UPSC Civil Services Main 2001 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let K be a field and G be a finite subgroup of the multiplicative group of the non-zero elements of K. Show that G is a cyclic group.*

Solution. Let $a \in G$ be chosen that $o(a) \geq o(b)\ \forall b \in G$ — this is possible because G is finite. We shall show that $G = \langle a \rangle$.

Step 1. For any $b \in G, o(b) \mid o(a)$. If not, there exists an element $b \in G$ s.t. $o(b) = p^l r, (p, r) = 1,\ o(a) = p^m s, (p, s) = 1$ where $l > m \geq 0$, because if all primes occurring in $o(b)$ have power less than that occurring in $o(a)$, then $o(b) \mid o(a)$. Define $x = b^r, y = a^{p^m} \Rightarrow o(x) = p^l, o(y) = s \Rightarrow o(xy) = p^l s (\because (o(x), o(y)) = 1, xy = yx) \Rightarrow o(xy) > o(a)$ which is a contradiction. Hence $o(b) \mid o(a)$.

Step 2. If $o(a) = n$, then $b^n = 1\ \forall b \in G$. Thus all elements of G are roots of $x^n - 1 = 0$. But this equation has at most n roots in K, thus $|G| \leq n$. But $o(a) = n \therefore 1, a, \ldots, a^{n-1}$ are all distinct in G. Therefore $o(G) \geq n$.

Thus $o(G) = n \Rightarrow \langle a \rangle = G$ so G is cyclic. ∎

Question 1(b) *Prove that the polynomial $1 + x + \ldots x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers.*

Solution. $f(x)$ is irreducible $\iff f(1 + x)$ is irreducible. $f(x) = \frac{x^p - 1}{x - 1}$. Thus

$$\begin{aligned} f(1+x) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + \binom{p}{p-1}x}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{r}x^{p-r-1} + \ldots + \binom{p}{p-1} \end{aligned}$$

Now $p \mid \binom{p}{r}$ for $r = 1, 2, \ldots, p-1$, as $\binom{p}{r} = \frac{p!}{r!(p-r)!}$, and $p \mid p!$, but $p \nmid r!, p \nmid (p-r)!$. Thus the Eisenstein criterion gives the result. ∎

Question 2(a) *Let N be a normal subgroup of a group G. Show that G/N is abelian $\Leftrightarrow$ for all $x, y \in G, xyx^{-1}y^{-1} \in N$.*

Solution. Let G/N be abelian, then $xNyN = yNxN \Rightarrow xyN = yxN \Rightarrow x^{-1}y^{-1}xyN = N \Rightarrow x^{-1}y^{-1}xy \in N$.

Conversely, $xyx^{-1}y^{-1} \in N \Rightarrow xyx^{-1}y^{-1}N = N \Rightarrow x^{-1}y^{-1}N = y^{-1}x^{-1}N \Rightarrow x^{-1}Ny^{-1}N = y^{-1}Nx^{-1}N$. Thus G/N is abelian. ∎

Question 2(b) *If R is a commutative ring with unit element and M is an ideal of R, show that M is a maximal ideal of R if and only if R/M is a field.*

Solution. Theorem 3.51, page 139 of Algebra by Herstein. ∎

Question 2(c) *Prove that every finite extension of a field is an algebraic extension. Give an example to show that the converse is not true.*

Solution. Let $K \mid k$ be a finite extension. Let $(K : k) = n$ i.e. dimension of K as a vector space over k is n. Let $\alpha \in K, \alpha \neq 0$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ are linearly dependent, i.e. there exist $a_0, a_1, \ldots, a_n \in k$ with at least one $a_i \neq 0$ such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$ i.e. α is a root of $f(x) = \sum_{i=0}^{n} a_i x^i$ with coefficients from k. Thus $K \mid k$ is an algebraic extension of k as every element of K is algebraic over k.

Example: Let $K = \mathbb{Q}(2^{1/n}, n = 2, 3, 4, \ldots)$. $K \mid \mathbb{Q}$ is algebraic but $(K : \mathbb{Q})$ is not finite. If $(K : \mathbb{Q}) = r$ then $2^{1/n}$ for $n > r + 1$ is a root of the polynomial of degree $\leq r + 1$, which is not possible because $2^{1/n}$ is a root of $x^n - 2 = 0$ which is an irreducible polynomial over $\mathbb{Q}$, showing that $2^{1/n}$ cannot be a root of a polynomial of degree $< n$.

$K \mid \mathbb{Q}$ is algebraic because every element is contained in a field L such that $\mathbb{Q} \subseteq L \subset K$ and $(L : \mathbb{Q}) < \infty \Rightarrow \alpha$ is algebraic over $\mathbb{Q}$. ∎