**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

$$R[X] \longrightarrow \mathbb{C}$$

$$P \longmapsto P(z)$$

where $R[X]$ is the ring of polynomials with coefficients in $R$.

(1) Let $A$ be the intersection of all subring of $\mathbb{C}$ containing $R$ and $z$ (you can check quickly for yourself that it is a subring of $\mathbb{C}$ containing $R$ and $z$). The map above is a morphism of rings and therefore its image $R[z]$ is a subring of $\mathbb{C}$ containing $R$ and $z$. So $R[z]$ contains $A$. Conversely, every polynomial expression in $z$ with coefficients in $R$ lies in any subring of $\mathbb{C}$ containing $R$ and $z$, so it lies in $A$: this means that $R[z]$ is contained in $A$. We have proved that $A = R[z]$.

(2) Find a quotient ring of $\mathbb{Q}[X]$ which is isomorphic to

(a) For $\mathbb{Q}[i\sqrt{7}]$ : the map

$$\phi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[i\sqrt{7}]$$

$$P \longmapsto P(i\sqrt{7})$$

is a surjective morphism of rings. Its kernel is

$$\ker(\phi) = \{P \in \mathbb{Q}[X], \ P(i\sqrt{7}) = 0\}.$$  

It contains $X^2 + 7$ so it also contains the ideal $(X^2 + 7)$ of $\mathbb{Q}[X]$ generated by $X^2 + 7$. Conversely let $P$ in the kernel of the map. We have $P(i\sqrt{7}) = 0$ and using the complex conjugation, we also have $P(-i\sqrt{7}) = 0$. Write the Euclidean division of $P$ by $X^2 + 7$ in $\mathbb{Q}[X]$ : there is $Q, R \in \mathbb{Q}[X]$ such that

$$P = (X^2 + 7)Q + R$$

where $R$ is either zero or a polynomial with degree 0 or 1. Evaluating at $\pm i\sqrt{7}$ we obtain $R(\pm i\sqrt{7}) = 0$ from which we easily deduce that $R = 0$ (do it!). Therefore, $X^2 + 7$ divides $P$ in $\mathbb{Q}[X]$ namely $P$ lies in $(X^2 + 7)$. We have proved that $\ker(\phi) = (X^2 + 7)$. Therefore

$$\mathbb{Q}[X]/(X^2 + 7) \cong \mathbb{Q}[i\sqrt{7}].$$

(b) $\mathbb{Q}[\frac{1 + \sqrt{5}}{2}]$ : the map

$$\phi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\frac{1 + \sqrt{5}}{2}]$$

$$P \longmapsto P(\frac{1 + \sqrt{5}}{2})$$

is a surjective morphism of rings. Its kernel is

$$\ker(\phi) = \{P \in \mathbb{Q}[X], \ P(\frac{1 + \sqrt{5}}{2}) = 0\}.$$
It contains $X^2 - X - 1$ so it also contains the ideal $(X^2 - X - 1)$ of $\mathbb{Q}[X]$ generated by $X^2 - X - 1$. Let $P$ in the kernel of the map. We have $P(\frac{1+\sqrt{5}}{2}) = 0$. Write the Euclidean division of $P$ by $X^2 - X - 1$ in $\mathbb{Q}[X]$ : there is $Q, R \in \mathbb{Q}[X]$ such that
\[
P = (X^2 - X - 1)Q + R
\]
where $R$ is either zero or a polynomial with degree 0 or 1 which we write in the form $aX + b$ with $a, b \in \mathbb{Q}$. Because $\sqrt{5}$ is not rational (you can prove it), we easily see that $a = b = 0$ so $R = 0$. Therefore, $X^2 - X - 1$ divides $P$ in $\mathbb{Q}[X]$ namely $P$ lies in $(X^2 - X - 1)$. We have proved that $\ker(\phi) = (X^2 - X - 1)$. Therefore
\[
\mathbb{Q}[X]/(X^2 - X - 1) \cong \mathbb{Q}[\frac{1+\sqrt{5}}{2}].
\]

(3) For the same question with $\mathbb{Z}$ instead of $\mathbb{Q}$ everything goes through the similarly because we end up doing Euclidean divisions in $\mathbb{Z}[X]$ by MONIC polynomials. So you can prove that we have isomorphisms or rings :
\[
\mathbb{Z}[X]/(X^2 + 7) \cong \mathbb{Z}[i\sqrt{7}], \quad \mathbb{Z}[X]/(X^2 - X - 1) \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}].
\]
Compare with : what if we wanted to write $\mathbb{Z}[\frac{1}{2}]$ as a quotient ring ?

(4) Let $A = \mathbb{Z}[\sqrt{10}]$ and $K = \mathbb{Q}[\sqrt{10}]$.

(a) Describe the elements of $A$ and the elements of $K$.
Let $z := \sqrt{10}$. By definition, the elements of $A$ (resp. $K$) are of the form $P(z)$ where $P \in \mathbb{Z}[X]$ (resp. $P \in \mathbb{Q}[X]$). But $z^2 = 10$ so $z^n$ lies in $\mathbb{Z}$ or in $z\mathbb{Z}$ for any $n \geq 1$. Therefore :
\[
A = \{a + zb, a, b \in \mathbb{Z}\} \quad \text{and} \quad K = \{a + zb, a, b \in \mathbb{Q}\}.
\]

(b) For an element $x \in K$ consider the multiplication $m_x : K \to K$. Check that it is a $\mathbb{Q}$-linear map on the finite dimensional $\mathbb{Q}$-vector space $K$. Denote by $T(x)$ its trace and by $N(x)$ its determinant. What happens when $x \in A$ ?

First note that $K$ is a $\mathbb{Q}$-vector space (as a $\mathbb{Q}$-subspace of $\mathbb{R}$ for example). Therefore, it makes sense to ask whether $m_x$ is linear, and indeed it it clear that for any $u, v \in K$ and $\lambda, \mu \in \mathbb{Q}$ we have
\[
m_x(\lambda u + \mu v) = x(\lambda u + \mu v) = \lambda xu + \mu xv = \lambda m_x(u) + \mu m_x(v).
\]
Using the previous question, $K$ is finite dimensional over $\mathbb{Q}$ so it makes sense to talk about the determinant and the trace of $x$. A basis of $K$ is given by the elements 1 and $\sqrt{10}$ (indeed, using the previous question this is a generating set, and it is easy to see that it is a basis because $\sqrt{10}$ is not a rational number). Given $x = a + \sqrt{10}b \in K$, the matrix of $m_x$ in that basis is
\[
\begin{pmatrix}
a & 10b \\
b & a
\end{pmatrix}
\]
so $N(a + \sqrt{10}b) = a^2 - 10b^2$ and $T(a + \sqrt{10}b) = 2a$. If $x \in A$ then $N(x), T(x) \in \mathbb{Z}$.

(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 $A$.

For $u, v \in K$ we have $m_{uv} = m_u \circ m_v$ therefore $N(uv) = N(u)N(v)$. From this we
deduce that if $x$ is a unit in $A$ then $N(x) = \pm 1$. Conversely, for $x = a + \sqrt{10} \in A$, if $N(x) = \pm 1$ then \( \frac{a - \sqrt{10}}{N(x)} \times x = 1 \)

it implies that $x$ is a unit of $A$. Therefore, an element $x$ of $A$ is a unit if and only if $N(x) = \pm 1$.

If $2 = xy$ with $x, y \in A$ and none of $x$ or $y$ is a unit, we have $N(2) = N(x)N(y)$ namely $4 = N(x)N(y)$. Therefore $N(x) = \pm 2$. Compute the squares in $\mathbb{Z}/10\mathbb{Z}$ and find a contradiction...

(d) Show that $(2)$ is not a prime ideal of $A$.

Use $2 \times 5 = 10 = (\sqrt{10})^2$ ...

\[\text{Problem 2.}\]

First recall that given a commutative ring $A$ with identity and $I$ an ideal of $A$, the ideals of the quotient ring $A/I$ are the $J/I$ where $J$ is an ideal of $A$ containing $I$. Let $J$ be such an ideal. The reduction map

$$
\phi : A \rightarrow A/J
$$

is a morphism of rings, the kernel of which contains $I$. Therefore it gives a surjective noninjective morphism of rings

$$
\tilde{\phi} : A/I \rightarrow A/J.
$$

The kernel of $\tilde{\phi}$ is the ideal $J/I$ or $A/I$, therefore, applying the isomorphism theorem, we get an isomorphism of rings

$$
\tilde{\phi} : (A/I)/(J/I) \xrightarrow{\sim} A/J.
$$

So, $(A/I)/(J/I)$ is an integral domain if and only if $A/J$ is an integral domain. This proves that among the ideals $J/I$ of $A/I$ (where $J$ is an ideal of $A$ containing $I$), the prime ideals are the ones of the form $J/I$ where $J$ is a prime ideal of $A$ containing $I$.

njk Recall that for any field $K$, the ring $K[X]$ is a PID. If $P$ is an irreducible polynomial in $K[X]$, let $I$ be an ideal of $K[X]$ containing $(P)$. There exists $Q \in K[X]$ such that $I = (Q)$. We have

$$
(P) \subset (Q) \subset K[X]
$$

and therefore $Q$ divides $P$. But $P$ is irreducible so $Q = uP$ where $u \in K^\times$ and $(P) = (Q)$, or $Q = u$ where $u \in K^\times$ and $(P) = K[X]$. We have proved that in $K[X]$ an irreducible polynomial generates a maximal ideal.

Remark. (we just saw this in class but I recall it here). In a PID

"$P$ irreducible $\Rightarrow$ $(P)$ maximal $\Rightarrow$ $(P)$ prime"

Recall that $P$ is called prime when $P \neq 0$ and $(P)$ is prime. Recall also that the implication "prime $\Rightarrow$ irreducible" is always true. So in a PID, for $P \neq 0$ :

"$P$ irreducible $\iff$ $(P)$ maximal $\iff$ $(P)$ prime $\iff$ $P$ prime"
(a) \( A = \mathbb{C}[X] \).

Prime ideals: \((X - \alpha)\) for \(\alpha \in \mathbb{C}\) and \(\{0\}\). Any other ideal which is not \(A\) is of the form \((P)\) where \(P \in \mathbb{C}[X]\) has degree \(\geq 2\) so it is a multiple of some \((X - \alpha)\) for \(\alpha \in \mathbb{C}\) and therefore \((P)\) is not maximal or prime (see above). You can also prove easily by hand (without using the green remark above) that if \(P \in \mathbb{C}[X]\) has degree \(\geq 2\) it does not generate a prime ideal (since it has a factor of degree 1...).

(b) \( A = \mathbb{R}[X]/(X^2 + X + 1) \). The only ideal of \(\mathbb{R}[X]\) containing \((X^2 + X + 1)\) strictly is \(\mathbb{R}[X]\) because \(X^2 + X + 1\) is an irreducible polynomial in \(\mathbb{R}[X]\). So the only prime ideal of \(A\) is \(\{0\}\).

(c) \( A = \mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6) \).

We have \((X^3 - 6X^2 + 11X - 6) = (X - 1)(X - 2)(X - 3)\) so the prime ideals of \(A\) are \((X - 1)/(X^3 - 6X^2 + 11X - 6)\), \((X - 2)/(X^3 - 6X^2 + 11X - 6)\), \((X - 3)/(X^3 - 6X^2 + 11X - 6)\). (Note that \(\{0\}\) here is not a prime ideal! why?)

(d) \( A = \mathbb{R}[X]/(X^4 - 1) \). Since \(X^4 - 1 = (X^2 + 1)(X^2 - 1)\) the prime ideals of \(A\) are \((X^2 + 1)/(X^4 - 1)\), \((X + 1)/(X^4 - 1)\), \((X - 1)/(X^4 - 1)\). (Note that \(\{0\}\) here is not a prime ideal! why?)

(2) For each of these rings \(A\) we can define a morphism of rings 

\[ \mathbb{R} \rightarrow A. \]

(This is enough to define a structure of \(\mathbb{R}\)-vector spaces on these rings, see blue comments at the end of the "solution" to HW1).

(3) A morphism of \(\mathbb{R}\)-algebra 

\[ f_0 : \mathbb{R}[X]/(X^4 - 1) \rightarrow \mathbb{C} \]

can be precomposed with the projection \(\text{pr} : \mathbb{R}[X] \rightarrow \mathbb{R}[X]/(X^4 - 1)\) which is also a morphism of \(\mathbb{R}\)-algebra. We obtain this way a morphism

\[ f := f_0 \circ \text{pr} : \mathbb{R}[X] \rightarrow \mathbb{C} \]

which contains \((X^4 - 1)\) in its kernel. But \(f\) being a morphism of \(\mathbb{R}\)-algebras, it is entirely determined by the image \(z := f(X)\) of \(X\). Since \(f(X^4 - 1) = 0\), we know that \(z^4 = 1\) so \(z \in \{\pm 1, \pm i\}\). We need to check that for each of these \(z\) there is a well defined map \(f_0\).

So for \(z \in \{\pm 1, \pm i\}\), we consider indeed the morphism of \(\mathbb{R}\)-algebras \(f : \mathbb{R}[X] \rightarrow \mathbb{C}\) determined by \(f(X) = z\). Its kernel contains \(X^4 - 1\) therefore, there is

\[ \tilde{f} : \mathbb{R}[X]/(X^4 - 1) \rightarrow \mathbb{C} \]

a morphism of rings such that \(\tilde{f} \circ \text{pr} = f\). It is easy to check that \(\tilde{f}\) is also a morphism of \(\mathbb{R}\)-algebras.

This proves that we have 4 possible morphisms of \(\mathbb{R}\)-algebras \(\mathbb{R}[X]/(X^4 - 1) \rightarrow \mathbb{C}\). They correspond to the roots of \(X^4 - 1\).

Alternatively, the kernel of a morphism of \(\mathbb{R}\)-algebras \(\mathbb{R}[X]/(X^4 - 1) \rightarrow \mathbb{C}\) is necessarily a prime ideal. WHY?

Since such a morphism of algebras is determined by the image of \(X\) mod \((X^4 - 1)\), it has to be one of the 4 ones we found above. Do you understand this argument?

\textbf{Problem 3.} Let \(k\) be a field with characteristic different from 2 and \(G = \{e, g\}\) the group with two elements. We consider the group ring \(A = k[G]\) (see Section 7.2).
(1) What are the ideals of $A$?

Consider the map $k[X] \rightarrow A$, $P(X) \mapsto P(g)$. It is a morphism of rings. Its kernel contains $X^2 - 1$ since $g^2 = e$. It does not contain $X - 1$ or $X + 1$ therefore the kernel is exactly the ideal generated by $X^2 - 1$. This proves that $A = k[X]/(X^2 - 1)$ which makes the rest of the problem very straightforward. For example, the proper ideals of $A$ correspond to the proper ideals of $k[X]/(X^2 - 1)$ namely $(X - 1)/(X^2 - 1)$ or $(X + 1)/(X^2 - 1)$ (note that $k$ has characteristic different from 2 therefore $X - 1 \neq X + 1$). Concretely in $A$ these ideals are $(g - e)A$ and $(g + e)A$.

To find these ideals without the isomorphism: notice that $A$ is a 2-dimensional vector space over $k$. A proper ideal of $A$ in particular a sub-$k$-vector space with dimension 1 so it has the form $k(\alpha e + \beta g)$ for $\alpha, \beta \in k$. But not all such vector spaces are ideals. If $k(\alpha e + \beta g)$ is an ideal $I$ then $\alpha g + \beta e = g(\alpha e + \beta g) \in k(\alpha e + \beta g)$ which means that the matrix $\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$ has determinant 1 namely $\alpha^2 = \beta^2$, i.e. $\alpha = \pm \beta$. So $I$ has to be $k(e + g)$ or $k(e - g)$. And indeed, one checks that these are indeed ideals of $A$.

(2) Is $A$ principal? No because it is not an integral domain $(g + e)(g - e) = 0$.

(3) What are the nilpotent elements of $A$? We look for $P \in k[X]$ such that its image $P$ in $k[X]/(X^2 - 1)$ is nilpotent namely there is $n \geq 1$ such that $P^n \in (X^2 - 1)$, which implies that $P^n(1) = (P(1))^n = 0$. But $k$ is a field so $P(1)^n = 0$ is equivalent to $P(1) = 0$. Likewise, we obtain $P(-1) = 0$. This means that $P$ is a multiple of $X^2 + 1$ (write the Euclidean division of $P$ by $X^2 + 1$ if you like and analyze the remainder...). Note that it matters here that $-1 \neq 1$ again... Therefore we have $P = 0$ and there is no nilpotent element in $k[X]/(X^2 - 1)$ and no nilpotent element in $A$.

Now if we want to work directly in $A$: since $k$ has characteristic different from 2 we can invert 2 in $k$ and consider

$$f_1 := \frac{1}{2}(e + g), \quad f_2 := \frac{1}{2}(e - g).$$

Notice $e = f_1 + f_2$ such that $f_1 f_2 = f_2 f_1 = 0$. This means that $A = f_1 A \times f_2 A$

as a ring, where $f_i A$ is a ring with identity element $f_i$. Therefore, we are reduced to looking for the nilpotent elements in each $f_i A$. But it is easy to see that $f_i A = k f_i$ and since $f_i$ is not nilpotent, there is no nilpotent element in $f_i A$ and therefore in $A$.

Note : by the Chinese Remainder Theorem, we have $k[X]/(X^2 - 1) \cong k[X]/(X - 1) \times k[X]/(X + 1)$.

Compare this with the decomposition of $A$ above!

Namely, which pieces correspond to each other? What element in $k[X]/(X^2 - 1)$ (and then in $A$) corresponds to $(1, 0)$? $(0, 1)$? $f_1$? $f_2$?

(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
1. \( a_0, \ldots, a_{m-1} \in \mathbb{Z} \),
2. there is a prime number \( p \) that divides \( a_0, \ldots, a_{m-1} \) and \( p^2 \) 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 primitive root of 1 in \( \mathbb{C} \). Let \( A = \mathbb{Z}[\epsilon] \) be the subring of \( A \) 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 a classic question. See wikipedia, Eisenstein Criterion, Cyclotomic polynomials...

Note that \( \Phi_p = \frac{X^p - 1}{X - 1} \). Let
\[
P = \Phi_p(X + 1) = \frac{(X + 1)^p - 1}{X} = \sum_{k=1}^{p} \left( \begin{array}{c} p \\ k \end{array} \right) X^{k-1}.
\]
It is a monic polynomial. For \( k \in \{1, \ldots, p\} \) we have \( k \left( \begin{array}{c} p \\ k \end{array} \right) = p \left( \begin{array}{c} p - 1 \\ k - 1 \end{array} \right) \) so \( p \) divides \( k \left( \begin{array}{c} p \\ k \end{array} \right) \). But when \( k \neq p \) it is prime to \( k \) therefore \( p \) divides \( \left( \begin{array}{c} p \\ k \end{array} \right) \) for \( k \in \{2, \ldots, p-1\} \).
The constant term of \( P \) is \( \left( \begin{array}{c} p \\ 1 \end{array} \right) \). It is not divisible by \( p^2 \). By Eisenstein criterion, \( P \) is irreducible over \( \mathbb{Q} \) and therefore \( \Phi_p \) is irreducible over \( \mathbb{Q} \).

2. The ideal \( \{ P \in \mathbb{Q}[X], P(\epsilon) \} \) is not equal to \( \mathbb{Q}[X] \) and it contains \( \Phi_p \) therefore it contains \( (\Phi_p) \). Furthermore, \( \mathbb{Q}[X] \) being principal, there is \( \Pi \in \mathbb{Q}[X] \) such that \( (\Pi) = \{ P \in \mathbb{Q}[X], P(\epsilon) \} \). It satisfies \( (\Pi) \subseteq (\Phi_p) \). But \( \Phi_p \), being irreducible in a PID it generates a maximal ideal so \( (\Pi) \subseteq (\Phi_p) \) (alternatively, \( (\Pi) \subseteq (\Phi_p) \) means that \( \Pi \) divides \( \Phi_p \) and since \( \Phi_p \) is irreducible, that \( \Pi \in \mathbb{Q}^\times \) or \( \Pi \) and \( \Phi_p \) are associate...... conclude.....

3. Show that the map
\[
F : \quad \mathbb{Z}^{p-1} \longrightarrow A
\]
\[
(x_0, \ldots, x_{p-2}) \longmapsto \sum_{i=0}^{p-2} x_i \epsilon^i
\]
is an isomorphism of additive groups. It is clearly a morphism of groups. First we want to check that it is surjective. It is enough to prove for any \( n \geq 0 \) that \( \epsilon^n \) is in the image of the map. If \( n \leq p - 2 \) it is clear. For \( n = p - 1 \), it is also clear because \( \epsilon^p = 1 \) and \( \epsilon \neq 1 \) so \( \Phi_p(\epsilon) = 0 \) therefore \( \epsilon^{p-1} = -1 - \epsilon - \cdots - \epsilon^{p-2} \). Suppose that \( \epsilon^n \) is in the image and consider \( \epsilon^{n+1} \). Let
\[
X^n = Q\Phi_p + R
\]
be the Euclidean division of \( X^n \) by \( \Phi_p \) in \( \mathbb{Q}[X] \) and in fact in \( \mathbb{Z}[X] \) since \( \Phi_p \) is monic. We have \( \deg R < p - 2 \) and \( R \in \mathbb{Z}[X] \) therefore
\[
\epsilon^n = R(\epsilon) \in \sum_{i=0}^{p-2} \mathbb{Z}\epsilon^i = \text{Im}(F).
\]
This proves that the map is surjective.

For the injectivity, let \((x_0, \ldots, x_{p-2}) \in \mathbb{Z}^{p-1}\) and suppose that it lies in the kernel of the map. It means that the polynomial \(x_0 + x_1X + \ldots, x_{p-2}X^{p-2}\) lies in the ideal \(\{P \in \mathbb{Q}[X], P(\epsilon) = 0\} = \Phi_p\mathbb{Q}[X]\). Because of the degrees, it means that \(x_0 + x_1X + \ldots, x_{p-2}X^{p-2}\) is the zero polynomial so \((x_0, \ldots, x_{p-2}) = (0, \ldots, 0)\) which concludes the proof.

(4) Show that the intersection of \(\mathbb{Z}\) with the ideal \((1 - \epsilon)A\) is equal to the ideal \(p\mathbb{Z}\) of \(\mathbb{Z}\).

Write the Euclidean division:
\[
\Phi_p = (X - 1)(X^{p-2} + 2X^{p-3} + \cdots + p - 2X + p - 1) + p
\]
It gives
\[
p = (1 - \epsilon)(\epsilon^{p-2} + 2\epsilon^{p-3} + \cdots + (p - 2)\epsilon + p - 1)
\]
and this equality happens in \(A\). This shows that \(p \in (1 - \epsilon)A\) so \(p\mathbb{Z} \subseteq (1 - \epsilon)A\). Since \((1 - \epsilon)A \cap \mathbb{Z}\) is an ideal of \(\mathbb{Z}\), it is enough to show that \((1 - \epsilon)A \cap \mathbb{Z} \neq \mathbb{Z}\) since \(p\mathbb{Z}\) is maximal. If \((1 - \epsilon)A \cap \mathbb{Z}\) was equal to \(\mathbb{Z}\) it would mean in particular that 1 lies in this intersection and in particular in \((1 - \epsilon)A\). So \((1 - \epsilon)\) would be invertible in \(A\). We know that it is invertible in \(\mathbb{C}\) and in fact we even know what is its inverse: it is
\[
\frac{\epsilon^{p-2} + 2\epsilon^{p-3} + \cdots + (p - 2)\epsilon + p - 1}{p}
\]
If it was an element in \(A\) we could find (by surjectivity of the map in Question (1)) an element \((x_0, \ldots, x_{p-2}) \in \mathbb{Z}^{p-1}\)
\[
x_0 + x_1\epsilon + \ldots x_{p-2}\epsilon^{p-2} = \frac{\epsilon^{p-2} + 2\epsilon^{p-3} + \cdots + (p - 2)\epsilon + p - 1}{p}
\]
But then by injectivity of the map, we would have \(1 = px_{p-2}\). Contradiction.

The morphism of rings \(\mathbb{Z} \to A/(1 - \epsilon)A\) is surjective because any element \(a\) in \(A\) can be written in the form \(a = x_0 + x_1\epsilon + \ldots x_{p-2}\epsilon^{p-2}\) for \((x_0, \ldots, x_{p-2}) \in \mathbb{Z}^{p-1}\). Therefore \(a \in x_0 + x_1 + \ldots x_{p-2} + (1 - \epsilon)A\).

The kernel of this map is \((1 - \epsilon)A \cap \mathbb{Z} = p\mathbb{Z}\). This proves that \(A/(1 - \epsilon)A \cong \mathbb{Z}/p\mathbb{Z}\).

(5) What can we say about the ideal \((1 - \epsilon)A\)? It is a maximal ideal of \(A\).