This exam has 5 questions on 5 pages, for a total of 25 points.

Duration: 60 minutes

- You need to show enough work to justify your answers.
- This is a closed-book examination. None of the following are allowed: documents or electronic devices of any kind (including calculators, cell phones, etc.)
- If your answers are not easily readable and well organized, they may not be read and credited.

LAST name: ________________________________

First name: ________________________________

Student Number: ____________________________

Signature: ________________________________

Instructor: Rachel Ollivier

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>12</td>
<td>6</td>
<td>25</td>
</tr>
<tr>
<td>Score</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
All the rings in this exam are **commutative and have an identity element**.

- Given a ring $A$ with unit $1_A$ we recall:
  - An ideal $I \neq A$ of $A$ is prime if $A/I$ is an integral domain.
  - An ideal $I \neq A$ of $A$ is maximal if and only if $A/I$ is a field.
  - Recall that given a unitary ring $A$ with unit $1_A$, there is a unique homomorphism of rings $\mathbb{Z} \rightarrow A$ sending $1 \in \mathbb{Z}$ onto $1_A \in A$. Its kernel is an ideal of $\mathbb{Z}$ and is therefore of the form $d\mathbb{Z}$ for $d \in \mathbb{Z}$, $d \geq 0$. This $d$ is called the characteristic of the ring $A$.

- Given $K$ a field consider the ring $K[X]$ of polynomials in the variable $X$ with coefficients in $K$. We recall that $K[X]$ is an Euclidean domain and therefore a principal ideal domain.

- Given a ring $A$, a subring $B$ of $A$ and $a \in A$, we admit that the map $P \mapsto P(a)$ is a homomorphism of rings $B[X] \rightarrow A$.

\[\star\]

1. Let $K$ be a field and $a, b \in K$ such that $a \neq b$.

(a) Show that $(X - a) + (X - b) = K[X]$.

It is enough to show that $1 \in (X - a) + (X - b)$ which is true because

\[1 = \frac{1}{b - a}(X - a) + \frac{1}{a - b}(X - b)\]

(b) Let $a = 1$ and $b = 0$. By the Chinese Remainder theorem, the map

\[
\begin{align*}
K[X]/(X(X - 1)) & \rightarrow K[X]/(X) \times K[X]/(X - 1) \\
P \mod X(X - 1) & \mapsto (P \mod X, P \mod X - 1)
\end{align*}
\]

is well defined and is an isomorphism of rings. What is its inverse?

Let denote by $F$ this map and by $G$ its inverse. Since $F$ is not only a morphism of rings but also a $K$-linear map, $G$ is also $K$-linear. Recall that $K[X]/(X - a) \cong K$ (by the map $P \mod (X - a) \mapsto P(a)$) therefore the right hand side $K[X]/(X) \times K[X]/(X - 1)$ is a 2-dimensional vector space with basis $\{e := (1 \mod X, 0), f := (0, 1 \mod X - 1)\}$.

We compute $G(e)$. It is the unique element $E$ in $K[X]/(X(X - 1))$ such that $E \equiv 1 \mod X$ and $E \equiv 0 \mod X - 1$. It is $E = 1 - X \mod X(X - 1)$.

We compute $G(f)$. It is the unique element $E$ in $K[X]/(X(X - 1))$ such that $E \equiv 0 \mod X$ and $E \equiv 1 \mod X - 1$. It is $E = X \mod X(X - 1)$. So

\[
\begin{align*}
K[X]/(X) \times K[X]/(X - 1) & \rightarrow K[X]/(X(X - 1)) \\
(\lambda \mod X, \mu \mod X - 1) & \mapsto \lambda(1 - X) + \mu X \mod X(X - 1)
\end{align*}
\]
2. Show that the characteristic of an integral domain \( A \) is 0 or a prime number.

The characteristic \( d \geq 0 \) of a unitary ring \( A \) is a generator of the kernel of the natural homomorphism of unitary rings \( \mathbb{Z} \rightarrow A \). We therefore have an injective homomorphism of unitary rings

\[
\psi : \mathbb{Z}/d\mathbb{Z} \rightarrow A.
\]

Its image is a subring of \( A \) which is isomorphic to \( \mathbb{Z}/d\mathbb{Z} \). If \( A \) is an integral domain then \( \psi(\mathbb{Z}/d\mathbb{Z}) \) is also an integral domain (since it is contained in \( A \)) and \( \mathbb{Z}/d\mathbb{Z} \) is an integral domain so \( d = 0 \) or \( d \) is a prime number.

3. Compute the remainder of the Euclidean division of \( X^2Y^2 + Y \) by \( XY + 1 \) in \( \mathbb{Q}(X)[Y] \).

In \( \mathbb{Q}(X)[Y] \) the polynomial \( B := XY + 1 \) has degree 1. There is \( Q \in \mathbb{Q}(X)[Y] \) and \( R \in \mathbb{Q}(X)[Y] \) such that

\[
A = QB + R
\]

and \( R \) has degree \( \leq 0 \) (with respect to \( Y \)) namely there is \( s(X) \in K(X) \) such that

\[
R = s(X).
\]

But \( B(X, -\frac{1}{X}) = 0 \), so

\[
A(X, -\frac{1}{X}) = R(X)
\]

and

\[
R(X) = X^2(\frac{1}{X})^2 - \frac{1}{X} = 1 - \frac{1}{X}.
\]
4. Denote by $\mathbb{F}_3$ the field $\mathbb{Z}/3\mathbb{Z}$.

(a) What are the units in $\mathbb{F}_3[X]$?

$\left(\mathbb{F}_3[X]\right)^\times = (\mathbb{F}_3)^\times = \{1, 2\}$

(b) Prove that $\mathbb{F}_3[X]/(X^2 + 1)$ is a field. First notice that $X^2 + 1$ is an irreducible polynomial in $\mathbb{F}_3[X]$. This is because otherwise, it would have a factor of degree 1 and therefore there would be $a \in \mathbb{F}_3$ such that $a^2 + 1 = 0$ but we see that it is not true. We want to prove that $(X^2 + 1)$ is a maximal ideal. Let $I$ is an ideal of $\mathbb{F}_3[X]$ containing $(X^2 + 1)$. Since the ideals of $\mathbb{F}_3[X]$ are principal, there is $P \in \mathbb{F}_3[X]$ such that $I = (P)$ and

$$(X^2 + 1) \subseteq (P) \subseteq A.$$ 

This implies that $X^2 + 1 \in (P)$ and therefore $P$ divides $X^2 + 1$. Therefore either $P$ is a nonzero constant and $I = (P) = A$ or there is $u \in \mathbb{F}_3^\times$ such that $P = u(X^2 + 1)$ and $I = (P) = (X^2 + 1)$.

2 marks

(c) In $\mathbb{F}_3[X]/(X^2 + 1)$, find the inverse of

i. $X + 1 \mod X^2 + 1$.

Notice that $X^2 + 1 = (X-1) - 1 = (X-1)(X+1) - 1$ so $(X+1)(X-1) \equiv 1 \mod X^2 + 1$ and

$$X - 1 \mod X^2 + 1$$

is the inverse of $X + 1 \mod X^2 + 1$.

(Or use Euclidean algorithm).

ii. $X^5 + 2 \mod X^2 + 1$

$X^5 + 2 \equiv X + 2 \equiv X - 1 \mod X^2 + 1$ so by the above calculation, its inverse is $X + 1 \mod X^2 + 1$.

2 marks

(d) Prove that the field $\mathbb{F}_3[X]/(X^2+1)$ has cardinality 9. By Euclidean division, $\mathbb{F}_3[X]/(X^2+1)$ is a 2-dimensional vector space over $\mathbb{F}_3$ with basis $\{1, X\}$. So it is isomorphic to $\mathbb{F}_3^2$ as a $\mathbb{F}_3$ vector space so it has the same cardinality namely $3^2 = 9$.

2 marks

(e) Give an example of field with cardinality 27 and justify your answer. Following the same arguments as above, if we find an irreducible polynomial $P \in \mathbb{F}_3[X]$ with degree 3, then $\mathbb{F}_3[X]/(P)$ will be a field with cardinality $3^3 = 27$. We can require that $P$ is monic namely of the form

$$P = X^3 + aX^2 + bX + c.$$ 

It is irreducible if and only if it does not have any factor of degree 1 namely if $P(0) \neq 0$, $P(1) \neq 0$, $P(-1) \neq 0$. We see that

$$P = X^3 - X + 1$$

works (there are many others). So $\mathbb{F}_3[X]/(X^3 - X + 1)$ is a field of cardinality 27.
5. We admit that the subring $K = \mathbb{Q}[i\sqrt{5}]$ of $\mathbb{C}$ generated by $\mathbb{Q}$ and $i\sqrt{5}$ is a $\mathbb{Q}$-vector space with basis 1 and $i\sqrt{5}$. Consider the subring $A = \mathbb{Z}[i\sqrt{5}]$ of $\mathbb{C}$ generated by $\mathbb{Z}$ and $i\sqrt{5}$. It is the image of the homomorphism of rings $\mathbb{Z}[X] \to \mathbb{C}$ sending $P$ onto $P(i\sqrt{5})$.

2 marks

(a) Prove that as an abelian group, $A$ is isomorphic to $\mathbb{Z}^2$. Consider the map

$$\phi : \mathbb{Z}^2 \to A$$

$$(a, b) \mapsto a + i\sqrt{5}b$$

It is well defined since $a + i\sqrt{5}b$ is the evaluation at $i\sqrt{5}$ of $a + bX \in \mathbb{Z}[X]$. It is clearly a homomorphism of groups. It is surjective because for any $P \in \mathbb{Z}[X]$, the Euclidean division in $\mathbb{Z}[X]$ by the monic polynomial $X^2 + 5 \in \mathbb{Z}[X]$ has a remainder of the form $a + bX \in \mathbb{Z}[X]$ so $P(i\sqrt{5}) = a + i\sqrt{5}b = \phi((a, b))$. It is injective because $0 = a + i\sqrt{5}b$ implies $a = b = 0$ (these are complex numbers, look at the real and imaginary part).

4 marks

(b) For $a, b \in \mathbb{Z}$, prove that $a + i\sqrt{5}b$ is invertible in $A$ if and only if $a^2 + 5b^2 = 1$.

First notice that for $a, b \in \mathbb{Z}$, and $x = a + i\sqrt{5}b \in A$ we have: if $a^2 + 5b^2 = 1$ then $xx' = 1$ where $x' := a - i\sqrt{5}b \in A$, so $x$ is invertible in $A$.

For the other implication:

A) Method inspired by the homework where we studied invertible elements in the ring of integers of real quadratic fields such as $\mathbb{Z}[\sqrt{10}]$:

Consider $K = \mathbb{Q}[i\sqrt{5}]$ the $\mathbb{Q}$-vector subspace of $\mathbb{C}$ with basis 1 and $i\sqrt{5}$.

Let $x = a + i\sqrt{5}b \in K$. The multiplication $m_x : K \to K, y \mapsto xy$ by $x$ is a linear map. Its matrix in the above basis is

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}.$$ 

Let $N(x) := \det(m_x) = a^2 + 5b^2$. For $x' \in K$, we have $m_{xx'} = m_x \circ m_{x'}$ therefore $N(xx') = N(x)N(x')$.

Notice furthermore that if $x \in A$, then $N(x) \in \mathbb{Z}$.

Let $x = a + i\sqrt{5}b \in A$ (with $a, b \in \mathbb{Z}$). If $x$ is invertible in $A$, there is $x' \in A$ such that $xx' = 1$ so $N(xx') = N(x)N(x') = N(1) = 1$. But $N(x) \in \mathbb{Z}$ and $N(x') \in \mathbb{Z}$ so $N(x) \in \{\pm 1\}$. Since $N(x) \geq 0$ in fact we have $N(x) = 1$.

B) But here, since we were working with a $\mathbb{Q}[i\sqrt{5}]$ (and not $\mathbb{Q}[\sqrt{5}]$) you could notice right that

$$N(xx') = N(x)N(x')$$

for $x, x' \in \mathbb{Q}[i\sqrt{5}]$ because $N(x)$ is here nothing but the square of the well known absolute value (or modulus) of the complex number $x$. Conclude as above.