UPSC Civil Services Main 1998 - Mathematics Algebra

Sunder Lal
Retired Professor of Mathematics
Panjab University
Chandigarh

December 16, 2007

Question 1(a) *Prove that if a group has only 4 elements then it must be abelian.*

Solution. Let G be a group of order 4. If it has an element of order 4, then G is cyclic and therefore abelian. If G has no elements of order 4, then the order of all elements other than identity is 2 because the order of an element must be a divisor of 4. Let $x, yinG$, then $(xy)^2 = xyxy = e \Rightarrow yx = x^{-1}ey^{-1} = x^{-1}y^{-1} = xy$ because $x^{-1} = x, y^{-1} = y$. Hence $xy = yx$ for every $x, y \in G$ so G is abelian. ∎

Question 1(b) *If H and K are subgroups of G then show that HK is a subgroup of G if and only if $HK = KH$.*

Solution. See Lemma 2.5.1 page 44 of Algebra by Herstein. ∎

Question 1(c) *Show that every group of order 15 has a normal subgroup of order 5.*

Solution. By Sylow's theorem a group G of order 15 has a subgroup of order 5. Again by one of Sylow's theorems the number of subgroups is $\equiv 1 \mod 5$, and this number divides 3. Therefore there is exactly 1 subgroup of order 5, say H. Now aHa^{-1} is also a subgroup of G of order 5, but H is the only such subgroup, so $aHa^{-1} = H$, hence H is a normal subgroup. Hence every group of order 15 has a normal subgroup of order 5. ∎

Question 2(a) *Let $(R, +, .)$ be a system satisfying all the axioms for a ring with unity with the possible exception of $a + b = b + a$. Prove that $(R, +, .)$ is a ring.*

Solution. Let e denote unity of R. Then $(a+b)(e+e) = a(e+e)+b(e+e) = ae+(a+b)e+be$. Also $(a+b)(e+e) = (a+b)e+(a+b)e = ae+be+ae+be$. Thus $ae+be = be+ae \Rightarrow a+b = b+a$. Thus R is a ring.

A similar question is the following. Let $(R, +, .)$ be a system satisfying all the axioms for a ring with the possible exception of $a + b = b + a$. If there is an element $c \in R$ such that $ac = bc \Rightarrow a = b$ for every $a, b \in R$, then show that R is a ring. ∎

Question 2(b) *If p is a prime then prove that $\mathbb{Z}_p$ is a field. Discuss the case when p is not a prime.*

Solution. $\mathbb{Z}_p$ is a commutative ring with unity. Let $[a] \in \mathbb{Z}_p$ such that $a \not\equiv 0 \mod p$ i.e. $[a] \neq [0]$. Let $\{[x_1], \ldots, [x_p]\} = \mathbb{Z}_p$. Then $[a][x_1], \ldots, [a][x_p]$ are all distinct, since $[a][x_i] = [a][x_j] \Rightarrow a(x_i - x_j) \equiv 0 \mod p \Rightarrow x_i \equiv x_j \mod p$ because $a \not\equiv 0 \mod p$. Thus there exists k such that $[a][x_k] = [1] \Rightarrow$ every non-zero element in $\mathbb{Z}_p$ has an inverse. Thus $\mathbb{Z}_p^* = \mathbb{Z}_p - \{[0]\}$ is a group, so $\mathbb{Z}_p$ is a field.

If p is not prime, then $\mathbb{Z}_p$ is not even an integral domain — if $p = n_1 n_2, n_1 > 1, n_2 > 1$, then $[n_1][n_2] = [0]$, but $[n_1] \neq [0], [n_2] \neq [0]$ in $\mathbb{Z}_p$.

See corollary to Lemma 3.2.2 page 128 of Algebra by Herstein. ∎

Question 2(c) *Let D be a principal ideal domain. Show that every element that is neither 0 nor a unit in D is a product of irreducible elements.*

Solution.

1. If $A_1 \subseteq A_2 \subseteq \ldots \subseteq A_k \subseteq A_{k+1} \subseteq \ldots$ is an ascending chain of ideals, then there exists an integer m thus that $A_m = A_{m+1} = \ldots$.

   Proof: Let $A = \bigcup_{i=1}^{\infty} A_i$, then we will show that A is an ideal — If $a, b \in A$, then $a \in A_r$ for some r, and $b \in A_s$ for some s. Hence $a, b \in A_s$ if $s \geq r$ (say), thus $a - b \in A_s$ because A_s is an ideal $\Rightarrow a - b \in A$. Let $a \in A, d \in D \Rightarrow a \in A_r \Rightarrow ra \in A_r$ because A_r is an ideal $\Rightarrow ra \in A$. Thus A is an ideal. Since D is a PID, $A = \langle a \rangle$, i.e.a generates A. By definition of A, there exists m s.t. $a \in A_m$. Thus $A = A_m = A_{m+1} = \ldots \subset= A$.

2. Every nonzero, non-unit element in D is divisible by an irreducible element.

   Proof: Let $a \in D, a \neq 0$, a non-unit. If a is not irreducible then we have nothing to prove. If a is irreducible, then a has a proper divisor, say $a_1 \Rightarrow \langle a_1 \rangle \subset \langle a \rangle$. Continuing this process, we have $a_2, a_3, \ldots$, such that a_s divides a_{s-1} for $s = 1, 2, \ldots$, where $a_0 = a$. But this sequence must terminate i.e. $\exists m$ such that $\langle a_m \rangle = \langle a_{m+1} \rangle = \ldots$ because of step 1. But this means that a_m has no proper factors i.e.a_m is irreducible.

3. Let $a \in D$, a non-unit. If a is irreducible, there is nothing to prove. If not, by step 2, $a = p_1 a_1$ where p_1 is irreducible, and $a_1 \mid a$ properly. If a_1 is a unit, then a is a product of irreducible factors. If not, then $a_1 = p_2 a_2$ where $a_2 \mid a_1$ properly. But this process cannot go on forever, by the same argument as in step 2. Thus we must have an integer k such that $a = p_1 p_2 \ldots p_k a_k$ where a_k is a unit. Thus a is a product of irreducible elements.

∎