Practice for the MIDTERM

ADVISE

• Please make sure that your understanding of the question has a mathematical sense.

• Ask yourself if you have a complete answer to a question before moving to another one.

• Think about all the ways at your disposal to answer the question, try to find out, which one has most chances to succeed.

• Make sure all the assumption of the theorem you want to use are in the exercise before using it.

• Do not forget that there can be connection between the questions. this can make you win a lot of time.

• Start with a problem that you know how to solve to build confidence.

• Remember that partial answers, as long as they make sense, can earn you come points.

Exercise 1: (⋆)
Show that $R := \mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} | a, b \in \mathbb{Z}\}$ is an integral domain (you may use without proof that $\mathbb{C}$ is a field) and that $2 + \sqrt{3}$ is a unit in $R$.

Exercise 2: (⋆⋆) Construct a field with 16 elements and show that it is a field. (Hint: Consider $(\mathbb{Z}/2\mathbb{Z}[x])/(x^4 + x + 1)$.)

Exercise 3: (⋆⋆) Let $F$ be a field and $A \in M_n(F)$ an $n \times n$ matrix. Show that the map $\theta : F[x] \to M_n(F)$, sending $p(x)$ to $p(A)$ (the polynomial evaluated at the matrix) is a ring homomorphism. Conclude that there is a polynomial $m_A(x) \in F[x]$, such that every polynomial $p(x) \in F[x]$ for which $p(A) = 0_{n \times n}$ is a multiple of $m_A$. ( $m_A$ is called the minimal polynomial of $A$.)

Exercise 4: (⋆)
Let $R$ be a commutative ring with 1. Show that $R$ is a field if and only if $\{0\}$ and $R$ are the only ideals of $R$.

Exercise 5: (⋆⋆)
1. Let $R$ be a ring and $I, J$ be ideal of $R$. Show that the map
\[ \theta : R \to R/I \times R/J \]
\[ r \mapsto (r + I, r + J) \]
is a ring homomorphism with kernel $I \cap J$. Show that if $I + J = R$, then $\theta$ is surjective.

2. Show that for $\gcd(m, n) = 1$ we have an isomorphism
\[ \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \]
(Hint: Let $I = m\mathbb{Z}$ and $J = n\mathbb{Z}$, use 1.)

3. Let $m, n$ as in 2) Let $\tilde{m}$ be the multiplicative inverse of $m$ modulo $n$ and $\tilde{n}$ the multiplicative inverse of $n$ modulo $m$. Show that the map
\[ \phi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z} \]
\[ (a + m\mathbb{Z}, b + n\mathbb{Z}) \mapsto (a.\tilde{n}.n + b.\tilde{m}.m) \]
is well defined and it is an inverse to
\[ \bar{\theta} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \]
\[ r + nm\mathbb{Z} \mapsto (r + m\mathbb{Z}, r + n\mathbb{Z}) \]

4. Determine all the integers $x$ such $x \equiv 3 \mod 1000$ and $x = 5 \mod 1001$.

Exercise 6: (*) Consider the polynomial $f(x) = x^2 + 2x + 3$ in $\mathbb{Z}/5\mathbb{Z}[x]$

1. Is $f(x)$ irreducible in $\mathbb{Z}/5\mathbb{Z}[x]$? If yes, explain why it is so, if not determine a proper factorization of $f(x)$ in $\mathbb{Z}/5\mathbb{Z}[x]$.

2. Consider the ring $F = \mathbb{Z}/5\mathbb{Z}[x]/\langle f(x) \rangle$. Prove that $\bar{x} + \langle f(x) \rangle$ is invertible in $F$ and determine the order of $\bar{x}$ in the multiplicative group $F^*$ of units of $F$.

3. Find, if exists, an element of order 3 in $F^*$.

Exercise 7: (**) Let $F$ be a field and let $F[x]$ be the ring of polynomials of one variable $x$ with coefficients in $F$. Prove that there are infinitely many irreducible monic polynomials in $F[x]$.

Exercise 8: (*) Let $p \in \mathbb{Z}$ be a prime number.

1. Does $f(x) = x^p - px - 1$ have a proper factorization in $\mathbb{Z}[x]$? If yes, show an explicit factorization of $f(x)$, if not justify your answer.

2. Show that the polynomial $g(x) = x^4 + 5x^2 + 3x + 2$ is irreducible in $\mathbb{Q}[x]$.

Exercise 9: (*) Let $A = C([0, 1], \mathbb{R})$ be the ring of continuous functions (for the Euclidean topology) $f : [0, 1] \to \mathbb{R}$ and let $I \subset A$ be the subset of functions which vanish at $1/2$.
1. Show that $I$ an ideal of $A$.

2. An ideal $I$ is said prime if for any $x, y \in I$ $xy \in I$ is equivalent to $x \in I$ or $y \in J$.
   Is $I$ a prime ideal? Prove it or disprove it.

3. Is $I$ a maximal ideal? Prove it or disprove it.