

The background features a repeating geometric pattern. It consists of a grid of white lines forming a lattice. Within the cells of this grid are various shapes: some are triangles with internal patterns, some are hexagons with internal patterns, and some are more complex, multi-lobed shapes. The colors used are red, blue, and gold. The overall effect is a dense, intricate tessellation.

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 2×2 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. $T(a) \in \{1, a, b, c\}$

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

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 ϕ_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

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

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

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

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

$$\text{If } \psi(g^i) = g \text{ then } g = \psi(g^2) = \psi(gg) \neq \underbrace{\psi(g)}_g \underbrace{\psi(g)}_g = g^2 \quad \phi_j(xy) = (xy)^j = x^j y^j = \phi_j(x)\phi_j(y)$$

$G = \{1, g, g^2, \dots, g^{n-1}\}$ has n homomorphisms $G \rightarrow G$, namely $\phi_k(x) = x^k$, $0 \leq k \leq n-1$ or $1 \leq k \leq n$.

How many of these are isomorphisms? (bijective)

$\phi_k: G \rightarrow G, x \mapsto x^k$ is one-to-one iff it's onto iff it's bijective iff $\gcd(k, n) = 1$

For $n=12$, $\phi_k: C_{12} \rightarrow C_{12}$ is bijective iff $k \in \{1, 5, 7, 11\}$. (k is relatively prime to n).

$\phi_3: C_{12} \rightarrow C_{12}$ has image $\phi_3(C_{12}) = \{1, g^3, g^6, g^9\}$ ϕ_3 is neither one-to-one nor onto.

$$\phi_3(1) = \phi_3(g^4) = 1$$

$$g \notin \phi_3(C_{12}) \quad \text{"} g^2 \text{"} \quad \text{"} g^7 \text{"}$$

The image of $f: G \rightarrow H$ is $f(G) = \{f(g) : g \in G\}$.

$\phi_5: C_{12} \rightarrow C_{12}$ is onto; its image is $\{1, g^5, g^{10}, g^{15}, g^{20}, g^{25}, g^{30}, g^{35}, g^{40}, g^{45}, g^{50}, g^{55}\}$

$\phi_9: C_{12} \rightarrow C_{12}$ is not onto; $\phi_9(C_{12}) = \{1, g^9, g^6, g^3, g^0\}$ $g^{60} = (g^{12})^5 = 1^5 = 1$

Euclid's Algorithm (extended form):

Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. Then there exist integers $r, s \in \mathbb{Z}$ such that $d = ra + sb$. (That is, d is an integer linear combination of a, b).

Ex. $a=369$, $b=126$. We will compute $d=\gcd(a,b)$ and write d as an integer linear combination of a,b .

$$369 = 2 \times 126 + 117$$

$$126 = 1 \times 117 + \boxed{9} \leftarrow d=9 = \gcd(a,b)$$

$$117 = 13 \times 9 + 0$$

$$\begin{array}{r} 369 \\ 252 \\ \hline 117 \end{array}$$

$$9 = 126 - 117$$

$$= 126 - (369 - 2 \times 126)$$

$$= 3 \times 126 - 369$$

$$12 = 2 \times 5 + 2$$

$$5 = 2 \times 2 + \boxed{1} = \gcd(12,5) =$$

$$2 = 2 \times 1 + 0$$

$$1 = 5 - 2 \times 2$$

$$= 5 - 2(12 - 2 \times 5)$$

$$= 5 \times 5 - 2 \times 12$$

$$k = 5k \times 5 - 2k \times 12$$

We want to show every element of C_{12} is the 5th power of some element.

$$g^k = g^{5k \times 5 - 2k \times 12} = (g^{5k})^5 \underbrace{(g^{12})^{-2k}}_1 = (g^{5k})^5$$

$(k \in \mathbb{Z})$

$$a = 369 = 3 \times 123 = 3^2 \times 41$$

$$b = 126 = 3 \times 42 = 2 \times 3 \times 21 = 2 \times 3 \times 3 \times 7 = 2 \times 3^2 \times 7.$$

There are n homomorphisms $\phi_k: C_n \rightarrow C_n$, $k \in \{1, 2, \dots, n\}$ $\phi_k(x) = x^k$.

There are $\phi(n)$ isomorphisms $C_n \rightarrow C_n$, namely ϕ_k , $1 \leq k \leq n$, $\gcd(k, n) = 1$.
Euler's totient function $\phi(n) =$ number of integers $k \in \{1, \dots, n\}$ such that $\gcd(k, n) = 1$.

$$\phi(12) = 4.$$

Sorry I'm using " ϕ " more than once.

There are exactly $\phi(n)$ elements $x \in C_n$ such that $\langle x \rangle = C_n$.

For $n=12$, $\phi(12) = 4$ since $1, 5, 7, 11$ are the only elements $k \in \{1, 2, \dots, 12\}$ such that $\gcd(k, 12) = 1$.

In $C_{12} = \{1, g, g^2, \dots, g^{11}\}$, $\langle g \rangle = C_{12} = \langle g^5 \rangle = \langle g^7 \rangle = \langle g^{11} \rangle$

Suppose $f: G \rightarrow H$ is a group homomorphism.

Then $f(1_G) = 1_H$ where 1_G is the identity element of G and 1_H is the identity element of H . Eg. if $T: V \rightarrow W$ is a linear transformation then

$$T(0) = 0$$

↑
zero vector.

Proof: $f(1_G) = f(1_G 1_G) = f(1_G) f(1_G)$. Multiply both sides on the left by $f(1_G)^{-1} \in H$
to get $1_H = f(1_G)^{-1} f(1_G) = \underbrace{f(1_G)^{-1} f(1_G)}_{1_H} f(1_G) = 1_H f(1_G) = f(1_G)$. \square

$$f(1_G)^{-1} (f(1_G) f(1_G)) = \underbrace{f(1_G)^{-1} f(1_G)}_{1_H} f(1_G)$$

More generally, $|f(g)|$ divides $|g|$ for every $g \in G$ (assuming $|g| < \infty$).

If $|g| = 6$ then $|f(g)| = 1, 2, 3$ or 6 .

If $|g| = 1$ then $|f(g)| = 1$ (which says $f(1_G) = 1_H$).

Proof? Note that $f(g^k) = f(\underbrace{g \cdot g \cdot g \cdots g}_{k \text{ times}}) = \underbrace{f(g) f(g) \cdots f(g)}_{k \text{ times}}$

$$f(gg) = f(g)f(g)$$

$$f(ggg) = f(g)f(gg) = f(g)f(g)f(g)$$

Now suppose $|g| = n$ and $d = |f(g)|$. We must show that $d | n$.

We have $n = qd + r$ for some integers q, r with $0 \leq r < d$. Then

$$1 = g^n \Rightarrow 1 = f(1) = f(g^n) = f(g)^n = f(g)^{qd+r} = (f(g)^d)^q f(g)^r = 1^q f(g)^r$$

By definition of the order of an element, $r=0$, i.e. $d | n$. $\square = f(g)^r$

One way in which group theory is different from linear algebra: If V, W are vector spaces and you take $v \in V, w \in W$. You can always find a linear transformation $T: V \rightarrow W$ such that $T(v) = w$ (unless $v=0$ and $w \neq 0$). Recall $T(0) = 0$.

If $f: C_{12} \rightarrow C_{12}$ is a homomorphism then we cannot have $f(g^3) = g^9$ since $|g^3| = 4$ does not divide $|g^3| = 4$. Every homomorphism $f: C_{12} \rightarrow C_{12}$ must take $f(g^3) \in \{1, g^3, g^6, g^9\}$. Use ϕ_0, ϕ_1, ϕ_2 to get these.

Careful: In S_4 , there are several homomorphisms $S_4 \rightarrow S_4$.

If $f: S_5 \rightarrow S_5$ is a homomorphism, $f((12)) \in \{1, (12), (12)(34), \dots\}$
elements of order 1 or 2

But what is an example of a homomorphism $f: S_5 \rightarrow S_5$ only.
such that $f((12)) = (12)(34)$?

You can say $f(\sigma) = \begin{cases} (1) & \text{if } \sigma \text{ is even} \\ (12)(34) & \text{if } \sigma \text{ is odd} \end{cases}$ (i.e. $\sigma \in A_5$)

This is not an isomorphism.

There is an isomorphism $\phi: S_5 \rightarrow S_5$ such that $\phi((12345)) = (12453)$?
Yes.

More generally if G is a multiplicative group and $a \in G$, then we can define an isomorphism $\psi_a: G \rightarrow G$, $\psi_a(x) = axa^{-1}$ (conjugation by a).

$$\psi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \psi_a(x)\psi_a(y) \text{ for all } xy \in G.$$

This shows that $\psi_a: G \rightarrow G$ is a homomorphism.

Why is it one-to-one? If $\psi_a(x) = \psi_a(x')$ then $axa^{-1} = ax'a^{-1}$ then $a^{-1}(axa^{-1})a = a^{-1}(ax'a^{-1})a$
so $x = x'$.

Why is it onto? For all $y \in G$, we must find $x \in G$ such that $\psi_a(x) = y$
 $axa^{-1} = y$

$\psi_a: G \rightarrow G$ is a bijection

and it is a homomorphism

so it is an isomorphism from G to G so it is an automorphism of G .

$$x = a^{-1}(axa^{-1})a = a^{-1}ya$$

ie. $\psi_a(a^{-1}ya) = y$

If G is abelian then $\psi_a(x) = axa^{-1} = a\cancel{a}^{-1}x = x$ i.e. $\psi_a = \text{identity}$.
 The center of G is $Z(G) = \{z \in G : z \text{ commutes with every element of } G\}$

$Z(G)$ is a subgroup of G . If $z_1, z_2 \in Z(G)$ then $z_1 z_2 \in Z(G)$ since

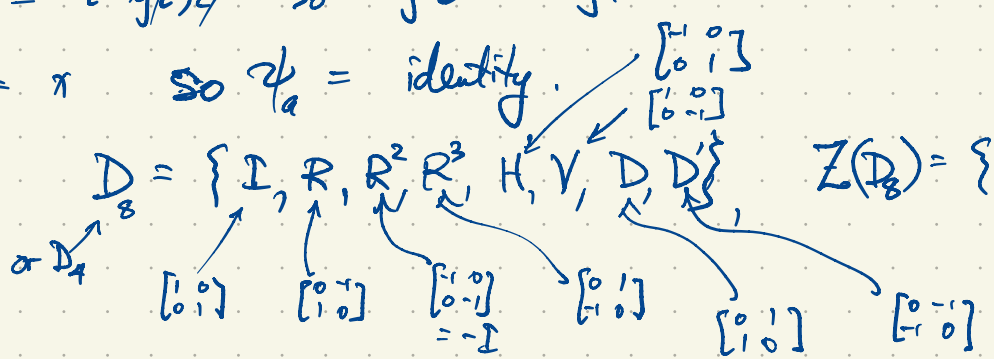
$$z_1 z_2 g = z_1 g z_2 = g z_1 z_2 \text{ for all } g \in G.$$

Clearly $1 = 1_G$ commutes with every $g \in G$ since $1g = g = g1$, $1 \in Z(G)$.

If $z \in Z(G)$ then $z^{-1} \in Z(G)$ since for all $g \in G$,
 $zg = gz$ so $z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1}$ so $gz^{-1} = z^{-1}g$.

If $a \in Z(G)$ then $\psi_a(x) = axa^{-1} = x\cancel{a}a^{-1} = x$ so $\psi_a = \text{identity}$.

In the dihedral group of order 8, $D_8 = \{I, R, R^2, R^3, H, V, D, D'\}$, $Z(D_8) = \{I, R^2\}$



We have an nontrivial automorphism of D_8

$$\psi_R(x) = RxR^{-1}$$

$$\psi_R(I) = I$$

$$\psi_R(-I) = -I$$

$$\psi_R(R) = RRR^{-1} = R$$

$$\psi_R(R^3) = RRR^3R^{-1} = R^{-1} = R^3$$

$$\psi_R(D) = D'$$

$$\psi_R(D') = D$$

$$\psi_R(H) = V$$

$$\psi_R(V) = H$$

$$\psi_R(-I) = R(-I)R^{-1} = -IRR^{-1} = -I$$

$$\psi_D(x) = DxD^{-1} = Dx D$$

$$\psi_D(I) = I$$

$$\psi_D(-I) = -I$$

$$\psi_D(R) = R^3$$

$$\psi_D(R^3) = R$$

$$\psi_D(R^2) = R^2$$

$$\psi_D(H) = V$$

$$\psi_D(V) = H$$

$$\psi_D(D) = D$$

$$\psi_D(D') = D'$$

Four automorphisms of D_8 :

$$\psi_I = \psi_{R^2} = \text{identity}$$

Since $I, R^2 \in Z(D_8)$

$$\psi_R = \psi_{R^3}$$

$$\psi_D = \psi_{D'}$$

$$\psi_H = \psi_V$$

If $a, x \in G$ then we say axa^{-1} is the conjugate of x by a .

Conjugation in G is the map $x \mapsto axa^{-1}$ for fixed $a \in G$.

We say two elements $x, y \in G$ are conjugate if $y = axa^{-1}$ for some $a \in G$.

In this case we often write $x \sim y$.

In $GL_n(\mathbb{R})$, two elements are conjugate iff they are similar.

Conjugacy (the relation \sim) is an equivalence relation.

D_8 has five conjugacy classes: $\{I\}$, $\{R^2\}$, $\{R, R^3\}$, $\{H, V\}$, $\{D, D'\}$.

In any group, the conjugacy classes of size 1 are $\{z\}$, $z \in Z(G)$.

$$aza^{-1} = zaa^{-1} = z$$

$Z(G)$ is the union of conjugacy classes of size 1 in G .