Algebraic integers, ring of integers of a number field

***Problem* 1.** Let $\mathcal{A}$ denote the set of roots in $\mathbb{C}$ of all monic polynomials of $\mathbb{Z}[X]$.

(1) Show that the following assertions are equivalent for $z \in \mathbb{C}$:
  (a) $z \in \mathcal{A}$
  (b) The subring $\mathbb{Z}[z]$ of $\mathbb{C}$ generated by z is finitely generated as a $\mathbb{Z}$-module (or equivalently as an abelian group).
  (c) There is a subring $\mathcal{B}$ of $\mathbb{C}$ containing z which is finitely generated as a $\mathbb{Z}$-module (or equivalently as an abelian group).
(2) Show that $\mathcal{A}$ is a subring of $\mathbb{C}$.
(3) Show that $\mathcal{A}$ is not noetherian that is to say there is a sequence of ideals $(\mathcal{I}_n)_{n\neq 1}$ such that $\mathcal{I}_n \subsetneq \mathcal{I}_{n+1}$.
(4) Let K be a number field that is to say a finite extension of $\mathbb{Q}$ and let $\mathcal{A}_K := \mathcal{A} \cap K$.
  (a) What is $\mathcal{A}_{\mathbb{Q}}$?
  (b) Let $d \in \mathbb{Z} - \{0, 1\}$ with no square factor (that is to say there is no prime p such that p^2 divides d). Let $K := \mathbb{Q}(\sqrt{d})$.
    (i) What are the $\mathbb{Q}$-morphisms of fields $K \to \mathbb{C}$?
    (ii) Define the following maps :
$$\begin{array}{cccc} & K & \longrightarrow & \mathbb{R} \\ T: & z & \longmapsto & \sum_{\sigma\in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \sigma(z) \\ N: & z & \longmapsto & \prod_{\sigma\in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \sigma(z). \end{array}$$
    Let $z \in K$. What is the determinant and the trace of the $\mathbb{Q}$-linear map
$$K \to K,\ x \mapsto zx?$$
    (iii) Find a condition involving $N(z)$ and $T(z)$ for $z \in K$ to be an element of $\mathcal{A}_K$.
    (iv) Show that
$$\mathcal{A}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \mod 4. \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \mod 4. \end{cases}$$

***Problem* 2.** Let A be a commutative unitary ring A with no zero divisor. An element $a \in A - A^{\times}$ is said
– **irreducible** if $a = bc$ with $b, c \in A$ implies a or $b \in A^{\times}$.
– **prime** if $A/(p)$ is an integral domain (i.e. has no zero divisor).
We say that $b \in A$ divides a if there is $c \in A$ such that $a = bc$.

(1) Show that if A is an integral domain, then « a prime » implies « a irreducible ».
(2) Compare the prime elements and the irreducible elements in $\mathbb{Z}$ (respectively in $k[X]$ where k is a field).
(3) Let $A := \mathbb{Z}[i\sqrt{5}]$ be the subring of $\mathbb{C}$ generated by $i\sqrt{5}$.
  (a) What are the invertible elements in A ?
  (b) Let $x = 3$ and $y = 2 + i\sqrt{5}$. Show that x and y are not invertible. Show that if $z \in A$ divides both x and y then z is a unit in A.

(c) Show that $9 \in (x) \cap (y)$ and that $(x) \cap (y)$ is not a principal ideal (so in some sense x and y don't have a lcm).

(d) Let $x = 9$ and $y = 3(2 + i\sqrt{5})$. What are the divisors of x (resp. y) in A ? Do x and y have a gcd ?

(e) Show that 3 is irreducible in A but not prime. This implies that A is not a factorial ring.

***Problem* 3.** Let p be an odd prime number.

(1) Let $n \geq 1$ and d a divisor of n. How many subgroups of order d does $\mathbb{Z}/n\mathbb{Z}$ contain ?

(2) How many subgroups of index 2 does $(\mathbb{Z}/p\mathbb{Z})^\times$ contain ?

(3) How many squares are there in $(\mathbb{Z}/p\mathbb{Z})^\times$?

(4) Let $x \in \mathbb{Z}$ not divisible by p. Show that x is a square mod p (i.e. $x \mod p$ is a square in $\mathbb{Z}/p\mathbb{Z}$) if and only if

$$x^{(p-1)/2} = 1 \mod p.$$

(5) Show that if p is a sum of two squares in $\mathbb{Z}$ then p is congruent to $1 \mod 4$.

(6) The converse is true but a bit more difficult. It can be proved by first checking that the ring $\mathbb{Z}[i]$ is Euclidean (i.e. endowed with an Euclidean division), therefore it is principal, and therefore factorial (compare with Problem 2, last question).

***Problem* 4.** *Proof that $A = \mathbb{Z}[i]$ is principal.*

(1) Find the list of invertible elements in A (use the norm $N : \mathbb{Q}[i] \to \mathbb{Q}$).

(2) Let $x \in \mathbb{C}$. Show that there is $q \in A$ such that $|q - x| \leq \sqrt{2}/2$.

(3) Let $\mathcal{I}$ be an ideal of A. We are going to prove that $\mathcal{I}$ is principal. Let $z_0 \in \mathcal{I}$ such that $N(z_0) = \min\{N(z),\ z \in \mathcal{I} - \{0\}\}$. We want to show that $\mathcal{I} = z_0 A$.

  (a) Why does z_0 exist ?

  (b) Let $z \in \mathcal{I}$ and let $x := z/z_0 \in \mathbb{Q}[i]$. We need to prove that $x \in A$.

    (i) Show that there is $q \in A$ such that $N(x - q) < 1$. Let $r := x - q$.

    (ii) Compute $N(z - z_0 q)$ and conclude.

  (c) This proves that A is principal : it is an integral domain whose ideals are all principal. Note that hidden in this proof is the fact that A is endowed with an Euclidean division (a Euclidean ring is always principal).

***Problem* 5.** *Fermat's theorem on sums of two squares.* Let p be an odd prime number.

(1) We admit that a principal ring is factorial. Show that in a factorial ring, the prime elements are exactly the irreducible elements.

(2) Let $\Sigma = \{a^2 + b^2,\ a, b \in \mathbb{N}\}$.

  (a) Show that Σ is stable by multiplication.

  (b) Show that $p \in \Sigma$ if and only if p is not irreducible in $A = \mathbb{Z}[i]$.

  (c) Show that $p \in \Sigma$ if and only if -1 is a square mod p if and only if $p \equiv 1 \mod 4$. *Note that the ring A/pA is isomorphic to $\mathbb{F}_p[X]/(X^2 + 1)$.*