THE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MATH3301 Assignment 1

Due Date: Sept 19, 2024, 23:59

Submission Guidelines

(i) Write your solution for Part II 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) As 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).*

Part I: Not to be handed in

1. Let I and J be ideals in $\mathbb{Z}$. Show that $I \cap J$ is also an ideal.

2. Let $m, n \in \mathbb{Z}$ and consider the ideals $\langle m \rangle$ and $\langle n \rangle$.
   If $(m, n) = 1$, show that $\langle m \rangle \cap \langle n \rangle = \langle mn \rangle$. What do you obtain if $(m, n) = d$?

3. (a) Use Corollary 1.2.11 (of Lecture Notes) to show:
   (i) If $d = (k, l)$, then k/d is relatively prime to l/d, i.e. $(\frac{k}{d}, \frac{l}{d}) = 1$.
   (ii) If $l|kn$ and $d = (k, l)$, then l/d divides n.
   Hence or otherwise, show that if $k|n$ and $l|n$ with $(k, l) = 1$, then $kl|n$.

   (b) Justify the statements in Part (a) again with the Fundamental Theorem of Arithmetic, i.e. Theorem 1.2.16 (instead of Corollary 1.2.11).

4. Let $1 < n \in \mathbb{N}$. Suppose $(a, n) = 1$. Show that there exists unique a' with $0 < a' < n$ and $(a', n) = 1$ such that $aa' \equiv 1 (\text{mod } n)$.

   [Hint: Use Corollary 1.2.11 and the Division Algorithm.]

5. Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ by $\varphi(a) = r$ where r is the remainder of a when divided by n.
   Prove that $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\forall\ a, b \in \mathbb{Z}$.

   Define $\psi : \mathbb{Z} \to \mathbb{Z}_n$ by $\psi(a) = r$ where r is the remainder of a^2 when divided by n.
   Show that ψ is a well-defined function. Must ψ be surjective? Does ψ preserve addition?

6. Let $G = \{a, b, c, d\}$ be a set of 4 elements and its multiplication table be

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

   Does G under the operation $*$ form a group? Explain your answer.

7. Write out the Cayley tables for $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_2^\times$, $\mathbb{Z}_3^\times$ and $\mathbb{Z}_4^\times$.

8. (a) Let X be a set, and $\mathrm{Perm}(X)$ be the set of all bijective maps from X to itself. Show that $(\mathrm{Perm}(X), \circ)$ is a group where $\circ$ is the composition of maps.

(b) Let $X = \{1,2,3\}$ and write $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ for the (bijective) function from X to X that $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$ respectively. Check that $\mathrm{Perm}(X)$ contains the six bijective functions below:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Evaluate $\rho_i \circ \rho_j$ $(1 \le i, j \le 2)$ and $\mu_\alpha \circ \mu_\beta$ $(1 \le \alpha, \beta \le 3)$ in terms of $e, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3$.

(c) Show that the group $\mathrm{Perm}(X)$ is non-abelian if X contains at least 3 elements.

(d) If X and Y are two sets and if $I : X \to Y$ is a bijection, show that

$$\phi_I : \quad \mathrm{Perm}(X) \longrightarrow \mathrm{Perm}(Y), \quad f \longmapsto I \circ f \circ I^{-1}, \quad f \in \mathrm{Perm}(X),$$

is an isomorphism from the group $\mathrm{Perm}(X)$ to $\mathrm{Perm}(Y)$.

(e) Let G be a group and define the maps $l_a : G \to G$, $l_a(x) = ax$ and

$$l : \quad G \longrightarrow \mathrm{Perm}(G), \quad a \longmapsto l_a \quad \forall\ a \in G,$$

Show that l is a group embedding. [Let G_1 and G_2 be groups. If $\phi : G_1 \to G_2$ is an injective group homomorphism, we call ϕ a **group embedding** or **embedding of G_1 into G_2**.]

Part II: To be handed in

1. Let G be a group and e be its identity. Consider the following statements.

   (1) G is an abelian group.

   (2) G is a finite group of even order.

   (3) There exists a non-identity element a in G satisfies $a^2 = e$.

   (4) Every non-identity element a in G satisfies $a^2 = e$.

   For each of these statements, determine which of the other statements can be implied. (For example, consider (1). Check if (1) implies (2), (1) implies (3) and (1) implies (4).) For each implication, provide a detailed justification. For each non-implication, provide a counterexample to illustrate why it does not hold.

2. Let H and K be subgroups of a group G. Consider $H \cup K$ and $H \cap K$.

   (a) Which of them is always a subgroup of G? Provide a justification for your answer, either by proof or counterexample.

   (b) For the situation where it is not always a subgroup, find all the cases where it can be a subgroup. Justify your answer.

3. Let G be a group and H a subgroup of G. Consider

   - the **center of** G: $Z = \{x \in G : gx = xg, \ \forall g \in G\}$;
   - the **centralizer of** H **in** G: $C(H) = \{g \in G : gh = hg, \ \forall h \in H\}$;
   - the **normalizer of** H **in** G: $N(H) = \{g \in G : ghg^{-1} \in H, \ \forall h \in H\}$.

   and $g^{-1}hg \in H$

   (a) Show that all of them are subgroups of G.

   (b) Determine whether they must be abelian. Provide a justification for your answer, either by proof or counterexample.

   [Hint: Part I Qn 8 provides a source of non-abelian groups.]

End