UPSC Civil Services Main 1991 - Mathematics Algebra

Brij Bhooshan

Asst. Professor

B.S.A. College of Engg & Technology

Mathura

Question 1(a) *If the group G has no non-trivial subgroups, show that G must be finite of prime order.*

Solution. Here we assume that G has more than one element.

G **is cyclic:** Let $a \in G, a \neq e$. Let H be the cyclic group generated by a. Then $H \neq \{e\}$, therefore $H = G$, so G is cyclic.

G **has finite order:** If order of G is infinite, then the group K generated by a^2 is a non-trivial subgroup of G, because $K \neq \{e\}, K \neq G$ as $a \notin K$ — note that $a \in K, a = (a^2)^m$ for some m shows that a is of finite order $\Rightarrow G$ is of finite order. This is a contradiction, hence order of G is finite.

The order of G is a prime number: If the order is $pq, p > 1, q > 1$, then order of a^p or equivalently the order of the group generated by a^p is $q \Rightarrow G$ has a nontrivial subgroup, which is a contradiction. Hence order of G is a prime number. ∎

Question 1(b) *Show that a group of order 9 must be abelian.*

Solution. We first prove that if G is a group with centre C such that G/C is cyclic, then G is abelian. Let G/C be generated by the coset aC. Let $x, y \in G$, then $xC = (aC)^r$ and $yC = (aC)^s$ for some integers r, s. This means that $x \in a^rC, y \in a^sC$ and therefore $x = a^rc_1, y = a^sc_2, c_1, c_2 \in C$. Now $xy = a^rc_1a^sc_2 = a^ra^sc_1c_2$ since $c_1 \in C$, so it commutes with every element of G. Similarly, $c_2 \in C$ so it commutes with a^r, so

$$xy = a^{r+s}c_1c_2 = a^{s+r}c_2c_1 = a^sc_2a^rc_1 = yx$$

Hence G is abelian.

Now we prove that a group G of order p^2, p prime, is abelian. In particular, a group of order 9 will be abelian. Let C be the center of G. Then C is of order p or p^2 as the center of a prime power group is non-trivial (Theorem 2.11.2 page 86 of Algebra by Herstein).

If the order of C is p^2, and $G = C$ so G is abelian.

If order of C is p, then G/C is of order p and therefore is a cyclic group. Thus G must be abelian as shown above. In either case G is abelian. ∎

Question 1(c) *If the characteristic of an integral domain D is finite, show that it is a prime number.*

Solution. If possible let m be the chararacteristic of D, where $m = pq, p, q > 1$. Let $a \in D, a \neq 0$. Then $0 = ma^2 = pa.qa$. But D is an integral domain, therefore either $pa = 0$ or $qa = 0$. Suppose without loss of generality that $pa = 0$. If $b \in D$ is arbitrary, then $0 = (pa)b = (pb)a$. But $a \neq 0$, therefore $pb = 0 \Rightarrow m$ is not the smallest positive integer such that $ma = 0$ for every $a \in D$. Thus the assumption m has a proper factorization is wrong, hence m is a prime number. ∎

Question 2(a) *Find the greatest common divisor (GCD) in $J[i]$, the ring of Gaussian integers of (i) $3 + 4i$ and $4 - 3i$ (ii) $11 + 7i$ and $18 - i$.*

Solution. (i) $4 - 3i = (-i)(3 + 4i)$, and $-i$ is a unit in $J[i]$ as $i(-i) = 1$. It follows that $4 - 3i$ and $3 + 4i$ are associates of each other. Thus the GCD of $4 - 3i$ and $3 + 4i$ can be taken to be either of them.

(ii) $N(11 + 7i) = (11 + 7i)(11 - 7i) = 170, N(18 - i) = 325$. Since $(170, 325) = 5$, we can find integers x, y such that $170x + 325y = 5$, or

$$(11 + 7i)[(11 - 7i)x] + (18 - i)[(18 + i)y] = 5$$

showing that if α divides $11 + 7i, 18 - i$ in $J[i]$, then α divides 5. Therefore the GCD of $11 + 7i, 18 - i$ is a factor of 5, i.e. $1, 2 - i, 2 + i, 5$.

Now $\frac{11+7i}{2+i} = \frac{(11+7i)(2-i)}{5} = \frac{29}{5} + \frac{3}{5}i$. Thus $2 + i \nmid 11 + 7i$.

$\frac{11+7i}{2-i} = \frac{(11+7i)(2+i)}{5} = 3 + 5i$. Thus $2 - i \mid 11 + 7i$. $\frac{18-i}{2-i} = \frac{(18-i)(2+i)}{5} = \frac{37}{5} + \frac{16}{5}i$, so $2 - i \nmid 18 - i$.

Thus the GCD of $11 + 7i$ and $18 - i$ is 1.

Note: We could have got this by Euclid's Algorithm also.

$$\begin{array}{rcll} 18 - i & = & (11 + 7i) + 7 - 8i & N(7 - 8i) < N(11 + 7i) \\ 11 + 7i & = & (7 - 8i)i + 3 & N(3) < N(7 - 8i) \\ 7 - 8i & = & (2 - 3i)3 + (1 + i) & N(1 + i) < N(3) \\ 3 & = & (1 + i)(1 - i) + 1 & N(1) < N(1 + i) \end{array}$$

Thus the GCD of $11 + 7i$ and $18 - i$ is 1. ∎

Question 2(b) *Show that every maximal ideal of a commutative ring R with unit element is a prime ideal.*

Solution. Let M be a maximal ideal. Let $ab \equiv 0 \mod M$, i.e. $ab \in M$. Suppose that $a \notin M$ i.e. $a \not\equiv 0 \mod M$. We shall show that $b \equiv 0 \mod M$, proving that M is a prime ideal. Consider $\langle M, a\rangle$, the ideal generated by M and a. Clearly $M \subseteq \langle M, a\rangle$ and $M \neq \langle M, a\rangle$ as $a \notin M$, therefore $\langle M, a\rangle = R$ as M is maximal. Thus $e \in \langle M, a\rangle$, where e is the unit element of R. Thus $e = m + xa$ where $m \in M, x \in R$, so $b = mb + xab$. $mb \in M, xab \in M$ because $ab \in M$. Hence $mb + xab = b \in M$, which was to be proved, showing that M is a prime ideal.

Remark. The converse of the above statement is not true. Let $R = \mathbb{Z}[x], P = \langle 2\rangle$, the ideal generated by 2, then P is prime but not maximal — in fact $\langle 2\rangle \subsetneq \langle 2, x\rangle \subsetneq R$. ∎

Question 2(c) *The field K is an extension of the field F. If $\alpha, \beta \in K$ are both algebraic over F, show that $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (if $\beta \neq 0$) are all algebraic over F.*

Solution. Let $p(x)$ be the minimal polynomial of α over F, then $F[x]/\langle p(x)\rangle \simeq F[\alpha]$, the homomorphism from $F[x]$ to $F[\alpha]$ being $f(x) = f(\alpha)$ with kernel $\langle p(x)\rangle$. Thus $F[\alpha] = F(\alpha)$ (the smallest field containing F and α in K). If $\deg p(x) = n$, then $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over F and generate $F(\alpha)$. Hence $(F(\alpha) : F) = n \Rightarrow$ if $\gamma \in F(\alpha), \gamma$ is algebraic over F as $1, \gamma, \ldots, \gamma^n$ are linearly dependent over F, so γ is a root of a polynomial of degree $\leq n$.

Now β being algebraic over F, is algebraic over $F(\alpha) \Rightarrow F(\alpha.\beta)$ is a finite extension of $F(\alpha)$, and $(F(\alpha, \beta) : F(\alpha)) =$ degree of the minimal polynomial of β over $F(\alpha) \leq$ degree of the minimal polynomial of β over F. Since $(F(\alpha, \beta) : F) = (F(\alpha, \beta) : F(\alpha))(F(\alpha) : F)$ (see question 2(c) of 1993), it follows that $F(\alpha, \beta)$ is an algebraic extension over F. In fact if $(F(\alpha, \beta) : F) = m$ and $\zeta \in F(\alpha, \beta)$, then $1, \zeta, \zeta^2, \ldots, \zeta^m$ are linearly dependent, so ζ is a root of a polynomial of degree $\leq m$. Thus $\alpha \pm \beta, \alpha\beta, \alpha/\beta$, being elements of $F(\alpha, \beta)$ are all algebraic over F. ∎