• All rings here are unitary and commutative.
• Let \( A \) be a ring. Let \( S \) be a nonempty subset of \( A \). One can show that the intersection of all the subrings of \( A \) containing \( S \) is a ring. It is called the subring of \( A \) generated by \( S \). It is contained in any subring of \( A \) containing \( S \).
• We also saw/will see in class that the intersection of all the ideals of \( A \) containing \( S \) is an ideal of \( A \). It is called the ideal of \( A \) generated by \( S \). It is contained in any ideal of \( A \) containing \( S \). It is denoted by \( (S) \).
• If \( S = \{a\} \), we write simply \( (a) \) for the ideal generated by \( S \). We have \( (a) = Aa \).
• Let \( K \) be a field. Recall the Euclidean division of polynomials in \( K[X] \): given \( A, B \in K[X] \) with \( B \neq 0 \), there is a unique pair \((Q, R) \in K[X]^2 \) satisfying
\[
A = BQ + R
\]
and \( \deg(R) < \deg(B) \) (recall that the zero polynomial has degree \(-\infty\) so it is possible that \( R \) is zero).

If \( A, B \in \mathbb{Z}[X] \) we may write the division of \( A \) by \( B \) in \( \mathbb{Q}[X] \) but the quotient and the remainder do not necessarily lie in \( \mathbb{Z}[X] \) (try with examples). However, we admit the following (it is not too difficult but a bit tedious to prove) : if \( A, B \in \mathbb{Z}[X] \) and \( B \) is a monic polynomial (namely the leading coefficient of \( B \) is 1), then the quotient \( Q \) and the remainder \( R \) of the Euclidean division of \( A \) by \( B \) in \( \mathbb{Q}[X] \) actually lie in \( \mathbb{Z}[X] \).

Problem 1. For \( R \) a subring of \( \mathbb{C} \) and \( z \in \mathbb{C} \) we denote by \( R[z] \) the image of the morphism of rings
\[
\begin{align*}
R[X] & \longrightarrow \mathbb{C} \\
P & \longmapsto P(z)
\end{align*}
\]
where \( R[X] \) is the ring of polynomials with coefficients in \( R \).

1. Show that \( R[z] \) is the subring of \( \mathbb{C} \) generated by \( R \) and \( z \).
   This is somewhat formal. You can denote by \( A \) the subring of \( \mathbb{C} \) generated by \( R \) and \( z \) and explain why the image \( R[z] \) of the above map is equal to \( A \).

2. Find a quotient ring of \( \mathbb{Q}[X] \) which is isomorphic to
   (a) \( \mathbb{Q}[i\sqrt{7}] \),
   (b) \( \mathbb{Q}\left[\frac{1+\sqrt{5}}{2}\right] \).

3. Find a quotient ring of \( \mathbb{Z}[X] \) which is isomorphic to
   (a) \( \mathbb{Z}[i\sqrt{7}] \),
   (b) \( \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \).

4. Let \( A = \mathbb{Z}[\sqrt{10}] \) and \( K = \mathbb{Q}[\sqrt{10}] \).
   (a) Describe the elements of \( A \) and the elements of \( K \). Justify your answer.
   (b) For an element \( x \in K \) consider the multiplication \( m_x : K \rightarrow K \). Check that it is a \( \mathbb{Q} \)-linear map on the 2-dimensional \( \mathbb{Q} \)-vector space \( K \). Give a basis of \( K \) as a \( \mathbb{Q} \)-vector space. If \( x = a + b\sqrt{10} \) with \( a, b \in \mathbb{Q} \), write the matrix of \( m_x \) in the basis you just gave. Denote by \( T(x) \) its trace and by \( N(x) \) its determinant. Explain without calculation why \( N(xy) = N(x)N(y) \). What happens when \( x \in A \)? namely where do \( N(x) \) and \( T(x) \) lie?
   (c) Show that \( 2 \) is irreducible in \( A \) namely that if \( 2 = xy \) with \( x, y \in A \) then \( x \) or \( y \) is a unit of \( A \).
   (d) Show that \( (2) \) is not a prime ideal of \( A \).
**Problem 2.** In a commutative and unitary ring $A$, an ideal $I$ is prime if $I \neq A$ and $A/I$ is an integral domain.

1. What are the prime ideals of
   (a) $A = \mathbb{C}[X]$,
   (b) $A = \mathbb{R}[X]/(X^2 + X + 1)$,
   (c) $A = \mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6)$,
   (d) $A = \mathbb{R}[X]/(X^4 - 1)$.
2. Explain why these rings are also vector spaces over $\mathbb{R}$.
3. (not to be handed in) Determine the morphisms of $\mathbb{R}$-algebras from these rings into $\mathbb{C}$ (respectively into $\mathbb{R}$), namely the morphisms of rings $A \rightarrow \mathbb{C}$ (respectively $A \rightarrow \mathbb{R}$) which fix $\mathbb{R}$.

**Problem 3.** Let $k$ be a field with characteristic different from 2 and $G = \{ e, g \}$ the group with two elements (the element $e$ is the identity in $G$ and in $A$). We consider the group ring $A = k[G]$ (see Section 7.2).

1. What are the ideals of $A$?
   You can notice that $A$ is a 2-dimensional vector space. Then check that an ideal of $A$ is also a sub-vector-space of $A$, therefore it can have dimension 0, 1 or 2. Then among the 1-dimensional vector subspaces of $A$, find the ones which are also ideals.

2. Is $A$ principal? Namely is it a principal ideal domain, see the definition in 8.2 of the book

3. What are the nilpotent elements of $A$, namely the elements $a$ such that there is $n \geq 1$ satisfying $a^n = 0$. This question is a bit more difficult. Two kinds of approaches:
   - Find two orthogonal idempotents $x$ and $y$ in $A$ such that $x + y = e$ (namely two elements $x$ and $y$ in $A$ such that $xy = yx = 0$ and $x^2 = x$, $y^2 = y$). It implies (prove it) that $A$ is isomorphic to the product of rings $Ax \times Ay$ (where $Ax$ has $x$ as identity element and $Ay$ has $y$ as identity element). Conclude....
   - Prove that $A$ is isomorphic to $k[X]/(X^2 - 1)$ and work with the latter ring, which most likely you understand better than $A$.
   Remark : if you understand both approaches, you can wonder how they relate to each other. Can you write $k[X]/(X^2 - 1)$ as a product of two rings? What happens if $k$ has characteristic 2? These are very good questions to think of, but they are not part of the problem set.

4. What is the intersection of all prime ideals of $A$?

**Problem 4.** Let $A$ be an integral domain and $a, b \in A$ such that $(a) = (b)$. What can you say about $a$ and $b$?

**Problem 5.** We admit the following result known as Eisenstein Criterion.

Let $f \in \mathbb{Q}[X]$ a monic polynomial with degree $m \geq 1$

$$f = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0.$$

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 $\mathbb{Q}$ namely if $f = gh$ with $g, h \in \mathbb{Q}[X]$ then $g$ or $h$ is a nonzero constant polynomial.

Let $p$ be a prime number and $\epsilon$ a $p^{th}$ primitive root of 1 in $\mathbb{C}$. Let $A = \mathbb{Z}[\epsilon]$ be the subring of $\mathbb{C}$ generated by $\epsilon$, namely the intersection of all subrings of $\mathbb{C}$ containing $\epsilon$. Note that $\mathbb{Z}$ is a subring of $A$.

1. Show that the polynomial $\Phi_p = 1 + X + \ldots + X^{p-1}$ is irreducible over $\mathbb{Q}$. This is the $p^{th}$ cyclotomic polynomial. You can introduce the polynomial $\Phi_p(X + 1)$ to prove its irreducibility. This is a classic result.
2. Deduce that $\Phi_p = 1 + X + \ldots + X^{p-1}$ is a generator for the ideal $\{ P \in \mathbb{Q}[X], P(\epsilon) = 0 \}$. 
(3) Show that the map

\[ \mathbb{Z}^{p-1} \rightarrow A \]

\[(x_0, \ldots, x_{p-2}) \mapsto \sum_{i=0}^{p-2} x_i \epsilon^i \]

is an isomorphism of additive groups.

**END OF PROBLEMSET 2. THE REST OF THIS PROBLEM AND PROBLEM 6 WILL BE PART OF PROBLEMSET 3.**

(4) Show that the intersection of \( \mathbb{Z} \) with the ideal \((1 - \epsilon)A\) is equal to the ideal \(p\mathbb{Z}\) of \(\mathbb{Z}\). (You can consider the Euclidean division of \(\Phi_p\) by \((X - 1)\)).

(5) Deduce \(A/(1 - \epsilon)A \cong \mathbb{Z}/p\mathbb{Z}\).

(6) What can we say about the ideal \((1 - \epsilon)A\)?

**Problem 6.** Problem 33 of Section 7.4 except for question (d).

**Problem 7.** Some recommended problems, not to be handed in:

Problems 9, 15, 16, 17 of Section 7.4

Problem 1 Section 7.6