Remarks for next Homework
For Exercise 8, just find a non-abelian group of order 75.
[You need not classify all groups of order 75.]

Remarks on This Exercise

Corollary 9 (Ch. 4) If \(|G| = p^2\) for \(p\) prime. Then either

(a) \(G \cong \mathbb{Z}_{p^2}\)

or (b) \(G \cong \mathbb{Z}_p \times \mathbb{Z}_p \cong \mathbb{F}_p^2 \cong \mathbb{F}_p^2 \) (2-D vector space over \(\mathbb{F}_p\)).

In case (a), \(\text{Aut}(\mathbb{Z}_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^* \cong \mathbb{Z}/p\mathbb{Z} - \{1, 2p, 3p, ..., p^2 - p\}\)

Thus \(|\text{Aut}(\mathbb{Z}_{p^2})| = p^2 - p\).

In case (b) \(\text{Aut}(\mathbb{F}_p^2) \cong GL_2(\mathbb{F}_p)\).

To find homomorphism \(\Phi: \mathbb{Z} \rightarrow \text{Aut}(\mathbb{F}_p^2)\), find \(A \in GL_2(\mathbb{F}_p)\) with \(A^k = I\). \(\Phi(a) \sim \langle A \rangle \leq \text{Aut}(\mathbb{F}_p^2)\)

\(a^m \rightarrow A^m\)
Chapter 7 Introduction to Rings

Definition A ring is a set \( R \) with two operations \( + \) and \( \cdot \) (plus and multiplication) satisfying:

(i) \((R, +)\) is an abelian group, identity 0.
(ii) Multiplication is associative. \((ab)c = a(bc) = abc\)
(iii) Distributive Law \((a+b)c = ac + bc, \quad a(b+c) = ab + ac\).

\( R \) is commutative if \( ab = ba \) \( \forall a, b \in R \).
\( R \) has an identity if \( \exists 1 \in R \) with \( 1a = a = a1 \) \( \forall a \in R \).

Examples: \( \mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}, \mathbb{M}_2 \)

Matrix Rings Given a ring \( R \), let \( M_n(R) \) be \( n \times n \) matrices with entries in \( R \). This is a ring under matrix addition and multiplication.

\( M_n(R) \) is not commutative if \( n \geq 2 \).

\( M_n(R) \) has identity \( I \) \( \iff \) \( R \) has identity 1.

Proposition 1
1. \( 0a = a0 = 0 \) \( \forall a \in R \)
2. \( -(a-b) = a - (-b) \)
3. \( (-a)(b) = ab \)
4. If \( a \in R \), then \( -a = (-1)a \)

Definition A ring \( R \) is called a division ring if \( 1 \in R \) and \( \forall a \in R \), \( \exists b \in R \), \( ab = 1 \). A commutative division ring is called a field.

Examples of fields: \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z} \) (\( p \) prime)

Example of a non-commutative division ring:

Quaternions \( \mathbb{H} = \{ a + bi + cj + dk | a, b, c, d \in \mathbb{R} \} \)
An Example of a non-commutative division ring.

Quaternions (Don't confuse them with Quaternion group $\mathbb{H}$).

For many years W. R. Hamilton (1805 - 1865) searched for an algebra of 3-D space.

1-D space $\mathbb{R}$ (field) basis is called a
2-D space $\mathbb{C}$ (field) basis is for complex analysis
3-D space $\mathbb{H}$ (quaternions - division algebra)
4-D space $\mathbb{H}$ (quaternions - division algebra)

\[ \mathbb{H} = \{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid z, w \in \mathbb{C} \} \]

\[ = \{ \begin{bmatrix} x + iy & u + iv \\ -u + iv & x - iy \end{bmatrix} \mid x, y, z, w \in \mathbb{R} \} \]

Operations Matrix addition (+) is associative &
Matrix multiplication (not commutative)

\[ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = z \overline{z} + w \overline{w} = |z|^2 + |w|^2 \neq 0 \text{ if } z, w \neq 0. \]

Thus every non-zero element of $\mathbb{H}$ is invertible.

Definitions $a \in \mathbb{R}$ is a zero divisor if $a \neq 0$
and $\exists b \in \mathbb{R}$, $b \neq 0$ with $ab = 0$.

Example $6 \in \mathbb{Z}/12\mathbb{Z}$ is zero divisor, as $6 \cdot 6 = 0$.

Definition $a \in \mathbb{R}$ is a unit if $\exists b \in \mathbb{R}$ with $ab = 1$.

Example $5 \in \mathbb{Z}/12\mathbb{Z}$ is a unit, as $5 \cdot 5 = 1$. 