

Notation : Z is the set of all integers, Q is the set of all rational numbers and R is the set of all real numbers.

一 Let $D = \{3n \mid n \in Z\}$ be a subring of Z and $I = \{15n \mid n \in Z\}$, $J = \{9n \mid n \in Z\}$ are two ideals of D .

(1) Is I a prime ideal? Is the quotient ring D/I a finite field? Prove your answer.

(2) Is J a prime ideal? Is the quotient ring D/J a finite field? Prove your answer.

(3) Find all prime ideals of D .

二 Let F be a finite field with order $|F| = m$ and we define that an element $\alpha \in F$ is called a multiple generator in F if $F = \{0, 1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{m-2}\}$. We have known that for any finite field F , there exist a multiple generator in F .

(1) If α is a multiple generator in F then is $\alpha^{m-1} = 1$ true? Prove your answer.

(2) If $F_{11} = \{0, 1, 2, \dots, 10\}$ is the finite field with order $|F_{11}| = 11$ then find a multiple generator in F_{11} . How many multiple generators in F_{11} ? Prove your answer.

(3) If $F_3 = \{0, 1, 2\}$ is the finite field with order $|F_3| = 3$, $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + x + 1$ are polynomials in the polynomial ring $F_3[x]$ and $I = (f(x))$, $J = (g(x))$ are principal ideals of $F_3[x]$.

Is the quotient ring $F_3[x]/I$ a finite field? If it is a finite field, find a multiple generator in $F_3[x]/I$? Prove your answer.

Is the quotient ring $F_3[x]/J$ a finite field? If it is a finite field, find a multiple generator in $F_3[x]/J$? Prove your answer.

(4) If F is the finite field with order $|F| = 25$ then how many multiple generators in F ? Prove your answer.

三 Let $i = \sqrt{-1}$, $u = 7 + 8i$ and $v = 2 + i$. Find four integers $a, b, c, d \in Z$ such that $u = v(a + bi) + (c + di)$ and $c^2 + d^2 < 5$.

四 Let E be the splitting field of $x^4 - 3$ over Q and F be the splitting field of $x^4 - 4$ over Q . Find the Galois group $Gal(E/Q)$ and the Galois group $Gal(F/Q)$.

五 Find the smallest positive integer n such that $n > 30$ and for any integer a , $a^n - a$ is divisible by 385.

六 Let G be a group and $H = \{a^2 \mid a \in G\}$. If H is a subgroup of G then is G an abelian group?

Prove your answer.