MA136 Introduction to Abstract Algebra

(1) Show that any subgroup of a cyclic group is cyclic.

(2) Let $G$ be an abelian group. Show that if $\sigma, \tau \in G$ have orders $r, s$ respectively, then $\sigma \tau$ has order dividing $\text{lcm}(r, s)$. Give a counterexample to show that this does not necessarily hold for a non-abelian group.

(3) Write $\mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[2i]$ is a subring of $\mathbb{C}$. Compute its unit group.

(4) Is $\{2a + 2bi : a, b \in \mathbb{Z}\}$ as subring of $\mathbb{C}$?

(5) Which of the following are subrings of $M_{2 \times 2}(\mathbb{R})$? If so, are they commutative?
   
   (i) $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$.
   
   (ii) $\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R} \right\}$.
   
   (iii) $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a \in \mathbb{R}, b \in \mathbb{Z} \right\}$.

(6) Let

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{Z}, b \in \mathbb{R} \right\}.$$ 

Show that $S$ is a ring under the usual addition and multiplication of matrices. Compute $S^\star$.

(7) Show that $(\mathbb{Z}/7\mathbb{Z})^\star$ is cyclic but $(\mathbb{Z}/8\mathbb{Z})^\star$ is not.

(8) Show that the only subring of $\mathbb{Z}$ is $\mathbb{Z}$. Show that the only subring of $\mathbb{Z}[i]$ containing $i$ is $\mathbb{Z}[i]$.

(9) Let

$$S = \left\{ \frac{a}{2^r} : a, r \in \mathbb{Z}, r \geq 0 \right\}.$$ 

Show that $S$ is a ring and find its unit group.

(10) Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{2}]$ is a ring and that $1 + \sqrt{2}$ is unit. What is its order?
(11) Let \( \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \). Show that \( \mathbb{Q}[\sqrt{2}] \) is a field.

(12) Let
\[
F = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.
\]
(a) Show that \( F \) is a field (under the usual addition and multiplication of matrices).
\( \text{(Hint: Begin by showing that } F \text{ is a subring of } M_{2 \times 2}(\mathbb{R}). \text{ You need to also show that } F \text{ is commutative and that every non-zero element has an inverse in } F.) \)
(b) Let \( \phi : F \to \mathbb{C} \) be given by \( \phi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi \). Show that \( \phi \) is a bijection that satisfies \( \phi(A + B) = \phi(A) + \phi(B) \) and \( \phi(AB) = \phi(A)\phi(B) \).
(c) Show that \( F' = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{C} \right\} \) is not a field.

(13) Let \( \zeta = e^{2 \pi i / 3} \) (this is a cube root of unity). Check that \( \overline{\zeta} = \zeta^2 \). Let \( \mathbb{Z}[\zeta] = \{a + b \zeta : a, b \in \mathbb{Z}\} \).
(a) Show that \( \zeta^2 \in \mathbb{Z}[\zeta] \) (\( \text{Hint: the sum of the cube roots of unity is } \ldots \)).
(b) Show that \( \mathbb{Z}[\zeta] \) is a ring.
(c) Show that \( \pm 1, \pm \zeta \) and \( \pm \zeta^2 \) are units in \( \mathbb{Z}[\zeta] \).
(d) (Hard) Show that \( \mathbb{Z}[\zeta]^* = \{\pm 1, \pm \zeta, \pm \zeta^2\} \). Show that this group is cyclic.

(14) A commutative ring \( R \) is an integral domain if it satisfies the following property:
for all \( x, y \in R \), if \( x \neq 0 \) and \( y \neq 0 \) then \( xy \neq 0 \).
(a) Show that every field is an integral domain.
(b) Show that \( \mathbb{Z}/m\mathbb{Z} \) is an integral domain if and only if \( m \) is prime.
(c) In Question (5) you showed that
\[
\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a \in \mathbb{R}, b \in \mathbb{Z} \right\}
\]
is a commutative ring. Is it an integral domain?
(d) Let \( R \) be an integral domain, and \( x \) a non-zero element of \( R \). Let \( f_x : R \to R \) be given by \( f_x(y) = xy \).
\( \text{(i) Show that } f_x \text{ is injective.} \)
\( \text{(ii) Suppose } R \text{ is finite. Show that } x \text{ is a unit } (\text{Hint: apply the pigeon-hole principle to } f_x). \)
\( \text{(iii) Deduce that a finite integral domain is a field.} \)