Chapter-13 Exercises

Q (49) Let x and y belong to a commutative ring R with prime characteristic p. $\therefore px = py = 0$.

(a) $(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p$

$= x^p + y^p$ $\left(\because px = py = 0 \text{ & } R \text{ is Commutative}\right)$

(b) TS $(x+y)^{p^n} = x^{p^n} + y^{p^n}$

use mathematical induction [for $n=1$, use Part(a)]

(c) In $\mathbb{Z}_4$ $(1+3)^4 = 0$

But $(1)^4 + (3)^4 = 1+1 = 2 \neq 0$.

Q. (52) $\because a \in R$ is nilpotent $\Rightarrow a^k = 0$ for some $k \in \mathbb{N}$.

$\because R$ is a commutative ring with unity 1 and prime characteristic p (say).

From Q (49)(b) $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ $\forall n \geq 1$

Now $(1+a)^{p^n} = (1)^{p^n} + (a)^{p^n}$

$\Rightarrow (1+a)^{p^n} = 1 + (a)^{p^n}$ $\forall n \geq 1$ ——— (1)

$\because a^k = 0$ for some $k \in \mathbb{N}$

So we can easily find a value of $n \in \mathbb{N}$ such that $p^n \geq k$. Let this $p^n = k$, where $k \geq k$

$a^k = a^{p^n} = a^{p^n - k} \cdot a^k = a^{p^n - k}(0) = 0$.

From eqn (1), $(1+a)^{p^n} = 1 + a^{p^n} = 1 + 0 = 1$

$\Rightarrow (1+a)^k = 1$, where $p^n = k$

Q. (51) **Is** Any finite field has order p^n, where p is prime

Sol^n: Let F be a finite field.

$\therefore$ Characteristic of field = $|1|$ and characteristic of a field is zero or prime.

$\therefore$ F is finite $\Rightarrow$ char. of F is prime.

$\Rightarrow |1| = p$ (prime) ——— (1) [Here $|1|$ → additive order of 1 i.e. $p.1 = 0$]

$\Rightarrow$ every non-zero element has order p [Q. (47)]

If the $|F|$ is divisible by a prime q, other than p.

Then F has an element of order q [Cayley's Theorem]

which contradicts that every non-zero element has order p.

$\therefore$ ~~$|F|$~~ $|F|$ is divisible by prime p only

$\Rightarrow |F| = p^n$ for some positive integer n.

Q. (52) $\mathbb{Z}_3[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}_3, 0 \le i \le n\}$ has characteristic 3.

Q. (53) try yourself

Q. (54) R is a ring and $|R| = m$.

Now char R = Smallest positive integer n such that $nx = 0 \ \forall\, x \in R$

$\Rightarrow$ char $R = \text{LCM}\{|x| \mid x \in R\}$ [Here $|x|$ = additive order of x]

$\therefore |R| = m$ & $x \in R$ be an arbitrary element [$\therefore |R| = m$ & $x \in R$ $\Rightarrow$ ~~$|x|$ divides $|R|$~~ $\Rightarrow |x|$ divides m $\forall x \in R$]

$\Rightarrow |x|$ divides $|R| \Rightarrow |x|$ divides m $\forall x \in R$

$\Rightarrow \text{LCM}\{|x| \mid x \in R\}$ divides m

$\Rightarrow$ char R divides m.

Q. (55) use Q. (54).

Q.56 Soln of $x^2 - x + 2 = 0$.

Use Hit & Trial

$\mathbb{Z}_3[i] = \{a+bi \mid a, b \in \mathbb{Z}_3\}$

$= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$

Q.57 $x^2 - 5x + 6$.

Use Hit & Trial

Q.59 $20.1 = 0 \Rightarrow$ 11 divides 20

$12.1 = 0 \Rightarrow$ 11 divides 12.

$\Rightarrow$ 11 divides both 12 and 20.

$\therefore R$ is I.D. $\Rightarrow$ Char R is Prime.

Now char $R = 11$.

$\therefore$ Char $R = 2$.

the only Prime that divides 12 & 20 is 2

Q.60 use subring test

Q.61 $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is the smallest subfield of R that contains $\sqrt{2}$.

If F is any subfield of R containing $\sqrt{2}$, then F contain K.

$\because \sqrt{2} \in F \Rightarrow b\sqrt{2} \in F \quad \forall b \in \mathbb{Q}$

$\Rightarrow b\sqrt{2} \in F \quad \forall b \in \mathbb{Q} \setminus \{0\}$

$\Rightarrow a + b\sqrt{2} \in F \quad \forall a, b \in \mathbb{Q}$

Q.62 $\because F\setminus\{0\}$ form a group

and Order of the set $F\setminus\{0\}$ is $n-1$.

$\therefore x^{n-1} = 1 \quad \forall x \in F\setminus\{0\}$

$\Rightarrow x^{n-1} = 1 \quad \forall x \neq 0 \& x \in F$.

Q.63 use Exercise (49).