THE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MATH3301

Assignment 5

**Due Date: Nov 28, 2024, 23:59.**

**Submission Guidelines**

(i) Write your solution on papers of about A4 size.

(ii) Scan your work properly and save it as **one** PDF file.

Warning: Please make sure that your work is properly scanned. Oversized, blurred or upside-down images will NOT be accepted.

(iii) While you can upload and save draft in moodle, you MUST click the "Submit" button to declare your final submission before the due date. Otherwise, you will be considered late.

**Preparation Guidelines**

(i) Your solution should be well written and organized. It is good to work out a draft for each question on a separate paper, polish/rewrite/reorganize your answer suitably and then write it (the final form) on the paper to be scanned.

(ii) You may imagine that you are teaching this course and writing a solution to demonstrate the answer. Hence, especially for proof-type questions, you have to convince everyone that your solution (proof) is correct, without any oral explanation from you. i.e. Another student should be able to understand the answer (proof) completely via your written word, and/or diagrams or tables you create in your solution.

(iii) Follow HKU's regulations on academic honesty. Plagiarism is inacceptable and may have severe consequences for your record. See `https://tl.hku.hk/plagiarism/` for "What is plagiarism?". *If you have used AI tools to explore, check or refine your work, please acknowledge and clearly identify the parts of your work that involve AI output to avoid plagiarism or related academic dishonesty. Indicate the extent to which the AI output is used (e.g. directly copied or paraphrased/modified or checked for errors or reorganized the presentation).*

## To be handed in

1. Find all prime ideals and all maximal ideals in $\mathbb{Z}_3 \times \mathbb{Z}_4$.

2. Let $S$ be a set with at least two elements, and $R$ be its power set, i.e. $R$ is the set containing all subsets of $S$. For any $A, B \in R$, we endow $R$ with the operations

$$A + B := A \ominus B, \quad A \cdot B := A \cap B$$

where $A \ominus B := (A \setminus B) \cup (B \setminus A)$ is the symmetric difference of $A$ and $B$. It is known that $(R, +)$ is a group, and the operation $\cdot$ is well-defined and associative.

   (a) Show that $(R, +, \cdot)$ is a commutative ring with unity. What are the zero and unity of this ring?

   (b) Evaluate the characteristic $\mathrm{char}(R)$ and the group of units $R^\times$ of $R$.

   (c) Show that every prime ideal $P$ of $R$ is maximal.

3. Let $R$ be a non-zero commutative ring with unity, $R[t]$ the polynomial ring over $R$ and $\mathrm{Map}(R, R)$ be the set of all functions (maps) from $R$ to $R$.

   commutative

   (a) Verify that $\mathrm{Map}(R, R)$ is a ring under the addition and multiplication of functions, i.e. $(\phi + \psi)(\alpha) := \phi(\alpha) + \psi(\alpha)$ and $(\phi \cdot \psi)(\alpha) := \phi(\alpha) \cdot \psi(\alpha)$ for any $\phi, \psi \in \mathrm{Map}(R, R)$ and $\alpha \in R$.

   (b) Define $F : R[t] \to \mathrm{Map}(R, R)$ by mapping a polynomial $f \in R[t]$ to the associated polynomial function $f_R \in \mathrm{Map}(R, R)$.

   (i) Show that $F$ is a ring homomorphism.

   (ii) If $R$ is a finite field, show that $F$ is surjective.

   (ii) If $R$ is an infinite field, show that $F$ is injective.

4. Show that an algebraically closed field must be infinite.

5. Which of $\mathbb{Q}[t]/\langle t^2 + 1 \rangle$, $\mathbb{Z}_3[t]/\langle t^2 + 1 \rangle$, $\mathbb{Z}_5[t]/\langle t^2 + 1 \rangle$, $\mathbb{Z}_2[t]/\langle t^3 + t^2 + 1 \rangle$ are fields? Justify your answer.

6. Let $f(t) = t^2 + 4t + 1$. Show that $F := \mathbb{Z}_5[t]/\langle f \rangle$ is a field of 25 elements, and hence show that the polynomial $f(t) = t^2 + 4t + 1$ has a root in $\mathbb{F}_q$ for $q = 5^2$ where $\mathbb{F}_q$ denotes **the**[†] finite field of 25 elements.

7. Let $\mathbb{F}_q$ be a finite field of $q$ elements. Show that $\alpha^{q-1} = 1$ for all nonzero $\alpha \in \mathbb{F}_q$.

*End*

[†]See Theorem 12.3.4 in lecture notes.