UPSC Civil Services Main 2005 - Mathematics Algebra

Sunder Lal

Retired Professor of Mathematics

Panjab University

Chandigarh

December 16, 2007

Question 1(a) *If M and N are normal subgroups of a group G such that $M \cap N = \{e\}$, show that every element of M commutes with every element of N.*

Solution. Let $x \in M, y \in N$. We consider the element $\alpha = xyx^{-1}y^{-1}$. Now $x^{-1} \in M$ and $y \in N \subseteq G$, and M is a normal subgroup of G, therefore $yx^{-1}y^{-1} \in M$, consequently $\alpha \in M$. Similarly since N is a normal subgroup of G and $y \in N$, $xyx^{-1} \in N$, hence $\alpha = xyx^{-1}y^{-1} \in N$. Thus $\alpha \in M \cap N$, which means that $\alpha = xyx^{-1}y^{-1} = e \Rightarrow xy = yx$ i.e. every element of M commutes with every element of N. ∎

Question 1(b) *Show that $(1 + i)$ is a prime element in the ring R of Gaussian integers.*

Solution. The ring of Gaussian integers is a Euclidean domain with Euclidean function $N(a + ib) = a^2 + b^2$, therefore any two elements $\alpha, \beta \in R$ have a GCD (greatest common divisor). If d is the GCD of α, β, then there exist $\gamma, \delta \in R$ such that $\alpha\gamma + \beta\delta = d$. Moreover α is a unit in R if and only if $N(\alpha) = 1$, because if $N(\alpha) = 1$ then $\alpha\overline{\alpha} = 1$, implying that α is a unit, and conversely, if α is a unit, then there exist $\beta \in R$ such that $\alpha\beta = 1$, and therefore $N(\alpha\beta) = N(\alpha)N(\beta) = 1 \Rightarrow N(\alpha) = N(\beta) = 1$ as both are positive integers.

First of all we prove that $1 + i$ is an irreducible element (note that it is not a unit as $N(1 + i) = 2$). Let $1 + i = \alpha\beta$. Taking norm of both sides, we get $N(\alpha\beta) = N(\alpha)N(\beta) = 2 \Rightarrow N(\alpha) = 1$ or $N(\beta) = 1$, so either α is a unit or β is a unit. Thus $1 + i$ is an irreducible element.

Let $1 + i$ divide $\alpha\beta$ and assume that $1 + i$ does not divide α. We shall show that $1 + i$ divides β. Since the only divisors of $1 + i$ are $1 + i$ and units, and $1 + i$ does not divide α, it follows that GCD of α and $1 + i$ is 1. Thus there exists $\gamma, \delta \in R$ such that $\gamma(1 + i) + \delta\alpha = 1$ or $\gamma\beta(1 + i) + \delta\alpha\beta = \beta$. Since $(1 + i)$ divides the left hand side of this equation, it follows that $1 + i$ divides β. Hence $1 + i$ is a prime element in R. ∎

Question 2(a) *1. Let H and K be two subgroups of a finite group G, such that $|H| > \sqrt{|G|}$ and $|K| > \sqrt{|G|}$. Prove that $H \cap K \neq \{e\}$.*

2. If $f : G \longrightarrow G'$ is an isomorphism, prove that the order of $a \in G$ is equal to the order of $f(a)$.

Solution.

1. We prove that $|HK| = \frac{|H||K|}{|H \cap K|}$.

   If $H \cap K = \{e\}$, then $hk = h_1 k_1 \Leftrightarrow h_1^{-1} h = k_1 k^{-1} \Leftrightarrow h_1^{-1} h, k_1 k^{-1} \in H \cap K \Leftrightarrow h_1^{-1} h = k_1 k^{-1} = e \Leftrightarrow h = h_1, k = k_1$. Thus there are no repetitions in $HK = \{hk \mid h \in H, k \in K\}$, so $|HK| = |H||K| = \frac{|H||K|}{|H \cap K|}$. (This is sufficient to prove the result, but for completeness we show the result when $H \cap K \neq \{e\}$.)

   If $H \cap K \neq \{e\}$, then $hk = h_1 k_1 \Leftrightarrow h_1^{-1} h, k_1 k^{-1} \in H \cap K \Leftrightarrow h_1^{-1} h = k_1 k^{-1} = u \in H \cap K \Leftrightarrow h = h_1 u, k = u^{-1} k_1$ with $u \in H \cap K$. Thus hk is duplicated at least $|H \cap K|$ times as $hk = (hu)(u^{-1}k)$ with $u \in H \cap K$. It is duplicated no more than $|H \cap K|$ times, because $hk = h_1 k_1 \Rightarrow h = h_1 u, k = u^{-1} k_1$ with $u \in H \cap K$. Hence $|HK| = \frac{|H||K|}{|H \cap K|}$.

   Now $|G| \geq |HK| = \frac{|H||K|}{|H \cap K|} \geq \frac{\sqrt{|G|}\sqrt{|G|}}{|H \cap K|}$ Thus $|H \cap K| > 1$, so $|H \cap K| \neq \{e\}$.

2. Let $o(a) =$ order of $a = m$ and order of $f(a) = o(f(a)) = n$. Then $e' = f(a^m) = f(a)^m$, where e' is the identity of G', showing that n divides m. Conversely, $f(e) = e' = f(a)^n = f(a^n) \Rightarrow a^n = e$ as f is one-one. This means that m divides n. Thus $m = n$, which was to be proved.

∎

Question 2(b) *Prove that any polynomial ring $F[x]$ over a field F is a UFD.*

Solution. We know that $F[x]$ is a Euclidean domain with the Euclidean function being the degree of the polynomial — the algorithm being: given $f(x), g(x) \neq 0$ belonging to $F[x]$, there exist $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Step 1. If $f(x), g(x) \in F[x]$, both not 0, then they have a GCD $d(x)$, and there exist $\lambda(x), \mu(x) \in F[x]$ such that $d(x) = f(x)\lambda(x) + g(x)\mu(x)$. Let $S = \{f(x)a(x) + g(x)b(x) \mid a(x), b(x) \in F[x]\}$. Then $S \neq \emptyset$, as $f(x), g(x) \in S$. Let $d(x)$ be a non-zero polynomial is S with minimal degree, i.e. $\deg d(x) \leq \deg h(x)$ for every nonzero $h(x) \in S$. Clearly if any $d'(x)$ divides $f(x)$ and $g(x)$, then $d'(x)$ divides $d(x)$ because $d(x)$ is of the form $f(x)a(x) + g(x)b(x)$. Moreover $d(x)$ divides both $f(x)$ and $g(x)$, otherwise we have $q(x), r(x) \in F[x]$ such that $f(x) = d(x)q(x) + r(x)$ where $\deg r(x) < \deg d(x)$, but this is not possible as $r(x) \in S$ as it is of the form $f(x)a(x) + g(x)b(x)$ so $\deg r(x) \geq \deg d(x)$. So $d(x)$ divides $f(x)$, and similarly $d(x)$ divides $g(x)$.

Step 2. An irreducible element of $F[x]$ is a prime element i.e. if $f(x)$ is irreducible and $f(x) \mid g(x)h(x)$ and $f(x) \nmid g(x)$ then $f(x) \mid h(x)$.

If $f(x) \nmid g(x)$, then $f(x)$ is irreducible implies its only divisors are units or associates of $f(x)$. Therefore the GCD of $f(x)$ and $g(x)$ is 1. By Step 1, we have $1 = f(x)a(x) + g(x)b(x)$ for some $a(x), b(x) \in F[x]$. Thus $h(x) = h(x)f(x)a(x) + h(x)g(x)b(x)$. Clearly $f(x)$ divides the right hand side, so $f(x) \mid h(x)$, as required.

Step 3. Every non-zero non-unit element in $F[x]$ can be written as the product of irreducible elements in $F[x]$.

The proof is by induction on the degree of $f(x)$. If $\deg f(x) = 0$, then $f(x)$ is a non-zero constant, therefore a unit in $F[x]$, so we have nothing to prove.

Let the result be true for all polynomials whose degree is $< \deg f(x)$. If $f(x)$ is irreducible, we have nothing to prove. If $f(x)$ is not irreducible, then there exist $g(x), h(x)$, $1 \leq \deg g(x), \deg h(x) < \deg f(x)$ such that $g(x)h(x) = f(x)$. Now by induction both $g(x)$ and $h(x)$ are products of irreducible elements, therefore $f(x)$ is the product of irreducible elements.

Step 4: Uniqueness. If possible let

$$f(x) = cf_1(x) \dots f_r(x) = dg_1(x) \dots g_s(x)$$

where $f_1, \dots, f_r, g_1, \dots, g_s$ are irreducible, and $c, d \in F$. We will show that $r = s$ and that the g_i's can be reordered such that each f_i is the associate of g_i.

Now $f_1(x)$ divides $g_1(x) \dots g_s(x)$, therefore by step 2, $f_1(x)$ must divide one of $g_1(x), \dots, g_s(x)$. Let us assume without loss of generality that $f_1(x) \mid g_1(x)$, but $g_1(x)$ is also irreducible and $f_1(x)$ is not a unit, therefore $f_1(x)$ and $g_1(x)$ are associates. Thus we get

$$c' f_2(x) \dots f_r(x) = d' g_2(x) \dots g_s(x)$$

If $r < s$, then after r steps we shall get $g_{r+1}(x) \dots g_s(x) = 1$, which is not possible, hence $r \geq s$, similarly $s \geq r$ so $r = s$. Now by relabelling $g_1, \dots, g_r$ we get each $f_i(x)$ is an associate of $g_i(x), 1 \leq i \leq r$. Hence $F[x]$ is a UFD. ∎