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 $V \to V$ is a linear transformation over the field F.

If $T : V \to V$ 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 $V \to V$.

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)

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

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

$F = \mathbb{F}_2 = \{0,1\}$ (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 $G \longrightarrow G$)

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

$ab = c$

$|a| = |b| = |c| = 2$

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

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

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 $\phi_j : G \longrightarrow G$, $\phi_j(g^i) = g^{ij}$.

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

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

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

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

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

$$\underbrace{\phi_0(ab)}_{1} = \underbrace{\phi_0(a)}_{1}\underbrace{\phi_0(b)}_{1}$$

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

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

$\phi_3(x) = x^3$

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

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

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

How many of these are isomorphisms? (bijective)

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

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

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

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

$g\notin\phi_3(C_{12})$

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

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

$g^{15}=g^3$, $g^{20}=g^8$, $g^{25}=g$, $g^{30}=g^6$, $g^{35}=g^{11}$, $g^{40}=g^4$, $g^{45}=g^9$, $g^{50}=g^2$, $g^{55}=g^7$

$g^{60}=(g^{12})^5=1^5=1$

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

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).

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

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

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

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

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

$$\begin{aligned} 9 &= 126 - 117 \\ &= 126 - (369 - 2 \times 126) \\ &= 3 \times 126 - 369 \end{aligned}$$

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

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

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

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2(12 - 2 \times 5) \\ &= 5 \times 5 - 2 \times 12 \end{aligned}$$

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

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

$$g^k = g^{5k \times 5 - 2k \times 12} = (g^{5k})^5 (\underbrace{g^{12}}_{1})^{-2k} = (g^{5k})^5$$

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

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

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

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

There are $\phi(n)$ isomorphisms $C_n \to C_n$, namely ϕ_k, $1 \le k \le n$, $\gcd(k,n) = 1$.

$\underbrace{\phi(n)}_{\text{Euler's totient function}}$ $\phi(n) =$ number of integers $k \in \{1, \cdots, n\}$ 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 $k \in \{1, 2, \cdots, 12\}$ such that $\gcd(k, 12) = 1$.

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

Suppose $f : G \to H$ 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 $T : V \to W$ 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 $1_H = f(1_G)^{-1} f(1_G) = \underbrace{f(1_G)^{-1} f(1_G)}_{1_H} f(1_G) = 1_H f(1_G) = f(1_G)$. $\square$

$$f(1_G)^{-1}(f(1_G) f(1_G)) = (f(1_G)^{-1} f(1_G)) f(1_G)$$

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 $0 \le r < d$. Then

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

By definition of the order of an element, $r = 0$, ie. $d | n$. $\square$

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 $T: V \to W$ such that $T(v) = w$ (unless $v = 0$ and $w \ne 0$). Recall $T(0) = 0$.

If $f: C_{12} \to C_{12}$ is a homomorphism then we cannot have $f(g^3) = g^4$

$\{1, g, g^2, \cdots, g^{11}\}$

since $|g^4| = 3$ does not divide $|g^3| = 4$.

$f: C_{12} \to C_{12}$ must take $f(g^4) \in \{1, g^4, g^8\}$.

Every homomorphism Use ϕ_0, ϕ_1, ϕ_2 to get these.

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

If $f: S_5 \to S_5$ is a homomorphism, $f((12)) \in \{ (), (12), (12)(34), \ldots \}$
elements of order 1 or 2 only.

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

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

This is not an isomorphism.

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

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

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

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

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

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

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

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

$\psi_a : G \to G$ is a bijection
and it is a homomorphism
so it is an isomorphism from G to G so it is an automorphism of G.

If G is abelian then $\psi_a(x) = axa^{-1} = aa^{-1}x = x$ i.e. ψ_a = identity.

The <u>center</u> of G is $Z(G) = \{z\in G : z$ commutes with every element of $G\}$

$\cancel{Z}$

$Z(G)$ is a <u>subgroup</u> of G. If $z_1, z_2 \in Z(G)$ then $z_1z_2\in Z(G)$ since

$$z_1z_2g = z_1gz_2 = gz_1z_2 \quad \text{for all } g\in G.$$

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 $g\in G$,

$$zg = gz \quad \text{so} \quad \cancel{z^{-1}}(\cancel{z}g)z^{-1} = z^{-1}(g\cancel{z})\cancel{z^{-1}} \quad \text{so} \quad gz^{-1} = z^{-1}g.$$

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

In the dihedral group of order 8, D_8 (or D_4) $= \{I, R, R^2, R^3, H, V, D, D'\}$, $Z(D_8) = \{I, R^2\}$

$I = \begin{bmatrix}1&0\\0&1\end{bmatrix}$, $R = \begin{bmatrix}0&-1\\1&0\end{bmatrix}$, $R^2 = \begin{bmatrix}-1&0\\0&-1\end{bmatrix} = -I$, $R^3 = \begin{bmatrix}0&1\\-1&0\end{bmatrix}$, $H = \begin{bmatrix}-1&0\\0&1\end{bmatrix}$, $V = \begin{bmatrix}1&0\\0&-1\end{bmatrix}$, $D = \begin{bmatrix}0&1\\1&0\end{bmatrix}$, $D' = \begin{bmatrix}0&-1\\-1&0\end{bmatrix}$

We have an nontrivial automorphism of D_8

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

$\psi_R(I) = I$

$\psi_R(-I) = -I$ $\quad\quad \psi_R(-I) = R(-I)R^{-1} = -I\cancel{RR^{-1}} = -I$

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

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

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

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

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

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

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

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

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

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

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 <u>conjugate</u> of x by a.

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

We say two elements $x, y \in G$ are <u>conjugate</u> 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).

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

φ_a is an automorphism of G: φ_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 σ by τ gives

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

Observe: σ 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?

$$\sigma = (1\,3\,7\,2\,5)(4\,8) \qquad \tau = (14)(2536)$$
$$\tau\sigma\tau^{-1} = (4\,6\,7\,5\,3)(1\,8) = (18)(34675)$$

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

$$(4\,5\,7)(1\,8\,2\,3) \qquad \tau = (142)(35786) \text{ works.}$$

OR

$$\begin{array}{c} (8) \\ \downarrow \\ (6) \end{array} \quad \tau(1\,3\,5)(2\,7\,4\,6)\tau^{-1} = (1823)(457)$$
$$(5\,7\,4)(2\,3\,1\,8) \qquad \tau = (154)(2)(37)(68) = (154)(37)(68)$$

Given $g \in G$, the <u>centralizer</u> of g is $C_G(g) = \{$ all elements of G that commute with $g\}$

$= \{z \in G : zg = gz\}$

Once again, $C_G(g) \le G$ ($C_G(g)$ is a <u>subgroup</u> 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 $1_G g = g = g 1_G$

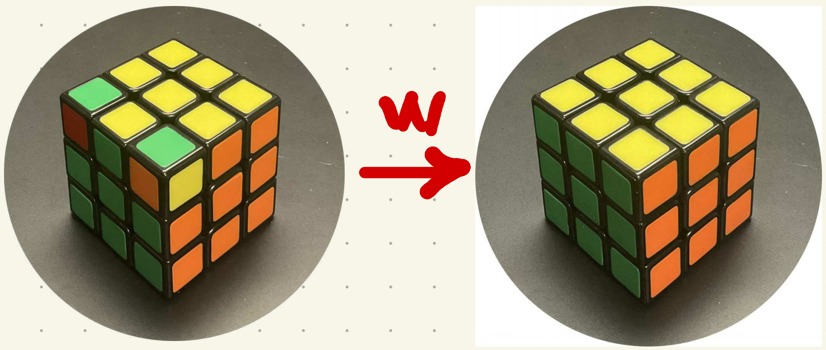
If $z \in C_G(g)$ then $z^{-1} \in C_G(g)$ as before (back 2 pages or so).

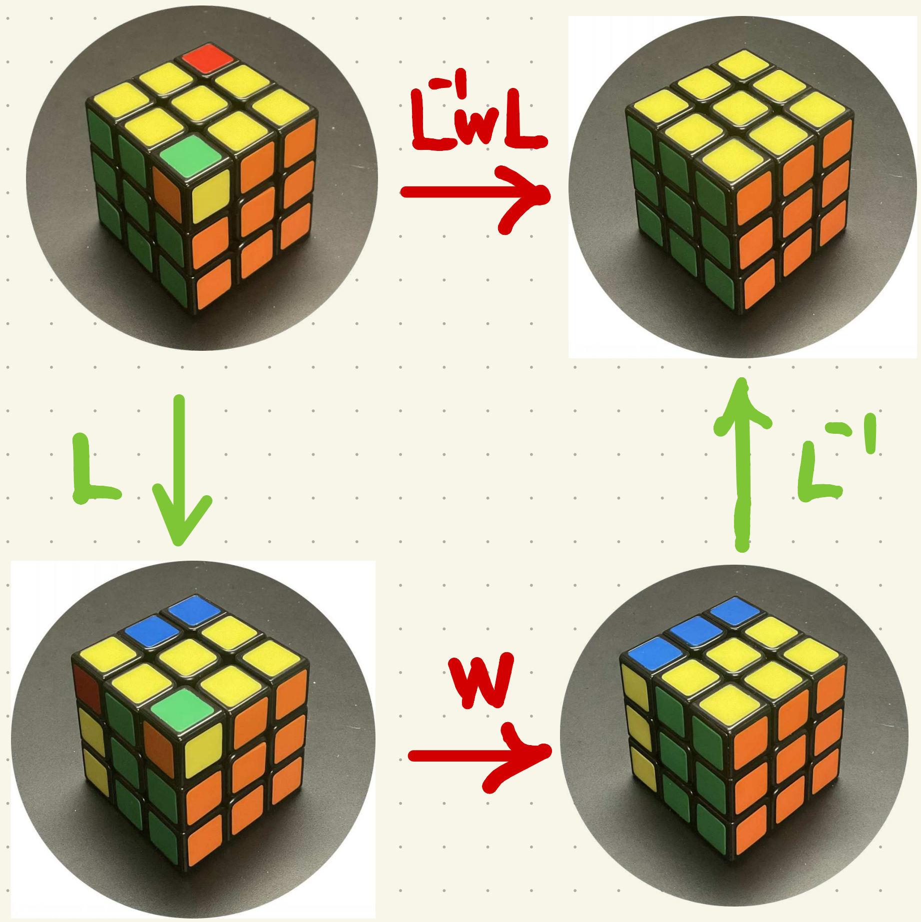
If x and y are conjugate in G then the number of elements $a \in G$ conjugating x to y is $|C_G(x)|$.

Eg. In $G = S_8$, how many elements $\tau \in S_8$ conjugate $(1\,3\,7\,2\,5)(4\,8)$ to $(4\,6\,7\,5\,3)(1\,8)$? Same as: How many elements commute with $\sigma = (1\,3\,7\,2\,5)(4\,8)$. Answer: 10 in this case.

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

$$w = U^2 B^{-1} U^2 B U B^{-1} U B U^2 B U^2 B^{-1} U^{-1} B U^{-1} B^{-1}$$

(right-to-left composition) but the standard guides for cubing would reverse this (using left-to-right composition as mathematicians prefer).