UPSC Civil Services Main 2003 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *If H is a subgroup of a group G such that $x^2 \in H$ for every $x \in G$ then prove that H is a normal subgroup of G.*

Solution. Let $h \in H, g \in G$. Then $h(h^{-1}g^{-1})^2g^2(g^{-1}hg)^2 = hh^{-1}g^{-1}h^{-1}g^{-1}g^2g^{-1}hgg^{-1}hg = g^{-1}hg$. Now $x \in G \Rightarrow x^2 \in H$, therefore $(h^{-1}g^{-1})^2, g^2, (g^{-1}hg)^2 \in H$ Consequently for any $h \in H, g^{-1}hg \in H$. Thus H is a normal subgroup of G.

Alternative solution. We shal prove that $Hx = xH$ for every $x \in G$. Clearly for any $h \in H, xh = xh.xh.h^{-1}x^{-1}x^{-1}x = h_1x$, where $h_1 = (xh)^2h^{-1}x^{-2} \in H$, this shows that $xH \subseteq Hx$. Similarly $hx = xx^{-1}x^{-1}h^{-1}hxhx = xh_1$ with $h_1 = x^{-2}h^{-1}(hx)^2 \in H$. Thus $Hx \subseteq xH$, so $xH = Hx$ for every $x \in G$. Hence H is a normal subgroup of G. ∎

Question 1(b) *Show that the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ of Gaussian integers is a Euclidean domain.*

Solution. For $\alpha = a + ib \in \mathbb{Z}[i]$, we define $N(\alpha) = a^2 + b^2$. Clearly (i) $N(\alpha) > 0$ for $\alpha \neq 0$, (ii) For $\alpha \neq 0, \beta \neq 0, N(\alpha\beta) = N(\alpha)N(\beta)$. Let $\alpha = a + ib, \beta = c + id \neq 0$. We shall find $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$ where $\delta = 0$ or $N(\delta) < N(\beta)$. This will prove $\mathbb{Z}[i]$ is a Euclidean domain for the Euclidean function $N(\alpha)$.

$$\frac{\alpha}{\beta} = \frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2} = p + iq$$

where p, q are rational numbers. We determine integers x, y so that $|p-x| \leq \frac{1}{2}, |q-y| \leq \frac{1}{2}$ — x, y are the integers nearest to p, q respectively. Let $\gamma = x + iy$. Then

$$\frac{\alpha}{\beta} = \gamma + (p - x) + (q - y)i \Rightarrow \alpha = \beta\gamma + \beta\eta = \beta\gamma + \delta$$

where $\delta = \beta\eta$. Clearly $\delta = \alpha - \beta\gamma$ is a Gaussian integer, and if $\delta \neq 0$, then $N(\delta) = N(\beta)[(p - x)^2 + (q - y)^2] \leq N(\beta)[\frac{1}{4} + \frac{1}{4}] < N(\beta)$. This completes the proof. ∎

Question 2(a) *1. Let R be the ring of all real-valued continuous functions on the closed interval $[0, 1]$. Let $M = \{f(x) \in R \mid f(\frac{1}{3}) = 0\}$. Show that M is a maximal ideal of R.*

2. Let M, N be two ideals of a ring R. Show that $M \cup N$ is an ideal of R if and only of either $M \subseteq N$ or $N \subseteq M$.

Solution.

1. <u>M is an ideal.</u> $M \neq \emptyset$ since the function $f(x) = 0$ clearly belongs to M.

   Let $f, g \in M$ then the function $(f - g)(x) = f(x) - g(x)$ is continuous everywhere on $[0, 1]$ and $(f - g)(\frac{1}{3}) = f(\frac{1}{3}) - g(\frac{1}{3}) = 0$, so $f - g \in M$. Thus M is a subgroup of the group $(R, +)$.

   If $g \in M$ and $f \in R$, then the function $(fg)(x) = f(x)g(x)$ is continuous everywhere on $[0, 1]$ and $(fg)(\frac{1}{3}) = f(\frac{1}{3})g(\frac{1}{3}) = 0$ as $g(\frac{1}{3}) = 0$, thus $fg \in M$. Thus M is an ideal of R. Note that R is a commutative ring with unity I, where $I(x) = 1$.

   Let $M \subseteq A \subseteq R$ where A is an ideal of R. If $M \neq A$, we shall show that $A = R$. Let $\beta \in A - M$, thus $\beta(\frac{1}{3}) = c \neq 0$. Define $\alpha : [0, 1] \longrightarrow [0, 1]$ by $\alpha(x) = c$ for all $x \in [0, 1]$. Then the function $\mu = \beta - \alpha \in M \subset A$ as $\mu(\frac{1}{3}) = 0$. Thus $\alpha = \beta - \mu \in A$ as $\beta, \mu \in A$. Now consider $\gamma : [0, 1] \longrightarrow [0, 1]$ defined by $\gamma(x) = \frac{1}{c}$ for all x. Clearly $\gamma \in R$. Since A is an ideal, $\gamma\alpha \in A$. But $\gamma\alpha(x) = \frac{1}{c}c = 1$, thus $\gamma\alpha = I \in A$. Since I is unity in R, it follows that $A = R$, hence M is a maximal ideal of R.

   Note: The converse of the above statement is also true i.e. if M is a maximal ideal of R, then there exists number $r \in [0, 1]$ such that $M = \{f \mid f \in R, f(r) = 0\}$. The proof needs compactness of $[0, 1]$ which is not an algebraic concept.

2. If $M \subseteq N$, then $M \cup N = N$ and if $N \subseteq M$, then $M \cup N = M$, so in both cases $M \cup N$ is an ideal of R.

   Conversely, let $M \cup N$ be an ideal of R. If possible, let us assume that $M \nsubseteq N$ and $N \nsubseteq M$, this means there exist $x \in M - N, y \in N - M$. Now $x \in M, y \in N \Rightarrow x, y \in M \cup N$. But $M \cup N$ is an ideal, thus $x - y \in M \cup N$, hence $x - y \in M$ or $x - y \in N$. If $x - y \in M$, then $x - (x - y) = y \in M$ as M is an ideal, but this is a contradiction. If $x - y \in N$, then $(x - y) + y = x \in N$, which is also not possible. Thus our assumption that $M \nsubseteq N$ and $N \nsubseteq M$ is incorrect, so if $M \cup N$ is an ideal, either $M \subseteq N$ or $N \subseteq M$.

$\blacksquare$

Question 2(b) *1. Show that $\mathbb{Q}(\sqrt{3}, i)$ is the splitting field for $x^5 - 3x^3 + x^2 - 3$ where $\mathbb{Q}$ is the field of rational numbers.*

2. Prove that $x^2 + x + 4$ is irreducible over F, the field of integers modulo 11 and prove further that $F[x]/\langle x^2 + x + 4\rangle$ is a field with 121 elements.

Solution.

1. $x^5 - 3x^3 + x^2 - 3 = x^3(x^2 - 3) + x^2 - 3 = (x^2 - 3)(x^3 + 1) = (x^2 - 3)(x + 1)(x^2 - x + 1)$. Thus the roots of $x^5 - 3x^3 + x^2 - 3$ are $-1, \pm\sqrt{3}, \frac{1 \pm i\sqrt{3}}{2}$. Consequently all the roots of the given polynomial lie in the field $\mathbb{Q}(\sqrt{3}, i)$. Conversely, if K is any field containing $\mathbb{Q}$, which contains the roots of the given polynomial, then $\sqrt{3} \in K$, and therefore $i \in K$, thus $\mathbb{Q}(\sqrt{3}, i) \subseteq K$. Thus $\mathbb{Q}(\sqrt{3}, i)$ is the smallest field containing all the roots of $x^5 - 3x^3 + x^2 - 3$. Thus $\mathbb{Q}(\sqrt{3}, i)$ is the splitting field of the given polynomial over $\mathbb{Q}$.

2. See question 2(c) from 1996 for the irreducibility of $x^2 + x + 4$ over F.

   See question 2(b) from 1992 for the second part.

∎

Question 2(c) *If R is a unique factorization domain (UFD), then prove that $R[x]$ is also a UFD.*

Solution. Let F denote the field of quotients of R.

Result 1. If $f(x) \in R[x]$ is irreducible, then $f(x)$ remains irreducible in $F[x]$. (Note that the converse is obvious as $R[x] \subseteq F[x]$.) Let $f(x)$ be reducible in $F[x]$ i.e. $f(x) = g(x)h(x)$, where $\deg g(x) < \deg f(x), \deg h(x) < \deg f(x)$ and $g(x), h(x) \in F[x]$. We can write $g(x) = a_1 b_1^{-1} g_1(x), h(x) = a_2 b_2^{-1} h_1(x)$, where $g_1(x), h_1(x) \in R[x]$ and are primitive and $a_1, b_1, a_2, b_2 \in R$ (b_1 is the LCM of all the denominators of $g(x)$, and a_1 is the GCD of the numerators). Thus $b_1 b_2 f(x) = a_1 a_2 g_1(x) h_1(x)$. But by Gauss Lemma, the product of two primitive polynomials is primitive, therefore $g_1(x)h_1(x)$ is primitive. Since $f(x)$ is irreducible in $R[x]$, therefore it is also primitive. Consequently $b_1 b_2 =$ content of $b_1 b_2 f(x) = a_1 a_2 =$ content of $a_1 a_2 g(x) h(x)$ and therefore we get $f(x) = g_1(x)h_1(x)$, thus $f(x)$ is reducible in $R[x]$. Hence if $f(x)$ is irreducible in $R[x]$ then it is irreducible in $F[x]$.

Result2. Factorization exists in $R[x]$. Let $f(x) \in R[x], f(x) \neq 0$ and $f(x)$ not a unit. Let $a = c(f) =$ content of f then $f = af^*$ where f^* is a primitive polynomial in $R[x]$ of the same degree as f. Since $F[x]$ is a UFD (being a Euclidean domain), we can write $f^*(x) = p_1(x) \ldots p_r(x)$, where each $p_i(x)$ is an irreducible element of $F[x]$. Let $p_i(x) = a_i b_i^{-1} q_i(x)$, where $a_i, b_i \in R$, and $q_i(x) \in R[x]$ is a primitive polynomial. Thus we get

$$b_1 \ldots b_r f^*(x) = a_1 \ldots a_r q_1(x) \ldots q_r(x)$$

But the product $q_1(x) \ldots q_r(x)$ is again primitive (Gauss Lemma), therefore equating the contents of both sides (note that $f^*(x)$ is primitive), we get $b_1 \ldots b_r = a_1 \ldots a_r$, therefore

$$f^*(x) = q_1(x) \ldots q_r(x)$$

where each $q_i(x) \in R[x]$ and is irreducible in $F[x]$ and therefore irreducible in $R[x]$. Since R is a UFD, $a = \pi_1 \ldots \pi_t$, where $\pi_1, \ldots, \pi_t$ are irreducible in R. Thus

$$f(x) = \pi_1 \ldots \pi_t q_1(x) \ldots q_r(x)$$

where $\pi_1, \ldots, \pi_t, q_1(x), \ldots, q_r(x)$ are irreducible elements of $R[x]$. Note that $\pi_1, \ldots, \pi_t$ being constants cannot have a proper factorization in $R[x]$ if they do not have one in R. Hence the result is established.

Result 3. Uniqueness. If possible, let

$$\pi_1 \ldots \pi_t q_1(x) \ldots q_r(x) = \pi'_1 \ldots \pi'_u g_1(x) \ldots g_s(x)$$

where $\pi_1, \ldots, \pi_t, \pi'_1, \ldots, \pi'_u$ are irreducible elements in R and $q_1(x) \ldots q_r(x), g_1(x) \ldots g_s(x)$ are irreducible elements of $R[x]$. Using Gauss Lemma, we get that the products $q_1(x) \ldots q_r(x)$, $g_1(x) \ldots g_s(x)$ are primitive. Comparing the contents of both sides, we get $\pi_1 \ldots \pi_t = \pi'_1 \ldots \pi'_u$. But R is a UFD, so $t = u$, and we can reorder the π'_i to ensure that each π_i is an associate of π'_i. Thus we are left with $q_1(x) \ldots q_r(x) = g_1(x) \ldots g_s(x)$. We consider this equation in $F[x]$. By the first result each $q_i, g_j, 1 \leq i \leq r, 1 \leq j \leq s$ is irreducible in $F[x]$. Since $F[x]$ is a UFD, we get $r = s$ and by reordering, we get that $q_i(x)$ is an associate of $g_i(x)$ in $F[x]$. We can assume w.l.o.g. that $q_i(x) = (\text{unit in } F[x])g_i(x), 1 \leq i \leq r$. Since units in $F[x]$ are non-zero constants, these are of the form cd^{-1} where $c, d \in R$. Thus we get $d_i q_i(x) = c_i g_i(x)$. Using contents, we conclude that $d_i = c_i$, thus $q_i(x)$ is an associate of $g_i(x)$ in $R[x]$, so the factorization is unique.

Thus $R[x]$ is a UFD. ∎