Henry Adams
Colorado State University

Math 366: Introduction to Abstract Algebra

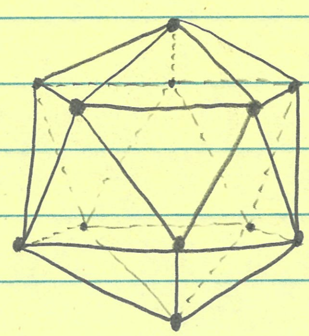
- Class syllabus and website.
- Come to class, read the book, and work with others.
- This is a <u>proof-based</u> class on difficult topic.
The beauty is only apparent after hard technical work.

<u>Course overview</u>

Weeks 1-10: Groups
(subgroups, cyclic groups, permutation groups, group homomorphisms, Lagrange's theorem, normal subgroups)
Groups are the language that mathematicians use to study symmetries.

Weeks 11-15: Rings, integral domains, and factorization (say of polynomials).
Fields and vector spaces.

Book: "Contemporary Abstract Algebra"
by Joseph Gallian



Chp 1 Introduction to Groups

Symmetries of a Square

R_0 = Rotation $0°$ (no change)

R_{90} = Rotation $90°$ (ccw)

R_{180} = Rotation $180°$

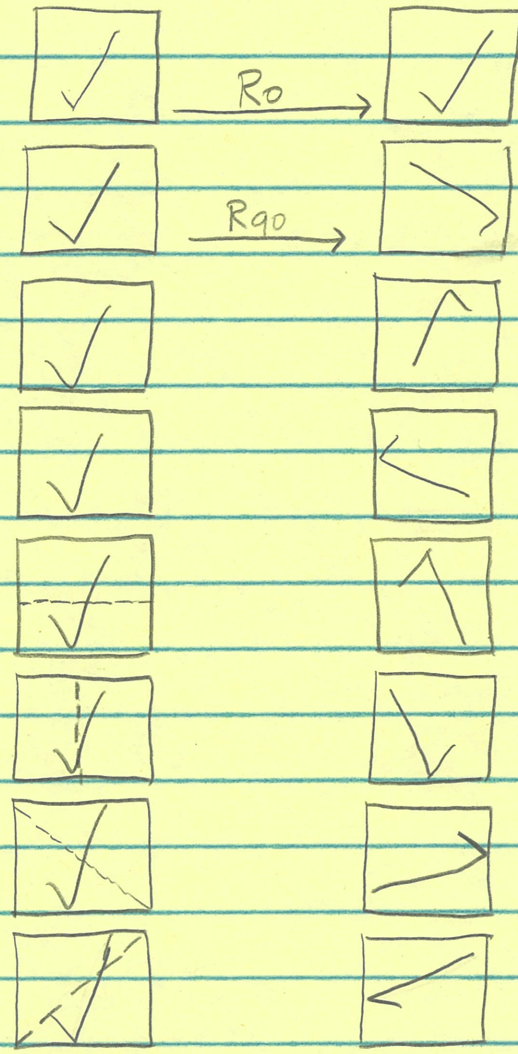
R_{270} = Rotation $270°$

H = Flip along horizontal

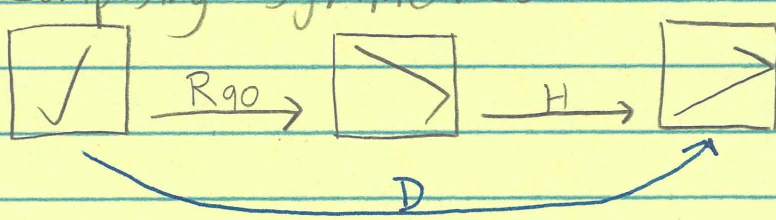
V = Flip along vertical

D = Flip along main diagonal

D' = Flip along other diagonal



Composing symmetries



We have verified the composition $\underbrace{H R_{90}}_{} = D$

(Ordering as in composition of functions)

Let $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ be the set of symmetries of the square (the 4-gon). When equipped with the <u>binary operation</u> (2 inputs, 1 output) given by composition, D_4 forms a group, called the <u>dihedral group of order 8</u>.

It's operation table / multiplication table / <u>Cayley table</u> is drawn below.

1^{st} operation

Do this column together

2nd operation

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	$\boxed{D}$	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

The boxed entry $\boxed{D}$ means $H R_{90} = D$

What patterns do you notice?

(Closure: each entry in the table is one of the 8 elements of our set D_4.)

- Identity: For all $A \in D_4$, note $R_0 A = A = A R_0$.
- Inverses: For all $A \in D_4$, there exists some $B \in D_4$ with $BA = R_0 = AB$.
- Associativity: For all $A, B, C \in D_4$, we have $C(BA) = (CB)A$

  Example $R_{90}(H R_{90}) = R_{90} D = H$ and $(R_{90} H) R_{90} = D' R_{90} = H$.

Associativity is too complicated to check by hand here, but it follows since symmetries of the square are functions and function composition is associative.

The above bullet points are the definition of a group!

Note it is not always true for $A, B \in D_4$ that $BA = BA$.

For example, $HD \neq DH$ since $HD = R_{90}$ but $DH = R_{270}$.

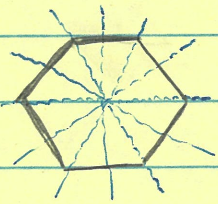
Hence we say that the group D_4 is not commutative or Abelian.

Note that each group element occurs exactly once in each row and column (like Sudoku)

Dihedral Groups

More generally, for $n \geq 3$, the symmetries of the regular n-gon form the dihedral group D_n of order $2n$.

Ex D_6



6 rotational symmetries
6 reflection symmetries

Chp 2 Groups

Definition and Examples of Groups

Def Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

Ex Let $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ be the set of integers. Then

$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $(a,b) \longmapsto a+b$,

$- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $(a,b) \longmapsto a-b$, and

$\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $(a,b) \longmapsto a \cdot b$

are binary operations.

Note $\div$ is not a binary operation on $\mathbb{Z}$, since ~~for~~ example $2 \div 5 \notin \mathbb{Z}$.

Ex For D_4 the set of symmetries of the square, we previously saw the composition binary operation $\circ : D_4 \times D_4 \rightarrow D_4$

Ex Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ be the set of integers modulo n.
(This is often instead denoted $\mathbb{Z}/n\mathbb{Z}$.)
Important binary operations include
$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $(a,b) \mapsto a+b \mod n$
$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $(a,b) \mapsto a \cdot b \mod n$.

Ex $10 + 6 \mod 12$ is 4.
$10 + 6 \mod 17$ is 16.
$7 \cdot 8 \mod 12$ is $56 \mod 12$,
which is 8 since $56 - 4(12) = 8$.

Definition (Group) Let G be a set together with a binary operation that assigns to each ordered pair (a,b) of elements of G an element of G denoted ab. closure

Then G is a <u>group</u> if
- (Identity) There is an element e in G (called the identity) such that $ae = ea = a$ for all a in G.
- (Inverses) For each element a in G, there is an element b in G (called the inverse of a) such that $ab = ba = e$.
- (Associativity) For all a, b, c in G, we have $c(ba) = (cb)a$.

Examples of Groups

Ex $(\mathbb{Z}, +)$ The integers with addition.
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

Ex $(\mathbb{Q}, +)$ The rationals with addition.
$\mathbb{Q}$: All fractions, i.e. all numbers of the form a/b for $a, b \in \mathbb{Z}$

Ex $(\mathbb{R}, +)$ The reals with addition.

In all three examples above, the identity is zero. Indeed, $a + 0 = 0 + a = a$.

In all three examples above, the inverse of an element a is $-a$, since
$a + (-a) = (-a) + a = 0$.

Non-Ex $(\mathbb{Z}, \cdot)$ The integers with multiplication do not form a group.

The identity would be 1 since $a1 = 1a = a$ for all $a \in \mathbb{Z}$.
But this is not a group since most elements don't have inverses!
For example, 3 has no inverse since there is no $b \in \mathbb{Z}$ with $3b = b3 = 1$.

Ex Let $\mathbb{Q}^*$ and $\mathbb{R}^*$ be the sets of rational and real numbers with 0 removed.

Then $(\mathbb{Q}^*, \cdot)$ and $(\mathbb{R}^*, \cdot)$ are groups.

Indeed, the identity is 1, since $a1 = 1a = a$.
The inverse of a is $1/a$, since $a(1/a) = (1/a)a = 1$.

You see why zero must be removed!

Non-Ex $\left(\underbrace{(\mathbb{R} \setminus \mathbb{Q})}\cup\{1\}, \ \cdot \right)$

The set of all irrational numbers with 1 added

This has an identity: 1.
It has inverses: the inverse of a is $1/a$.
It is also associative: $c(ba) = (cb)a$.
However it is not a group since $\cdot$ is not a binary relation on $\mathbb{R}\setminus\mathbb{Q}$, i.e., since it is not "closed".
Indeed, note $\sqrt{2} \in \mathbb{R}\setminus\mathbb{Q}$, but $\sqrt{2}\cdot\sqrt{2} = 2 \notin \mathbb{R}\setminus\mathbb{Q}$.

Ex $\left(\{1, -1, i, -i\}, \cdot\right)$ is a group

		First			
		1	-1	i	$-i$
Second	1	1	-1	i	$-i$
	-1	-1	1	$-i$	i
	i	i	$-i$	-1	1
	$-i$	$-i$	i	1	-1

The identity is 1. The inverse of -1 is -1.
The elements i and $-i$ are inverses.

Ex The set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a,b,c,d \in \mathbb{R}$ is a group under entry-wise addition:

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}.$$

The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

Ex The <u>determinant</u> of the 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the number $ad-bc$.

The set $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \begin{array}{l} a,b,c,d \in \mathbb{R} \\ ad-bc \neq 0 \end{array} \right\}$

is a (non-Abelian) group under matrix multiplication:

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix}$$

The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

why we need $ad-bc \neq 0$

Note this is a binary operation since if A and B are matrices with determinants $\det(A) \neq 0$ and $\det(B) \neq 0$, then AB is a matrix with determinant $\det(AB) = \det(A)\det(B) \neq 0$.

Rmk Since we may have $AB \neq BA$, this group is not "abelian" or "commutative"

Ex The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a group under the operation addition modulo n.

The identity is 0, and the inverse of $j \neq 0$ is $n-j$.

Ex Let $U(n)$ be the set of all positive integers less than n and relatively prime to n (no common divisors).

Then $U(n)$ is a group under multiplication modulo n.

For instance, $U(10) = \{1, 3, 7, 9\}$

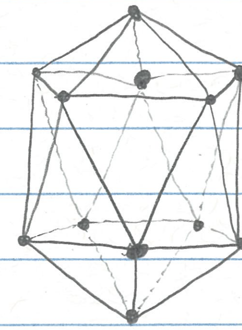
	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Non-Ex $(\mathbb{Z}, -)$ is not a group since subtraction is not associative:

$$c - (b - a) \neq (c - b) - a$$

since $c - b + a \neq c - b - a$ for $a \neq 0$.

Ex The set of symmetries of the icosahedron (or any Platonic solid, or really any object) form a group under composition.



Elementary Properties of Groups

Thm 2.1 In a group G, there is only one identity element

Pf Suppose both e and e' are identities in G. (So $ae = ea = a$ and $ae' = e'a = a$ for all a in G.) We will show $e = e'$, meaning there is only one identity

Indeed, note $e \underset{\substack{\uparrow \\ \text{since } e' \text{ is} \\ \text{an identity}}}{=} ee' \underset{\substack{\uparrow \\ \text{since } e \text{ is} \\ \text{an identity}}}{=} e'$. $\square$

Thm 2.2 (Cancellation) In a group G, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

Pf Suppose $ba = ca$. Let a^{-1} be an inverse of a.

So $(ba)a^{-1} = (ca)a^{-1}$ — multiply on right by a^{-1}

$\Longrightarrow b(aa^{-1}) = c(aa^{-1})$ — by associativity

$\Longrightarrow be = ce$ — by def$^{\underline{n}}$ of a^{-1}, where e is the identity

$\Longrightarrow b = c$ — by def$^{\underline{n}}$ of the identity.

A similar proof shows that $ab = ac$ implies $b = c$. $\square$

<u>Caution</u> It is <u>not</u> the case that $ab=ca$ implies $b=c$ (although this is true if the group is "Abelian", i.e., "commutative").

You can use the cancellation property to show that in the Cayley table / multiplication table for a group, each group element appears exactly once in each row and column (like Sudoku) (See Exercise 31).

<u>Thm 2.3</u> For each element a in a group G, there is a $\boxed{\text{unique}}$ element $b \in G$ such that $ab = ba = e$.

one and only one!

<u>Pf</u> Suppose b and c are both inverses of a.

So $ab \underset{\substack{\text{since } b \text{ is} \\ a\text{'s inverse}}}{=} e \underset{\substack{\text{since } c \text{ is} \\ a\text{'s inverse}}}{=} ac$.

By the cancellation property, we get $b=c$ as desired.

<u>Rmk</u> Since inverses are unique, instead of "an inverse of a", we can now say "the inverse of a", which we denote a^{-1}.

Now that we have some exposure, we give a more terse definition of a group (this is worth memorizing).

Don't omit!

Def A *group* is a set G $\boxed{\text{equipped with a binary operation}}$ such that

- (Identity) There is some $e \in G$ such that $ae = ea = a$ for all $a \in G$
- (Inverses) For each $a \in G$, there is some $a^{-1} \in G$ with $aa^{-1} = a^{-1}a = e$
- (Associativity) For all $a, b, c \in G$, we have $c(ba) = (cb)a$.

Rmk The two sentences

"There is some $e \in G$ such that $ae = ea = a$ for all $a \in G$"

and

"For all $a \in G$ there is some $e \in G$ such that $ae = ea = a$"

mean different things; do you see why?

Def A group is *commutative* or *Abelian* if $ab = ba$ for all $a, b \in G$.

Ex $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\{\pm 1, \pm i\}, \cdot)$, $(\mathbb{Z}_n, +)$, $(U(n), \cdot)$ are all commutative.

Non-Ex $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$, D_5, and $GL(2, \mathbb{R})$ are *not* commutative.

Multiplicative vs additive notation

	Multiplicative notation	Additive notation
The binary operation	$a \cdot b$ or ab	$a+b$
Identity	e or 1	0
Inverse of a	a^{-1}	$-a$
Combining a w/ itself n times	$\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}} = a^n$	$\underbrace{a + \ldots + a}_{n \text{ times}} = na$

We remark that a^n makes sense for any $n \in \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, since for example, $a^{-3} = (a^{-1})^3 = a^{-1}a^{-1}a^{-1}$.
However, $a^{1/2}$ or $a^{2.178}$ do not usually make sense!

Additive notation is really only used when the group is commutative.

Rmk For non-commutative groups, we typically have $(ab)^n = \underbrace{(ab)(ab) \cdot \ldots (ab)}_{n \text{ times}} \neq a^n b^n$.

Thm 2.4 (Socks-Shoes Property) In a group we have
$$(ab)^{-1} = b^{-1}a^{-1}.$$

Pf Note $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$
and $(b^{-1}a^{-1})(ab) = b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$

Hence by the definition of an inverse, we have $(ab)^{-1} = b^{-1}a^{-1}$. $\square$

Chp 3 Subgroups

Def The order of a group G, denoted $|G|$, is the number of elements in G.

Ex $|D_4| = 8$
$|D_5| = 10$
$|\{1, -1, i, -i\}| = 4$
$|\mathbb{Z}_n| = n$
$|\mathbb{Z}| = \infty$

Def For G a group, the order of an element $g \in G$, denoted $|g|$, is the smallest $n \geq 1$ with $g^n = e$.

Ex In D_4, $|R_{90}| = 4$ and $|R_{180}| = 2 = |H|$.
In $\mathbb{Z}_{10}$, $|4| = 5$ since $4+4+4+4+4 = 20 \equiv 0 \mod 10$
In $\{1, -1, i, -i\}$, we have
$|1| = 1$, $|-1| = 2$, $|-i| = 4$ and $|i| = 4$.
In $\mathbb{Z}$, we have $|3| = \infty$ since there is no such n. More generally, in $\mathbb{Z}$, $|m| = \infty$ for all $m \neq 0$.

Preview We will later learn that in a finite group G, we have that $|g|$ divides $|G|$ for all $g \in G$.
(This will be Corollary 2 of Lagrange's Theorem (Thm 7.1))

<u>Def</u> If a subset H of a group G is itself a group under the binary operation of G, then we say that H is a <u>subgroup</u> of G, and we write $H \leq G$.

<u>Ex</u> $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ and $\mathbb{Z} \leq \mathbb{R}$

(The binary operation in all groups above is $+$).

$(\{R_0, R_{90}, R_{180}, R_{270}\}, \circ) \leq D_4$

$(\{R_0, H\}, \circ) \leq D_4$

$(\{R_0, R_{180}, H, V\}, \circ) \leq D_4$

	R_0	H
R_0	R_0	H
H	H	R_0

<u>Non-Ex</u> $(\{H, V, D, D'\}, \circ) \not\leq D_4$ since it is not a group — there is no identity element.

$(\{R_0, H, V, D, D'\}, \circ) \not\leq D_4$ since it is not equipped with a (closed) binary operation: we have $H \circ V = R_{180} \notin \{R_0, H, V, D, D'\}$.

$\mathbb{Z}_{10} \not\leq \mathbb{Z}$, even though $\mathbb{Z}_{10} \subseteq \mathbb{Z}$, since the binary operation on $\mathbb{Z}_{10}$ is <u>not</u> the same as that on $\mathbb{Z}$.

Indeed, in $\mathbb{Z}$ we have $9+9=18$, whereas in $\mathbb{Z}_{10}$ we have $9+9=18 \equiv 8 \mod 10$.

Ex Let G be any group. We always have the <u>trivial subgroup</u> $\{e\} \leq G$.

	e
e	e

Subgroup Tests

Thm 3.2 (Two-Step Subgroup Test)
Let G be a group and let H be a nonempty subset of G. If
- $ab \in H$ whenever $a, b \in H$, and
- $a^{-1} \in H$ whenever $a \in H$,

then H is a subgroup of G.

Pf Omitted — but really just H nonempty $\Rightarrow \exists\, a \in H \Rightarrow a^{-1} \in H \Rightarrow e = aa^{-1} \in H$.

Ex One can use this test to show $(\{R_0, R_{90}, R_{180}, R_{270}\}, \circ) \leq D_4$.

Def Given G a group and $a \in G$, let $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ be the <u>cyclic group generated by a</u>.

Ex In D_4, $\langle R_{90} \rangle = \{R_0, R_{90}, R_{180}, R_{70}\}$.

In D_4, $\langle H \rangle = \{R_0, H\}$.

In $\mathbb{R}$, $\langle 1 \rangle = \mathbb{Z} \leq \mathbb{R}$.

In $\{1, -1, i, -i\}$, $\langle -1 \rangle = \{1, -1\}$ and $\langle i \rangle = \{1, -1, i, -i\}$.

Ex In $U(10)$,

$\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$ since
$3^1 = 3$
$3^2 = 3 \cdot 3 = 9$
$3^3 = 3 \cdot 9 = 27 \equiv 7 \mod 10$
$3^4 = 3 \cdot 7 = 21 \equiv 1 \mod 10$

$\langle 7 \rangle = \{7, 9, 3, 1\} = U(10)$ since
$7^1 = 7$
$7^2 = 49 \equiv 9 \mod 10$
$7^3 = 7 \cdot 9 = 63 \equiv 3 \mod 10$
$7^4 = 7 \cdot 3 = 21 \equiv 1 \mod 10$

$\langle 9 \rangle = \{9, 1\}$ since
$9^1 = 9$
$9^2 = 81 \equiv 1 \mod 10$

$\langle 1 \rangle = \{1\}$ is the trivial group since
$1^2 = 1$.

Thm 3.4 If G is a group and $a \in G$, then $\langle a \rangle$ is a subgroup of G.

Pf Let's use the Two-Step Subgroup Test.
Since $a \in \langle a \rangle$, we know $\langle a \rangle$ is nonempty.

- Given arbitrary elements $a^n, a^m \in \langle a \rangle$, we have $a^n a^m = a^{n+m} \in \langle a \rangle$, as required.
- Given $a^n \in \langle a \rangle$, note $(a^n)^{-1} = a^{-n} \in \langle a \rangle$, as required.

Hence $\langle a \rangle$ is a subgroup of G by the Two-Step Subgroup Test.

Thm 3.1 (One-Step Subgroup Test)
Let G be a group and H a nonempty subset of G. If

- $ab^{-1} \in H$ whenever $a, b \in H$,

then H is a subgroup of G

Pf Sketch Identity: H nonempty $\Rightarrow$ there exists some $x \in H$
$\Rightarrow e = xx^{-1} \in H$ (taking $a=x$, $b=x$).

Inverses: For any $x \in H$, we have
$$x^{-1} = ex^{-1} \in H \quad (\text{taking } a=e,\ b=x).$$

Associativity: Follows since G associative

Binary operation on H (closure):
Given $x, y \in H$, we already know $y^{-1} \in H$, giving
$$xy = x(y^{-1})^{-1} \in H \quad (\text{taking } a=x,\ b=y^{-1}). \qquad \square$$

Ex Use the One-Step Subgroup Test to show if G is a group and $a \in G$, then $\langle a \rangle$ is a subgroup of G.

<u>Def</u> The <u>center</u> $Z(G)$ of a group G is the subset of elements that commute with all elements of G.

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}.$$

<u>Ex</u> The center of $GL(2,\mathbb{R})$, the set of all 2×2 matrices with nonzero determinant, is

$$Z(GL(2,\mathbb{R})) = \left\{ \begin{bmatrix} t & 0 \\ 0 & t \end{bmatrix} \;\middle|\; t \neq 0 \right\},$$

the set of (nonzero) diagonal matrices.

For example, $\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 2 & 5 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 6 & 15 \\ 3 & -3 \end{bmatrix} = \begin{bmatrix} 2 & 5 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$.

<u>Thm 3.5</u> The center $Z(G)$ of a group G is a subgroup of G.

<u>Pf</u> We use the One-Step Subgroup Test.
Note $Z(G)$ is nonempty since $e \in Z(G)$.
Given $a, b \in Z(G)$, note $ab^{-1} \in Z(G)$ since for any $x \in G$, we have

$ax = xa$ since $a \in Z(G)$

$\Longrightarrow axb = bxa$ since $b \in Z(G)$

$\Longrightarrow ax = bxab^{-1}$ multiply on right by b^{-1}

$\Longrightarrow b^{-1}ax = xab^{-1}$ multiply on left by b^{-1}

$\Longrightarrow (ab^{-1})x = x(ab^{-1})$ since $a \in Z(G)$. $\square$

Chp 4 Cyclic Groups

Recall from Chp 3 that ...

Def A group G is cyclic if there is an element $a \in G$ such that
$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Ex $U(10) = \{1, 3, 7, 9\}$ is cyclic since $U(10) = \langle 3 \rangle$, or since $U(10) = \langle 7 \rangle$.
Note $U(10) \neq \langle 1 \rangle$ and $U(10) \neq \langle 9 \rangle$.

Question to answer later How do we identify all the generators of a cyclic group, i.e., those elements $a \in G$ such that $G = \langle a \rangle$?

Important fact There are really only "two types" of cyclic groups:

- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \langle 1 \rangle$ under addition. This is the infinite cyclic group.
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \langle 1 \rangle$ under addition modulo n. This is the finite cyclic group of order n.

Ex We'll see that $U(10)$ is "isomorphic" to $\mathbb{Z}_4$:

$\mathbb{Z}_4$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$U(10)$

	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

Rmk We'll see later (Corollary 4 on page 80) that $k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(k,n) = 1$. (greatest common divisor)

Ex $\mathbb{Z}_4 = \langle 1 \rangle$ and $\mathbb{Z}_4 = \langle 3 \rangle$ but
$\mathbb{Z}_4 \neq \langle 0 \rangle$ and $\mathbb{Z}_4 \neq \langle 2 \rangle$.

Ex In $\mathbb{Z}_{14}$, where $14 = 2 \cdot 7$,

$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \mathbb{Z}_{14}$

$\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 12 \rangle = \{0,2,4,6,8,10,12\}$

$\langle 7 \rangle = \{0,7\}$

$\langle 0 \rangle = \{0\}$.

Greatest Common Divisor

Def For a, b positive integers, their greatest common divisor, denoted $\gcd(a,b)$, is the largest positive integer dividing both a and b.

Ex $\gcd(60,18) = \gcd(2^2 \cdot 3 \cdot 5,\ 2 \cdot 3^2) = 2 \cdot 3 = 6$

$\gcd(15,94) = \gcd(3 \cdot 5,\ 2 \cdot 47) = 1$

Def We say a and b are relatively prime when $\gcd(a,b) = 1$.

The Euclidean Algorithm is a way to compute $\gcd(a,b)$ without computing prime factorizations (which are hard).

(See the YouTube videos linked in homework; one mistakenly says "greatest common denominator" instead of "greatest common divisor".)

Euclidean Algorithm for $\gcd(60,18)$

$60 = 18(3) + \overset{\gcd(60,18)}{\boxed{6}}$

$18 = 6(3) + 0$

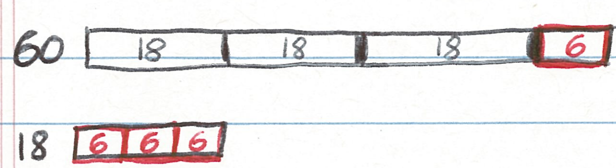
Rewrite

$60 - 18(3) = 6$

Find solution to $60s + 18t = \gcd(60,18)$

$60 - 18(3) = 6 = \gcd(60,18)$

Note $s = 1,\ t = -3$ solves $60s + 18t = \gcd(60,18)$.



Euclidean Algorithm for gcd(15, 94)

$$94 = 15(6) + 4$$
$$15 = 4(3) + 3$$
$$4 = 3(1) + \boxed{1} \leftarrow \gcd(15,94)$$
$$3 = 1(3) + 0$$

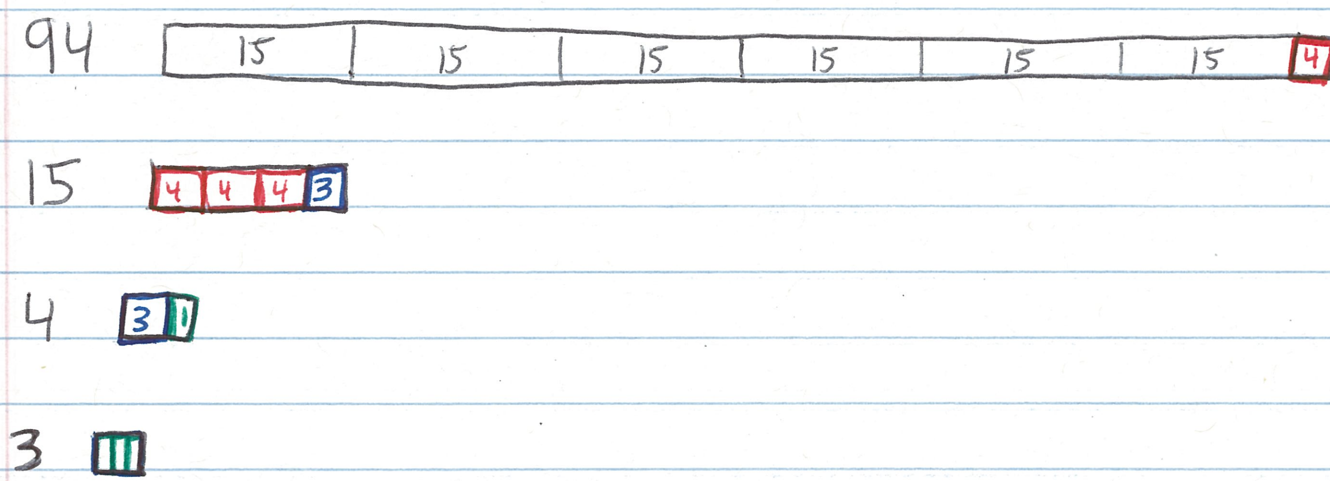
Rewrite

$$94 - 15(6) = 4$$
$$15 - 4(3) = 3$$
$$4 - 3(1) = 1$$

Find solution to $15s + 94t = \gcd(15, 94)$

$$4 - 3(1) = 1$$
$$4 - (15 - 4(3)) = 1$$
$$4(4) - 15 = 1$$
$$(94 - 15(6))(4) - 15 = 1$$
$$94(4) - 15(25) = 1$$

Note $s = -25$ and $t = 4$ solves $15s + 94t = \gcd(15, 94)$.



Bezout's Theorem (Thm 0.2 in our book) says there exist integers $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$.

Corollary 4 on page 80 (Generators of $\mathbb{Z}_n$)
Element $k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(k, n) = 1$.

IE, n and k are relatively prime

Ex $n = 14$, $k = 3$
$\gcd(3, 14) = 1$ should imply

$$\mathbb{Z}_{14} = \langle 3 \rangle = \{3, 6, 9, 12, 1, 4, 7, 10, 13, 2, 5, 8, 11, 0\}.$$

$2 \cdot 3$, $3 \cdot 3$, $4 \cdot 3$, $5 \cdot 3$, $6 \cdot 3$, $7 \cdot 3$, $8 \cdot 3$, $9 \cdot 3$, $10 \cdot 3$, $11 \cdot 3$, $12 \cdot 3$, $13 \cdot 3$, $14 \cdot 3$

Indeed, $\gcd(3, 14) = 1$ implies, by Bezout's Theorem, that there exist $s, t \in \mathbb{Z}$ with $3s + 14t = \gcd(3, 14) = 1$.
(Here $s = 5$ and $t = -1$.)

Reducing modulo 14 gives $3s \equiv 1 \mod 14$
(Here $s = 5$)

So $1 = 3s \in \langle 3 \rangle = \{3m \mid m \in \mathbb{Z}\}$

Additive, not multiplicative notation

Once $1 \in \langle 3 \rangle$, this will imply every element of $\mathbb{Z}_{14}$ is in $\langle 3 \rangle$.
Indeed, $1 = 3s \in \langle 3 \rangle$
implies: $2 = 3(2s) \in \langle 3 \rangle$
$3 = 3(3s) \in \langle 3 \rangle$ $\quad 3s = 15 \equiv 1 \mod 14$
$4 = 3(4s) \in \langle 3 \rangle$ $\quad 4s = 20 \equiv 6 \mod 14$
$5 = 3(5s) \in \langle 3 \rangle$
$\vdots$
$13 = 3(13s) \in \langle 3 \rangle$
$0 = 3(14s) \in \langle 3 \rangle$

So we've argued why $\langle 3 \rangle = \mathbb{Z}_{14}$.

More generally, let's show that $\gcd(k,n)=1$ implies that k generates $\mathbb{Z}_n$.

Pf If $\gcd(k,n)=1$, then there exist $s,t\in\mathbb{Z}$ with $ks+nt=1$

$\Longrightarrow$ $ks \equiv 1 \mod n$

$\Longrightarrow$ $1 \in \langle k \rangle := \{ km \mid m \in \mathbb{Z} \}$

This implies $\mathbb{Z}_n = \langle k \rangle$

(Indeed, to see $a \in \langle k \rangle$ for any $a \in \mathbb{Z}_n$, multiply both sides of $ks \equiv 1 \mod n$ by a to get $k(sa) \equiv a \mod n$.)

<u>Corollary 4 on page 80</u> An integer k is a generator of $\mathbb{Z}_n$ if and only if $\gcd(k,n)=1$.

Last time, we saw the proof of $(\Longleftarrow)$
Maybe we'll do the proof of $(\Longrightarrow)$ as homework?

More generally,
<u>Corollary 3 on page 80</u> Let G be a group and $a \in G$ with $|a| = n$.
Then $\langle a \rangle = \langle a^k \rangle$ if and only if $\gcd(k,n)=1$.

Note Corollary 4 is the special case where $G = \mathbb{Z}_n = \langle 1 \rangle$, where $a=1$ with $|a|=n$, and so $\mathbb{Z}_n = \langle 1 \rangle = \langle k \rangle$ if and only if $\gcd(k,n)=1$.

<u>Ex</u> Use Corollary 3 on page 80 and the knowledge that 2 generates $U(9)$ to find all generators of $U(9)$.

<u>Ans</u> $U(9) = \{1,2,4,5,7,8\}$ $\qquad |U(9)| = 6$
$\langle 2 \rangle = \{2,4,8,7,5,1\} = U(9)$ $\qquad |2| = 6$

So $U(9) = \langle 2 \rangle \stackrel{?}{=} \langle 2^k \rangle$ if and only if $\gcd(k,6)=1$.

So the complete list of generators for $U(9)$ is $2^1 = 2$, $2^5 = 5$.

Ex Use Corollary 3 on page 80 and the knowledge that 3 generates $U(50)$ to find all generators of $U(50)$.

Ans $U(50)=\{1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39,41,43,47,49\}$ $|U(50)|=2$

$\langle 3\rangle=\{3,9,27,31,43,29,37,11,33,49,47,\ldots\}=U(50)$ $|3|=20$

So $U(50)=\langle 3\rangle \stackrel{?}{=} \langle 3^k\rangle$ if and only if $\gcd(k,20)=1$.

So the complete list of generators for $U(50)$ is

$3^1 \bmod 50 = 3$

$3^3 \bmod 50 = 27$

$3^7 \bmod 50 = 37$

$3^9 \bmod 50 = 33$

$3^{11} \bmod 50 = 47$

$3^{13} \bmod 50 = 23$

$3^{17} \bmod 50 = 13$

$3^{19} \bmod 50 = 17$

Ex The subgroup of D_6  of all rotations is $\{R_0, R_{60}, R_{120}, R_{180}, R_{240}, R_{300}\}$.
Clearly R_{60} generates this subgroup.
Since $|R_{60}|=6$, Corollary 3 on page 80 says the only other generator of this subgroup is $(R_{60})^5=R_{300}$ (since $\gcd(5,6)=1$).

Corollary 1 on page 77

For G a group and $a \in G$, we have $|a| = |\langle a \rangle|$.

(Recall for G a group, the order $|G|$ was defined as the # of elements in G, and for $a \in G$, the order $|a|$ was defined as the smallest $n \geq 1$ with $a^n = e$.)

Hence "order" is a reasonable name for $|a|$!

Ex In $\mathbb{Z}_{14}$, $|7| = 2$ since $7 = 7$ and $7 + 7 = 14 \equiv 0 \mod 14$.
Also $|\langle 7 \rangle| = |\{7, 0\}| = 2$.

In $\mathbb{Z}_{14}$, $|4| = 7$ since
$4 = 4$
$2 \cdot 4 = 8$
$3 \cdot 4 = 12$
$4 \cdot 4 = 16 \equiv 2 \mod 14$
$5 \cdot 4 \equiv 6 \mod 14$
$6 \cdot 4 \equiv 10 \mod 14$
$7 \cdot 4 \equiv 0 \mod 14$
Also $|\langle 4 \rangle| = |\{4, 8, 12, 2, 6, 10, 0\}| = 7$.

Corollary (Subgroups of $\mathbb{Z}_n$) on page 82

The subgroups of $\mathbb{Z}_n$ are the (cyclic) subgroups $\langle n/k \rangle$, of order k, where k varies over all positive divisors of n.

Ex The subgroups of $\mathbb{Z}_{14}$ are

$k=1$: $\langle 14/1 \rangle = \langle 14 \rangle = \langle 0 \rangle = \{0\}$ order 1

$k=2$: $\langle 14/2 \rangle = \langle 7 \rangle = \{7, 0\}$ order 2

$k=7$: $\langle 14/7 \rangle = \langle 2 \rangle = \{2,4,6,8,10,12,0\}$ order 7

$k=14$: $\langle 14/14 \rangle = \langle 1 \rangle = \{1,2,3,\ldots,12,13,0\}$ order 14

Ex The subgroups of $\mathbb{Z}_{30}$ are

$k=1$: $\langle 30/1 \rangle = \langle 30 \rangle = \langle 0 \rangle = \{0\}$ order 1

$k=2$: $\langle 30/2 \rangle = \langle 15 \rangle = \{15, 0\}$ order 2

$k=3$: $\langle 30/3 \rangle = \langle 10 \rangle = \{10, 20, 0\}$ order 3

$k=5$: $\langle 30/5 \rangle = \langle 6 \rangle = \{6,12,18,24,0\}$ order 5

$k=6$: $\langle 30/6 \rangle = \langle 5 \rangle = \{5,10,15,20,25,0\}$ order 6

$k=10$: $\langle 30/10 \rangle = \langle 3 \rangle = \{3,6,9,\ldots,27,0\}$ order 10

$k=15$: $\langle 30/15 \rangle = \langle 2 \rangle = \{2,4,6,\ldots,28,0\}$ order 15

$k=30$: $\langle 30/30 \rangle = \langle 1 \rangle = \{1,2,3,\ldots,29,0\}$ order 30

Ex How many subgroups does $\mathbb{Z}_{18}$ have?

Ans $\langle 18 \rangle = \langle 0 \rangle$, $\langle 9 \rangle$, $\langle 6 \rangle$, $\langle 3 \rangle$, $\langle 2 \rangle$, $\langle 1 \rangle$, so 6 in total.

Ex How many subgroups of order 6 does $\mathbb{Z}_{18}$ have?

Ans One, the subgroup $\langle 18/6 \rangle = \langle 3 \rangle = \{3,6,9,12,15,0\}$.

More generally,

<u>Thm 4.3</u> (Fundamental Theorem of Cyclic Groups)
If $|\langle a\rangle| = n$, then the subgroups of $\langle a\rangle$ are the (cyclic) subgroups $\langle a^{n/k}\rangle$, of order k, where k varies over all positive divisors of n.

<u>Ex</u> Suppose $G = \langle a\rangle$ with $|G| = 30$.
Then the subgroups of G are $\langle a^{30/k}\rangle$, of order k, for $k = 1, 2, 3, 5, 6, 10, 15, 30$.

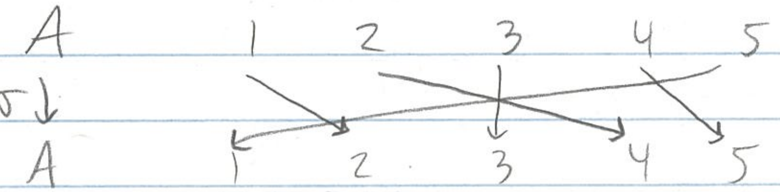
Chapter 5 Permutation Groups

Def A *permutation* of a set A is a function $f: A \to A$ that is both 1-to-1 and onto
injective surjective

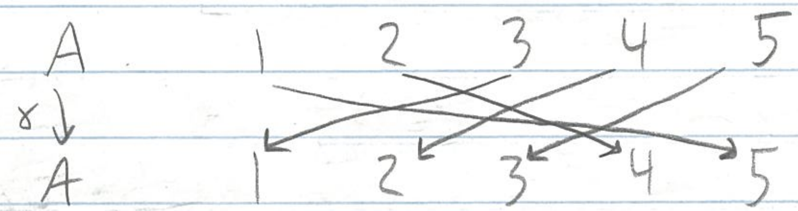
Def A *permutation group* of a set A is a set of permutations that form a group under function composition.

Ex $A = \{1,2,3,4,5\}$

$\sigma: A \to A$ by $\sigma(1)=2$, $\sigma(2)=4$, $\sigma(3)=3$ $\sigma(4)=5$ $\sigma(5)=1$

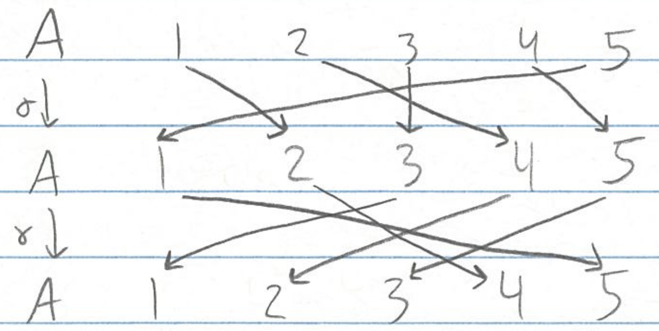


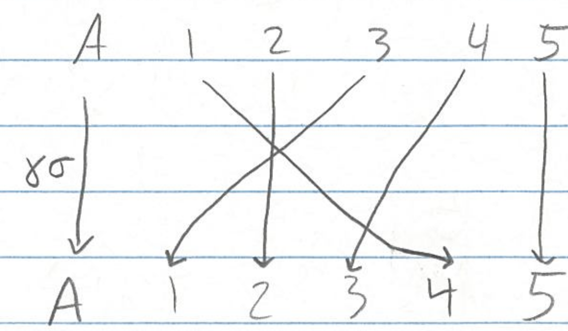
$\gamma: A \to A$ by $\gamma(1)=5$, $\gamma(2)=4$, $\gamma(3)=1$, $\gamma(4)=2$, $\gamma(5)=3$



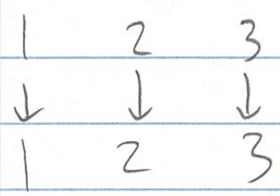
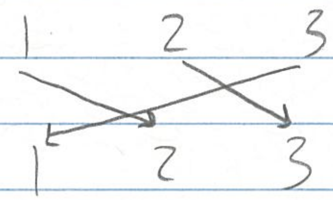
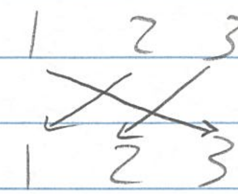
Composition $\gamma\sigma: A \to A$ via $\gamma\sigma(1) = \gamma(2) = 4$, $\gamma\sigma(2) = \gamma(4) = 2$

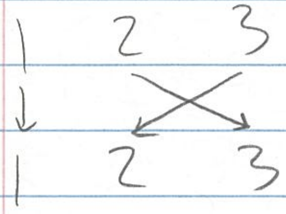
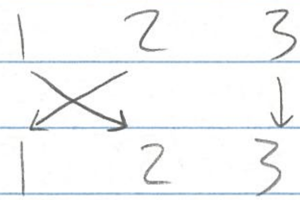
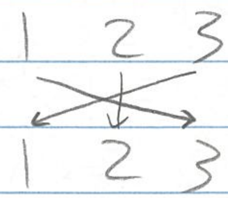
$\gamma\sigma(3) = \gamma(3) = 1$ $\gamma\sigma(4) = \gamma(5) = 3$ $\gamma\sigma(5) = \gamma(1) = 5$





<u>Ex</u> Let S_3 be the set of permutations of $\{1,2,3\}$.
This set has $\underset{\overset{\shortparallel}{3!}}{6}$ elements:

id 
(123) 
(132) 

(23) 
(12) 
(13) 

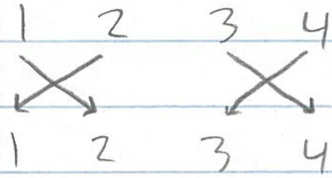
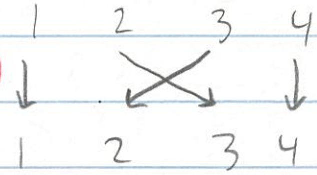
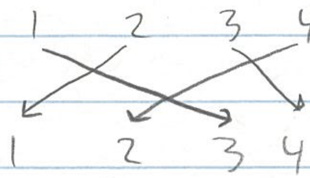
Called <u>cycle notation</u>

It is a group under function composition.
Can you identify the identity, and the inverse of each element?

(123) and (132) are inverses of each other.
(23), (12), (13) are each their own inverse.

Ex Let S_4 be the group of permutations of $\{1,2,3,4\}$, under function composition. This group has $24 = 4!$ elements.

Some of these elements are:

$(12)(34)$  (23)  (1342) 

called cycle notation

Note under function composition, we have

$$\big((23)\big)\big((12)(34)\big) = (1342)$$

Plug in 1 $\quad 3 \leftarrow 2 \leftarrow 1 \quad$ (13

Plug in 3 $\quad 4 \leftarrow 3 \quad$ (134

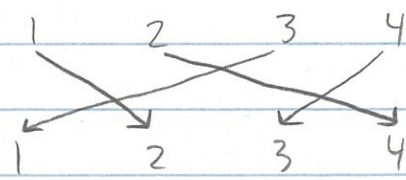
Plug in 4 $\quad 2 \longleftarrow 3 \leftarrow 4 \quad$ (1342

Plug in $\quad 1 \leftarrow 2 \quad$ (1342)

This is how we multiply in cycle notation

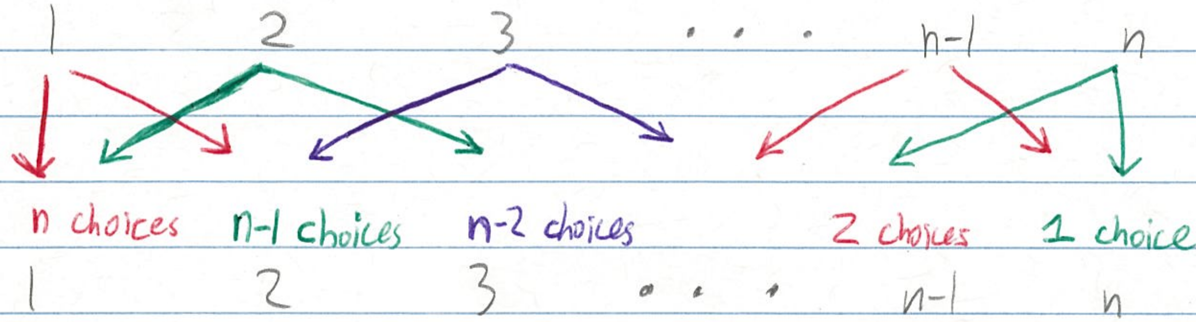
Alternatively, we have

$$\big((12)(34)\big)\big((23)\big) = (1243)$$



Def Let S_n denote the group of permutations of $\{1, 2, 3, \dots, n-1, n\}$, under function composition.

Fact This group has $n! = n(n-1)(n-2)\cdot\ldots\cdot 3\cdot 2\cdot 1$ elements. Do you see why?



Thm 5.1 Every permutation of a finite set can be written as a product of disjoint cycles.

no repeated #s

Ex

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 6 & 7 & 4 & 9 & 2 & 5 & 8 & 11 & 1 & 10 \end{array}$$

$$(1\ 3\ 7\ 5\ 9\ 11\ 10)(2\ 6)(4)(8)$$

Start with 1

Start with next smallest element that hasn't yet appeared

Rmk Cycles of length 1 are often dropped, leaving $(1\,3\,7\,5\,9\,11\,10)(2\,6)$.

<u>Ex</u>

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 8 & 1 & 9 & 5 & 3 & 11 & 10 & 2 & 4 & 6 & 7 \end{array}$$

$$(1\ 8\ 2)(3\ 9\ 4\ 5)(6\ 11\ 7\ 10)$$

<u>Ex</u> Rewrite $(1\ 3)(2\ 4)(3\ 2)(1\ 4\ 3)$ as a product of <u>disjoint</u> cycles

<u>Ans</u> $(1\ \ 2)(3)(4) = (1\,2)$

Start with 1

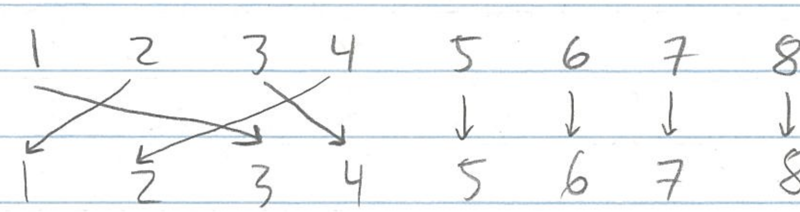
Start with next smallest element that hasn't yet appeared

<u>Ex</u> Rewrite $(1\ 3\ 2)(2\ 4\ 3)(1\,2)(3\ 1\,2)$ as a product of <u>disjoint</u> cycles

<u>Ans</u> $(1\ 3\ 4\ 2)$

<u>Rmk</u> In the above two examples we were working in S_4, but really we could have been working in S_n for any $n \geq 4$.

$(1\ 3\ 4\ 2)$



You now already know how to multiply (compose) elements in S_n !

<u>Ex</u> What's $\big((13)(24)\big) \circ (32) \circ (143)$?

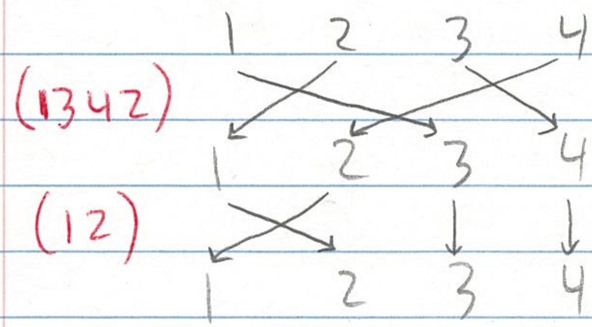
<u>Ans</u> As we saw before, it's $(12)(3)(4) = (12)$.

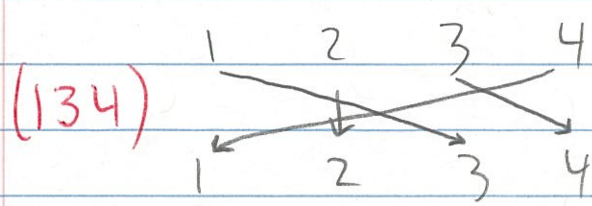
<u>Ex</u> What's $(132) \circ (243) \circ (12) \circ (312)$?

<u>Ans</u> It's (1342).

<u>Ex</u> What's $(12)(1342)$?

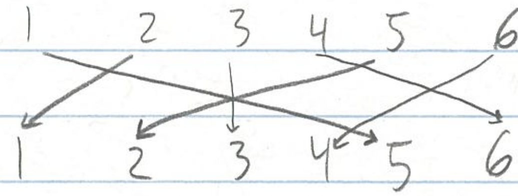
<u>Ans</u> It's $(134)(2) = (134)$



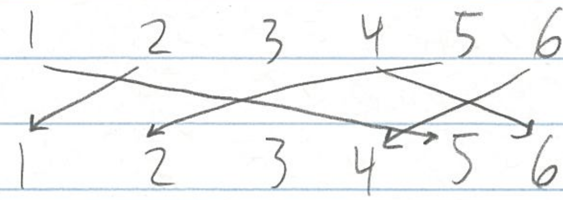


Thm 5.2 (Disjoint cycles commute)
If α and β are cycles with no entries in common, then $\alpha\beta = \beta\alpha$.

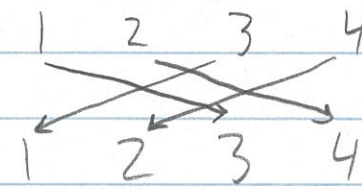
Ex $(1\,5\,2)(4\,6)$ is



Also, note
$(4\,6)(1\,5\,2)$ is



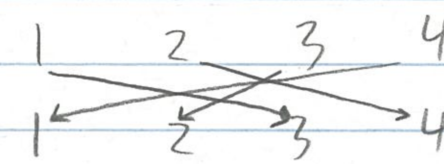
Ex $(13)(24)$ and $(24)(13)$ are both



Rmk Non-disjoint cycles need not commute!

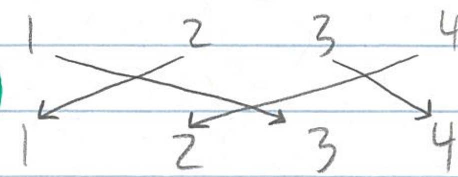
Ex $(132)(24)$ is

(1324)



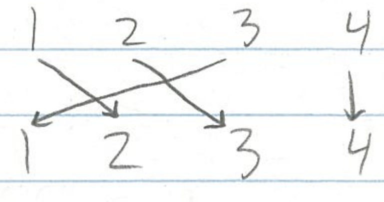
but $(24)(132)$ is

(1342)



Thm 5.3 (Order of a permutation) (Ruffini, 1799)
The order of a permutation written as a product of disjoint cycles is the least common multiple of the lengths of the cycles.

Ex



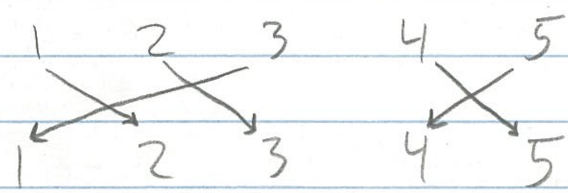
The order of $(123)(4) = (123)$ is 3:

$(123)^1 = (123)$

$(123)^2 = (123)(123) = (132)$

$(123)^3 = (123)^2(123) = (132)(123) = id$

Ex



The order of $\alpha = (123)(45)$ is 6.

Inefficient verification

$\alpha^1 = \alpha = (123)(45)$

$\alpha^2 = \alpha\alpha = (123)(45)\circ(123)(45) = (132)$

$\alpha^3 = \alpha^2\alpha = (132)\circ(123)(45) = (45)$

$\alpha^4 = \alpha^3\alpha = (45)\circ(123)(45) = (123)$

$\alpha^5 = \alpha^4\alpha = (123)\circ(123)(45) = (132)(45)$

$\alpha^6 = \alpha^5\alpha = (132)(45)\circ(123)(45) = id$

Efficient verification Using that disjoint cycles commute!

$\alpha^1 = (123)^1(45)^1 = (123)(45)$

$\alpha^2 = (123)^2(45)^2 = (132)$

$\alpha^3 = (123)^3(45)^3 = (45)$

$\alpha^4 = (123)^4(45)^4 = (123)$

$\alpha^5 = (123)^5(45)^5 = (132)(45)$

$\alpha^6 = (123)^6(45)^6 = id$

Ex $|(1456)(327)| = \underline{lcm}(4,3) = 12$

least common multiple

Ex $|(1456)(327)(89)| = lcm(4,3,2) = 12$

Ex $|(123456)(789)| = lcm(6,3) = 6$

Ex $|(12)(1342)| \neq lcm(2,4) = 4$

The cycles are not disjoint!

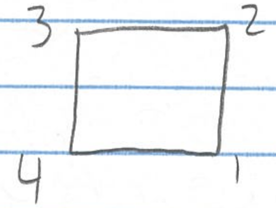
$(12)(1342) = (134)$

So

$|(12)(1342)| = |(134)| = 3.$

We will later see (Cayley's Theorem, Thm 6.1) that every finite group is "the same as" a subgroup of S_n for some n.

Ex For example, $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ can be seen as a subgroup of S_4:



$R_0 \longleftrightarrow id$ $\qquad$ $R_{90} \longleftrightarrow (1,2,3,4)$

$R_{180} \longleftrightarrow (1,3)(2,4)$ $\qquad$ $R_{270} \longleftrightarrow (1,4,3,2)$

$H \longleftrightarrow (1,2)(3,4)$ $\qquad$ $V \longleftrightarrow (1,4)(2,3)$

$D \longleftrightarrow (2,4)$ $\qquad$ $D' \longleftrightarrow (1,3)$

Clearly D_4 is not all of S_4!

$|D_4| = 8$ $\qquad$ $|S_4| = 4! = 24$.

Ex Similarly, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ can be seen as a subgroup of S_4:

$0 \longleftrightarrow id$

$1 \longleftrightarrow (1,2,3,4)$

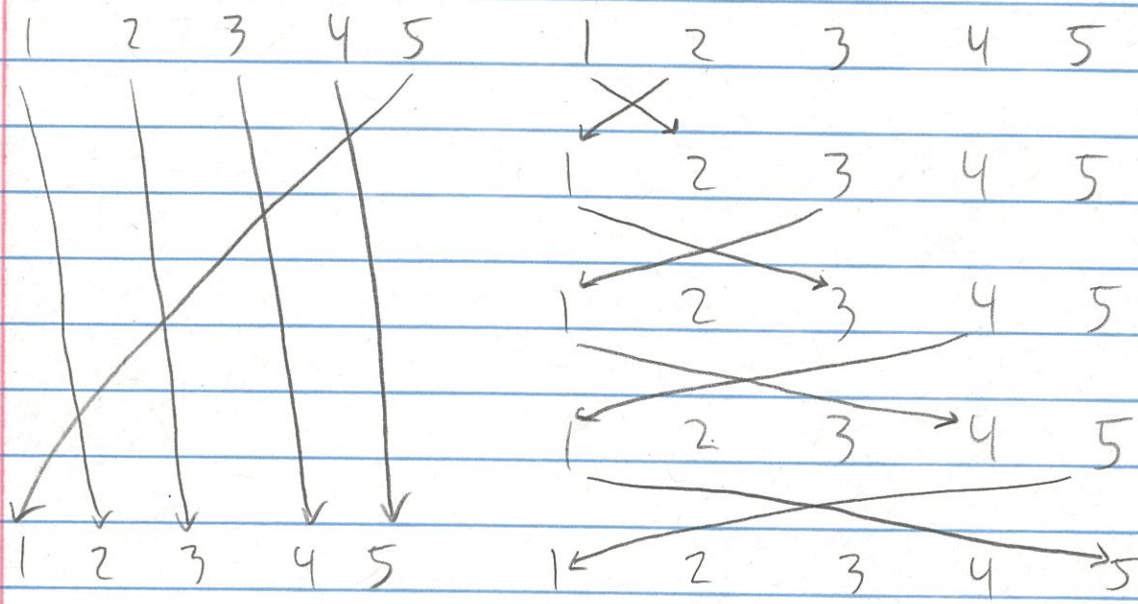
$2 \longleftrightarrow (1,3)(2,4)$

$3 \longleftrightarrow (1,4,3,2)$

$\langle 1 \rangle$ $\qquad$ $\langle (1,2,3,4) \rangle$

Thm 5.4 (Product of 2-cycles)
Every permutation in S_n (for $n>1$) is a product of 2-cycles.

Ex $(1\ 2\ 3\ 4\ 5) = (15)(14)(13)(12)$



Ex $(4\ 6\ 9\ 2\ 7\ 1) = (41)(47)(42)(49)(46)$

Ex $(3\ 1\ 4\ 6\ 8) = (38)(36)(34)(31)$

Ex $(5\ 4\ 2)(1\ 6\ 7\ 8) = (52)(54)(18)(17)(16)$

Ex $id = (12)(12)$

<u>Thm 5.5</u> (Always even or always odd)
If a permutation α can be expressed as an even (respectively odd) # of 2-cycles, then α <u>can't</u> be expressed as an odd (respectively even) # of 2-cycles.

<u>Ex</u>
$id = (12)(21)$ 2 2-cycles
$id = id$ 0 2-cycles
$id = (12)(34)(12)(34)$ 4 2-cycles
$id = (12)(23)(23)(12)$ 4 2-cycles
$id \neq (ab)$ for any a, b
$id \neq (ab)(cd)(ef)$ for any a,b,c,d,e,f

<u>Ex</u>
$(12) = (13)(23)(13)$ 3 2-cycles
$(12) = (13)(24)(51)(24)(51)$ 5 2-cycles
$(12) \neq (ab)(cd)$ for any a,b,c,d

<u>Proof Sketch</u>
First, show that id can only be written as an even product of 2-cycles
[We omit this.]

Next, suppose an arbitrary permutation α can be written as both
$\alpha = \beta_1 \beta_2 \cdot \ldots \cdot \beta_r$ and
$\alpha = \gamma_1 \gamma_2 \cdot \ldots \cdot \gamma_s$
with $\beta_1, \ldots, \beta_r$ and $\gamma_1, \ldots, \gamma_s$ all 2-cycles.

Note that $\beta_1\beta_2\cdot\ldots\cdot\beta_r = \alpha = \gamma_1\gamma_2\cdot\ldots\cdot\gamma_s$ implies

$$id = \gamma_1\gamma_2\cdot\ldots\cdot\gamma_s\beta_r^{-1}\beta_{r-1}^{-1}\cdot\ldots\cdot\beta_2^{-1}\beta_1^{-1}$$

$$= \gamma_1\gamma_2\cdot\ldots\cdot\gamma_s\beta_r\beta_{r-1}\cdot\ldots\cdot\beta_2\beta_1$$

since $\beta_i^{-1} = \beta_i$.

Hence $s+r$ is even, which means that either s and r are both even or both odd.

An important subgroup of the symmetric group S_n is the alternating group A_n.

Ex A_4 is the subgroup of S_4 with elements

id, $(12)(34)$, $(13)(24)$, $(14)(23)$,
(123), (132), (124), (142),
(134), (143), (234), (243).

Note a 3-cycle can be written as a product of two (non-disjoint) 2-cycles:

$(123) = (13)(12)$
$(143) = (13)(14)$
$(234) = (24)(23)$

Def The alternating group A_n is the subgroup of S_n consisting of all permutations that can be written as a product of an even number of 2-cycles

not necessarily disjoint

Chp 6 Isomorphisms

Lots of groups appear to have the same structures!

Ex $(\mathbb{Z}_4, + \text{ mod } 4)$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\{R_0, R_{90}, R_{180}, R_{270}\}, \circ)$

	R_0	R_{90}	R_{180}	R_{270}
R_0	R_0	R_{90}	R_{180}	R_{270}
R_{90}	R_{90}	R_{180}	R_{270}	R_0
R_{180}	R_{180}	R_{270}	R_0	R_{90}
R_{270}	R_{270}	R_0	R_{90}	R_{180}

$(U(10), \cdot \text{ mod } 10)$

	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

$(U(5), \cdot \text{ mod } 5)$

	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

These groups are all "isomorphic" to each other!

We will define this momentarily

The most common name for this collection of groups is $\mathbb{Z}_4$, the cyclic group of order 4.

Ex $(U(8), \cdot \text{ mod } 8)$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$(U(12), \cdot \text{ mod } 12)$

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

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

$\circ$	id	(12)(34)	(13)(24)	(14)(23)
id	id	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	id	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	id	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	id

$(\mathbb{Z}_2 \times \mathbb{Z}_2$, component-wise addition mod 2$)$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

These groups are all isomorphic to each other! None of them are isomorphic to $\mathbb{Z}_4$.

The most common name for this collection of groups is $\mathbb{Z}_2 \times \mathbb{Z}_2$, the <u>Klein four-group</u>.

It turns out that <u>every</u> group of order 4 (ie, size 4) is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

<u>Ex</u> Is $(\{1,-1,i,-i\},\cdot)$ isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$?

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

This <u>almost</u> looks like $\mathbb{Z}_2 \times \mathbb{Z}_2$, but it's not!

	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Now we see this group is isomorphic to $\mathbb{Z}_4$.

So $\{1,-1,i,-i\} = \langle i \rangle$ is the cyclic group of order 4, in exactly the same way that we have:

$\mathbb{Z}_4 = \langle 1 \rangle$ — Generator 1 or 3

$\{R_0, R_{90}, R_{180}, R_{270}\} = \langle R_{90} \rangle$ — Generator R_{90} or R_{270}

$U(10) = \langle 3 \rangle$ — Generator 3 or 7

$U(5) = \langle 2 \rangle$. — Generator 2 or 3

By contrast, the Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (or $U(8)$ or $U(12)$, for example) <u>cannot</u> be generated by a single element.

Means injective and surjective, i.e. one-to-one and onto.

Def An <u>isomorphism</u> $\phi: G \to H$ is a bijective function from G to H such that for all $a, b \in G$, we have $\phi(ab) = \phi(a)\phi(b)$

We say that "ϕ preserves the group operation."

If there is an isomorphism from G to H, then we say that G and H are <u>isomorphic</u>, and write $G \approx H$.

Rmk It turns out that if $\phi: G \to H$ is an isomorphism, then so is $\phi^{-1}: H \to G$.

Ex The map $\phi: \mathbb{Z}_4 \to \{R_0, R_{90}, R_{180}, R_{270}\}$ defined by $\phi(0) = R_0$, $\phi(1) = R_{90}$, $\phi(2) = R_{180}$, $\phi(3) = R_{270}$ is an isomorphism.

For example, note
$\phi(1+1) = \phi(2) = R_{180} = R_{90} \circ R_{90} = \phi(1) \circ \phi(1)$.
Similarly, note
$\phi(2+3) = \phi(1) = R_{90} = R_{180} \circ R_{270} = \phi(2) \circ \phi(3)$.

This is true in general: for all $a, b \in \mathbb{Z}_4$ we have $\phi(a+b) = \phi(a) \circ \phi(b)$.

Note $\phi(j) = R_{90 \cdot j}$ for all $j = 0, 1, 2, 3$.

Ex The map $\phi: \mathbb{Z}_4 \to \{1,-1,i,-i\}$ defined by
$\phi(0)=1$
$\phi(1)=i$
$\phi(2)=-1$
$\phi(3)=-i$
is an isomorphism.

Note $\phi(j)=i^j$ for all $j=0,1,2,3$.

Ex The map $\phi: U(8) \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by
$\phi(1) = (0,0)$
$\phi(3) = (1,0)$
$\phi(5) = (0,1)$
$\phi(7) = (1,1)$
is an isomorphism.

For example, note
$\phi(3\cdot 5 \bmod 8) = \phi(7) = (1,1) = (1,0)+(0,1) = \phi(3)+\phi(5)$

This is true in general: for all $a,b \in U(8)$, we have $\phi(a\cdot b) = \phi(a)+\phi(b)$.

Ex Any infinite cyclic group $\langle a \rangle$ (here $|a| = \infty$) is isomorphic to $\mathbb{Z}$ via the map $\phi : \langle a \rangle \to \mathbb{Z}$ defined by $\phi(a^j) = j$

Ex Any finite cyclic group $\langle a \rangle$ of order n (here $|a| = n$) is isomorphic to $\mathbb{Z}_n$ via the map $\phi : \langle a \rangle \to \mathbb{Z}_n$ defined by $\phi(a^j) = j \bmod n$.

Ex $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$ are isomorphic via the map $\phi : \mathbb{R} \to \mathbb{R}_{>0}$ defined by $\phi(x) = 2^x$ (with inverse $\phi^{-1} : \mathbb{R}_{>0} \to \mathbb{R}$ via $\phi^{-1}(y) = \log_2(y)$).
Indeed, note ϕ is bijective, and $\phi(x+y) = 2^{x+y} = 2^x 2^y = \phi(x) \cdot \phi(y)$.

Non-Ex The map $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined by $\phi(x) = x^3$ is bijective, but it is <u>not</u> an isomorphism since $\phi(x+y) = (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 \neq x^3 + y^3 = \phi(x) + \phi(y)$.

Non-Ex $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$ $\quad$ $\mathbb{Q}^*$ means 0 is excluded
Indeed, if we had an isomorphism $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$, then there would be some $q \in \mathbb{Q}$ with $\phi(q) = -1$. But then

$$-1 = \phi(q) = \phi\left(\tfrac{q}{2} + \tfrac{q}{2}\right) = \phi\left(\tfrac{q}{2}\right) \cdot \phi\left(\tfrac{q}{2}\right) = \left(\phi\left(\tfrac{q}{2}\right)\right)^2.$$

But -1 is not the square of any rational number.

Thm 6.1 <u>Cayley's Theorem (1854)</u>
Every group is isomorphic to a group of permutations.

Pf For $g \in G$, note $T_g : G \to G$ defined by
$T_g(x) = gx$ for all $x \in G$
is a <u>permutation</u> of G.

(This follows from the cancellation law.)

Note $\overline{G} = \{T_g \mid g \in G\}$ is a group of permutations of G, with operation given by function composition.

Define an isomorphism $\phi : G \to \overline{G}$ by
$\phi(g) = T_g$.

a group of permutations

Clearly ϕ is bijective.

Also, for $g, g' \in G$ we have
$\phi(gg') = T_{gg'} = T_g \circ T_{g'} = \phi(g) \circ \phi(g')$.

Indeed, to see that $T_{gg'} = T_g \circ T_{g'}$, note that for any $x \in G$ we have
$T_{gg'}(x) = (gg')x = g(g'x) = T_g(g'x) = T_g(T_{g'}(x)) = (T_g \circ T_{g'})(x)$

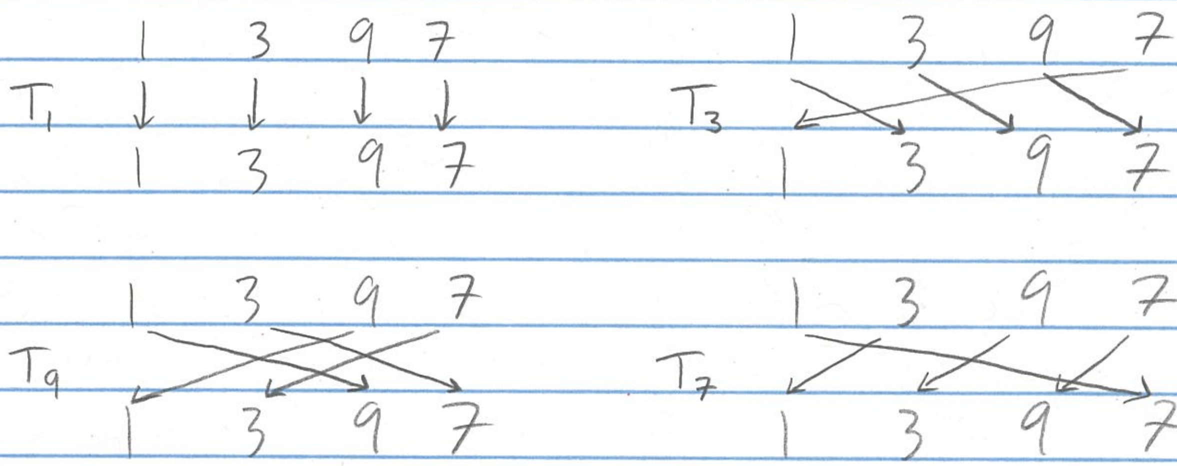
Hence $G \approx \overline{G}$. $\square$

Ex $(U(10), \cdot \bmod 10)$

$G = U(10)$

	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

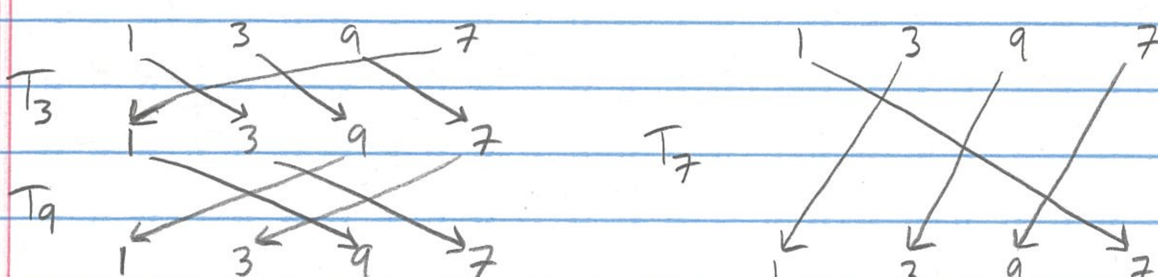
For $g \in U(10)$, define the permutation $T_g : U(10) \to U(10)$ by $T_g(x) = gx$



group of ermutations! $\overline{G}$

$$\left\{\begin{array}{l} T_1 = id : \{1,3,9,7\} \longrightarrow \{1,3,9,7\} \\ T_3 = (1397) : \{1,3,9,7\} \longrightarrow \{1,3,9,7\} \\ T_9 = (19)(37) : \{1,3,9,7\} \longrightarrow \{1,3,9,7\} \\ T_7 = (1793) : \{1,3,9,7\} \longrightarrow \{1,3,9,7\} \end{array}\right.$$

$$T_9 \circ T_3 = T_{9 \cdot 3 \bmod 10} = T_7$$



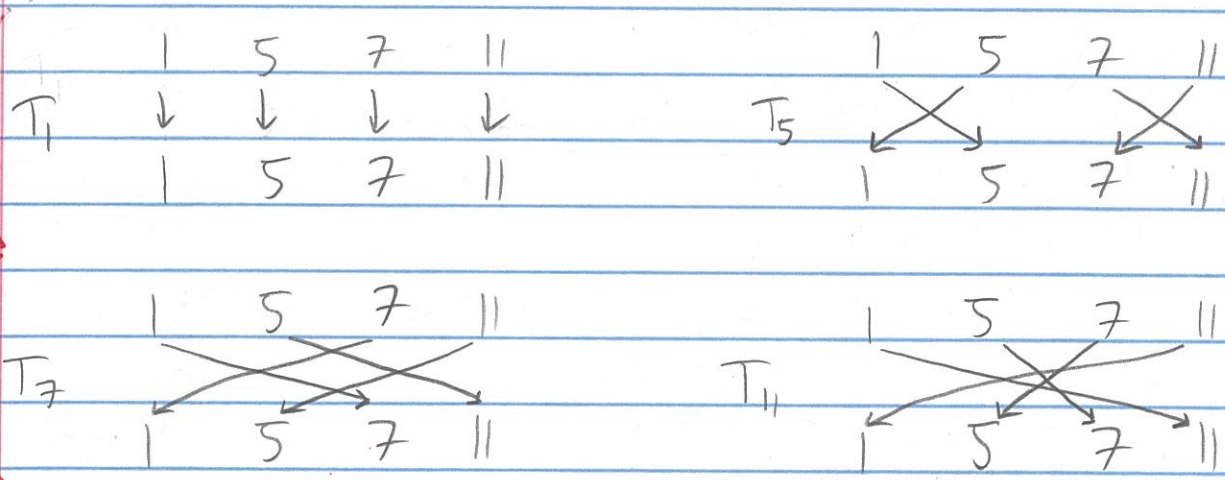
Ex $(U(12), \cdot \bmod 12)$

G

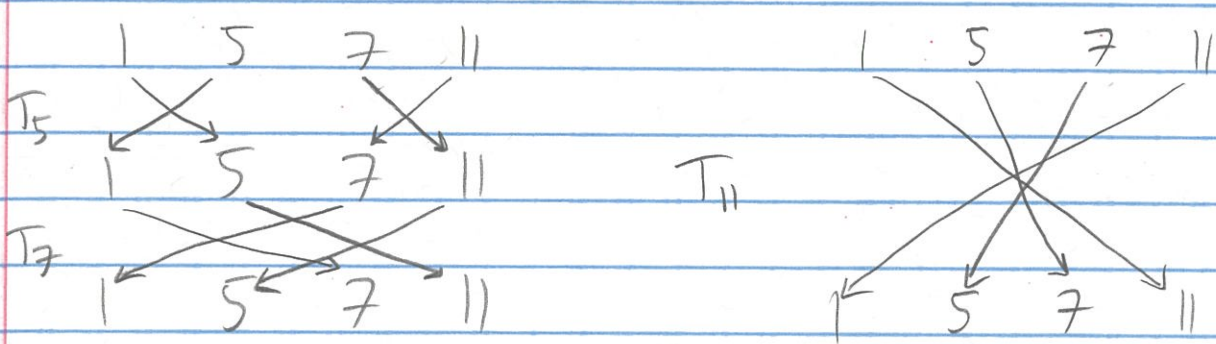
	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

group of
ermutations!

$\overline{G}$



$$T_7 \circ T_5 = T_{7 \cdot 5 \bmod 12} = T_{11}$$



Surprising fact that's very hard to prove:
$(\mathbb{R}, +) \approx (\mathbb{C}, +)$.

Theorems 6.2 and 6.3 say that an isomorphism $\phi: G \to \overline{G}$ preserves all group-theoretic properties:

- $\phi(id_G) = id_{\overline{G}}$
- $\phi(a^n) = \phi(a)^n$ for all $a \in G$ and $n \in \mathbb{Z}$
- $ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$
- $G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle$
- $|a| = |\phi(a)|$ for all $a \in G$
- $\phi^{-1}: \overline{G} \to G$ is an isomorphism
- G is abelian $\iff$ $\overline{G}$ is abelian
- G is cyclic $\iff$ $\overline{G}$ is cyclic
- If H is a subgroup of G, then $\phi(H) := \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$

There are many ways to show $G \not\approx \overline{G}$:

- If $|G| \neq |\overline{G}|$, then $G \not\approx \overline{G}$
- If G is cyclic and $\overline{G}$ is not, then $G \not\approx \overline{G}$.
- If G is abelian and $\overline{G}$ is not, then $G \not\approx \overline{G}$.
- If the order of $a \in G$ is larger than the order of any element of $\overline{G}$, then $G \not\approx \overline{G}$.

Ex $\mathbb{Z}_{12}$, D_6, and A_4 are all groups of order 12.

$$|\mathbb{Z}_{12}| = |D_6| = |A_4| = 12.$$

The largest order of an element in these groups is 12, 6, and 3, respectively.

So no two of these groups are isomorphic.

Ex $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$ since in $(\mathbb{Q}, +)$, every non-identity element has infinite order, whereas in $(\mathbb{Q}^*, \cdot)$ we have $|-1| = 2$ since $(-1)\cdot(-1) = 1$ (which is the identity).

Automorphisms

Def An isomorphism $\phi: G \to G$ from a group G to itself is called an automorphism of G.

Ex $\phi: \mathbb{C} \to \mathbb{C}$ given by $\phi(a+bi) = a - bi$ is an automorphism of the complex numbers $\mathbb{C}$.

Ex What are the automorphisms of $\mathbb{Z}_{10}$?

First note that an automorphism $\alpha: \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ is determined by $\alpha(1)$. This is because for any $k \in \mathbb{Z}_{10}$, we have:

$$\alpha(k) = \alpha(\underbrace{1 + 1 + \ldots + 1}_{k \text{ times}})$$

$$= \underbrace{\alpha(1) + \alpha(1) + \ldots + \alpha(1)}_{k \text{ times}}$$

$$= \alpha(1) \cdot k.$$

Now, Thm 6.2 says $G = \langle a \rangle \iff \overline{G} = \langle \alpha(a) \rangle$.
Here $G = \mathbb{Z}_{10} = \overline{G}$.
So $\mathbb{Z}_{10} = \langle 1 \rangle \iff \mathbb{Z}_{10} = \langle \alpha(1) \rangle$.
So the possible choices for $\alpha(1)$ are the generators of $\mathbb{Z}_{10}$, namely $\underbrace{1, 3, 7, 9}_{\text{relatively prime to } 10}$

Hence there are four automorphisms of $\mathbb{Z}_{10}$:
$\alpha_1 : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ by $\alpha_1(1) = 1$; hence $\alpha_1(k) = 1 \cdot k$
$\alpha_3 : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ by $\alpha_3(1) = 3$; hence $\alpha_3(k) = 3 \cdot k$
$\alpha_7 : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ by $\alpha_7(1) = 7$; hence $\alpha_7(k) = 7 \cdot k$
$\alpha_9 : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ by $\alpha_9(1) = 9$; hence $\alpha_9(k) = 9 \cdot k$

Pic $\qquad \mathbb{Z}_{10} \xrightarrow{\quad \alpha_3 \quad} \mathbb{Z}_{10}$

	0	1	2	3	4	…
0	0	1	2	3	4	
1	1	2	3	4		
2	2	3	4			
3	3	4				
4	4					
⋮						

	$\overset{0\cdot 3}{\shortparallel}$ 0	$\overset{1\cdot 3}{\shortparallel}$ 3	$\overset{2\cdot 3}{\shortparallel}$ 6	$\overset{3\cdot 3}{\shortparallel}$ 9	$\overset{4\cdot 3}{\shortparallel}$ 2	…
0	0	3	6	9	2	
3	3	6	9	2		
6	6	9	2			
9	9	2				
2	2					
⋮						

$$\alpha_3(a+b) = 3(a+b) = 3 \cdot a + 3 \cdot b = \alpha_3(a) + \alpha_3(b)$$

(Addition here is mod 10)

Thm 6.4 If G is a group, then the set $\text{Aut}(G)$ of automorphisms of G is also a group (under composition).

Ex $\text{Aut}(\mathbb{Z}_{10})$ is a group, and indeed $\text{Aut}(\mathbb{Z}_{10}) \approx U(10)$.

Note $\alpha_9 \circ \alpha_7 = \alpha_3$ since for any $k \in \mathbb{Z}_{10}$, we have

$$\begin{aligned}(\alpha_9 \circ \alpha_7)(k) = \alpha_9(\alpha_7(k)) &= \alpha_9(7 \cdot k) \\ &= 9 \cdot (7 \cdot k) \\ &= (9 \cdot 7) \cdot k \\ &= (63 \bmod 10) \cdot k \\ &= 3 \cdot k \\ &= \alpha_3(k)\end{aligned}$$

$(\text{Aut}(\mathbb{Z}_{10}), \circ)$

	α_1	α_3	α_9	α_7
α_1	α_1	α_3	α_9	α_7
α_3	α_3	α_9	α_7	α_1
α_9	α_9	α_7	α_1	α_3
α_7	α_7	α_1	α_3	α_9

$(U(10), \cdot \bmod 10)$

	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

Thm 6.5 For $n \geq 1$, $\text{Aut}(\mathbb{Z}_n) \approx U(n)$.

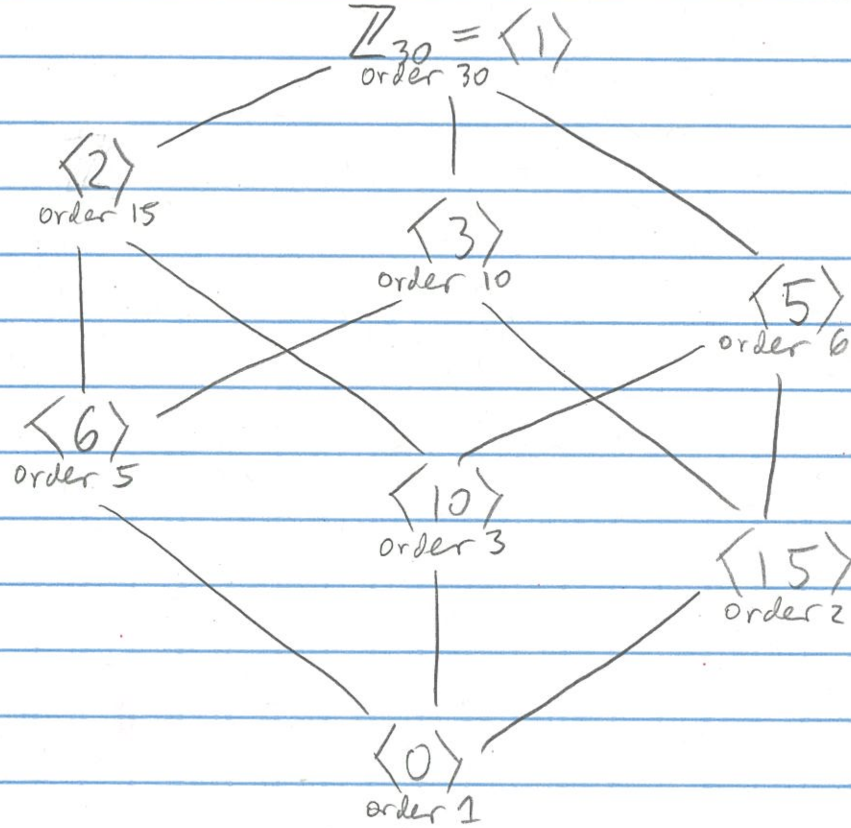
Chp 7 Cosets and Lagrange's Theorem

Thm 7.1 (Lagrange's Theorem)
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Moreover, the number of distinct left (respectively, right) cosets of H in G is $|G|/|H|$.

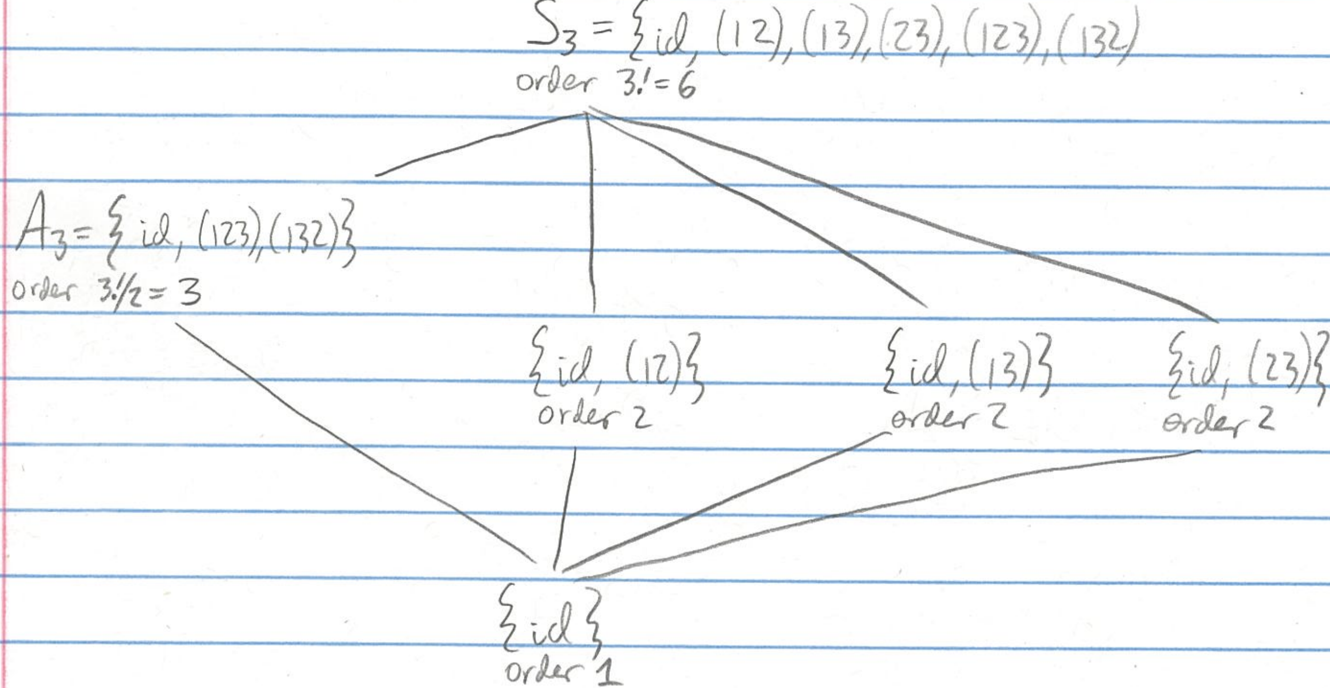
not yet defined

Ex



Note 1, 2, 3, 5, 6, 10, and 15 all divide 30.

Ex



Def (Coset of H in G)
Let G be a group and H a subgroup of G. For $a \in G$, define $aH := \{ah \mid h \in H\}$ to be the <u>left coset of H in G containing a</u>. Similarly, $Ha := \{ha \mid h \in H\}$ is the <u>right coset of H in G containing a</u>.

Ex $G = \mathbb{Z}_{12}$ and $H = \langle 3 \rangle = \{0, 3, 6, 9\}$.

$0 + H = \{0, 3, 6, 9\} = 3 + H = 6 + H = 9 + H$
$1 + H = \{1, 4, 7, 10\} = 4 + H = 7 + H = 10 + H$ Not a group
$2 + H = \{2, 5, 8, 11\} = 5 + H = 8 + H = 11 + H$ Not a group

- Note cosets are not necessarily subgroups.
- We may have $aH = bH$ for $a \neq b$.

Note the cosets of $H = \langle 3 \rangle$ partition $G = \mathbb{Z}_{12}$ into disjoint sets of equal size!

means non-overlapping

$G = \mathbb{Z}_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
$0+H$	0			3			6			9		
$1+H$		1			4			7			10	
$2+H$			2			5			8			11

This is what we'll use to prove Lagrange's Theorem, namely that $|H|$ divides $|G|$.

<u>Ex</u> $G = S_3$ and $H = \langle (13) \rangle = \{id, (13)\}$.

$id\,H = \{id, (13)\} = (13)H$

$(12)H = \{(12), (12)(13)\} = \{(12), (132)\} = (132)H$

$(23)H = \{(23), (23)(13)\} = \{(23), (123)\} = (123)H$

$G = S_3$	id	(12)	(23)	(13)	(132)	(123)
$id\,H$	id			(13)		
$(12)H$		(12)			(132)	
$(23)H$			(23)			(123)

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

So we don't necessarily have $aH = Ha$ unless G is abelian.

Properties of Cosets (page 139 of book)

Let H be a subgroup of G, with $a, b \in G$. Then

- $a \in aH$
- Either $aH = bH$ or else $aH \cap bH = \phi$.
  (IE, aH and bH are either equal or disjoint.)
- $|aH| = |bH|$
  (IE, aH and bH have the same size.)

Proof of Thm 7.1, Lagrange's Theorem

Let $a_1H, a_2H, \ldots, a_rH$ be the distinct left cosets of H in G.

By the first bullet above, each $a \in G$ is in some coset, so

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH.$$

By the second bullet above, these cosets are disjoint, so

$$|G| = |a_1H| + |a_2H| + \ldots + |a_rH|.$$

By the third bullet above, these cosets all have the same size, so

$$|G| = r|H|.$$

Rmk The converse to Lagrange's Theorem is not true: $|A_4| = 4!/2 = 12$, and 6 divides 12, but A_4 has no subgroups of order 6.

Corollary (page 143) If G is a finite group and $a \in G$, then $|a|$ divides $|G|$.

Pf Recall $|a| = |\langle a \rangle|$, where $\langle a \rangle$ is a subgroup of G. Then apply Lagrange's Theorem.

Corollary (page 143) If G is a group with order a prime number, then G is cyclic.

Pf Let G be a group with prime order.
Let $a \in G$ with $a \neq id$.
So $|a| \neq 1$.
Also $|a|$ divides $|G| =$ prime, which implies $|a| = |G|$, so $\langle a \rangle = G$ and G is cyclic.

Ex Any group of order 7 is cyclic, and therefore isomorphic to $\mathbb{Z}_7$.

Ex Any group of order 11 is cyclic, and therefore isomorphic to $\mathbb{Z}_{11}$.

Corollary (page 143) Let G be a finite group and $a \in G$. Then $a^{|G|} = id$.

Pf Since $|a|$ divides $|G|$, we have $|G| = |a| \cdot k$ for some integer k, and so

$$a^{|G|} = a^{|a| \cdot k} = (a^{|a|})^k = id^k = id.$$

Corollary (Fermat's Little Theorem)

For p prime, $a^p \bmod p = a \bmod p$ for all integers a.

Ex Try this for $p=7$ prime and $a=0,1,2,\ldots,5,6$.

Pf It suffices to check for $a \in \{0,1,2,\ldots,p-1\}$.
The case $a=0$ is clear.
The case $a \in \{1,2,\ldots,p-1\}$, i.e. $a \in U(p)$, follows since for p prime, $|U(p)| = p-1$, giving

$$a^{p-1} = a^{|U(p)|} = 1 \mod p,$$

which implies

$$a^p = a \cdot a^{p-1} = a \cdot 1 = a \mod p.$$

Rmk Fermat's Little Theorem is used (for example) to show that some large numbers are not prime.

For example, $p = 2^{257} - 1$ is not prime since

$$10^p \neq 10 \mod p.$$

Rmk One can use Lagrange's Theorem to show for p prime, any group of size $2p$ is isomorphic to either $\mathbb{Z}_{2p}$ or D_p (this is Thm 7.3 in our book; it requires elbow grease).

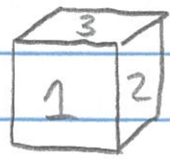
An Application of Cosets to Permutation Groups

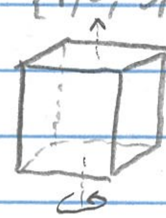
This theory will allow us to study...

The Rotation Group of a Cube and a Soccer Ball

Ex 9 Let G be the group of rotational symmetries of a cube. What is the size of G ?

Each rotation in G can be seen as a permutation of the 6 faces $\{1,2,3,4,5,6\}$.





The size of G is

$$\underbrace{\left(\begin{array}{c}\text{\# faces that face 1}\\ \text{can be rotated to}\end{array}\right)}_{\text{the \# of cosets of that subgroup}} \cdot \underbrace{\left(\begin{array}{c}\text{\# rotations mapping}\\ \text{face 1 to itself}\end{array}\right)}_{\text{A subgroup of } G}$$

$$= 6 \cdot 4$$

$$= 24.$$

Indeed, it turns out that G is isomorphic to S_4, where $|S_4| = 4! = 24$.

Ex 10 Let G be the group of rotational symmetries of a soccer ball. What is the size of G?

Each rotation in G can be seen as a permutation of the 12 pentagons in a soccer ball.

The size of G is

$$\underbrace{\begin{pmatrix}\text{\# pentagons that pentagon 1}\\ \text{can be rotated to}\end{pmatrix}}_{\text{\# cosets of that subgroup}} \cdot \underbrace{\begin{pmatrix}\text{\# rotations mapping}\\ \text{pentagon 1 to itself}\end{pmatrix}}_{\text{A subgroup of } G}$$

$$= 12 \cdot 5$$

$$= 60.$$

Indeed, $G \approx A_5$, where $|A_5| = \frac{5!}{2} = \frac{120}{2} = 60.$

Alternatively, each rotation in G can be seen as a permutation of the 20 hexagons.

The size of G is

$$\begin{pmatrix}\text{\# hexagons that hexagon 1}\\ \text{can be rotated to}\end{pmatrix} \cdot \begin{pmatrix}\text{\# rotations } \underline{\text{in } G} \text{ mapping}\\ \text{hexagon 1 to itself}\end{pmatrix}$$

$$= 20 \cdot 3$$

$$= 60.$$

only 3 of the 6 rotations of a single hexagon are in G. Indeed, the other 3 rotations don't map pentagons to pentagons, and hence aren't symmetries of the soccer ball!

<u>Def</u> Let G be a group of permutations of a set S. For each $i \in S$, define the <u>stabilizer of i in G</u> to be $\mathrm{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$.

<u>Ex</u> If G is the rotational symmetries of the cube, then $\mathrm{stab}_G(\text{face } 1) \approx \{R_{90}, R_{180}, R_{270}, R_0\}$.

<u>Ex</u> If $G = S_3$, then:

$$\mathrm{stab}_G(1) = \{id, (23)\}$$
$$\mathrm{stab}_G(2) = \{id, (13)\}$$
$$\mathrm{stab}_G(3) = \{id, (12)\}.$$

<u>Ex</u> If $G = S_4$, then:

$$\mathrm{stab}_G(1) = \{id, (23), (24), (34), (234), (243)\}$$
$$\vdots$$
$$\mathrm{stab}_G(4) = \{id, (12), (13), (23), (123), (132)\}.$$

<u>Rmk</u> A stabilizer $\mathrm{stab}_G(i)$ is always a subgroup of G.

Def Let G be a group of permutations of a set S. For each $i \in S$, define the <u>orbit of i under G</u> to be $\mathrm{orb}_G(i) = \{\phi(i) \mid \phi \in G\}$.

Ex If $G = S_3$, then $\mathrm{orb}_G(1) = \{1, 2, 3\}$

$id(1)=1$ $\qquad$ $\phi(1)=2$ for $\phi=(12)$ $\qquad$ $\phi(1)=3$ for $\phi=(13)$

Ex If $G = S_4$, then $\mathrm{orb}_G(1) = \{1, 2, 3, 4\}$

$\phi(1)=1$ for $\phi=id$ $\qquad$ $\phi(1)=2$ for $\phi=(12)$ $\qquad$ $\phi(1)=3$ for $\phi=(13)$ $\qquad$ $\phi(1)=4$ for $\phi=(14)$

Ex Let G be the following subgroup of S_8:

$$G = \{id, (132)(465)(78), (132)(465), (123)(456), (123)(456)(78), (78)\}$$

Then

$\mathrm{orb}_G(1) = \{1, 3, 2\}$ $\qquad$ $\mathrm{stab}_G(1) = \{id, (78)\}$

$\mathrm{orb}_G(2) = \{2, 1, 3\}$ $\qquad$ $\mathrm{stab}_G(2) = \{id, (78)\}$

$\mathrm{orb}_G(4) = \{4, 6, 5\}$ $\qquad$ $\mathrm{stab}_G(4) = \{id, (78)\}$

$\mathrm{orb}_G(7) = \{7, 8\}$ $\qquad$ $\mathrm{stab}_G(7) = \{id, (132)(465), (123)(456)\}$

Thm 7.4 Orbit-Stabilizer Theorem

Let G be a finite group of permutations of a set S. Then, for any $i \in S$, we have
$|G| = |orb_G(i)| \cdot |stab_G(i)|$.

Ex Check on our prior examples with $G=S_3$, $G=S_4$, or $G < S_8$.

Ex Check on our prior examples of the group of rotational symmetries of a cube or soccer ball.

Pf (Sketch)

The proof follows from Lagrange's Theorem, after showing that $stab_G(i)$ is a subgroup of G, and that
$|orb_G(i)| = \#$ cosets of $stab_G(i)$ in G.

Chp 9 Normal subgroups and quotient groups

sometimes called factor groups

A quotient group is what you get when you "divide" one group by another.

Ex In $\mathbb{Z}/3\mathbb{Z}$, the elements $\{0,1,2\}$ really correspond to the three cosets

$0+3\mathbb{Z} = 3\mathbb{Z} = \{\ldots,-6,-3,0,3,6,\ldots\}$
$1+3\mathbb{Z} = \{\ldots,-5,-2,1,4,7,\ldots\}$
$2+3\mathbb{Z} = \{\ldots,-4,-1,2,5,8,\ldots\}$

Here we have "divided" $\mathbb{Z}$ by its (normal) subgroup $3\mathbb{Z}$.

Ex Let $Rot = \{R_0, R_{90}, R_{180}, R_{270}\}$ be the subgroup of rotations of D_4.
We can define the quotient group D_4/Rot, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Elements of D_4/Rot		Elements of $\mathbb{Z}/2\mathbb{Z}$
$id\, Rot = Rot = \{R_0, R_{90}, R_{180}, R_{270}\}$	$\longleftrightarrow$	0
$V\, Rot = \{V, D, H, D'\}$	$\longleftrightarrow$	1

Ex S_3/A_3 is also isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Elements of S_3/A_3		Elements of $\mathbb{Z}/2\mathbb{Z}$
$id\, A_3 = A_3 = \{(id), (123)(132)\}$	$\longleftrightarrow$	0
$(12)A_3 = \{(12), (23), (13)\}$	$\longleftrightarrow$	1

As you can see, if G is a group and H is a (normal) subgroup, then we will define the quotient group G/H to have as its elements the cosets aH for $a \in G$.

What will the group operation be?
We'll define $G/H \times G/H \longrightarrow G/H$ via
$(aH)(bH) = abH$.

This will work so long as H is normal in G, i.e., $aH = Ha$ for all $a \in G$. Then

$$(aH)(bH) = a(Hb)H \underset{\boxed{\text{since } H \text{ normal}}}{=} a(bH)H = (ab)HH \underset{\text{since } H \text{ a subgroup}}{=} abH.$$

Two cosets of H multiply to give one coset of H

This will not work when H is not a normal subgroup of G.
Take for example $G = S_3$ and $H = \{id, (12)\}$.
H is not normal in G, since
$(23)H = \{(23)id, (23)(12)\} = \{(23), (132)\}$ is not equal to
$H(23) = \{id(23), (12)(23)\} = \{(23), (123)\}$.

$\boxed{\text{The step in blue above fails.}}$

For H not normal, $(aH)(bH)$ need not give a coset of H.
For example,

$$((23)H)((23)H) = \{(23), (132)\}\{(23), (132)\} = \{(23)(23), (23)(132), (132)(23), (132)(132)\}$$
$$= \{id, (12), (13), (123)\}$$

is too large to be a coset of H, which all have size 2.

Rmk You can't make a quotient group dividing by *any* subgroup! Only by "normal" subgroups! $\boxed{\text{sometimes called factor groups}}$

Def (Due to Galois)
A subgroup H of G is a normal subgroup of G, denoted $H \triangleleft G$, if $aH = Ha$ for all $a \in G$.

Rmk This means any element ah with $h \in H$ can also be written as $h'a$ for some $h' \in H$, and vice-versa.

Ex Every subgroup of an Abelian group is normal (since $ah = ha$).

☆ You can quotient an abelian group G by *any* subgroup H.

Ex The alternating group $H = A_n$ of even permutations is a normal subgroup of $G = S_n$.

Indeed for $a = (12) \in S_n$ and $h = (123) \in A_n$, we have

$$ah = (12)(123) = (1)(23) = (132)(12) = h'a$$

for $h' = (132) \in A_n$.

Similarly for $a = (12) \in S_n$ and $h = (13)(24) \in A_n$, we have

$$ah = (12)(13)(24) = (1324) = (14)(23)(12) = h'a$$

for $h' = (14)(23) \in A_n$.

Ex More explicitly, $H = A_3 = \{id, (123), (132)\}$ is a normal subgroup of $G = S_3 = \{id, (12), (13), (23), (123), (132)\}$.

Indeed,

$id\, A_3 = A_3 = A_3\, id$ since $id \in A_3$
$(123) A_3 = A_3 = A_3 (123)$ since $(123) \in A_3$
$(132) A_3 = A_3 = A_3 (132)$ since $(132) \in A_3$

$(12) A_3 = \{(12), (12)(123), (12)(132)\} = \{(12), (23), (13)\}$
$A_3 (12) = \{(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}$
So $(12) A_3 = A_3 (12)$

$(13) A_3 = \{(13), (13)(123), (13)(132)\} = \{(13), (12), (23)\}$
$A_3 (13) = \{(13), (123)(13), (132)(13)\} = \{(13), (23), (12)\}$
So $(13) A_3 = A_3 (13)$

$(23) A_3 = \{(23), (23)(123), (23)(132)\} = \{(23), (13), (12)\}$
$A_3 (23) = \{(23), (123)(23), (132)(23)\} = \{(23), (12), (13)\}$
So $(23) A_3 = A_3 (23)$

Non-Ex Recall, however, that $H = \{id, (12)\}$ is <u>not</u> a normal subgroup of S_3, since
$(23) H = \{(23), (132)\}$ is not equal to
$H (23) = \{(23), (123)\}$.

Ex In the dihedral group D_n, any subgroup consisting solely of rotations is normal in D_n.

Indeed, for any rotation R and flip F we have $FR = R^{-1}F$, and any two rotations commute.

Ex $Rot := \{R_0, R_{90}, R_{180}, R_{270}\}$ is normal in D_4:

$R_0\, Rot = Rot = Rot\, R_0$ since $R_0 \in Rot$

$\vdots$

$R_{270}\, Rot = Rot = Rot\, R_{270}$ since $R_{270} \in Rot$

$H\, Rot = \{HR_0, HR_{90}, HR_{180}, HR_{270}\} = \{H, D, V, D'\}$

$$\shortparallel$$

$Rot\, H = \{R_0H, R_{90}H, R_{180}H, R_{270}H\} = \{H, D', V, D\}$

Similarly,
$V\,Rot = Rot\,V$
$D\,Rot = Rot\,D$
$D'\,Rot = Rot\,D'$

Thm 9.2 Let G be a group and let $H \triangleleft G$ be a normal subgroup of G. Then the set $G/H = \{aH \mid a \in G\}$ of cosets of H in G is a group under the operation $(aH)(bH) = abH$.

Ex $G = \mathbb{Z}/12\mathbb{Z}$ $\qquad H = \langle 4 \rangle = \{0, 4, 8\}$

The elements of G/H are

$0 + H = \{0, 4, 8\}$

$1 + H = \{1, 5, 9\}$

$2 + H = \{2, 6, 10\}$

$3 + H = \{3, 7, 11\}$

The Cayley table for G/H is

	$0+H$	$1+H$	$2+H$	$3+H$
$0+H$	$0+H$	$1+H$	$2+H$	$3+H$
$1+H$	$1+H$	$2+H$	$3+H$	$0+H$
$2+H$	$2+H$	$3+H$	$0+H$	$1+H$
$3+H$	$3+H$	$0+H$	$1+H$	$2+H$

Note $G/H \approx \mathbb{Z}/4\mathbb{Z}$.

Ex $G = D_4$ $\quad K = \{R_0, R_{180}\}$

The elements of D_4/K are

$K = \{R_0, R_{180}\}$

$R_{90}K = \{R_{90}, R_{270}\}$

$HK = \{H, V\}$

$DK = \{D, D'\}$

The Cayley table for D_4/K is

	K	$R_{90}K$	HK	DK
K	K	$R_{90}K$	HK	DK
$R_{90}K$	$R_{90}K$	K	DK	HK
HK	HK	DK	K	$R_{90}K$
DK	DK	HK	$R_{90}K$	K

Note $D_4/K \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We can see D_4/K "living inside" the Cayley table for D_4:

		R_0	R_{180}	R_{90}	R_{270}	H	V	D	D'
K	R_0	R_0	R_{180}	R_{90}	R_{270}	H	V	D	D'
	R_{180}	R_{180}	R_0	R_{270}	R_{90}	V	H	D'	D
$R_{90}K$	R_{90}	R_{90}	R_{270}	R_{180}	R_0	D'	D	V	H
	R_{270}	R_{270}	R_{90}	R_0	R_{180}	D	D'	H	V
HK	H	H	V	D	D'	R_0	R_{180}	R_{90}	R_{270}
	V	V	H	D'	D	R_{180}	R_0	R_{270}	R_{90}
DK	D	D	D'	V	H	R_{270}	R_{90}	R_0	R_{180}
	D'	D'	D	H	V	R_{90}	R_{270}	R_{180}	R_0

Chp 10 Group Homomorphisms

Def A homomorphism between groups G and $\overline{G}$ is a function $\phi: G \to \overline{G}$ satisfying $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Ex Isomorphisms are homomorphisms (that also happen to be bijective).

Def The kernel of a homomorphism $\phi: G \to \overline{G}$ is $\ker \phi = \{x \in G \mid \phi(x) = id_{\overline{G}}\}$.

Ex $\phi: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ defined by $\phi(0) = 0$ and $\phi(1) = 2$ is a homomorphism that is not surjective.
Here $\ker \phi = \{0\} \subseteq \mathbb{Z}/2\mathbb{Z}$.

$$\begin{array}{ccc} \underline{\mathbb{Z}/2\mathbb{Z}} & & \underline{\mathbb{Z}/4\mathbb{Z}} \\ 0 & \longmapsto & 0 \\ & & 1 \\ 1 & \longmapsto & 2 \\ & & 3 \end{array}$$

For example, note $\phi(1+1) = \phi(0) = 0 = 2+2 = \phi(1) + \phi(1)$.

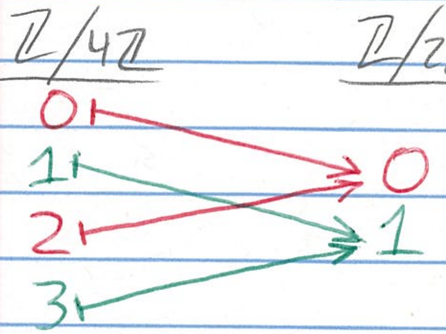
$\mathbb{Z}/2\mathbb{Z}$

	0	1
0	0	1
1	1	0

$\mathbb{Z}/4\mathbb{Z}$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ex $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $\phi(j) = j \bmod 2$, or equivalently $\phi(0)=0$, $\phi(1)=1$, $\phi(2)=0$, $\phi(3)=1$, is a homomorphism that is not injective. Here $\ker\phi = \{0,2\} \subseteq \mathbb{Z}/4\mathbb{Z}$.



For example, note
$\phi(2+3) = \phi(1) = 1 = 0+1 = \phi(2)+\phi(3)$.
Alternatively, note
$\phi(2+2) = \phi(0) = 0 = 0+0 = \phi(2)+\phi(2)$.

$\mathbb{Z}/4\mathbb{Z}$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}/2\mathbb{Z}$

	0	1
0	0	1
1	1	0

Ex Let $n \geq 1$ be an integer. Then $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi(j) = j \bmod n$ is a homomorphism with kernel
$\ker\phi = \langle n \rangle = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$.

Ex $\phi : S_n \to \mathbb{Z}/2\mathbb{Z}$ defined by
$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \in A_n \\ 1 & \text{if } \sigma \notin A_n \end{cases}$$
is a homomorphism with $\ker\phi = A_n \subseteq S_n$.

79

▮ EXAMPLE 11 The mapping from S_n to Z_2 that takes an even permutation to 0 and an odd permutation to 1 is a homomorphism. Figure 10.2 illustrates the telescoping nature of the mapping. ▮

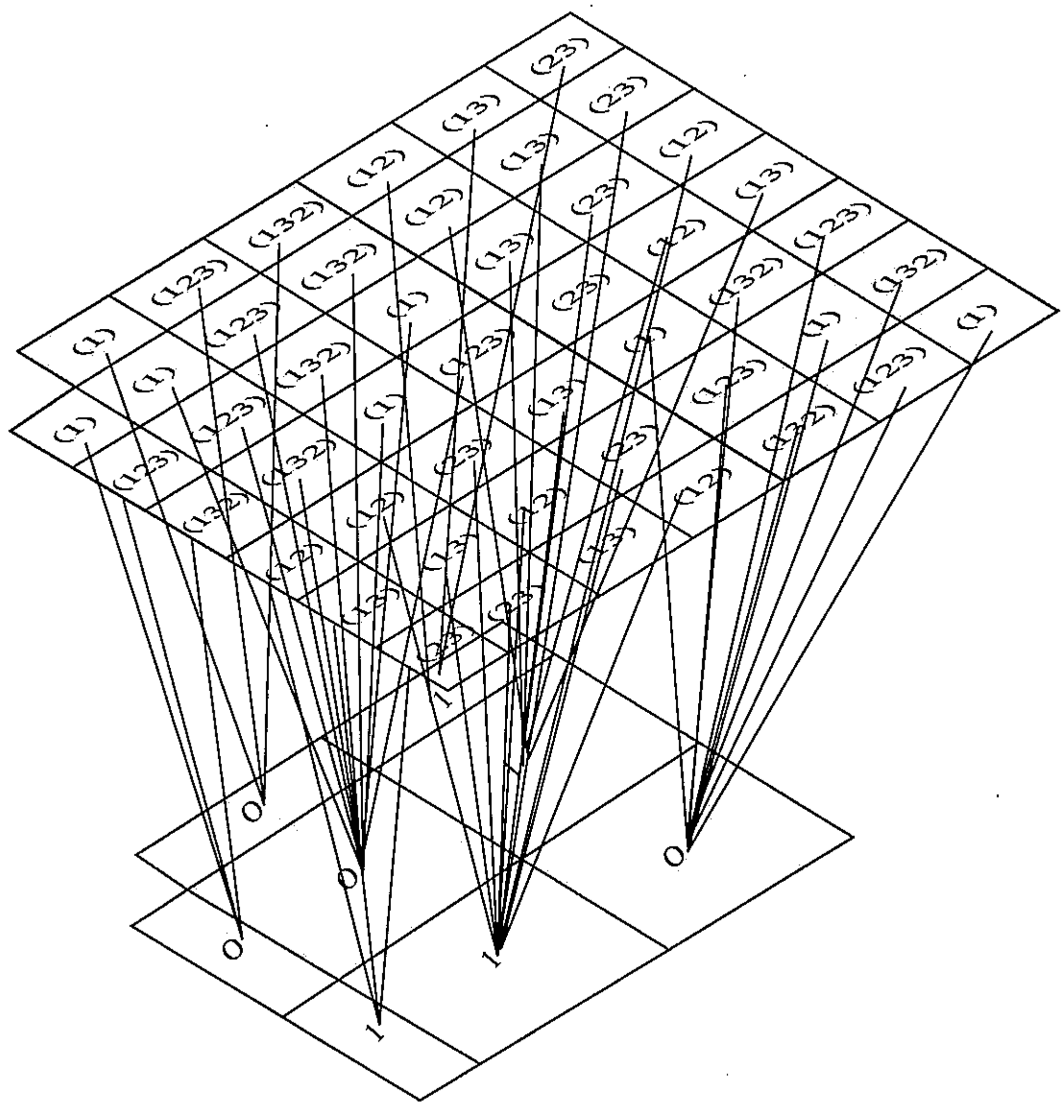


Figure 10.2 Homomorphism from S_3 to Z_2.

Ex $\phi: D_n \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is a rotation} \\ 1 & \text{if } \sigma \text{ is a reflection} \end{cases}$$

is a homomorphism with $\ker\phi$ equal to the subgroup of rotations in D_n.

Indeed, the fact this is a homomorphism follows since ...

rotation ∘ rotation = rotation	$0+0=0$
rotation ∘ flip = flip	$0+1=1$
flip ∘ rotation = flip	$1+0=1$
flip ∘ flip = rotation	$1+1=0$

Non-Ex $\phi: (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined by $\phi(x) = x^2$ is not a homomorphism since

$\phi(a+b) = (a+b)^2 = a^2 + 2ab + b^2$

need not equal

$\phi(a) + \phi(b) = a^2 + b^2$.

* means 0 excluded

Ex $\phi: (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ defined by $\phi(x) = x^2$ is a homomorphism since

$\phi(a \cdot b) = (a \cdot b)^2 = abab = a^2 b^2 = \phi(a) \cdot \phi(b)$

for all $a, b \in \mathbb{R}^*$.

Here $\ker \phi = \{1, -1\}$.

Ex Let $GL(2,\mathbb{R})$ be the set of all 2×2 invertible (determinant nonzero) matrices with entries in $\mathbb{R}$.
Then $\phi: GL(2,\mathbb{R}) \to (\mathbb{R}^*, *)$ defined by
$$\phi(A) = \det(A)$$
is a group homomorphism.
Here $\ker\phi$ is the subgroup of all matrices with determinant 1.

Thm 10.1 Let $\phi: G \to \overline{G}$ be a group homomorphism and let $g \in G$. Then

- $\phi(id_G) = id_{\overline{G}}$.

  Proof $\phi(id_G)\phi(id_G) = \phi(id_G \cdot id_G) = \phi(id_G) = \phi(id_G) \cdot id_{\overline{G}}$.
  So $\phi(id_G) = id_{\overline{G}}$ by cancellation law.

- $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$.
  In particular, $\phi(g^{-1}) = \phi(g)^{-1}$.

Thm 10.2 Let $\phi: G \to \overline{G}$ be a group homomorphism, let H be a subgroup of G, and let $\overline{K}$ be a subgroup of $\overline{G}$. Then

- $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.
- If H is cyclic / Abelian / normal in H, then $\phi(H)$ is cyclic / Abelian / normal in $\phi(G)$.
- $\phi^{-1}(\overline{K}) = \{x \in G \mid \phi(x) \in \overline{K}\}$ is a subgroup of G.
- If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K})$ is a normal subgroup of G.

"Subgroups of G map under ϕ to subgroups of $\overline{G}$, and vice-versa."

Ex Since $\{id_{\overline{G}}\}$ is a subgroup of $\overline{G}$, Thm 10.2 says that

$\phi^{-1}(\{id_{\overline{G}}\}) = \{x \in G \mid \phi(x) = id_{\overline{G}}\} = \ker \phi$

is a subgroup of G.

Moreover, note $\{id_{\overline{G}}\}$ is a <u>normal</u> subgroup of $\overline{G}$.

(Indeed, for any $a \in \overline{G}$, we have
$a\{id_{\overline{G}}\} = \{a\} = \{id_{\overline{G}}\}a$.)

Hence Thm 10.2 says that

$\phi^{-1}(\{id_{\overline{G}}\})$ is a <u>normal</u> subgroup of G.

Ex Let $n \geq 1$ be an integer.

Define homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\phi(j) = j \bmod n$.

Indeed $\ker \phi = \langle n \rangle = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

is a normal subgroup of $\mathbb{Z}$.

Ex Define homomorphism $\phi: S_n \to \mathbb{Z}/2\mathbb{Z}$ by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \in A_n \\ 1 & \text{if } \sigma \notin A_n. \end{cases}$$

Indeed $\ker \phi = A_n$ is a normal subgroup of S_n.

Thm 10.3 First Isomorphism Thm (Jordan, 1870)

Let $\phi: G \to \overline{G}$ be a homomorphism.
Then the function $\underbrace{G/\ker\phi}_{\text{defined since } \ker\phi \text{ is normal in } G} \longrightarrow \underbrace{\phi(G)}_{= \{\phi(g) \mid g \in G\}}$

defined by $\underbrace{g\ker\phi}_{\text{a coset of } \ker\phi\text{, i.e. an element of } G/\ker\phi} \longmapsto \phi(g)$

is an isomorphism.
In symbols, $G/\ker\phi \approx \phi(G)$.

Ex Let's apply this to the homomorphism
$\phi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi(j) = j \bmod n$.
Note $\ker\phi = \langle n \rangle = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$
Note $\phi(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ since ϕ is surjective.

So Thm 10.3 (First Isomorphism Thm) says

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\phi \underset{\text{Thm 10.3}}{\approx} \phi(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

This is not surprising; really this is how the name of the group $\mathbb{Z}/n\mathbb{Z}$ was chosen! But at least it checks out.

<u>Ex</u> Applying Thm 10.3 to the homomorphism $\phi: S_n \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \in A_n \\ 1 & \text{if } \sigma \notin A_n \end{cases}$$

gives

$$S_n/A_n \underset{\substack{\uparrow \\ \text{since } A_n = \ker\phi}}{=} S_n/\ker\phi \underset{\substack{\uparrow \\ \text{Thm 10.3}}}{\approx} \phi(S_n) \underset{\substack{\uparrow \\ \text{since } \phi \text{ is surjective}}}{=} \mathbb{Z}/2\mathbb{Z}.$$

The First Isomorphism Theorem, namely Thm 10.3, is one of the best ways to understand the structure of quotient groups!

<u>Ex</u> Applying Thm 10.3 to the homomorphism $\phi: \underbrace{GL(2,\mathbb{R})}_{\substack{\text{invertible} \\ 2\times 2 \text{ matrices}}} \longrightarrow \underbrace{(\mathbb{R}^*, \cdot)}_{\text{Nonzero reals}}$ defined by

$\phi(A) = \det(A)$ gives

$$GL(2,\mathbb{R})/SL(2,\mathbb{R}) = GL(2,\mathbb{R})/\ker\phi \underset{\substack{\uparrow \\ \text{Thm 10.3}}}{\approx} \phi(GL(2,\mathbb{R})) = \mathbb{R}^*,$$

where $SL(2,\mathbb{R})$ is the set of 2×2 matrices of determinant 1.

So the (apparently complicated) quotient group $GL(2,\mathbb{R})/SL(2,\mathbb{R})$ is actually quite simple; it's isomorphic to $(\mathbb{R}^*, \cdot)$.

A "partial converse" to the First Isomorphism Theorem is also true:

<u>Thm 10.4</u> Every normal subgroup of a group G is a kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the homomorphism $\phi: G \to \underline{G/N}$ defined by $\phi(g) = gN$

This quotient group is defined since N is normal in G.

<u>Ex</u> $5\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, and it is the kernel of the homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ defined by $\phi(j) = j + 5\mathbb{Z}$.

<u>Ex</u> A_n is a normal subgroup of S_n, and it is the kernel of the homomorphism $\phi: S_n \to S_n/A_n$ defined by $\phi(\sigma) = \sigma A_n$.

Chapter 8 Direct products

Direct products are a way to combine groups to get larger ones!

(Or to decompose a group into smaller parts.)

Def If G and H are groups, then their direct product group is
$$G \oplus H = \{ (g,h) \mid g \in G,\ h \in H \}$$
with componentwise operation:
$$(g,h)(g',h') = (gg', hh').$$

Def If $G_1, \dots, G_n$ are groups, then their direct product group is
$$G_1 \oplus G_2 \oplus \dots \oplus G_n = \left\{ (g_1, g_2, \dots, g_n) \,\middle|\, \begin{array}{l} g_i \in G_i \text{ for} \\ \text{all } i \end{array} \right\},$$
with componentwise operation:
$$(g_1, \dots, g_n)(g_1', \dots, g_n') = (g_1 g_1', \dots, g_n g_n').$$

Ex $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ has as its elements $(0,0), (0,1), (1,0), (1,1)$.

Example addition in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$:
$(1,0) + (1,1) = (2,1) = (0,1)$.

Ex In $D_4 \oplus \mathbb{Z}/3\mathbb{Z}$ we have
$(R_{90}, 2)(R_{180}, 1) = (R_{270}, 0)$.

Ex $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$

$\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$

Ex $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

$= \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$

Fact For G and H finite groups,
$|G \oplus H| = |G| \cdot |H|.$

Fact For $G_1, \ldots, G_n$ finite groups,
$|G_1 \oplus \cdots \oplus G_n| = |G_1| \cdot \ldots \cdot |G_n|.$

What's the order of the element $(1,1)$ in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$?

Ans $\langle (1,1) \rangle = \{(1,1), (0,2), (1,0), (0,1), (1,2), (0,0)\}$

$|(1,1)| = 6$, i.e., $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

is cyclic with $(1,1)$ as a generator.

Thm 8.2 For G and H finite cyclic groups, we have $G \oplus H$ is cyclic $\Longleftrightarrow$ $|G|$ and $|H|$ are relatively prime.

Ex $G = \mathbb{Z}/2\mathbb{Z}$ size 2 cyclic
$H = \mathbb{Z}/3\mathbb{Z}$ size 3 cyclic
2, 3 relatively prime $\Rightarrow$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is cyclic.

Ex $G = \mathbb{Z}/2\mathbb{Z}$ size 2 cyclic
$H = \mathbb{Z}/2\mathbb{Z}$ size 2 cyclic

2, 2 not relatively prime

$\Rightarrow$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ not cyclic.