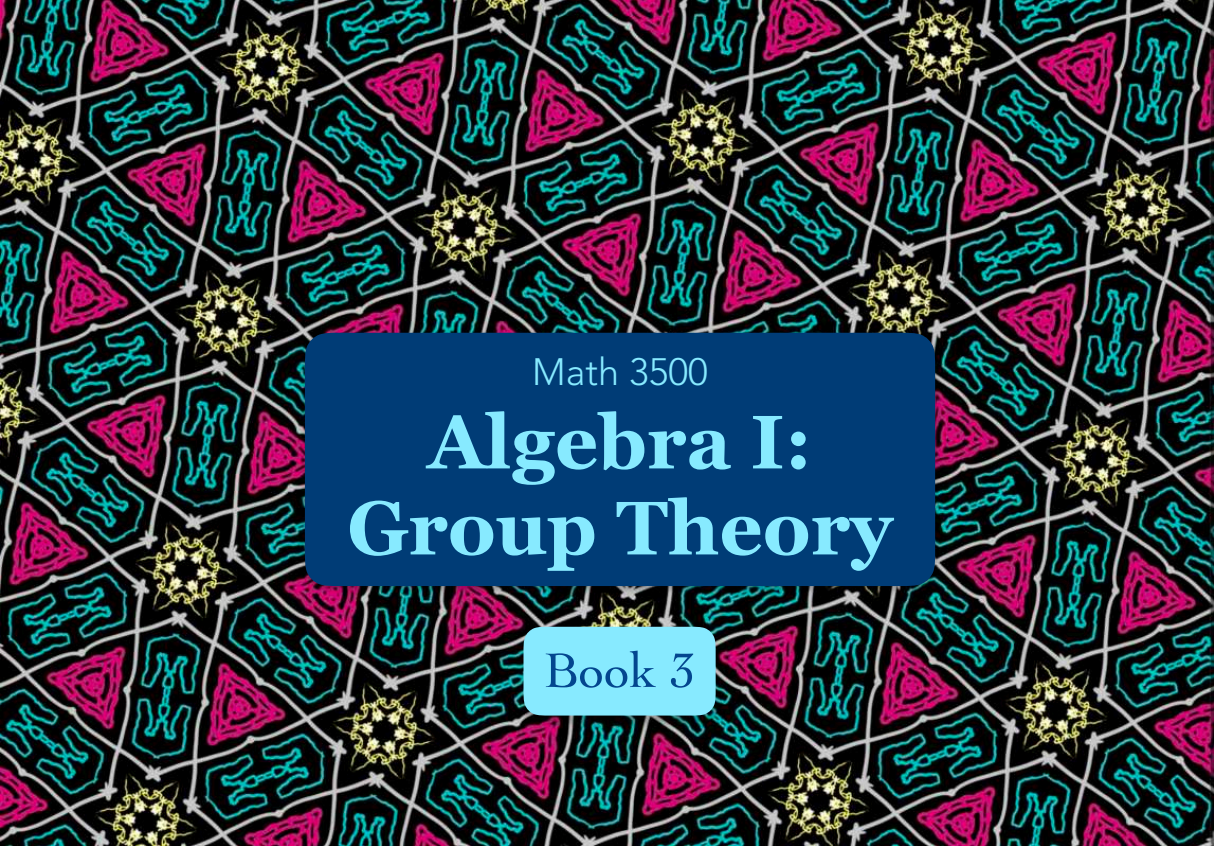

Math 3500
Algebra I:
Group Theory
Book 3

Eg. $F = \mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$ 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)

	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

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

	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 $T: G \to G$

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

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. $\phi = \phi_i$. □

---

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
$\phi_0(ab) = \phi_0(a)\phi_0(b)$
$1 \quad 1 \quad 1$

$\phi_1(g^i) = g^{1i} = g^i$ 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.

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

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

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 $\{1, g^5, g^{10}, g^{15}, g^{20}, g^{25}, g^{30}, g^{35}, g^{40}, g^{45}, g^{50}, g^{55}\}$

$\qquad\qquad = g^3 \qquad = g^8 \qquad = g \qquad = g^6 \qquad = g \qquad = g^4 \qquad = g^9$

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

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).

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

$369 = 2 \times 126 + 117$

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

$117 = 13 \times 9 + 0$

$369 \;\; 252 \;\; 117$

$9 = 126 - 117$

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

$= 3 \times 126 - 369$

$12 = 2 \times 5 + 2$

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

$2 = 2 \times 1 + 0$

$1 = 5 - 2 \times 2$

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

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

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

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

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

$(k \in \mathbb{Z})$ ($g^{12} = 1$)

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

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

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, $1 \le k \le n$, $\gcd(k,n) = 1$.

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

$T(0) = 0$

(left 0: zero vector)

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

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

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

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 $d \mid n$.

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. $d \mid n$. □

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 $w \neq 0$). Recall $T(0) = 0$.

If $f: C_{12} \to C_{12}$ is a homomorphism then we cannot have $f(g^3) = g^4$ since $|g^4| = 3$ does not divide $|g^3| = 4$. Every homomorphism $f: C_{12} \to C_{12}$ must take $f(g^4) \in \{1, g^4, g^8\}$. Use ϕ_0, ϕ_1, ϕ_2 to get these.

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

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

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

But what is an example of a homomorphism $f: S_5 \to S_5$ only.

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 $a^{-1}(axa^{-1})a = a^{-1}(ax'a^{-1})a$ so $x = x'$.

Why is it onto? For all $y \in G$, we must find $x \in G$ such that $\psi_a(x) = y$

$axa^{-1} = y$

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

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 $Z(G) = \{z \in G : z \text{ commutes with every element of } G\}$

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

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

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

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

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

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

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

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

We have a nontrivial automorphism of D_8

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

$\psi_R(I) = I$

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

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

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

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

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

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

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

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

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

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

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

Four automorphisms of D_8:

$\psi_I = \psi_{R^2}$ = 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 $x \longmapsto axa^{-1}$ 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 $a, x \in G$, $\psi_a(x) = axa^{-1}$ (the conjugate of x by a).

$\psi_a : G \to G$ which is conjugation by a.

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

Eg. Conjugation in S_n takes permutations to permutations of the same cycle structure (i.e. 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

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

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?

$\sigma = (13725)(48)$ $\quad \tau = (14)(2536)$

$\tau\sigma\tau^{-1} = (46753)(18) = (18)(34675)$

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

$(457)(1823)$ $\quad \tau = (142)(35786)$ works.

OR $\quad \tau(135)(2746)\tau^{-1} = (1823)(457)$

$(574)(2318)$ $\quad \tau = (154)(2)(37)(68) = (154)(37)(68)$

Given $g \in G$, the centralizer of g is $C_G(g) = \{$ all elements of G 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 $(1372 5)(4 8)$ to $(4675 3)(1 8)$? Same as: How many elements commute with $\sigma = (13725)(48)$. Answer: 10. in this case.

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

$\sigma = (\ldots, i, \sigma(i), \ldots)(\ldots)\cdots(\ldots)$

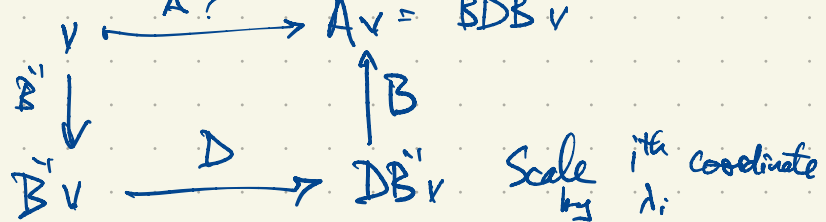
$(\tau\sigma\tau^{-1})(\tau(i)) = \tau\sigma\tau^{-1}\tau(i) = \tau(\sigma(i))$ i.e.

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

Similarly in $GL_n(F)$:

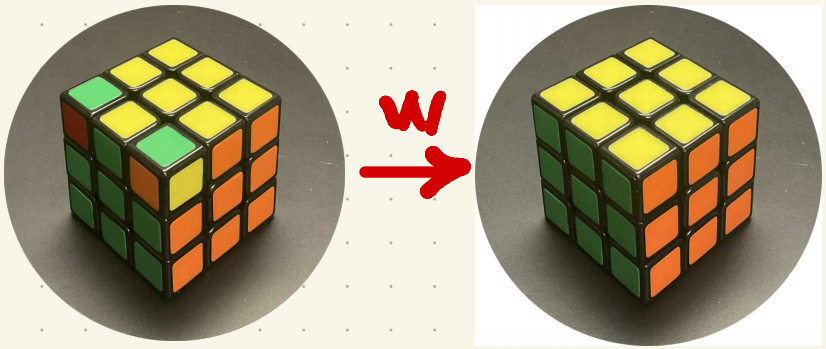
$D = \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & & \lambda_n \end{bmatrix}$ Scales $e_i \mapsto \lambda_i e_i$ where $e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ i^{th}

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 $B \in GL_n(F)$.



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).

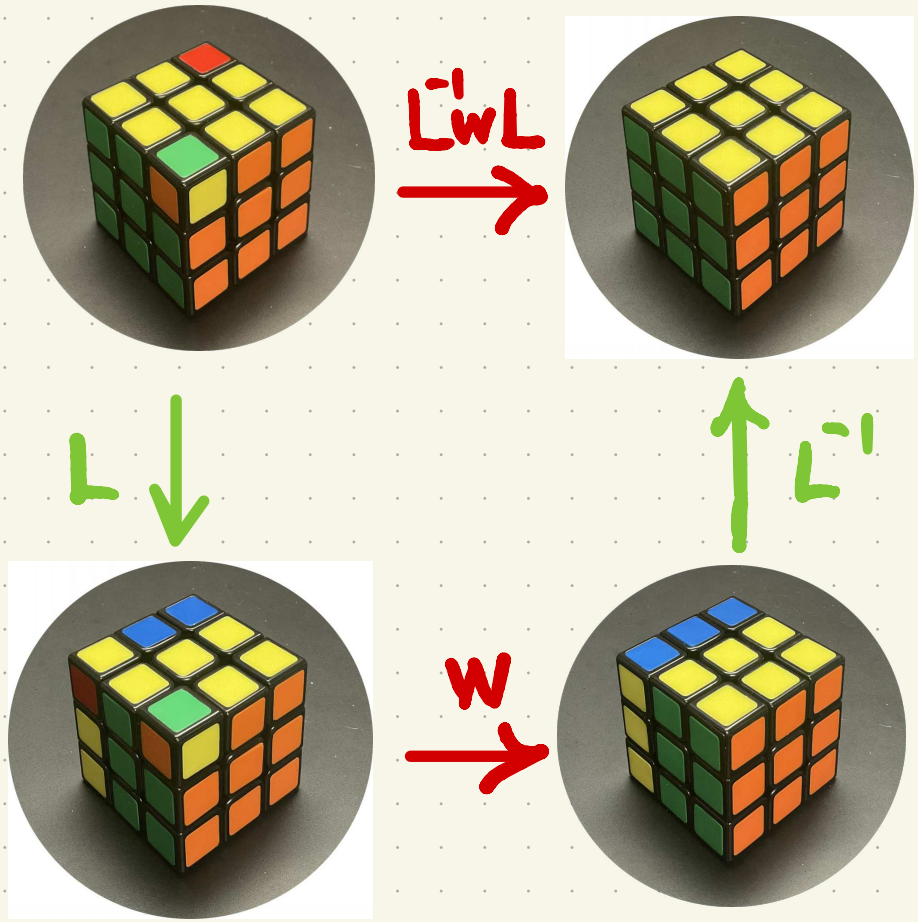
An example of conjugation in G:

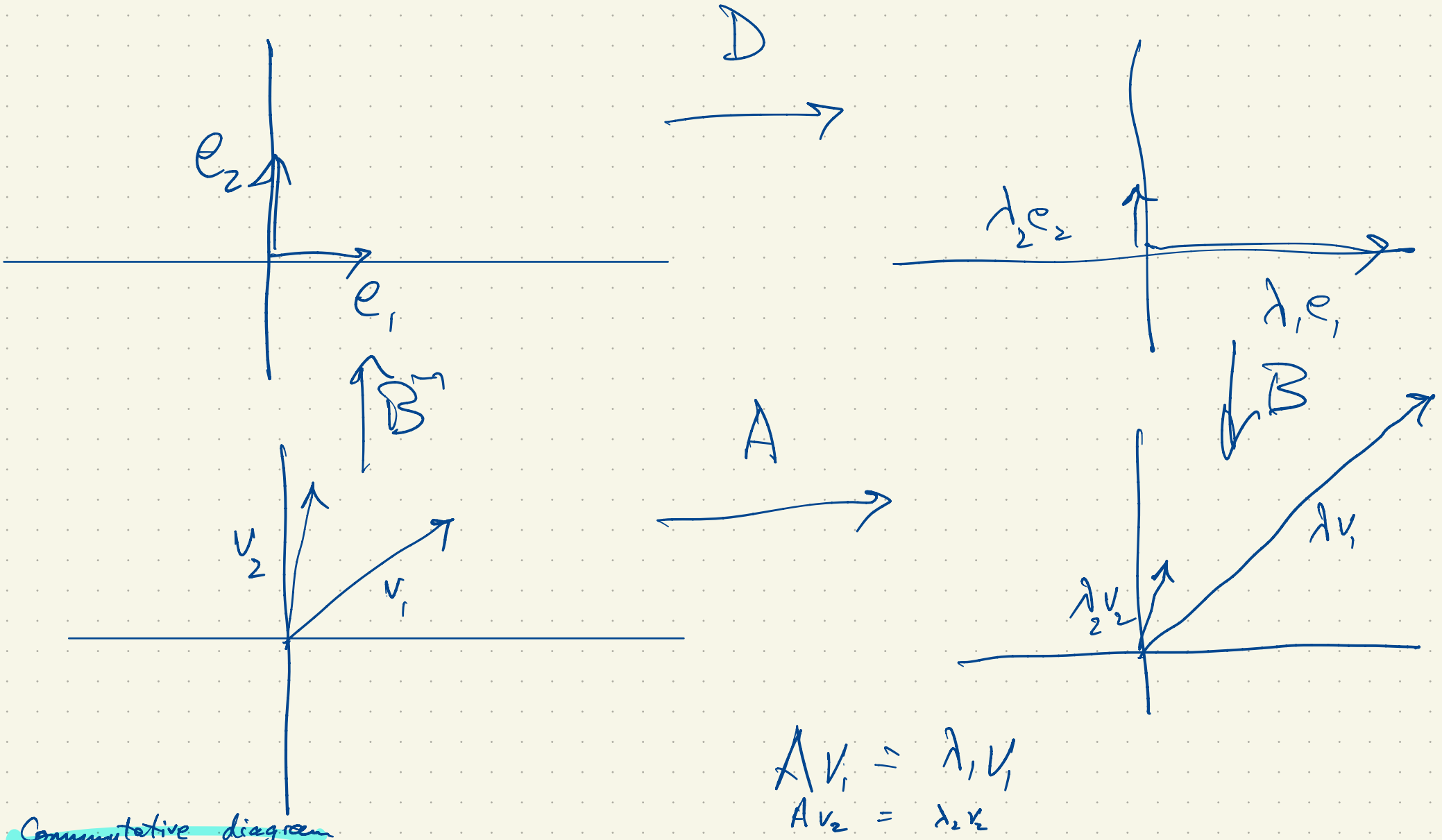


In our class, we might write

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

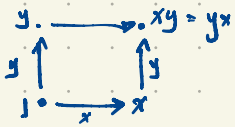
(right-to-left composition) but the standard guides for cubing would reverse this (using left-to-right composition as mathematicians prefer).





$$A v_1 = \lambda_1 v_1$$
$$A v_2 = \lambda_2 v_2$$

Commutative diagram



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

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

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

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

$\phi_1(x) = x$ 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. $\mathrm{Aut}(G) = \{\text{all automorphisms of } G\}$ is a group (not to be confused with G), the automorphism group of G.

$G = C_n$ $\quad \mathrm{Aut}(C_6) = \{\phi_1, \phi_5\} \cong C_2$ (ϕ_1: identity)

$\circ$	ϕ_1	ϕ_5
ϕ_1	ϕ_1	ϕ_5
ϕ_5	ϕ_5	ϕ_1

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

	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

this is not that! $G \ncong \mathrm{Aut}\, G$.

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)
$id: G \to G$, $id(g) = g$. $id(gh) = gh = id(g)\,id(h)$ $id \in \mathrm{Aut}\,G$ (not 1_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.

$\mathrm{Aut}(F^n) \geq GL_n(F)$
Each $A \in GL_n(F)$ gives an automorphism of F^n, $A: v \to Av$
This is a homomorphism $F^n \to F^n$ since $A(v+w) = Av + Aw$
Since A is invertible, $A: F^n \to F^n$ is bijective. The inverse of $A: v \to Av$ is
$A^{-1}: v \to A^{-1}v$.
Sometimes F^n has more automorphisms than these but often not.
An inner automorphism of F^n is a function of the form $\phi_a: v \to a + v + (-a) = v$. $a, v \in F^n$

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

Eg. $\mathrm{Aut}(S_n) \cong S_n$ if $n \neq 6$. S_6 has outer automorphisms (automorphisms that are not inner)
There is $f \in \mathrm{Aut}(S_6)$ such that $f((12)) = (12)(34)(56)$ and this cannot be an inner automorphism.

Theorem There is a homomorphism $G \to \mathrm{Aut}\,G$ defined by $a \mapsto \phi_a$. Shoe-Sock Theorem
Proof $\phi_{ab} = \phi_a \phi_b$ because $(\phi_a \circ \phi_b)(g) = \phi_a(\phi_b(g)) = a(bgb^{-1})a^{-1} = (ab)g(b^{-1}a^{-1}) = (ab)g(ab)^{-1} = \phi_{ab}(g)$
for all $a, b, g \in G$.

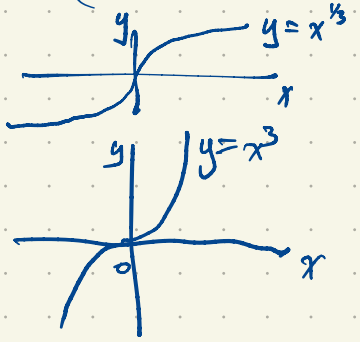
$GL_4(\mathbb{F}_2) \cong A_8$. of order 20160 $\mathrm{Aut}(GL_4(\mathbb{F}_2)) \cong S_8$. of order 40320.

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 $GL_n(\mathbb{R})$.
$\mathrm{Aut}\, GL_n(\mathbb{R})$ includes inner automorphisms. $\phi_B(A) = BAB^{-1}$
$GL_2(\mathbb{R})$ has an automorphism $\phi(A) = (\det A)A$.

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

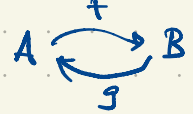
Why is $\phi : GL_2(\mathbb{R}) \to GL_2(\mathbb{R})$ bijective?
Suppose $\phi(A) = \phi(B)$ i.e. $(\det A)A = (\det B)B$.
$(\det A)^3 = (\det B)^3 \Rightarrow \det A = \det B \Rightarrow A = B$.



Why is ϕ onto?
Given $A \in GL_2(\mathbb{R})$, find $X \in GL_2(\mathbb{R})$ such that $\phi(X) = A$. Answer: $X = (\det A)^{-\frac{1}{3}} A$.
The inverse of $\phi : GL_2(\mathbb{R}) \to GL_2(\mathbb{R})$, $A \mapsto (\det A)A$
is $\phi^{-1}(A) = (\det A)^{-1/3} A$.
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 $f : A \to B$ from set A to set B is bijective iff it has a (well-defined) inverse $g : B \to A$. $g = f^{-1}$



ie. $f \circ g : B \to B$ is the identity on B
$b \mapsto b$ for all $b \in B$.
$g \circ f : A \to A$ is the identity $A \to A$ is $a \mapsto a$ for all $a \in A$.

All automorphisms of $SL_2(\mathbb{R})$ are inner: they have the form
$\phi : SL_2(\mathbb{R}) \to SL_2(\mathbb{R})$
$\phi(A) = BAB^{-1}$, $B \in SL_2(\mathbb{R})$

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 $n \geq 3$, $\phi : SL_n(\mathbb{R}) \to SL_n(\mathbb{R})$, $\phi(A) = A^T$ 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

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

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

The other five automorphisms of K are outer automorphisms.

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

$G \times H = \{(g, h) : g \in G, h \in H\}$ (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. $C_n = \{1, g, g^2, \ldots, g^{n-1}\}$ cyclic of order n

$C_m = \{1, h, h^2, \ldots, h^{m-1}\}$ " " " m

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

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

Powers of (g, h):

$(g,h)^0 = (1,1)$
$(g,h)^1 = (g,h)$
$(g,h)^2 = (g^2, h^2)$
$(g,h)^3 = (1, h^3)$
$(g,h)^4 = (g, h^4)$
$(g,h)^5 = (g^2, 1)$
$(g,h)^6 = (1, h)$
$(g,h)^7 = (g, h^2)$ ← (g^7, h^7)
$(g,h)^8 = (g^2, h^3)$
$(g,h)^9 = (1, h^4)$
$(g,h)^{10} = (g, 1)$
$(g,h)^{11} = (g^2, h)$
$(g,h)^{12} = (1, h^2)$
$(g,h)^{13} = (g, h^3)$
$(g,h)^{14} = (g^2, h^4)$
$(g,h)^{15} = (1,1)$ $\quad |(g,h)| = 15$

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

$C_2 \times C_2 \not\cong C_4$

$\{1, g\}$ $\quad$ $\{1, g\}$

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

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

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

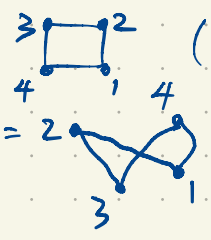
Groups of order 8: there are three abelian groups of order 8: C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$.

There are two nonabelian groups of order 8: dihedral, quaternion.

$C_2 \times C_2 \times C_2$: addition in F^3, $F = \{0,1\} = \mathbb{F}_2$.

Graphs (Math 3700: Combinatorics)

A (finite) graph (labelled) has vertices $1, 2, \cdots, n$. Every pair of vertices (plural of vertex) is either joined by an edge or not.

eg. $\Gamma =$ 

(a 4-cycle) has order 4 (the number of vertices) and 4 edges

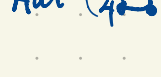
$\{1,2\}, \{2,3\}, \{3,4\}, \{1,4\}$

$= $

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

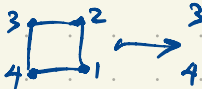
$1 \sim 2$, $1 \not\sim 3$.

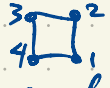
A graph of order n has $\binom{n}{2} = \frac{n(n-1)}{2}$ pairs of vertices. This is the maximum number of edges in a graph of order n.

$\mathrm{Aut}($ 

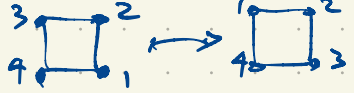
$) =$ automorphism group of this graph = the set of all permutations of the vertices which preserves the adjacency relation between vertices.

$= \langle (1234), (13) \rangle$

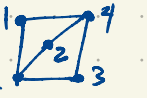
(12) is not an automorphism of this graph: it maps 

, a different graph isomorphic to 

but different.

(13) is an automorphism of the graph: it maps 

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

$\mathrm{Aut}($ 

$) \cong S_5 \cong \mathrm{Aut}($ 

$)$

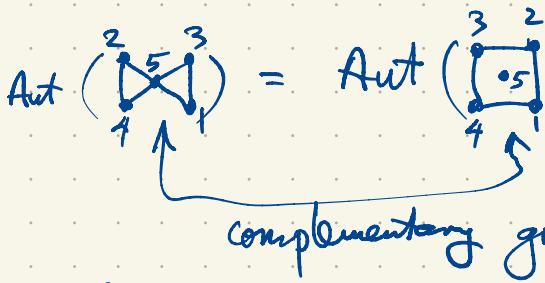
↑ Complete graph K_5 of order 5.

Given a graph Γ of order n, the complementary graph Γ' of order n has the complementary set of edges: for $i \neq j$ in $\{1,2,\dots,n\}$, i,j are adjacent in Γ' iff they're not adjacent in Γ.

$\mathrm{Aut}\,\Gamma' = \mathrm{Aut}\,\Gamma$.

$\mathrm{Aut}\left(\begin{smallmatrix}3&&2\\&4&\\&&1\end{smallmatrix}\right) = \mathrm{Aut}\left(\begin{smallmatrix}3&&2\\&4&\\&&1\end{smallmatrix}\right) = \mathrm{Aut}\left(\begin{smallmatrix}3&&4\\&&\\1&&2\end{smallmatrix}\right) = \langle (1234), (13) \rangle = \{ (1), (13), (24), (13)(24), (12)(34), (1234), (1432), (14)(23) \}$

$\mathrm{Aut}\left(\begin{smallmatrix}2&&3\\&5&\\4&&1\end{smallmatrix}\right) = \mathrm{Aut}\left(\begin{smallmatrix}3&&2\\&5&\\4&&1\end{smallmatrix}\right) = \langle (1234), (13) \rangle$ dihedral group of order 8



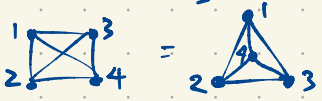
$\mathrm{Aut}\left(\begin{smallmatrix}1&2&3\\4&5&6\end{smallmatrix}\right) = \langle (12), (123), (45), (456), (14)(25)(36) \rangle = \langle (12), (123), (14)(25)(36) \rangle$

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)

$\mathrm{Aut}\left(\begin{smallmatrix}&1&\\2&&4\\&3&\end{smallmatrix}\right) = \mathrm{Aut}(K_4) \cong S_4$ of order 24.

complete graph on 4 vertices

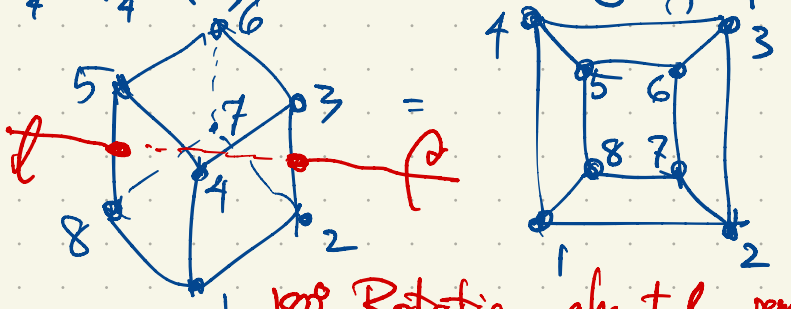


Half of these are rotational symmetries (direct isometries) forming a subgroup $\cong A_4$.

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) $\cong S_4 \times C_2$

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



This graph of order 8 has the same aut. gp. as the symmetry group of the cube. $G = \mathrm{Aut}$ (cube) (see HW4, Γ_3)

There are four diagonals joining each vertex with its opposite vertex $\{1,6\}$, $\{2,5\}$, $\{3,8\}$, $\{4,7\}$.
" a " b " c " d

Rotations of the cube give every permutation of the four diagonals exactly once. So the rotational symmetry group $\cong S_4$.

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

The inversion $-I = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$ is a symmetry of the cube permuting vertices as $(16)(25)(38)(47)$, commuting with all elements of G = symmetry group of cube $= \{\pm A : A \text{ rot. symmetry}\}$

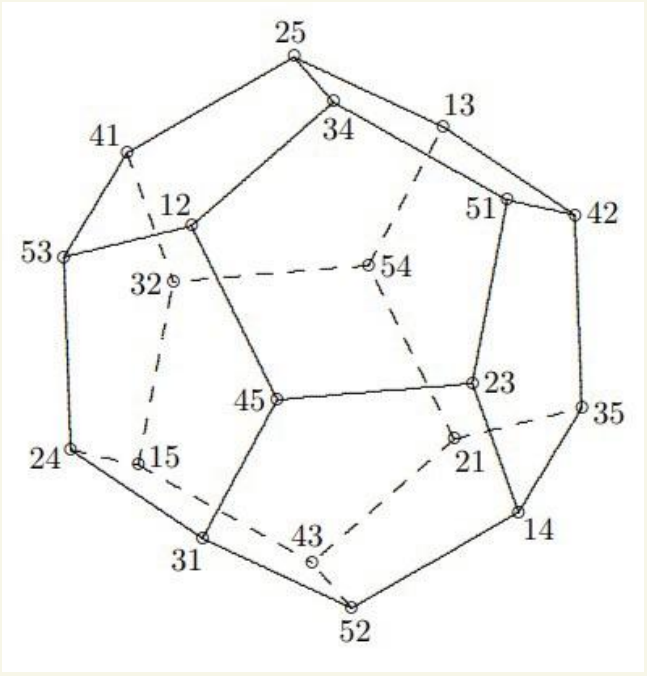
$$(\pm A)(\pm B) = \pm AB$$

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

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 sym. group is $\cong A_5 \times C_2$ ↪ $\{\pm I\}$ where $-I$ is inversion $v \mapsto -v$

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)

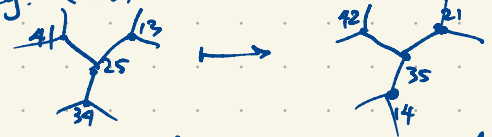
Why does a regular dodecahedron have rotational symmetry group $\cong A_5$?



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

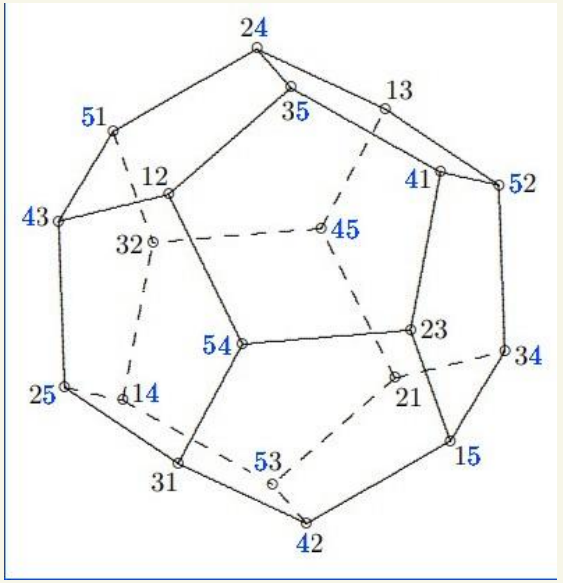
A_5 permuting 1,2,3,4,5

eg. (123): $25 \mapsto 35$

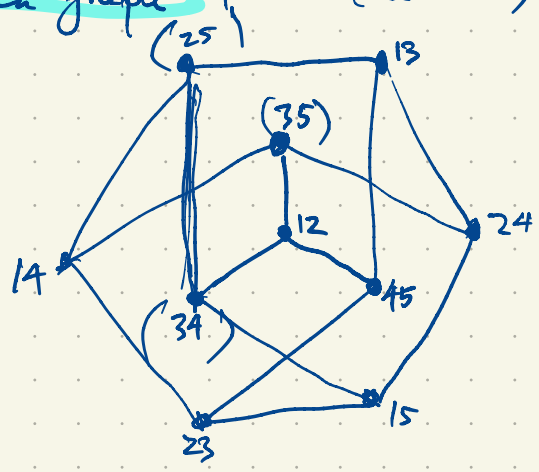


Odd permutations of 1,2,3,4,5 do not preserve the dodecahedron.

Odd permutations change this dodecahedron with another

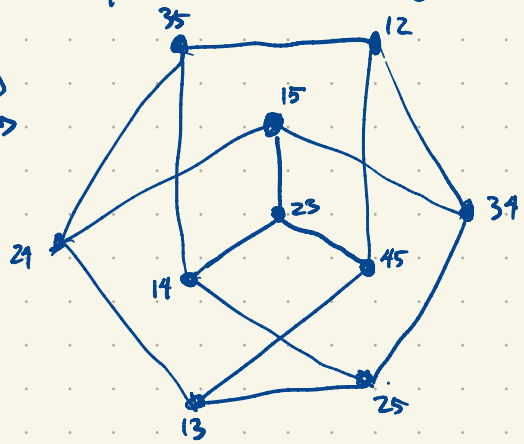


Petersen graph P (see HW4) has 120 automorphisms. $\mathrm{Aut}\, P \cong S_5$



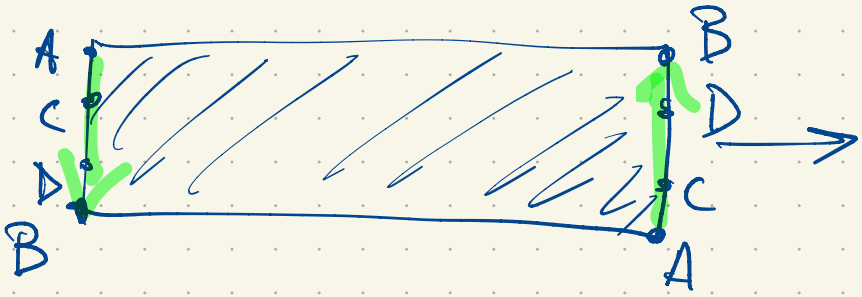
Join two pairs if they are disjoint.

(123) →



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

$\{i,j\} = \{j,i\} = ij$



$\mathbb{Z} \longrightarrow \mathbb{Z}/7\mathbb{Z}$

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) $\mathrm{Aut}\, P$. A little more explanation can be given to explanation to justify that S_5 is the full automorphism group of P. $\mathrm{Aut}\, P \cong S_5$.

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 $+, -, \times, \div, \sqrt{}$ (square roots, cube roots, etc.)
For $n=2,3,4$ such formulas are known.

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

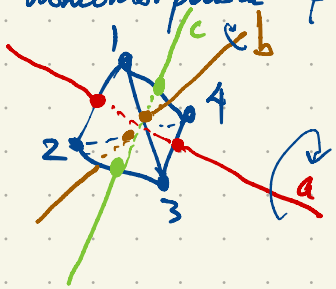
A homomorphism $\phi: S_3 \longrightarrow S_2$ which is onto:

$()\to()$, $(12)\to(12)$, $(13)\to(12)$, $(23)\to(12)$, $(123)\to()$, $(132)\to()$

$$\phi(\sigma) = \begin{cases} () & \text{if } \sigma \text{ is even;} \\ (12) & \text{" " " odd.} \end{cases}$$

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

A homomorphism $\phi: S_4 \longrightarrow S_3$ 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 $180°$ 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 $(a\,c\,b)$ ie. $a \mapsto c \mapsto b \mapsto a$.
(12) permutes $(b\,c)$ $a \mapsto a$, $b \mapsto c \mapsto b$.

It is (more or less) obvious that ϕ is a homomorphism. It's onto $\operatorname{Sym}\{a,b,c\} \cong S_3$ (all 6 permutations of a,b,c)

ϕ: (1), $(12)(34)$, $(13)(24)$, $(14)(23)$ $\longrightarrow ()$
(123), (134), (142), (243) $\longrightarrow (a\,c\,b)$
(132) (143), (124), (234) $\longrightarrow (a\,b\,c)$
(1324), (1423), (12), (34) $\longrightarrow (b\,c)$
(1243), (1342), (14), (23) $\longrightarrow (a\,b)$
(1234), (1432), (13), (24) $\longrightarrow (a\,c)$

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

Another explanation of the homomorphism $\phi: S_4 \to S_3$ (Conto!)

Start with the homomorphism $\phi: S_4 \to \mathrm{Aut}\, S_4$

$\tau \mapsto \phi_\tau$ where $\phi_\tau(\sigma) = \tau\sigma\tau^{-1}$ (ϕ_τ permutes all 24 elements of S_4).

One of the conjugacy classes in S_4 is the set of three double transpositions $\{(12)(34), (13)(24), (14)(23)\}$, where $a = (12)(34)$, $b = (13)(24)$, $c = (14)(23)$.

We need to prove Lagrange's Theorem: If $H \le G$ (H is a subgroup of G, finite groups only) then $|H| \mid |G|$.

In particular if $g \in G$ then $|g|$ divides $|G|$. (Recall: $|g| = |\langle g\rangle|$.)

We did prove Lagrange's Theorem in the very special case of cyclic groups.

Next let's consider an abelian group G of order n. We'll show that every $g \in G$ has order dividing n.

Consider the product of all the elements of G. If $G = \{g_1, g_2, \ldots, g_n\}$. Then $\pi = g_1 g_2 \cdots g_n \in G$ (possibly $=1$, possibly $\ne 1$) but because we're only considering G abelian, π is well-defined (i.e. it doesn't depend on the order in which I have listed the group elements). Then $G = \{gg_1, gg_2, gg_3, \ldots, gg_n\}$ so $\pi = (gg_1)(gg_2)(gg_3)\cdots(gg_n) = g^n \underbrace{(g_1 g_2 \cdots g_n)}_{\pi} = g^n \pi$.

Cayley Table

	g_1	g_2	$\cdots$	g_n
1	g_1	g_2	$\cdots$	g_n
$\vdots$				
g	gg_1	gg_2	$\cdots$	gg_n
$\vdots$				

Multiply both sides by $\pi^{-1} \in G$, to get $g^n = 1$.

Recall: this implies $|g| = d$ divides n.

$n = qd + r$, $0 \le r < d$.

$g^{qd+r} = 1$

$\underbrace{(g^d)^q}_{1} g^r = 1 \Rightarrow r = 0$

$g^r = 1$

$\Rightarrow r = 0$

$\Rightarrow n = qd$. $\square$

General case: G is a finite group of order n and H is a subgroup. We are no longer assuming G to be abelian. A <u>coset</u> of H in G is a subset of the form

$$gH = \{gh : h \in H\} \subseteq G,$$ where $g \in G$.

$\mathbb{R}^3$ has many subspaces of dimension 1, 2 (also dimension 0 or 3: $\{0\}$ and $\mathbb{R}^3$).

(dimension 1: lines through the origin; dimension 2: planes through the origin.)

The points, lines, planes in $\mathbb{R}^3$ are all cosets of the subspaces.

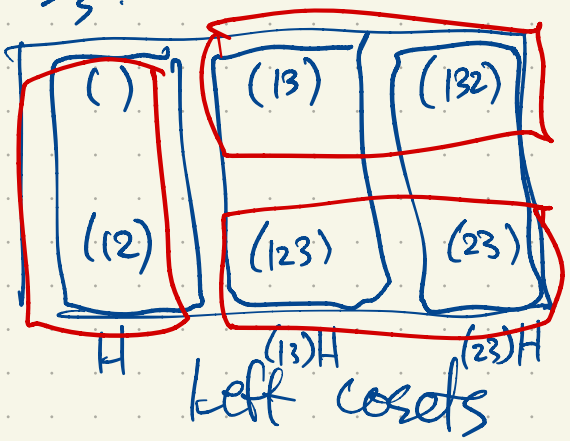
For $G = S_3$ and $H = \langle (12) \rangle$ we have three cosets

$()H = H = \{(), (12)\}$

$(13)H = (13)\{(), (12)\} = \{(13), (123)\} = (123)H$

$(23)H = (23)\{(), (12)\} = \{(23), (132)\}$

S_3:

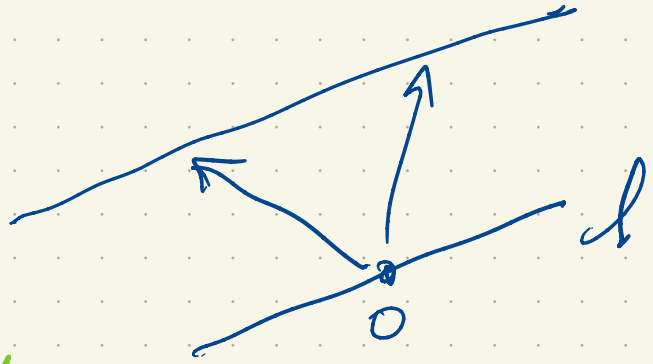


Left cosets

Right cosets

$|G| = 6 = 2 \times 3$

$|H|$ ↑ ↑ index of H = $[G:H]$ = number of (left) cosets



$gH = \{gh : h \in H\}$ is a left coset of H

$Hg = \{hg : h \in H\}$ " " right coset on H

Using (left) cosets $gH = \{gh : h \in H\}$, $g \in G$,

the cosets partition G and $|gH| = |H|$ for all $g \in H$ so

$|G| = |H| \times$ number of cosets. Proof: $H \to gH$, $h \mapsto gh$ is a bijection.

Every $g \in G$ lies in the left coset gH since $g = g1 \in gH$. If two left cosets overlap (i.e. non-disjoint) then they must be equal:

If $g \in xH \cap yH$ then $xH = yH = gH$, since $g = xh_1 = yh_2$ for some $h_1, h_2 \in H$

so $gh_1^{-1} = x$ and $xH = gh_1^{-1}H = gH$ and $yH = gh_2^{-1}H = gH$.

Since $|G| = |H| \times [G:H]$, $|H|$ divides $|G|$. (Lagrange's Theorem). Corollary Every element of G has order dividing $|G|$.

Corollary Every group of prime order is cyclic.

Proof Let G be a group of prime order $p \in \{2, 3, 5, 7, 11, 13, 17, \ldots\}$ and let $g \in G$ be a non-identity element. Then $|g| = |\langle g \rangle| \geq 2$ since $1, g \in \langle g \rangle$ are distinct. And $|g|$ divides p. So $|g| = |\langle g \rangle| = p$ so $\langle g \rangle = G$ i.e. G is cyclic.

Caution: If d divides $|G|$, must there be a subgroup of order d? No.
$|A_4| = 12$. A_4 has subgroups of order $1, 2, 3, 4$ only, not 6. $K = \langle (12)(34), (13)(24) \rangle$ has order 4.
A_4 has elements of order $1, 2, 3$ only. Not 4, 6.

The "converse" of Lagrange's Theorem.

Groups of order $2p$ are either Klein four-group (if $p=2$) or dihedral (if p is an odd prime). (proof omitted because of time) or cyclic.

The dihedral group of order $2n$ (denoted D_n or D_{2n}) is the symmetry group of a regular n-gon. It has a cyclic subgroup of order n and $D_n = \langle x, y : x^n = 1, y^2 = 1, yxy = x^{-1} \rangle$ (presentation for D_n).

Theorem If n is odd then every group of order $2n$ has a subgroup of order n.

This needs one more lemma:

Cauchy's Theorem If a prime p divides $|G|$, then G has an element of order p.

Proof: Suppose $|G| = 2n$ where n is odd. By Cauchy's Theorem, there exists $\tau \in G$ such that $|\tau| = 2$.

Cayley table:

	g_1	g_2	g_3	g_4	$\cdots$	g_{2n-1}	g_{2n}
1	g_1	g_2	g_3	g_4	$\cdots$	g_{2n-1}	g_{2n}
$\vdots$							
τ	g_2	g_1	g_4	g_3	$\cdots$	g_{2n}	g_{2n-1}
$\vdots$							

$\tau g_1 = g_2$
$\tau g_2 = g_1$
Left-mult. by τ in G is a product of n disjoint transpositions
So τ is an odd permutation.

The rows of Cayley Table express G as a permutation group of degree $2n$.
Half of these (the even permutations) give a subgroup of order n. □