Homework 2

Problem 1. Let k be a field and A a k-algebra. A morphism of k-algebras $A \to A$ is called an endomorphism of A. If furthermore it is bijective, then it is called an automorphism of A. The set of all automorphisms of A is denoted by $\mathrm{Aut}_k(A)$.

(1) Check that there is an operation $\star$ for which the set $(\mathrm{Aut}_k(A), \star)$ is a group. What is the neutral element ?

(2) Show that for $T \in k[X]$, the map

$$\begin{aligned}\theta_T : k[X] &\longrightarrow k[X]\\ P &\longmapsto P(T(X))\end{aligned}$$

is a endomorphism of the k-algebra $k[X]$. For which T is θ_T the neutral element of $(\mathrm{Aut}_k(k[X]), \star)$?

(3) Give a condition on T for θ_T to be an automorphism.

(4) Show that if we define on $k^\times \times k$ the operation

$$(a, b) \times (a', b') := (aa', ab' + b)$$

then $(k^\times \times k, \times)$ is a group. Is it commutative ?

(5) Show that the group $(\mathrm{Aut}_k(k[X]), \star)$ is isomorphic to $(k^\times \times k, \times)$.

Problem 2. Describe a system of representatives of the quotient $\mathbb{Q}[X]/\mathfrak{I}$ where $\mathfrak{I}$ is the ideal of $\mathbb{Q}[X]$ generated by

$$X^4 + X^3 + X^2 - 2X - 6 \text{ and } 3X^7 - 6X^5 - X^2 + 2.$$

Is $\mathbb{Q}[X]/\mathfrak{I}$ a field ? Justify.

Problem 3. (1) Given A and B two rings (respectively two k-algebras, where k is a field), recall what is the natural structure of ring (respectively of k-algebra) on the cartesian product $A \times B$.

(2) Find a natural morphism of rings

$$\mathbb{R}[X]/\langle X^2 - 3X + 2\rangle \longmapsto \mathbb{R} \times \mathbb{R}$$

which is an isomorphism of $\mathbb{R}$-algebras.

(3) Is the ring $\mathbb{R} \times \mathbb{R}$ a field ? Justify.

(4) Remark to ponder : this isomorphism could have been obtained as an application of the Chinese Remainder Theorem over $\mathbb{R}[X]$.

Problem 4 (Quadratic extensions)**.** Let k be a field with characteristic different from 2 and K/k be a quadratic extension that it to say : k is a subfield of K and $[K : k] = 2$.

(1) Show that there is $x \in K - k$ such that $x^2 \in k^\times$ and $K = k(x)$.
Hint : check that there is a basis of K as a k-vector space of the form $\{1, z\}$. Express z^2 using 1 and z and find x...

(2) Check that any other element $y \in K - k$ satisfying $y^2 \in k^\times$ can be written $y = \lambda x$ for $\lambda \in k$.

(3) Let $\mathbb{Q} \subset k \subset \mathbb{C}$ and suppose that $k/\mathbb{Q}$ is quadratic. Show that $k = \mathbb{Q}[\sqrt{n}]$ or $k = \mathbb{Q}[i\sqrt{n}]$ where $n \in \mathbb{N} - \{0, 1\}$ has no square factor (that is to say n is a product of distinct prime numbers).

Problem 5. Let $\alpha = \sqrt{3} + \sqrt{5}$. Denote by $\mathbb{Q}[\alpha]$ the sub-$\mathbb{Q}$-algebra of $\mathbb{R}$ generated by α.

(1) Let $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$ be the sub-$\mathbb{Q}$-algebra of $\mathbb{R}$ generated by $\sqrt{3}$ and $\sqrt{5}$. Show that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}, \sqrt{5}]$.

(2) Prove that $\alpha = \sqrt{3} + \sqrt{5}$ is algebraic (over $\mathbb{Q}$), give its minimal polynomial Π and its degree.

(3) Give an expression of $\dfrac{1}{1+\alpha}$ as a linear combination of 1, α, α^2 and α^3 with rational coefficients.
(You can proceed by first finding the greatest common divisor of Π and $B = X+1$ and two polynomials U and W in $\mathbb{Q}[X]$ such that $U\Pi + BV = 1$. There is also a more elementary method to solve this question.)

(4) What are the subfields of $\mathbb{Q}[\alpha]$? You may use the result of Problem 4 (3).

Problem 6. We admit the following result known as *Eisenstein Criterion*.
Let $f \in \mathbb{Q}[X]$ a unitary polynomial with degree $m \geq 1$

$$f = X^m + a_{m-1}X^{n-1} + \cdots + a_1 X + a_0.$$

Suppose that
(i) $a_0, \ldots, a_{m-1} \in \mathbb{Z}$,
(ii) there is a prime number p that divides $a_0, \ldots, a_{m-1}$ and
(iii) p^2 does not divide a_0.
Then f is irreducible over $\mathbb{Q}$.

Let p be a prime number. Consider $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(1) Apply the criterion to $\Phi_p(X+1)$ and show that Φ_p is irreducible over $\mathbb{Q}$.

(2) What is the degree d of $x_p := e^{2i\pi/p}$ over $\mathbb{Q}$?

(3) Let $a_p := \cos(2\pi/p)$.
   (a) Show that $\mathbb{Q}[a_p]$ is a subfield of $\mathbb{Q}[x_p]$.
   (b) Show that x_p is algebraic with degree 2 over $\mathbb{Q}[a_p]$.
   (c) What is the degree of $\cos(2\pi/p)$ over $\mathbb{Q}$?