

The background of the entire image is a dense, repeating geometric pattern. It consists of interlocking shapes in three primary colors: red, blue, and gold. The red shapes are triangles with internal patterns, the blue shapes are hexagons with internal patterns, and the gold shapes are star-like or floral motifs. These shapes are arranged in a grid-like fashion, creating a complex, tessellated effect. The overall appearance is reminiscent of traditional Islamic or Arabesque art.

Math 3500

# Algebra I: Group Theory

Book 3

Eg.  $F = \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$  where  $p$  is a prime  
(finite field of order  $p$ ).

Take  $n=2$  and consider the vector space  $V = F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$ ,  
an additive abelian group of order  $p^2$ .

Every homomorphism  $V \rightarrow V$  is a linear transformation over the field  $F$ .

If  $T: V \rightarrow V$  is a homomorphism then  $T(v+w) = T(v) + T(w)$ .

$$T(2v) = T(v+v) = T(v) + T(v) = 2T(v)$$

$$T(3v) = T(2v+v) = T(2v) + T(v) = 2T(v) + T(v) = 3T(v)$$

In fact  $T(kv) = kT(v)$  for all  $k \in \mathbb{F}_p$ .

So  $Tv = Av$  for some  $2 \times 2$  matrix  $A$  over  $F$ .

There are exactly  $p^4$  homomorphisms  $V \rightarrow V$ .

How many of these  $p^4$  homomorphisms are automorphisms of  $V$ ?

$$(p^2-1)(p^2-p) = |GL_2(F)|.$$

The Klein four-group (any group of order 4 which is not cyclic)

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

eg.  $G \cong \{1, 3, 5, 7\}$  under multiplication mod 8

or  $\langle (12)(34), (13)(24) \rangle < S_4$

$$= \{(), (12)(34), (13)(24), (14)(23)\}$$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$$F = \mathbb{F}_2 = \{0, 1\} \quad (\text{integers mod } 2)$$

$G \cong F^2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in F \right\} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$  is an additive abelian group

This is another way to look at the Klein four-group.

It has 6 automorphisms i.e. isomorphisms from the group to itself.

The group  $G$  (Klein four-group) has 16 endomorphisms

(homomorphisms  $G \rightarrow G$ )

Why? To define an endomorphism  $T$  of  $G = \{1, a, b, c\}$   
 $= \langle a, b \rangle$

$$\begin{aligned} ab &= c \\ |a| &= |b| = |c| = 2 \end{aligned}$$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

think of  $T$  as a linear transformation  $T: G \rightarrow G$

there are four choices of  $T(a) \in G$  i.e.  $T(a) \in \{1, a, b, c\}$

... ..  $T(b) \in G$

$$\text{Then } T(c) = T(ab) = T(a)T(b)$$

Only 6 of these 16 homomorphisms are invertible.

How many endomorphisms does a finite cyclic group have?

Take  $G = C_n = \{1, g, g^2, \dots, g^{n-1}\}$ ,  $|g| = n$ .

How many homomorphisms are there from this group to itself? Exactly  $n$ .

They are the maps  $\phi_0, \phi_1, \dots, \phi_{n-1}$  where  $\phi_j: G \rightarrow G$ ,  $\phi_j(g^i) = g^{ij}$ .

Note that  $\phi_j(xy) = (xy)^j = x^j y^j = \phi_j(x) \phi_j(y)$  so  $\phi_j$  is a homomorphism.

Note that  $\phi_j \neq \phi_k$  for  $j \neq k$  in  $\{0, 1, \dots, n-1\}$

Since  $\phi_j(g) = g^j \neq g^k = \phi_k(g)$  so we have at least  $n$  different homomorphisms  $C_n \rightarrow C_n$ .

Conversely, suppose  $\phi: C_n \rightarrow C_n$  is any homomorphism.  
 Then  $\phi(g) = g^i \in G$ ,  $0 \leq i \leq n-1$ . In this case we claim  $\phi = \phi_i$ .

$$\phi(g^2) = \phi(gg) = \phi(g)\phi(g) = g^i g^i = g^{2i} = (g^2)^i = \phi_i(g^2)$$

$$\phi(g^3) = \phi(g^2g) = \phi(g^2)\phi(g) = g^{2i} g^i = g^{3i} = (g^3)^i = \phi_i(g^3)$$

Inductively we get  $\phi(x) = \phi_i(x)$  for all  $x \in G$  i.e.  $\phi = \phi_i$ .  $\square$

eg.  $G = C_4 = \{1, g, g^2, g^3\}$  has four endomorphisms  $\phi_0, \phi_1, \phi_2, \phi_3$  defined by

$$\phi_j(g^i) = g^{ij}$$

$x$	$\phi_0(x)$	$\phi_1(x)$	$\phi_2(x)$	$\phi_3(x)$
1	1	1	1	1
$g$	1	$g$	$g^2$	$g^3$
$g^2$	1	$g^2$	1	$g^2$
$g^3$	1	$g^3$	$g^2$	$g$

$$\phi_0(g^i) = g^{0i} = g^0 = 1$$

trivial homomorphism

$$\phi_0(ab) = \phi_0(a)\phi_0(b)$$

$$\phi_1(g^i) = g^{1i} = g^i \text{ is the identity}$$

$$\phi_2(g^i) = g^{2i}, \quad \phi_2(x) = x^2$$

$$\phi_3(x) = x^3$$

$$\text{If } \psi(g^i) = g \text{ then } g = \psi(g^2) = \psi(gg) \neq \underbrace{\psi(g)}_g \underbrace{\psi(g)}_g = g^2$$

$$\phi_j(xy) = (xy)^j = x^j y^j = \phi_j(x)\phi_j(y)$$