UPSC Civil Services Main 2000 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let n be a fixed positive integer and let $\mathbb{Z}_n$ be the ring of integers modulo n. Let*

$$G = \{[a] \in \mathbb{Z}_n \mid a \neq 0, (a, n) = 1\}$$

Show that G is a group under multiplication defined in $\mathbb{Z}_n$. Hence or otherwise show that $a^{\phi(n)} \equiv 1 \mod n$ for all integers a relatively prime to n, where $\phi(n)$ denotes the number of positive integers that are less than n and relatively prime to n.

Solution. The only thing we have to show is that every element in G is invertible as we already know that G is multiplicatively closed, and has identity element namely $[1]$. Let $a_1, \ldots, a_m, m = \phi(n)$ be representatives of prime residue classes modulo n. Let a be any integer such that $(a, n) = 1$, i.e. a is coprime with n. Then $[aa_1], [aa_2], \ldots, [aa_m]$ are all distinct because $aa_i \equiv aa_j \mod n \Rightarrow a(a_i - a_j) \equiv 0 \mod n$, but $(a, n) = 1$, therefore $a_i - a_j \equiv \mod n$, which is not true. Thus there exists a j such that $aa_j \equiv 1 \mod n$, note that $G = \{[a_1], [a_2], \ldots, [a_m]\} = \{[aa_1], [aa_2], \ldots, [aa_m]\}$ and $[1] \in G$. Consequently $[a]$ is invertible, in fact $[a][a_j] = [1]$.

We know that if G is a group of order n, then $x \in G \Rightarrow x^n = e$ for every $x \in G$, where e is the identity of G — consider H the cyclic subgroup of G generated by x. Using Lagrange's theorem, which says that the order of a subgroup divides the order of a group if the group is finite, we get $o(x) = o(H) \mid o(G) = n$. Thus $n = o(x)k$, so $x^n = x^{o(x)k} = e^k = e$.

Thus if a is any integer such that $(a, n) = 1$, then $[a] \in G \Rightarrow [a]^{\phi(n)} = [1]$ because $o(G) = \phi(n)$. Hence $a^{\phi(n)} \equiv 1 \mod n$. ∎

Question 1(b) *Let M be a subgroup and N a normal subgroup of a group G. Show that MN is a subgroup of G and MN/N is isomorphic to $M/M \cap N$.*

Solution.

1. $MN \neq \emptyset$

2. $x, y \in MN \Rightarrow x = m_1n_1, y = m_2n_2$ where $m_1, m_2 \in M, n_1, n_2 \in N$. Then $xy = m_1n_1m_2n_2 = m_1m_2m_2^{-1}n_1m_2n_2$. Since N is a normal subgroup, $m_2^{-1}n_1m_2 \in N$, therefore $xy = m_1m_2n_1^*n_2$ where $n_1^* = m_2^{-1}n_1m_2$, showing that $xy \in MN$.

3. $x \in MN \Rightarrow x^{-1} = n_1^{-1}m_1^{-1} = m_1^{-1}m_1n_1^{-1}m_1^{-1} \in MN$

Thus MN is a subgroup of G.

Consider the function $f : M \longrightarrow MN/N$ defined by $f(m) = mN$. Then

1. $f(m_1m_2) = m_1m_2N = m_1Nm_2N = f(m_1)f(m_2)$ as N is a normal subgroup.

2. f is onto. If xN is any element of MN/N where $x = mn$, then $xN = mnN = mN = f(m)$.

3. $\ker f = \{m \mid f(m) = mN = N \Leftrightarrow m \in N\} = M \cap N$.

Thus f is a homomorphism, and by the fundamental theorem of homomorphisms, $M/M \cap N \simeq MN/N$. ∎

Question 2(a) *Let F be a finite field. Show that the characteristic of F must be a prime integer p and the number of elements in F must be p^m for some positive integer m.*

Solution. Let characteristic $F = n$. Let $n = \lambda\mu$ and let $a \in F, a \neq 0, 0 = na^2 = \lambda a\mu a = 0 \Rightarrow \lambda a = 0$ or $\mu a = 0$. Suppose $\lambda a = 0$. Then for any $b \in F, b \neq 0, \lambda ab = a.\lambda b = 0 \Rightarrow \lambda b = 0$ because $a \neq 0$. Thus $\lambda x = 0$ for every $x \in F$, so $\lambda = n$ because n is the smallest such integer. Thus if $n = \lambda\mu$, then $\lambda = n$ or $\mu = n$, so n is prime, say p.

Consider the mapping $f : \mathbb{Z} \longrightarrow F$ defined by $f(n) = ne$ where e is the multiplicative identity of F. It is obvious that f is a homomorphism, and that $\ker f$ is $\langle p\rangle$, the ideal generated by p. Thus $\mathbb{Z}/\langle p\rangle$ is isomorphic to a subfield of F. In other words F contains a field Λ having p elements. If $(F : \Lambda) = m$, then F has p^m elements. For details see question 2(c)(ii) year 2002. ∎

Question 2(b) *Let F be a field and $F[x]$ denote the set of all polynomials defined over F. If $f(x)$ is an irreducible polynomial in $F[x]$, show that the ideal $\langle f(x)\rangle$ generated by $f(x)$ in $F[x]$ is maximal and $F[x]/\langle f(x)\rangle$ is a field.*

Solution. Let A by an ideal, $A \supset \langle f(x)\rangle$. Since $F[x]$ is a principal ideal domain, let $A = \langle g(x)\rangle$. Then $A \supset \langle f(x)\rangle \Rightarrow f(x) = g(x)h(x)$. But $f(x)$ is irreducible, so either $g(x)$ is a unit or $g(x)$ is an associate of $f(x)$. Thus $\langle g(x)\rangle = F[x]$ or $\langle g(x)\rangle = \langle f(x)\rangle \Rightarrow \langle f(x)\rangle$ is maximal.

In order to show that $F[x]/\langle f(x)\rangle$ is a field, the only thing we have to show is that any non-zero element in $F[x]/\langle f(x)\rangle$ is invertible. Let $g(x) + \langle f(x)\rangle$ be any non-zero element in $F[x]/\langle f(x)\rangle$ i.e.$f(x) \nmid g(x)$. This means that $f(x), g(x)$ are comprime, therefore there exist

$a(x), b(x)$ such that $a(x)g(x) + b(x)f(x) = 1$. Consequently $a(x)g(x) \equiv 1 \mod f(x)$, thus $g(x) + \langle f(x) \rangle$ has $a(x) + \langle f(x) \rangle$ as an inverse in $F[x]/\langle f(x) \rangle$.

Alternately, let $g(x)$ be as above. Consider $M =$ ideal generated by $f(x), g(x)$. Since $f(x) \nmid g(x)$, $M \neq \langle f(x) \rangle$, and as $\langle f(x) \rangle$ is maximal, $M = F[x]$. Thus there exists $a(x), b(x) \in F[x]$ such that $a(x)g(x) + b(x)f(x) = 1$ and we get the same conclusion as above. ∎

Question 2(c) *Show that a finite commutative ring with no zero divisors must be a field.*

Solution. See Lemma 3.2.2 page 127 of Algebra by Herstein. ∎