Homework 1, review of rings, fields, polynomials

Problem* 1 *(Characteristic of a ring). Let $(A, +, \times)$ be a commutative ring.

(1) Show that there is a unique morphism of rings $f_A : \mathbb{Z} \to A$.
(2) Show that there is a unique $n \in \mathbb{N}$ such that $\ker(f_A) = n\mathbb{Z}$. This integer is called the characteristic of A and (sometimes) denoted by $\mathrm{char}(A)$.
(3) Suppose that the cardinality of A is finite. Then show that the characteristic of A is not zero.
(4) Suppose that A does not contain any zero divisor (that is to say : for any $a, b \in A$, $ab = 0_A$ implies $a = 0_A$ or $b = 0_A$). What can you say about its characteristic ?
(5) Give an example of a field with characteristic 0. Give an example of a field with prime characteristic.
(6) Let p be a prime.
   (a) Give an example of a ring with characteristic p which is not a field.
   (b) Give an example of infinite field with characteristic p.
(7) Let A and B be two commutative rings and suppose that there is a morphism of rings $\varphi : A \to B$. Show that if the characteristic of A is not zero, then the characteristic of B is not zero and it divides the characteristic of A.
(8) Is there a morphism of rings $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}$?

***Problem* 2.** Let A and B be two (unitary, commutative) rings and $f \in \mathrm{Hom}(A, B)$. Show that f induces a morphism of groups $A^\times \to B^\times$.

Problem* 3 *(Review of Chinese Lemma in $\mathbb{Z}$ and Euler φ function). Given $a, b \in \mathbb{Z} - \{0\}$ we call greatest common divisor of a and b and denote by $a \wedge b$ or $gcd(a, b)$ the largest integer which divides both a and b.

(1) Show that $gcd(a, b)$ is the unique positive generator of the ideal $a\mathbb{Z} + b\mathbb{Z}$. (We know that any ideal of $\mathbb{Z}$ is principal, the proof relies on the Euclidean division in $\mathbb{Z}$.)
(2) We say that a and b are coprime if $gcd(a, b) = 1$. Show that a and b are coprime if and only if there is $u, v \in \mathbb{Z}$ such that $1 = au + bv$ (this is known as Bézout theorem).
(3) Let a and b such that $gcd(a, b) = 1$. Show carefully, using the previous question, that for any $k \in \mathbb{Z}$, we have :
   (a divides k) and (b divides k) implies (ab divides k).

(4) For $n \in \mathbb{N}$, $n \geq 1$, set

$$\varphi(n) = |\{k,\ 1 \leq k \leq n,\ gcd(n,k) = 1\}|.$$

Show that $(\mathbb{Z}/n\mathbb{Z})^\times$ has cardinality $\varphi(n)$.

(5) Let a and b such that $gcd(a,b) = 1$.

(a) Show that there exists a well defined morphism of rings

$$\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

sending $k + ab\mathbb{Z}$ onto $(k + a\mathbb{Z},\ k + b\mathbb{Z})$. Show that this morphism is an isomorphism (that is to say, it is bijective).

(b) Deduce from (a) that the groups $(\mathbb{Z}/ab\mathbb{Z})^\times$ and $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ are isomorphic, that is to say there is an isomorphism of groups

$$(\mathbb{Z}/ab\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

(c) Show that $\varphi(ab) = \varphi(a)\varphi(b)$.

(6) Compute (without using the previous questions) the value of $\varphi(p^\alpha)$ for p a prime number and $\alpha \geq 1$.

(7) Compute (using the previous questions) the value of $\varphi(n)$ when $n \geq 1$ decomposes as $n = \prod_p p^{\alpha_p}$ where p ranges over a finite family of prime numbers and $\alpha_p \geq 1$.

(8) Suppose that $n \in \mathbb{N}$ is such that $\varphi(n)$ is a power of 2. Show that n is of the form

$$n = 2^\alpha N$$

where $\alpha \geq 0$ and N is a product of distinct primes p such that $p-1$ is a power of 2. One can prove that such a prime is always a Fermat number.

(9) Is $\mathbb{Z}/9\mathbb{Z}$ isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ as a group ? Justify.

***Problem* 4.** Let A be a commutative ring and p be a prime number. Let

$$\phi : A \to A,\ x \mapsto x^p.$$

(1) Show that, ϕ is not a morphism of rings in general (*i.e.* give an example of ring A for which ϕ is not a morphism).

(2) Suppose that A has characteristic p. Show that ϕ is a morphism of rings and that the restriction of ϕ to $A^\times$ induces a morphism of groups $A^\times \to A^\times$.

(3) If $A = \mathbb{Z}/p\mathbb{Z}$, check that A is a field and give the the kernel of ϕ. What is the image of ϕ ? What is ϕ ?

(4) If $A = \mathbb{Z}/p^2\mathbb{Z}$, what is $A^\times$? What are the ideals of A ? What is the kernel of ϕ ?

(5) If $A = \mathbb{Z}/p\mathbb{Z}[X]$, what is the kernel of ϕ ? The image of ϕ ?

***Problem* 5.** (1) Show that $X^4 + 1$ and $X^6 + X^3 + 1$ are irreducible over $\mathbb{Q}$.

(2) Show that a polynomial with degree 3 is not irreducible in $\mathbb{R}$.

(3) Is $X^3 - 5X^2 + 1$ irreducible over $\mathbb{Q}$?

Problem 6. (1) Let $\alpha \in \{\sqrt{7},\, e^{2i\pi/17},\, \sqrt{2} + \sqrt[3]{5}\}$. Show that α is algebraic over $\mathbb{Q}$ by finding (for each different α) of a polynomial P in $\mathbb{Q}[X]$ such that $P(\alpha) = 0$.

(2) Show that any complex number $z \in \mathbb{C}$ is algebraic over $\mathbb{R}$ by giving a polynomial P in $\mathbb{R}[X]$ such that $P(z) = 0$.

Problem 7. (1) Show that $X^3 - 2$ is irreducible over $\mathbb{Q}$. Is it irreducible over $\mathbb{R}$?

(2) Show that $\sqrt[3]{2}$ cannot be written in the form $a + b\sqrt{c}$ with $a, b, c \in \mathbb{Q}$.

(3) Find $a, b, c \in \mathbb{Q}$ such that $\dfrac{1}{\sqrt[3]{4} - 1} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. *Can you justify for yourself why they exist, before even finding a, b and c?*