\rangle$:

$$\begin{aligned}\phi([1]) &= [2]\\ \phi([1]+[1]) &= \phi([2]) = [2]^2 = [4]\\ \phi([3]) &= \phi(3.[1]) = [2]^3 = [3]\\ \phi([4]) &= \phi(4.[1]) = [2]^4 = [1]\end{aligned}$$

$f : \mathbb{Z}/\langle 5\rangle \longrightarrow \mathbb{Z}/(4)$.

$$\begin{aligned}f([2]) &= [1]\\ f([4]) &= f([2]^2) = f([2]) + f([2]) = [2]\\ f([3]) &= f([2]^3) = f([2]) + f([2]) + f([2]) = [3]\\ f([1]) &= f([2]^4) = f([2]) + f([2]) + f([2]) + f([2]) = [4]\end{aligned}$$

∎

Question 2(a) *Find all the units of the integral domain of Gaussian integers.*

Solution. Let $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Let $N(a + ib) = a^2 + b^2$. We will show that $\alpha \in \mathbb{Z}[i]$ is a unit $\Leftrightarrow N(\alpha) = 1$.

If α is a unit then $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[i] \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta) = 1 \Rightarrow N(\alpha) = 1$ because $N(\alpha), N(\beta)$ are positive integers.

Conversely, $N(\alpha) = 1 \Rightarrow a^2 + b^2 = 1 \Rightarrow (a + ib)(a - ib) = 1 \Rightarrow \alpha$ is a unit.

Now the only integer solutions to $N(\alpha) = a^2 + b^2 = 1$ are $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Thus the only units are $\{\pm 1, \pm i\}$. ∎

Question 2(b) *Prove or disprove: The polynomial ring $I[x]$ over the ring of integers is a Principal Ideal Domain (PID).*

Solution. It is not a PID. The ideal generated by 2 and x is not a principal ideal. Suppose $\langle 2, x\rangle = \langle f(x)\rangle$. Then $2 \in \langle f(x)\rangle \Rightarrow f(x)g(x) = 2$ for some $g(x)$. This means that $f(x)$ is a constant and divides 2, so $f(x) = 1 or 2$.

$f(x) = 2 \Rightarrow x \notin \langle f(x)\rangle \because 2g(x) = x$ is not possible for any $g(x) \in I[x]$.

$f(x) = 1 \Rightarrow 1 \in \langle 2, x\rangle \Rightarrow 1 = 2p(x) + xq(x) \Rightarrow 2\times$ the constant term of $a(x) = 1$, which is not possible. Thus $\langle 2, x\rangle$ is not a principal ideal. ∎

Question 2(c) *Let R be an integral domain (not necessarily a unique factorization domain), and F its field of quotients. Show that any element $f(x) \in F[x]$ is of the form $f(x) = \frac{f_0(x)}{a}$ where $f_0(x) \in R[x]$ and $a \in R$.*

Solution. $f(x) = a_0 + a_1x + \ldots a_mx^m$, where $a_i \in F$. Now $a_i = b_i/c_i$, where $b_i, c_i \in R$. Then $f(x)\prod_i c_i = A_0 + A_1x + \ldots + A_mx^m$ where $A_i \in R$.

Thus $f(x) = \frac{f_0(x)}{a}$, where $f_0(x) = A_0 + A_1x + \ldots + A_mx^m$, and $a = \prod_i c_i$. ∎