## 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) $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \cong \mathbb{F}_p \times \mathbb{F}_p \cong \mathbb{F}_p^2$ (2-D vector space over $\mathbb{F}_p$)

In Case (a), $\mathrm{Aut}(\mathbb{Z}_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p^2\mathbb{Z} - \underbrace{\{1p, 2p, 3p \cdots pp=0\}}_{p}$

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

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

To find homomorphism $\varphi : \mathbb{Z}_k \longrightarrow \mathrm{Aut}(\mathbb{F}_p^2)$, find $A \in GL_2(\mathbb{F}_p)$ with $A^k = I$. $\varphi : \langle a \rangle \xrightarrow{\sim} \langle A \rangle \leq \mathrm{Aut}(\mathbb{F}_p^2)$

$$a^m \longmapsto A^m$$

# 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 $(a+b)c = ac+bc$, $a(b+c) = ab+ac$.

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

Examples: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$, $n\mathbb{Z}$

Matrix Rings Given a ring $R$, let $M_n(R)$ = $n \times n$ 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 $(-a)b = a(-b) = -(ab)$
③ $(-a)(-b) = ab$
④ If $1 \in R$, 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~~ $\cancel{\mathbb{H} = \{ [}$

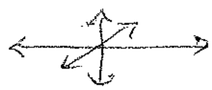
## An Example of a non-commutative division ring.

**Quaternions** (Don't confuse them with Quaternion group $Q_8$)

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

1-D space $\longleftrightarrow$ $\mathbb{R}$ (field) basis for calculus.

2-D space  $\mathbb{C}$ (field) basis for complex analysis

3-D space  Is this a field?? No!

4-D space  $\mathbb{H}$ (quaternions – division algebra)

$$\mathbb{H} = \left\{ \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \,\middle|\, z, w \in \mathbb{C} \right\}$$

$$= \left\{ \begin{bmatrix} x+iy & u+vi \\ -u+vi & x-yi \end{bmatrix} \,\middle|\, x, y, z, w \in \mathbb{R} \right\}$$

Operations: Matrix addition (+), Matrix mult. (not commutative) $\Big\}$ associative & distributive laws hold by linear algebra.

$$\begin{vmatrix} z & w \\ -\bar{w} & \bar{z} \end{vmatrix} = z\bar{z} + w\bar{w} = |z|^2 + |w|^2 \neq 0 \quad \text{if } z, w \neq 0.$$

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

**Definitions** $a \in R$ is a <u>zero divisor</u> if $a \neq 0$ and $\exists\, b \in R$, $b \neq 0$ with $ab = 0$.

**Example** $\bar{6} \in \mathbb{Z}/12\mathbb{Z}$ is zero divisor, as $\bar{6} \cdot \bar{2} = \bar{0}$.

**Definition** $a \in R$ is a <u>unit</u> if $\exists\, b \in R$ with $ab = ba = 1$

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