

The background features a repeating geometric pattern. It consists of a grid of white lines forming a lattice of triangles and hexagons. Within these shapes, there are intricate, stylized designs in red and cyan. Interspersed throughout the pattern are small, golden, star-like motifs. The overall effect is a dense, colorful, and mathematically inspired 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  $2 \times 2$  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.  $T(a) \in \{1, a, b, c\}$

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

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

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

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

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

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

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

$G = \{1, g, g^2, \dots, g^{n-1}\}$  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  $\phi_3(C_{12}) = \{1, g^3, g^6, g^9\}$   $\phi_3$  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 5<sup>th</sup> 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  $\phi_k$ ,  $1 \leq k \leq n$ ,  $\gcd(k, n) = 1$ .  
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 " $\phi$ " 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

In  $C_{12} = \{1, g, g^2, \dots, g^{11}\}$ ,  $\langle g \rangle = C_{12} = \langle g^5 \rangle = \langle g^7 \rangle = \langle g^{11} \rangle$   $\gcd(k, 12) = 1$ .

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

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

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

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  $\phi_0, \phi_1, \phi_2$  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  $\psi_a(x) = axa^{-1} = aa^{-1}x = x$  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

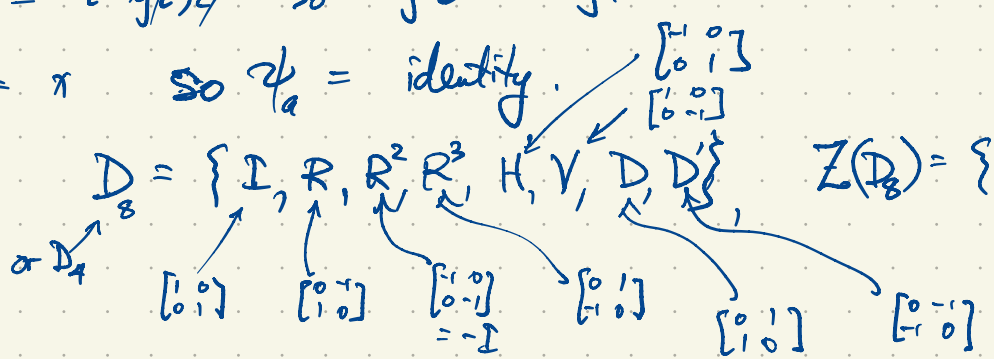
$$z_1 z_2 g = z_1 g z_2 = g z_1 z_2 \text{ for all } g \in G.$$

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  $\psi_a(x) = axa^{-1} = xaa^{-1} = x$  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  $D_8$

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

$$\psi_R(I) = I$$

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

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

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

$$\psi_R(D) = D' \quad \psi_R(H) = V$$

$$\psi_R(D') = D \quad \psi_R(V) = H$$

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

$$\psi_D(I) = I \quad \psi_D(H) = V$$

$$\psi_D(-I) = -I \quad \psi_D(V) = H$$

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

$$\psi_D(R^3) = R \quad \psi_D(D') = D'$$

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

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  $G$ .

Given  $a, x \in G$ ,  $\varphi_a(x) = axa^{-1}$  (the conjugate of  $x$  by  $a$ ).

$\varphi_a: G \rightarrow G$  which is conjugation by  $a$ .

$\varphi_a$  is an automorphism of  $G$ :  $\varphi_a$  is bijective and  $\varphi_a(xy) = \varphi_a(x)\varphi_a(y)$ .

Eg. Conjugation in  $S_n$  takes permutations to permutations of the same cycle structure (ie. it preserves cycle structure).

When we count elements of  $S_n$  according to their cycle structure, we are actually counting group elements by conjugacy classes.

For  $n=8$ ,  $\sigma = (13725)(48)$ ,  $\tau = (14)(2536)$ . Conjugating  $\sigma$  by  $\tau$  gives

$$\varphi_{\tau}(\sigma) = \tau\sigma\tau^{-1} = \underbrace{(14)(2536)}_{\tau} \underbrace{(13725)(48)}_{\sigma} \underbrace{(14)(2635)}_{\tau^{-1}} = (18)(2)(34675) = \underline{(18)(34675)}$$

Observe:  $\sigma$  and  $\tau\sigma\tau^{-1}$  are not only the same order, they have the same cycle structure.

But conversely, if two permutations have the same cycle structure, they must be conjugate. Why?

$$\begin{array}{l} \sigma = (13725)(48) \\ \quad \downarrow \downarrow \downarrow \downarrow \downarrow \quad \downarrow \downarrow \\ \tau\sigma\tau^{-1} = (46753)(18) = \underline{(18)(34675)} \end{array} \quad \tau = (14)(2536)$$

Eg. Find  $\tau \in S_8$  such that  $\tau(135)(2746)\tau^{-1} = (1823)(457)$

$$\begin{array}{l} \downarrow \downarrow \downarrow \quad \downarrow \downarrow \downarrow \\ (457)(1823) \end{array} \quad \tau = (142)(35786) \text{ works.}$$

$$\underline{\text{OR}} \quad \begin{array}{l} (8) \\ \downarrow \\ (6) \end{array} \tau(135)(2746)\tau^{-1} = (1823)(457)$$

$$\begin{array}{l} \downarrow \downarrow \downarrow \quad \downarrow \downarrow \downarrow \\ (574)(2318) \end{array} \quad \tau = (154)(2)(37)(68) = (154)(37)(68)$$

Given  $g \in G$ , the centralizer of  $g$  is  $C_G(g) = \{ \text{all elements of } G \text{ that commute with } g \}$   
 $= \{ z \in G : zg = gz \}$

Once again,  $C_G(g) \leq G$  ( $C_G(g)$  is a subgroup of  $G$ )

If  $z_1, z_2 \in C_G(g)$  then  $z_1 z_2 \in C_G(g)$  since  $(z_1 z_2)g = z_1 g z_2 = g z_1 z_2$ .

$1_G \in C_G(g)$  since  $1_G g = g = g 1_G$

If  $z \in C_G(g)$  then  $z^{-1} \in C_G(g)$  as before (back 2 pages or so).

If  $x$  and  $y$  are conjugate in  $G$  then the number of elements  $a \in G$  conjugating  $x$  to  $y$  is  $|C_G(x)|$ .

Eg. In  $G = S_8$ , how many elements  $\tau \in S_8$  conjugate  $(13725)(48)$  to

$(46753)(18)$ ? Same as: How many elements commute with

$\sigma = (13725)(48)$ . Answer: 10. in this case.

Why is  $\tau \sigma \tau^{-1}$  the same as  $\sigma$  with all symbols in the cycle structure replaced by  $i \mapsto \tau(i)$ ?

$$\sigma = (\dots, i, \sigma(i), \dots) (\dots) \dots (\dots)$$

$$(\tau \sigma \tau^{-1})(\tau(i)) = \tau \sigma \tau^{-1}(\tau(i)) = \tau(\sigma(i)) \text{ i.e.}$$

$$\tau \sigma \tau^{-1} = (\dots, \tau(i), \tau(\sigma(i)), \dots) \dots (\dots)$$

If  $A \in GL_n(F)$  is diagonalizable (which happens over  $\mathbb{C}$  "most" of the time)

then  $A$  is similar (i.e. conjugate) to a diagonal matrix in  $GL_n(F)$ , i.e.  $A = BDB^{-1}$  for some diagonal matrix  $D$  and  $B \in GL_n(F)$ .

$$\begin{array}{ccc} v & \xrightarrow{A} & Av = BDB^{-1}v \\ B^{-1} \downarrow & & \uparrow B \\ B^{-1}v & \xrightarrow{D} & DB^{-1}v \end{array}$$

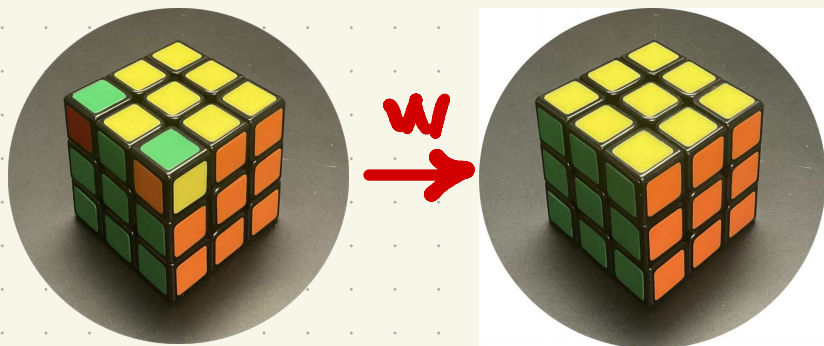
Scale by  $\lambda_i$   $i^{\text{th}}$  coordinate

Similarly in  $GL_n(F)$ :

$$D = \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ 0 & & \lambda_n \end{bmatrix} \text{ scales } e_i \mapsto \lambda_i e_i \text{ where } e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{i^{\text{th}}}$$

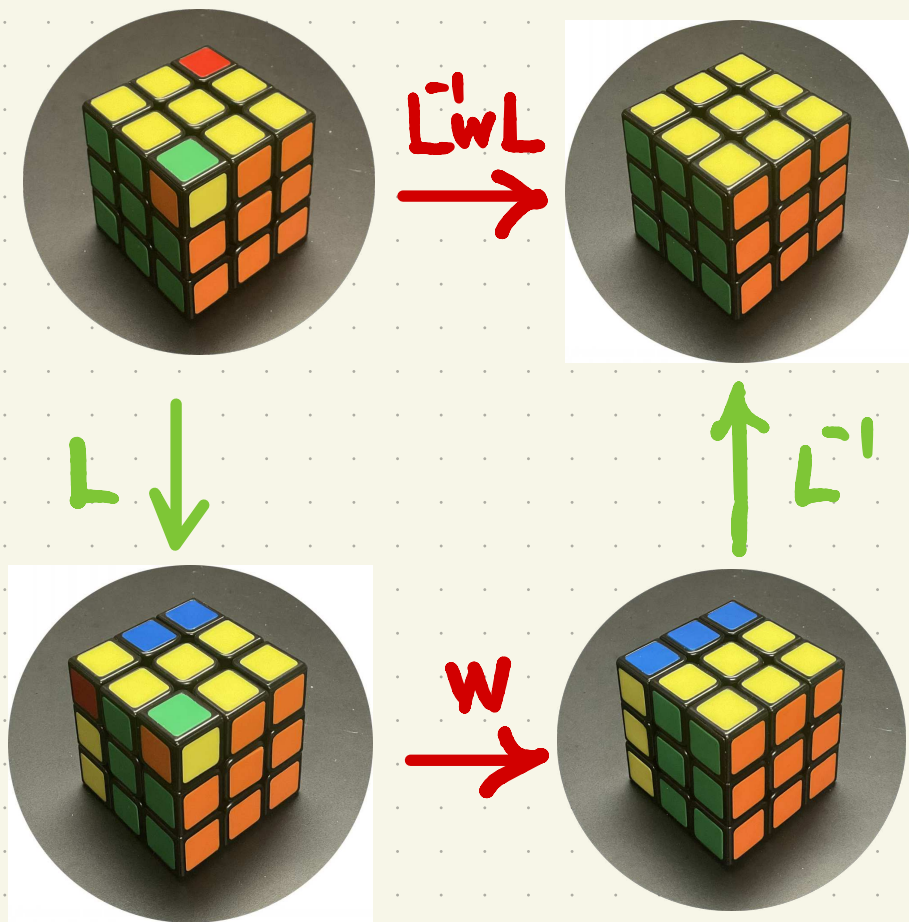
Example: The group  $G$  of legal moves of Rubik's Cube has order  $|G| = 43252003274489856000$  (depending a little on whether or not we count moves that move the six center pieces).

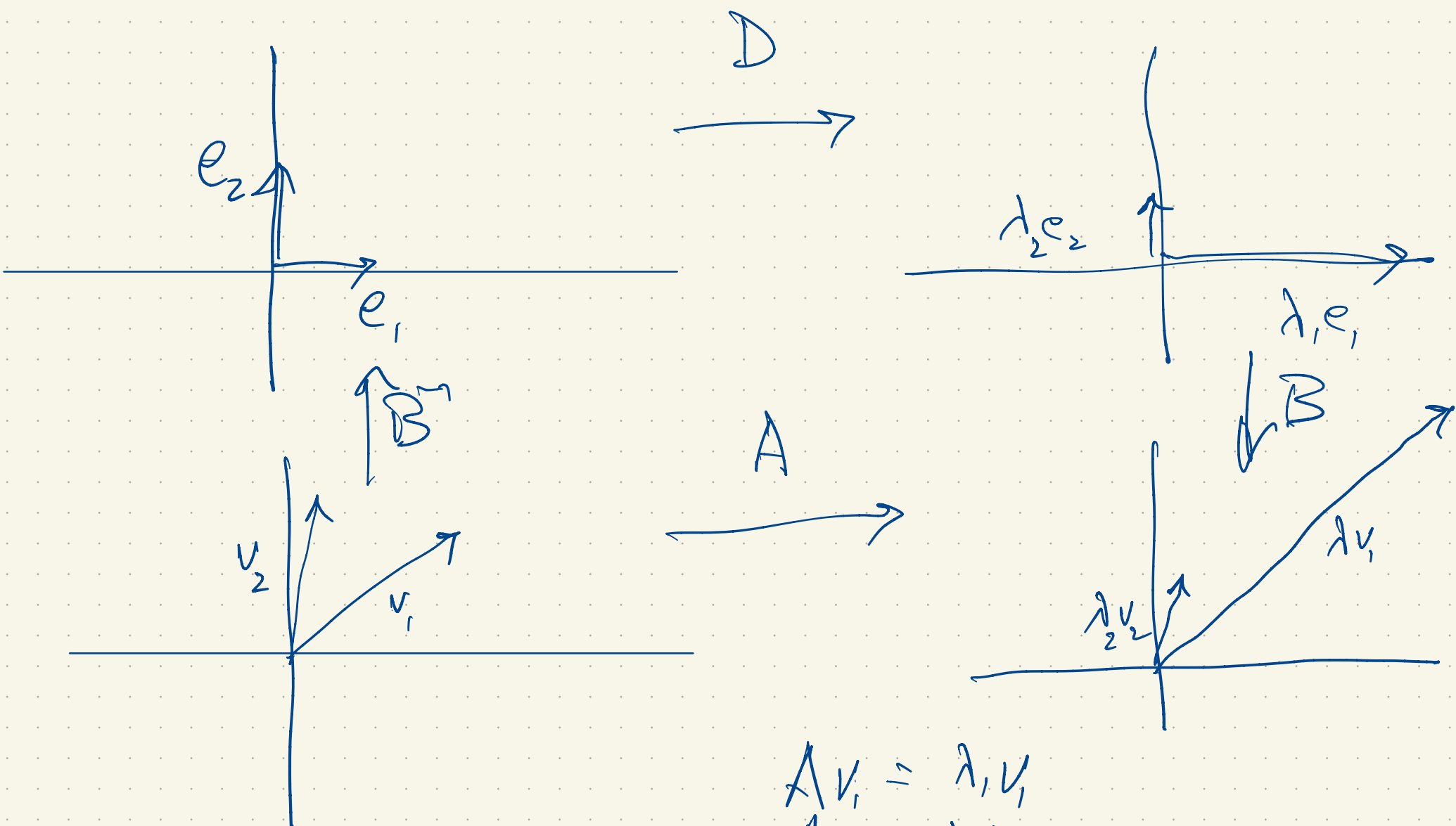
An example of conjugation in  $G$ :



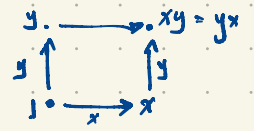
In our class, we might write  

$$W = U^2 B U^2 B U B' U B U^2 B U^2 B U^2 B U^2 B U^2 B$$
 (right-to-left composition) but the standard guides for cubing would reverse this (using left-to-right composition as mathematicians prefer).





Commutative diagram



$$\begin{aligned}
 Av_1 &= \lambda_1 v_1 \\
 Av_2 &= \lambda_2 v_2
 \end{aligned}$$

If  $G$  is any group then an automorphism of  $G$  is a bijection  $\phi: G \rightarrow G$  such that  $\phi(gh) = \phi(g)\phi(h)$  for all  $g, h \in G$ .

Eg. If  $G = C_n = \langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$  <sup>cyclic</sup> of order  $n$ , then there are  $\phi(n)$  automorphisms of  $C_n$  where  $\phi(n) = |\{k : 1 \leq k \leq n, \gcd(k, n) = 1\}|$ .  $\phi$  is Euler's totient function.

$\phi_k(x) = x^k, \phi_k(g^i) = g^{ki}$  is a homomorphism  $C_n \rightarrow C_n$ ; it's an automorphism iff  $\gcd(k, n) = 1$ .

If  $n=6$ , there are 6 homomorphisms  $\phi_k: C_6 \rightarrow C_6, x \mapsto x^k$ .

$\phi_1(x) = x$  identity

$\phi_2(x) = x^2$  is not one-to-one since  $\phi_2(g^3) = (g^3)^2 = g^6 = 1 = \phi_2(1)$

$\phi_3(x) = x^3$  is not one-to-one since  $\phi_3(g^2) = (g^2)^3 = g^6 = 1 = \phi_3(1) = \phi_3(g^4) = g^{12} = 1$

$\phi_4(x) = x^4$  is not one-to-one since  $\phi_4(g^3) = (g^3)^4 = g^{12} = 1 = \phi_4(1)$

$\phi_5(x) = x^5 = x^{-1}$  is one-to-one and onto.

$x$	$\phi_5(x)$
1	1
$g$	$g^5$
$g^2$	$g^4$
$g^3$	$g^3$
$g^4$	$g^2$
$g^5$	$g$

Eg.  $\text{Aut}(G) = \{\text{all automorphisms of } G\}$  is a group (not to be confused with  $G$ ), the automorphism group of  $G$ .

$G = C_n$

$\text{Aut}(C_6) = \{\phi_1, \phi_5\} \cong C_2$

↑  
identity

	$\phi_1$	$\phi_5$
$\phi_1$	$\phi_1$	$\phi_5$
$\phi_5$	$\phi_5$	$\phi_1$

eg.  $\phi_5 \phi_5(x) = (x^5)^5 = x^{25} = x^{24} \cdot x = 1 \cdot x = x = \phi_1(x)$

This is not that!  $G \neq \text{Aut } G$ .

	1	$g$	$g^2$	$g^3$	$g^4$	$g^5$
1	1	$g$	$g^2$	$g^3$	$g^4$	$g^5$
$g$	$g$	$g^2$	$g^3$	$g^4$	$g^5$	1
$g^2$	$g^2$	$g^3$	$g^4$	$g^5$	1	$g$
$g^3$	$g^3$	$g^4$	$g^5$	1	$g$	$g^2$
$g^4$	$g^4$	$g^5$	1	$g$	$g^2$	$g^3$
$g^5$	$g^5$	1	$g$	$g^2$	$g^3$	$g^4$

If  $a \in G$  then  $\phi_a(x) = axa^{-1}$  (conjugation by  $a \in G$ ) is an inner automorphism of  $G$ .

This gives lots of examples of automorphisms of  $G$  if  $G$  is nonabelian.

Abelian groups tend to have lots of automorphisms but they're not inner (except for the identity  $\text{id}: G \rightarrow G$ ,  $\text{id}(g) = g$ ,  $\text{id}(gh) = gh = \text{id}(g)\text{id}(h)$ ,  $\text{id} \in \text{Aut } G$  (not  $\text{id}_G$ )).

If  $F$  is any field then  $V = F^n$  is usually thought of as a vector space of dimension  $n$  over  $F$ . Ignoring scalar multiplication, this is a group under  $+$  with identity element the zero vector.

If  $F = \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ . In this case  $F$  is a cyclic group under addition and automorphisms of this group are scalar multiplication by nonzero elements of  $F$ .

$\text{Aut}(F^n) \cong GL_n(F)$

Each  $A \in GL_n(F)$  gives an automorphism of  $F^n$ ,  $A: v \rightarrow Av$

This is a homomorphism  $F^n \rightarrow F^n$  since  $A(v+w) = Av + Aw$

Since  $A$  is invertible,  $A: F^n \rightarrow F^n$  is bijective. The inverse of  $A: v \rightarrow Av$  is  $A^{-1}: v \rightarrow A^{-1}v$ .

Sometimes  $F^n$  has more automorphisms than these but often not.

An inner automorphism of  $F^n$  is a function of the form  $\phi_a: v \rightarrow a + v + (-a) = v$ ,  $a, v \in F^n$

$\phi_a(v) = v$  i.e.  $\phi_a = \text{id}$  for all  $a \in V$ .

Ex.  $\text{Aut}(S_n) \cong S_n$  if  $n \neq 6$ .  $S_6$  has outer automorphisms (automorphisms that are not inner)

There is  $f \in \text{Aut}(S_6)$  such that  $f((12)) = (12)(34)(56)$  and this cannot be an inner automorphism.

Theorem There is a homomorphism  $G \rightarrow \text{Aut } G$  defined by  $a \mapsto \phi_a$ . Shoer-Sock Theorem

Proof  $\phi_{ab} = \phi_a \phi_b$  because  $(\phi_a \circ \phi_b)(g) = \phi_a(\phi_b(g)) = a(bg b^{-1})a^{-1} = (ab)g(ba^{-1}) = (ab)g(aba^{-1}) = \phi_{ab}(g)$

for all  $a, b, g \in G$ .

$GL_4(\mathbb{F}_2) \cong A_8$  of order 20160

$\text{Aut}(GL_4(\mathbb{F}_2)) \cong S_8$  of order 40320.

All automorphisms of  $SL_2(\mathbb{R})$  are inner. (I think)

For  $n > 2$ , there are outer automorphisms of  $SL_n(\mathbb{R})$ .

Let's explain starting with  $GL_n(\mathbb{R})$ .

Aut  $GL_n(\mathbb{R})$  includes inner automorphisms.  $\phi_B(A) = BAB^{-1}$

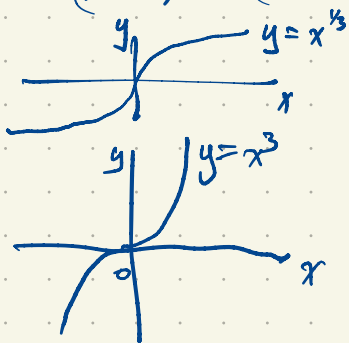
$GL_2(\mathbb{R})$  has an automorphism  $\phi(A) = (\det A)A$ .

$$\phi(AB) = \det(AB)AB = (\det A)(\det B)AB = (\det A)A \cdot (\det B)B = \phi(A)\phi(B).$$

Why is  $\phi: GL_2(\mathbb{R}) \rightarrow GL_2(\mathbb{R})$  bijective?

Suppose  $\phi(A) = \phi(B)$  i.e.  $(\det A)A = (\det B)B$ .

$$(\det A)^3 = (\det B)^3 \Rightarrow \det A = \det B \Rightarrow A = B.$$



Why is  $\phi$  onto?

Given  $A \in GL_2(\mathbb{R})$ , find  $X \in GL_2(\mathbb{R})$  such that  $\phi(X) = A$ . Answer:  $X = (\det A)^{-1/3}A$ .

The inverse of  $\phi: GL_2(\mathbb{R}) \rightarrow GL_2(\mathbb{R})$ ,  $A \mapsto (\det A)A$

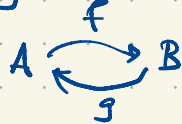
$$\text{is } \phi^{-1}(A) = (\det A)^{-1/2}A$$

also an automorphism of  $GL_2(\mathbb{R})$

If a linear transformation is invertible, then its inverse is also a linear transformation.

If a group homomorphism is invertible, then its inverse function is also a group homomorphism.

A function  $f: A \rightarrow B$  from set  $A$  to set  $B$  is bijective  $\iff$  it has a (well-defined) inverse  $g: B \rightarrow A$ .



$$\text{i.e. } f \circ g: B \rightarrow B$$

is the identity on  $B$

$$b \mapsto b \text{ for all } b \in B.$$

$g \circ f: A \rightarrow A$  is the identity  $A \rightarrow A$  is  $a \mapsto a$  for all  $a \in A$ .

All automorphisms of  $SL_2(\mathbb{R})$  are inner: they have the form

$$\phi: SL_2(\mathbb{R}) \rightarrow SL_2(\mathbb{R})$$

$$\phi(A) = BAB^{-1}, \quad B \in SL_2(\mathbb{R})$$

eg.  $\phi(A) = A^{-T}$  i.e.  $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} = BAB^{-1}$  where  $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ .

For  $n \geq 3$ ,  $\phi: SL_n(\mathbb{R}) \rightarrow SL_n(\mathbb{R})$ ,  $\phi(A) = A^T$  is an automorphism. And for  $n \geq 3$ , this is not inner. Perhaps later we'll explain why.

A Klein four-group  $K = \{1, a, b, c\}$  has six automorphisms

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

$$\text{Aut } K \cong S_3 \quad (\text{all six permutations of } a, b, c).$$

The only inner automorphism of  $K$  is the identity  $\text{id}(x) = x$  eg.  $\phi(x) = axa^{-1} = x$

The other five automorphisms of  $K$  are outer automorphisms.

If  $G$  and  $H$  are groups then the direct product of  $G$  and  $H$  is

$$G \times H = \{(g, h) : g \in G, h \in H\} \quad (\text{the Cartesian product})$$

where  $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ .  $(g, h)^{-1} = (g^{-1}, h^{-1})$  identity in  $G \times H$  is  $1_{G \times H} = (1_G, 1_H)$ .

$\mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\} = \mathbb{R}^2$  with usual addition of vectors. (componentwise addition)

eg.  $C_n = \{1, g, g^2, \dots, g^{n-1}\}$  cyclic of order  $n$

$C_m = \{1, h, h^2, \dots, h^{m-1}\}$  ... ..  $m$

$$C_3 \times C_5 = \{(g^i, h^j) : i, j \in \mathbb{Z}\} \quad g^3 = 1 = h^5$$

$\cong C_{15}$  generated by  $(g, h)$

Powers of  $(g, h)$ :

$$\begin{aligned} (g, h)^0 &= (1, 1) \\ (g, h)^1 &= (g, h) \\ (g, h)^2 &= (g^2, h^2) \\ (g, h)^3 &= (1, h^3) \\ (g, h)^4 &= (g, h^4) \\ (g, h)^5 &= (g^2, 1) \\ (g, h)^6 &= (1, h) \\ (g, h)^7 &= (g, h^2) \leftarrow (g^7, h^7) \\ (g, h)^8 &= (g^2, h^3) \\ (g, h)^9 &= (1, h^4) \end{aligned}$$

$$C_2 \times C_2 \not\cong C_4$$

$$\begin{matrix} \uparrow \{1, g\} & \uparrow \{1, h\} \\ C_2 & \times & C_2 \end{matrix}$$

$C_2 \times C_2 = \{(1, 1), (g, 1), (1, h), (g, h)\}$  is a Klein four-group.

$$(g, h)^0 = (g, 1)$$

$$(g, h)^1 = (g^2, h)$$

$$(g, h)^2 = (1, h^2)$$

$$(g, h)^3 = (g, h^3)$$

$$(g, h)^4 = (g^2, h^4)$$

$$(g, h)^5 = (1, 1)$$

$$|(g, h)| = 15$$

$$C_3 \times C_5 = \langle (g, h) \rangle \cong C_{15}$$

Every abelian group is (isomorphic to) a direct product of cyclic groups.

Groups of order 4 are abelian:  $C_4, C_2 \times C_2$ .

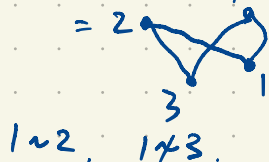
Groups of order 8: there are three abelian groups of order 8:  $C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$ .

There are two nonabelian groups of order 8: dihedral, quaternion. addition in  $F^3, F = \{0, 1\} = \mathbb{F}_2$ .

Graphs (Math 3700: Combinatorics)

A (finite) graph has vertices  $1, 2, \dots, n$ . Every pair of vertices <sup>plural of vertex</sup> is either joined by an edge or not.

(labelled) eg.  $\Gamma =$  (a 4-cycle) has order 4 (the number of vertices) and 4 edges  $\{1,2\}, \{2,3\}, \{3,4\}, \{1,4\}$ .



Vertices  $i$  and  $j$  are adjacent if  $\{i,j\}$  is an edge, and then we write  $i \sim j$  ( $j \sim i$ ).

A graph of order  $n$  has  $\binom{n}{2} = \frac{n(n-1)}{2}$  pairs of vertices. This is the maximum number of edges in a graph of order  $n$ .

$\text{Aut}(\Gamma) =$  automorphism group of this graph = the set of all permutations of the vertices which preserves the adjacency relation between vertices.  
 $= \langle (1234), (13) \rangle$

$(12)$  is not an automorphism of this graph: it maps  $\rightarrow$  a different graph isomorphic but different.

$(13)$  is an automorphism of the graph: it maps  $\rightarrow$  is the same graph.

has automorphism group  $\langle (13), (4,5), (23) \rangle \cong S_3 \times S_2 = S_3 \times C_2$   
all 6 permutations of 1,2,3 all 2 permutations of 4,5

$\text{Aut}(K_5) \cong S_5 \cong \text{Aut} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$   
 Complete graph  $K_5$  of order 5.

Given a graph  $\Gamma$  of order  $n$ , the complementary graph  $\Gamma'$  of order  $n$  has the complementary set of edges.

for  $i \neq j$  in  $\{1, 2, \dots, n\}$ ,  $i, j$  are adjacent in  $\Gamma'$  iff they're not adjacent in  $\Gamma$ .

$$\text{Aut } \Gamma' = \text{Aut } \Gamma.$$

$$\text{Aut} \left( \begin{array}{c} 3 \\ \square \\ 4 \end{array} \right) = \text{Aut} \left( \begin{array}{c} 3 \\ \times \\ 4 \end{array} \right) = \text{Aut} \left( \begin{array}{c} 3 \\ 1 \\ 4 \\ 2 \end{array} \right) = \langle (1234), (13) \rangle = \left\{ (1), (13), (24), (13)(24), \right. \\ \left. (12)(34), (1234), (1432), (11)(23) \right\}$$

$$\text{Aut} \left( \begin{array}{c} 2 \\ \square \\ 4 \end{array} \right) = \text{Aut} \left( \begin{array}{c} 3 \\ \square \\ 4 \end{array} \right) = \langle (1234), (13) \rangle \quad \text{dihedral group of order 8}$$

complementary graphs

$$\text{Aut} \left( \begin{array}{c} 1 \\ \square \\ 6 \end{array} \right) = \langle (12), (123), (45), (456), (14)(25)(36) \rangle = \langle (12), (123), (14)(25)(36) \rangle$$

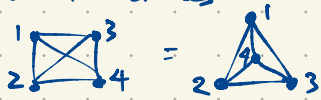
group of order 72 having  $\langle (12), (123), (45), (456) \rangle \cong S_3 \times S_3$  as a subgroup of order 36

Aut (regular tetrahedron)  
(Symmetry group)

$$\text{Aut} \left( \begin{array}{c} 1 \\ \triangle \\ 3 \end{array} \right) = \text{Aut}(K_4) \cong S_4 \text{ of order 24.}$$

complete graph on 4 vertices

Half of these are rotational symmetries (direct isometries) forming a subgroup  $\cong A_4$ .



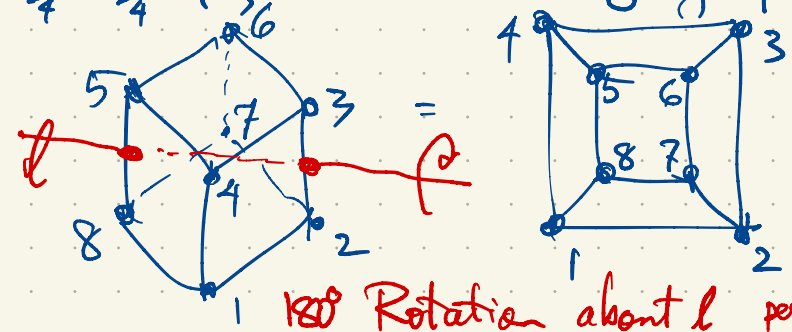
these isometries include 12 direct isometries (rotations with determinant 1) and 12 indirect isometries with determinant -1.

Aut (cube) = symmetry group of cube has order 48 (HW2)  $\cong S_4 \times C_2$

$$S_4 \cong S_4 \times \{1\} = \text{direct isometry group of cube} = \text{rotational symmetry group of cube.}$$

This graph of order 8 has the same aut. gp. as the symmetry group of the cube,  $G = \text{Aut}(\text{cube})$  (see HW4, T<sub>2</sub>)

There are four diagonals joining each vertex with its opposite vertex  $\{1,6\}, \{2,5\}, \{3,8\}, \{4,7\}$ . Rotations of the cube give every permutation of the four diagonals exactly once. So the rotational symmetry group  $\cong S_4$ .



180° Rotation about  $l$  permutes  $ab, cd$  as  $(bc)$  fixing  $a, d$ .

Rotational symmetries of the cube can be thought of as  $3 \times 3$  matrices of determinant 1. (assuming the origin of  $\mathbb{R}^3$  is the center of the cube).

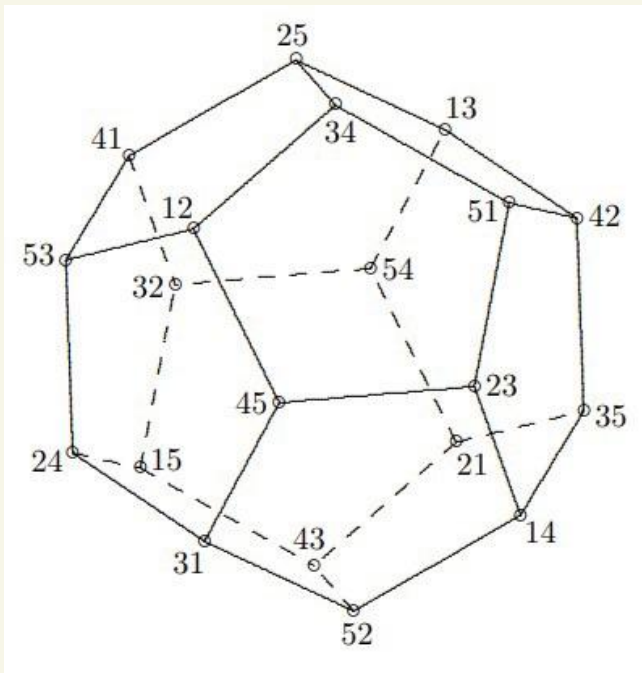
The inversion  $-I = \begin{bmatrix} -1 & & \\ & -1 & \\ & & -1 \end{bmatrix}$  is a symmetry of the cube permuting vertices as  $(16)(25)(38)(47)$ , commuting with all elements of  $G = \text{symmetry group of cube} = \{ \pm A : A \text{ rot. symmetry} \}$

$$(\pm A)(\pm B) = \pm AB$$

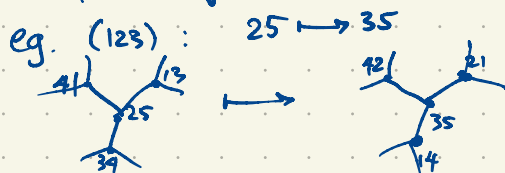
$$G = S_4 \times \{ \pm I \}$$

Regular dodecahedron has 12 faces which are regular pentagons. Its symmetry group has order 120 (direct isometries form a subgroup of order 60, the rotational symmetry group  $\cong A_5$ ; the full symm. group is  $\cong A_5 \times C_2$  where  $-I$  is inversion  $v \rightarrow -v$ )

The symmetry group has  $\{ \pm I \}$  in its center, so this group can't be  $\cong S_5$  since  $Z(S_5) = 1$  (trivial subgroup). Why does a regular dodecahedron have rotational symmetry group  $\cong A_5$ ?

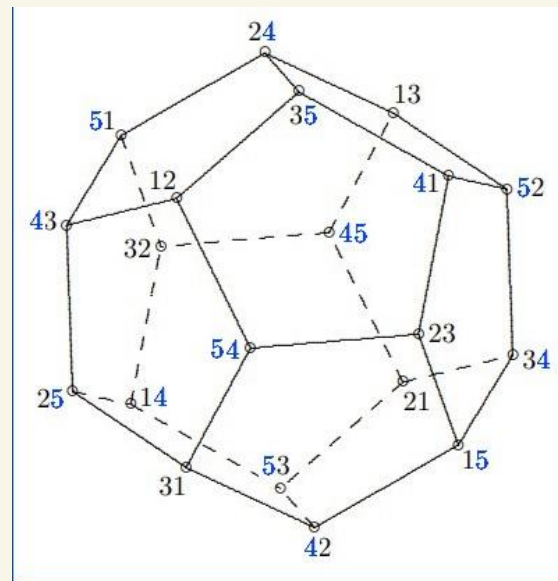


Label the 20 vertices as  $ij$  ( $i, j$  distinct in  $\{1, 2, 3, 4, 5\}$ )  $ij, ji$  antipodal.  $A_5$  permuting  $1, 2, 3, 4, 5$ .

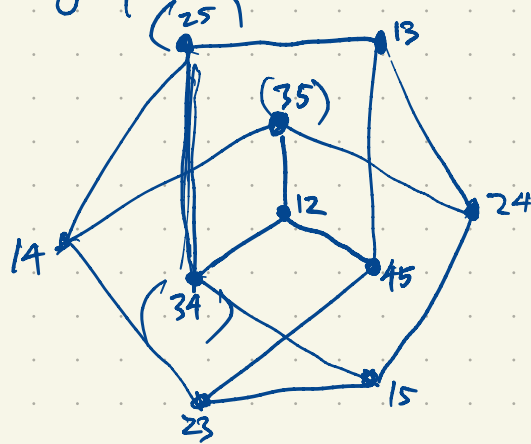


Odd permutations of  $1, 2, 3, 4, 5$  do not preserve the dodecahedron.

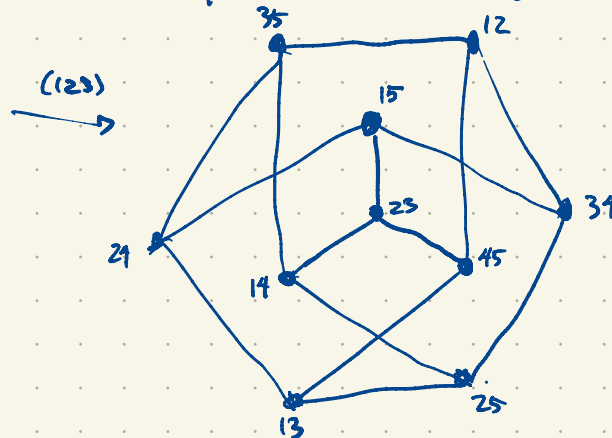
Odd permutations interchange this dodecahedron with another



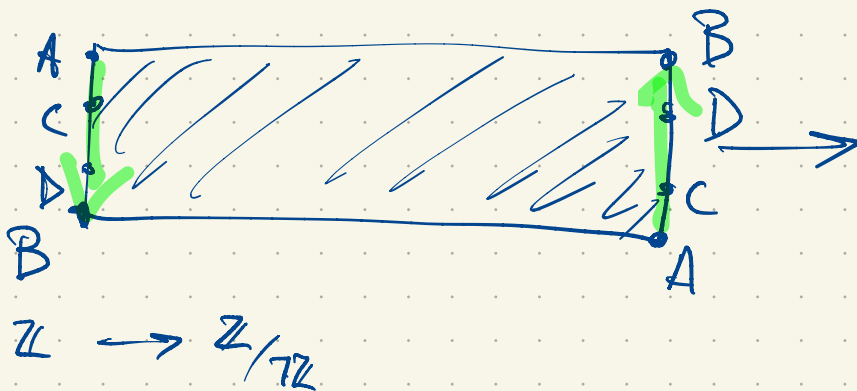
Petersen graph  $P$  (see HW4) has 120 automorphisms.  $\text{Aut } P \cong S_5$



Join two pairs if they are disjoint.



Label vertices  $\{i,j\}$ ,  $i \neq j$  in  $\{1,2,3,4,5\}$   
 $\{i,j\} = \{j,i\} = ij$



Möbius strip

$S_5$  has 10 transpositions  $(ij)$ .

$S_5$  permutes them using 120 inner automorphisms.

The Petersen graph has as its ten vertices the ten transpositions  $(ij)$  in  $S_5$  ( $1 \leq i < j \leq 5$ ).  
 Two vertices  $(ij)$ ,  $(kl)$  are adjacent  $((ij) \sim (kl))$  iff these two transpositions are distinct and they commute (i.e.  $\{i,j\} \cap \{k,l\} = \emptyset$ ). This is why  $S_5$  is (at least a subgroup of)  $\text{Aut } P$ . A little more explanation can be given to explanation to justify that  $S_5$  is the full automorphism group of  $P$ .  $\text{Aut } P \cong S_5$ .

For  $n=2,3,4$ , there is a homomorphism from  $S_n$  onto  $S_{n-1}$ , say  $\phi(S_n) = S_{n-1}$ .

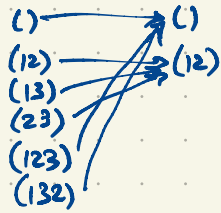
For  $n \geq 5$ , this does not hold.

This fact underlies the fact that a polynomial in  $x$  of degree  $n \geq 5$  cannot in general have roots expressible in terms of the coefficients taking  $+, -, \times, \div, \sqrt{\quad}$  (square roots, cube roots, etc.)

For  $n=2,3,4$  such formulas are known.

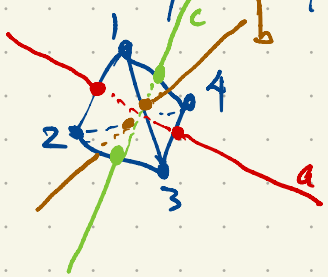
A homomorphism  $\phi: S_2 \xrightarrow{\text{onto}} S_1$   
 $\{(1), (12)\} \rightarrow \{(1)\}$       $\phi(\sigma) = (1)$ . This is the trivial homomorphism. It's not one-to-one but it is onto.

A homomorphism  $\phi: S_3 \rightarrow S_2$  which is onto:  $\phi(\sigma) = \begin{cases} (1) & \text{if } \sigma \text{ is even;} \\ (12) & \text{if } \sigma \text{ is odd.} \end{cases}$



$\phi$  is really the sign homomorphism  $\phi: S_n \rightarrow \{\pm 1\}$   
 $\phi(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even;} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$

A homomorphism  $\phi: S_4 \rightarrow S_3$  which is onto?



$a, b, c$  are three lines through the center of the regular tetrahedron with vertices  $1, 2, 3, 4$ . Any two of  $a, b, c$  are at right angles. They are the axes of the  $180^\circ$  rotations in the symmetry group  $\cong S_4$ . Every  $\sigma \in S_4$  (thought of as a symmetry of the tetrahedron) permutes  $a, b, c$ .

Eg.  $(123)$  permutes  $(a, b, c)$  i.e.  $a \mapsto c \mapsto b \mapsto a$ .  
 $(12)$  permutes  $(b, c)$  i.e.  $a \mapsto a, b \mapsto c \mapsto b$ .

It is (more or less) obvious that  $\phi$  is a homomorphism. It's onto  $\text{Sym}\{a, b, c\} \cong S_3$

$\phi: \begin{array}{l} (1), (12)(34), (13)(24), (14)(23) \longrightarrow (1) \\ (123), (134), (142), (243) \longrightarrow (acb) \\ (132), (143), (124), (234) \longrightarrow (abc) \\ (1324), (1423), (12), (34) \longrightarrow (bc) \\ (1243), (1342), (14), (23) \longrightarrow (ab) \\ (1234), (1432), (13), (24) \longrightarrow (ac) \end{array}$

all 6 permutations of  $a, b, c$

There is no homomorphism from  $S_3$  onto  $S_4$ . But this takes a little more group theory to explain.