UPSC Civil Services Main 1990 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *Let G be a group having no proper subgroup. Show that G should be a finite group of order which is a prime, or unity.*

Solution. See question 1(a), 1991. Once we have proved that G is finite, then we observe that G has exactly one element if and only if the order of G is 1. If the order of $G > 1$, then we show that it is a prime number. ∎

Question 1(b) *If the order of a group is 20, show that its 5-Sylow subgroup is a normal subgroup. Also prove that a group of order 16 has a proper normal subgroup.*

Solution. We know from various Sylow theorems that the numbr of 5-Sylow subgroups $\equiv 1 \mod 5$ and is a divisor of 20 and therefore 4. Thus G, a group of order 20, has exactly one Sylow subgroup of order 5, say H. Now aHa^{-1} for any $a \in G$ is also a subgroup of order 5, therefore by uniqueness, $aHa^{-1} = H$. Thus H is normal in G.

For the second part, we prove a general theorem of which this is a special case.

Theorem. Let G be a group of order p^r, p a prime, then G has a normal subgroup of order p^s for every $s, 0 \leq s < r$.

Proof: By induction on r. If $r = 1$, then G is cyclic of prime order, hence the result is true. Assume true for groups of order $p^m, m < r$. Since G is a group of order p^r, the power of a prime, its center is non-trivial. Since the order of the center is $p^n, n \geq 1$, the center has an element, say a, of order p (Cauchy's theorem, Theorem 2.11.3 of Algebra by Herstein). Let $H = \langle a \rangle$ be the group generated by a. Since $a \in$ center of G, H is a normal subgroup of G. Now G/H is a group of order p^{r-1}. Using the induction hypothesis, we see that G/H has a normal subgroup N^* of order $p^{s-1}, 0 \leq s-1 < r-1$. Let $\eta : G \longrightarrow G/H$ be the natural homomorphism. Set $N = \eta^{-1}(N^*)$, we show that N is a normal subgroup of G of order p^s. $\eta^{-1}(N^*) \neq \emptyset$. If $x, y \in N$, then $\eta(x), \eta(y) \in N^*$, then $\eta(x)(\eta(y))^{-1} \in N^* \Rightarrow \eta(xy^{-1}) \in N^* \Rightarrow xy^{-1} \in N$, so N is a subgroup of G. For $x \in N, a \in G, \eta(x) \in N^* \Rightarrow \eta(a)\eta(x)\eta(a)^{-1} = \eta(axa^{-1}) \in N^*$ as N^* is a normal subgroup of G/H. Thus $axa^{-1} \in N$, so N is a normal subgroup of G. $N \supseteq H$ is immediate as $\forall h \in H . \eta(h) = H$, the identity element of G/H. Consider $\eta : N \longrightarrow N^*$, then η is a homomorphism with kernel $H \Rightarrow N/H \simeq N^* \Rightarrow o(N) = o(N^*)o(H) = p^s$.

Now for a group of order 16, $p = 2, r = 4$, and the above theorem shows that it has normal groups of order 2, 4, and 8. ∎

Question 1(c) *If C is the center of a group G, and G/C is cyclic, prove that G is abelian.*

Solution. See question 1(c), 1991. ∎

Question 2(a) *Show that the set of Gaussian integers is a Euclidean ring. Find an HCF of $5i$ and $3+i$.*

Solution. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain as it is a subring of the field of complex numbers.

An integral domain R is said to be a Euclidean domain if there exists a function $N : R \to \mathbb{Z}$ (the ring of integers) such that

1. $N(a) \geq 0$
2. $N(ab) \geq N(a)$ where $a, b \neq 0$
3. Given $a, b \in R, b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ where $r = 0$ or $N(r) < N(b)$.

For $\mathbb{Z}[i]$, let $N(\alpha) = N(a + ib) = a^2 + b^2$. Clearly

1. $N(\alpha) \geq 0$ for every $\alpha \in \mathbb{Z}[i]$.
2. $N(\alpha\beta) \geq N(\alpha)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ because $N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\beta) \geq 1$ if $\beta \neq 0$.
3. Let $\alpha = a + ib, \beta = m + ni, \beta \neq 0$. Then $frac\alpha\beta = \frac{a+ib}{m+ni} = x + iy, x \in \mathbb{Q}, y \in \mathbb{Q}$. Determine $p, q \in \mathbb{Z}$ such that $|x-p| \leq \frac{1}{2}, |y-q| \leq \frac{1}{2}$ (take $p = [x]$ if $x = [x]+\theta, 0 \leq \theta \leq \frac{1}{2}$ and $p = [x] + 1$ if $x = [x] + \theta, \frac{1}{2} < \theta < 1$).

   Now $\frac{\alpha}{\beta} - (p + qi) = x - p + i(y - q)$. Thus $N(\frac{\alpha}{\beta} - (p + qi)) = (x - p)^2 + (y - q)^2 < 1$.

   Now $\alpha = (p + qi)(m + ni) + \gamma$ where $\gamma = (x - p + i(y - q))(m + ni)$. Clearly $\gamma \in \mathbb{Z}[i]$ and $N(\gamma) = N(\beta)((x - p)^2 + (y - q)^2) < N(\beta)$, which is what we wanted to prove.

Thus $\mathbb{Z}[i]$ is a Euclidean ring.

Now $5i = (3 + i)(2i) + (2 - i)$, and $3 + i = (2 - i)(1 + i) \Rightarrow (5i, 3 + i) = 2 - i$.

Note: In this case writing the division algorithm was easy, otherwise $N(5) = 25, N(3 + i) = 10 \Rightarrow$ GCD is a factor of $5 = (25, 10)$. Thus the GCD can be $1, 2 - i, 2 + i, 5$. We rule out $2 + i, 5$ by showing that $2 + i \not| 3 + i$. $2 - i$ then fits the bill. ∎

Question 2(b) *If K is a finite extension of a field F of degree n, prove taht any element of K is algebraic over F with degree m where m divides n.*

Solution. Let $\alpha \in K$, then the $n+1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent over F, because $(K : F) =$ degree of K over $F = n$. Thus there exist $a_0, a_1, \ldots, a_n \in F$, not all 0, such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0 \Rightarrow \alpha$ is a root of $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x] \Rightarrow \alpha$ is algebraic over F.

Let $p(x)$ be the minimal polynomial of α over F, $\deg p(x) = m$. Then $(F(\alpha) : F) = m$ — first of all $1, \alpha, \ldots, \alpha^{m-1}$ are linearly independent over F, because otherwise α will be the root of a non-zero polynomial of degree less than m. We know that α algebraic over F implies $F(\alpha) = F[\alpha]$ as $F(\alpha)$ is the smallest field containing F and α, and $F[\alpha]$ is a field[1].

Now any element of $F[\alpha]$ is a linear combination of $1, \alpha, \ldots \alpha^{m-1}$. Take $f(\alpha)$ again. $f(x) = q(x)p(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < m$. Thus $f(\alpha) = r(\alpha)$, hence $(F(\alpha) : F) = m$. We also know that $(K : F) = (K : F(\alpha))(F(\alpha) : F)$ (See 2(c), 1993 — if $\{v_1, \ldots, v_r\}$ is a basis of K over $F(\alpha)$, and $\{w_1, \ldots, w_m\}$ is a basis of $F(\alpha)$ over F, then $\{v_i w_j \mid 1 \leq i \leq r, 1 \leq j \leq m\}$ is a basis for K over F).

Thus m divides n. ∎

Question 2(c) *Find the minimum polynomial over $\mathbb{Q}$ (the field of rationals) of $\sqrt{5 - \sqrt{2}}$ and $i + \sqrt{3}$.*

Solution. Let $x = i + \sqrt{3}$, then $(x - i)^2 = 3 \Rightarrow x^2 - 2ix + i^2 = 3 \Rightarrow x^2 - 4 = 2ix \Rightarrow (x^2 - 4)^2 = -4x^2 \Rightarrow x^4 - 4x^2 + 16 = 0$. We shall show that $x^4 - 4x^2 + 16$ is irreducible over $\mathbb{Q}$. If possible, let $x^4 - 4x^2 + 16 = (x^2 + ax + b)(x^2 + cx + d)$, then $a + c = 0, ac + b + d = -4, ad + bc = 0, db = 16$. Using $a + c = 0, ac + bd = 0$, we get $c(b - d) = 0$. If $c = 0$, then $a = 0$, so $b + d = -4, bd = 16$ so b, d are roots of $x^2 + 4x + 16$, thus b, d are not real numbers. Thus $b = d \Rightarrow b = d = \pm 4 \Rightarrow ac = -12$ or $ac = 0$ (not possible). Thus a, c are roots of $x^2 - 12 = 0$, thus are not rationals. Hence $x^4 - 4x^2 + 16$ is not reducible.

A simpler way of seeing the above is that $t^2 - 4t + 16$ has non-real roots, hence is irreducible over $\mathbb{Q}$, so $x^4 - 4x^2 + 16$ is not reducible over $\mathbb{Q}$.

Let $x = \sqrt{5 - \sqrt{2}}$. Then $x^2 - 5 = -\sqrt{2} \Rightarrow x^4 - 10x^2 + 23 = 0$ is a polynomial satisfied by $\sqrt{5 - \sqrt{2}}$. It is the minimal polynomial of $\sqrt{5 - \sqrt{2}}$ because it is irreducible over $\mathbb{Q}$, since $t^2 - 10t + 23$ has non real roots.

Hence the degree of $\sqrt{5 - \sqrt{2}}$ and $i + \sqrt{3}$ is 4. ∎

[1]Let $f(\alpha) = a_0 + a_1\alpha + \ldots + a_r\alpha^r$ be any non-zero element of $F[\alpha]$. Then the polynomial $p(x) \not| f(x) \Rightarrow (f(x), p(x)) = 1 \Rightarrow$ there exist $b(x), c(x) \in F[x]$ such that $p(x)b(x) + f(x)c(x) = 1 \Rightarrow f(\alpha)c(\alpha) = 1 \Rightarrow f(\alpha)$ is invertible