Abstract Algebra Part 2

Disclaimer: Work in progress. Portions of these written materials are incomplete.

Textbooks

- First Semester Abstract Algebra (html) by Jessica K. Sklar
- Visual Group Theory by Nathan Carter
  - Lots of good videos available on YouTube channel

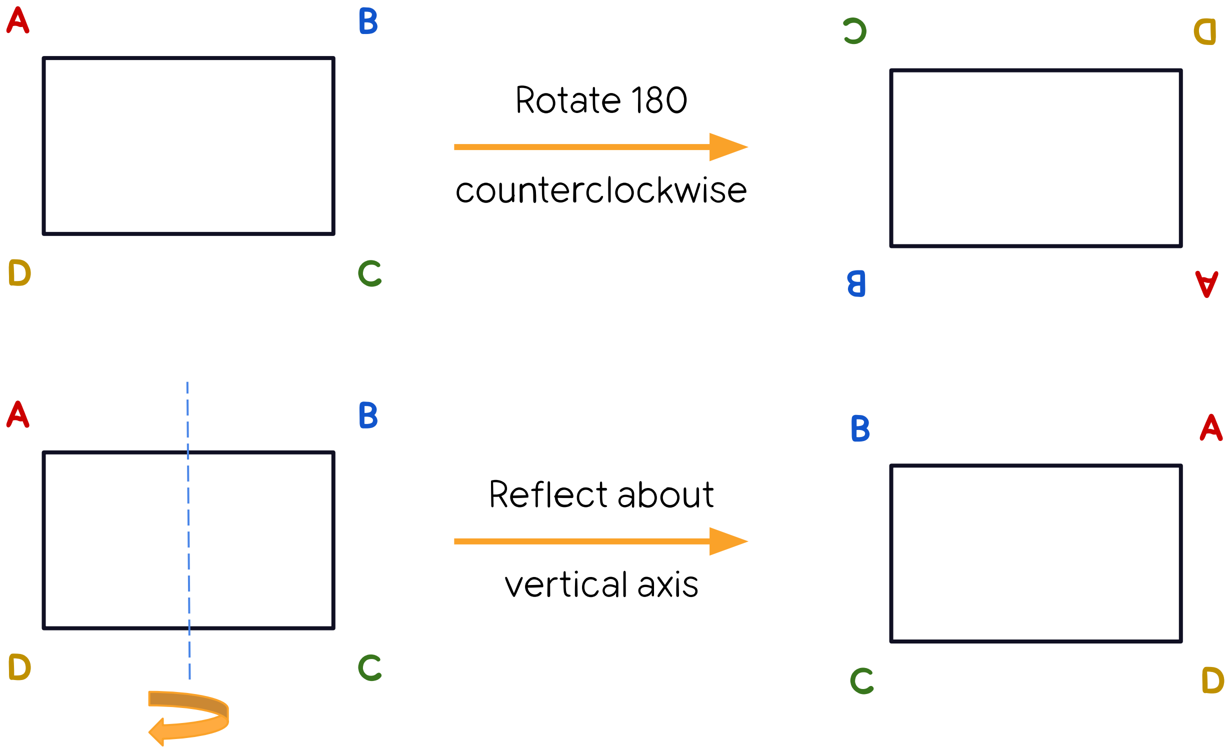
Recap of Week 1

Groups intuitively

Last time we talked about symmetries (structure preserving transformations) of objects and three important properties:

- Symmetries can be combined or composed
- Symmetries always have an inverse
- There is always an identity symmetry

Symmetries of a rectangle



$$r^2 = 1$$

$$s^2 = 1$$

Groups: Formal definition

Mathematically, a **group** is defined as a set G with an **associative** binary operation * such that:

- [**Closure**] For any two elements g, h in G, we have $g * h$ is also in G
- [**Identity**] There is an identity element e such that $g * e = g = e * g$ for all elements g
- [**Inverses**] Every element of g has a two sided inverse $g * g^{-1} = e = g^{-1} * g$

Multiplicative vs Additive notation for groups

	Multiplicative	**Additive**
Identity	1 or e	0 or e
Operation	$a * b$ or just ab	$a + b$
Associativity	$a(bc) = (ab)c$	$a + (b + c) = (a+b) + c$
Inverse	a^{-1} with $a*a^{-1} = 1 = a^{-1}a$	$-a$ with $a + (-a) = 0 = -a + a$
Element order: smallest **n** with	$a^n = 1$	$na = 0$

Abelian groups

If the group operation is always commutative, that is for all **a, b** in **G**

- [multiplicatively] $ab = ba$
- [additively] $a + b = b + a$

Niels Henrik Abel

then we say the group is **abelian**. It's common to use additive group notation for abelian groups (but not required of course).

Abelian groups are easier to work with and have a simpler structure.

Abelian vs non-Abelian groups

In non-abelian groups, inverse changes the operation order

- $1 = (ab)^{-1}(ab) \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

If the group is **abelian**, then we can rewrite

- $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ for all elements a and b

Non-abelian groups: $\mathbf{ab \neq ba}$ in general. Best we can say is $|ab| = |ba|$

- Why? If $\mathbf{|ab| = n}$ then $1 = (ab)^n = ab\ ab \ldots ab = a\,(ba)^n\,a^{-1}$
- So $(ba)^n = 1 \Rightarrow |ba| \leqslant |ab|$
- Swap a and b to get $\mathbf{|ab| \leqslant |ba| \Rightarrow |ba| = |ab|}$

Algebraic examples

Integers, Reals, and Complex numbers

Last time we talked about many geometric examples, but there are also many groups that you are likely already familiar with:

- Integers, rationals, reals, complexes with operation +, identity 0
- Integers modulo n with operation +, identity 0
- Non-zero rationals, reals, complexes with operation *, identity 1
- Matrices with operation +, identity the zero matrix
- Invertible matrices with operation *, identity is the identity matrix
- Functions on a vector space f: V → R with operation +, identity 0

Modular Integers with addition

Modular arithmetic is a concrete instantiation of a cyclic group $\mathbb{Z}_n$

- Generator: 1 (mod n) since k = 1 + 1 + … + 1 (mod n)
- Inverse: k + (–k) = 0 (mod n)
- Order of elements:
  - |0| = 1 (identity)
  - If k divides n, then the order is |k| = n/k
    - Since (n/k) * k = n = 0 (mod n)
  - Otherwise |k| = n

Modular Integers with addition

Example $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

- $|0| = 1$
- $|1| = |5| = 6$
- $|2| = |4| = 3$
- $|3| = 2$

Multiplicative notation

$$|C_6| = 6$$
$$|1| = 1$$
$$|r| = 6 = |r^{-1}| = |r^5|$$
$$|r^2| = 3 = |r^4|$$
$$|r^3| = 2$$

Modular Integers with multiplication

- Integers mod p (prime) multiplicatively form a cyclic group of size $(p-1)$
  - Usually denoted $\mathbb{Z}_p^{\times}$
- Inverses: need b such that $ba = 1 \pmod{p}$
- Use Bezout's theorem / GCD algorithm to find inverses
  - There integers are b, m such that $ba + mp = \gcd(a, p) = 1$
  - Take modulo p, then $ba + 0 \;\; = 1 \pmod{p}$
  - So $b \pmod{p}$ is the (multiplicative) inverse of $a \pmod{p}$
  - Works for prime modulus because $\gcd(a, p) = 1$ for $0 < a < p$

Modular Integers with multiplication

- Integers mod p (prime) multiplicatively form a cyclic group of size (p-1)
  - Usually denoted $\mathbb{Z}_p^{\times}$
- Inverses: need b such that ba = 1 (mod p)
- Use Bezout's theorem / GCD algorithm to find inverses
  - There integers are b, m such that ba + mp = gcd(a, p) = 1
  - Take modulo p, then ba + 0 = 1 (mod p)
  - So b (mod p) is the (multiplicative) inverse of a (mod p)
  - Works for prime modulus because gcd(a, p) = 1 for 0 < a < p

Example: For p = 11, these are the multiplicative inverses

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

Subgroups

Subgroups

Defn: A **subgroup** H of a group G is a subset of G that satisfies all the properties of a group within itself. We denote this by H <= G

- In the dihedral group $D_n = \langle r, s \mid r^n = 1 = s^2, rs = sr^{-1}\rangle$
    - Reflections: $\{1, s\}$ is a subgroup of order 2
        - $\{1, r^k s\}$ is also a subgroup of order 2, for any k (the other reflections)
    - Rotations: $\{1, r, r^2, \ldots, r^{n-1}\}$ is a subgroup of order n
- In the symmetric group of permutations S_n we have that S_{n-1} is a subgroup of order $(n-1)!$
    - Fix any element and allow the others to permute by any element of S_{n-1}
    - Also means that $S_k \leqslant S_n$ for all $0 \leqslant k \leqslant n$
- $\{1\}$ and G are always subgroups of any group

Subgroup generated by an element

Given an element g of G, the **subgroup generated by the element** is

- $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ where $|g| = n$
- Orders: $|\langle g \rangle| = |g|$

Examples:

- D_n has $\langle s \rangle = \{1, s\}$ and $\langle r \rangle = \{1, r, r2, \ldots, rn{-}1\}$
- Integers $\mathbb{Z} = \langle 1 \rangle$ is the infinite cyclic group
  - Even integers: $\langle 2 \rangle \leqslant \mathbb{Z}$
- Modular integers: $\mathbb{Z}_p = \langle 1 \ (\mathrm{mod}\ n) \rangle$
- Identity subgroup: $\langle e \rangle = \{e\}$

Subgroup generated by an element

Given an element g of G, the **subgroup generated by the element** is

- $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ where $|g| = n$
- Orders: $|\langle g \rangle| = |g|$

Examples:

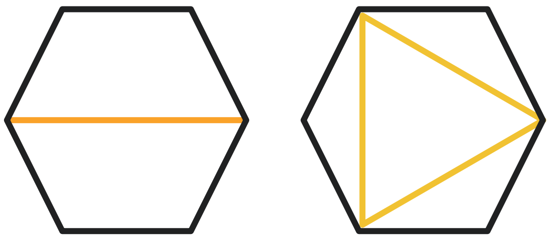
- D_n has $\langle s \rangle = \{1, s\}$ and $\langle r \rangle = \{1, r, r2, \dots, rn-1\}$
- Integers $\mathbb{Z} = \langle 1 \rangle$ is the infinite cyclic group
  - Even integers: $\langle 2 \rangle \leqslant \mathbb{Z}$
- Modular integers: $Z_n = \langle 1 \pmod{n} \rangle$
- $\langle e \rangle = \{e\}$

Subgroups of finite cyclic groups

- One for each divisor of the group order

Example $\mathbb{Z}_6$:

- $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$
- $\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle$
- $\langle 3 \rangle = \{0, 3\}$

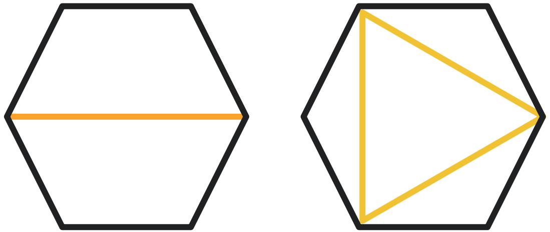


Subgroups of finite cyclic groups

- One for each divisor of the group order

Example $\mathbb{Z}_6$:

- $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$
- $\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle$
- $\langle 3 \rangle = \{0, 3\}$



Example $\mathbb{Z}_{12}$:

- $\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$ (no shared divisors with 12 except 1 and 12)
- $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\} = \langle 10 \rangle$
- $\langle 4 \rangle = \{0, 4, 8\} = \langle 8 \rangle \leqslant \langle 2 \rangle$
- $\langle 3 \rangle = \{0, 3, 6, 9\} = \langle 9 \rangle$
- $\langle 6 \rangle = \{0, 6\} \leqslant \langle 2 \rangle$ and also $\leqslant \langle 3 \rangle$

Subgroups of finite cyclic groups

$C_{pq} = \langle r \rangle$, **p** and **q** both prime and different

Subgroups: $\langle 1 \rangle$, $\langle r^p \rangle$, $\langle r^q \rangle$, C_{pq}

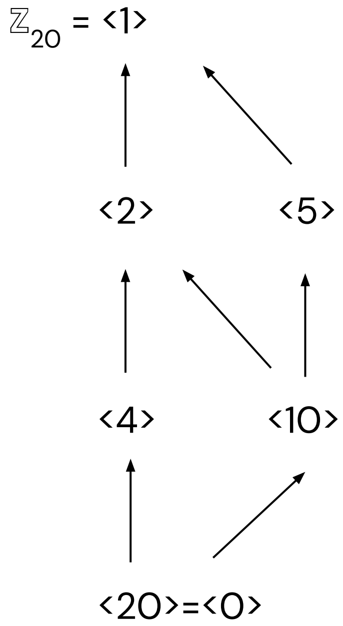
[Fundamental theorem of cyclic groups] For Cyclic groups, there is exactly one subgroup for every divisor d of $|C_n|$, the subgroup generated by $\langle r^{n/d} \rangle$

Subgroup Lattice

The subgroups of a group fit together into a lattice (as subsets)

Here’s the lattice for the cyclic group of order 20 = 2 * 2* 5

The divisors of 20 are 1, 2, 4, 5, 10, and 20

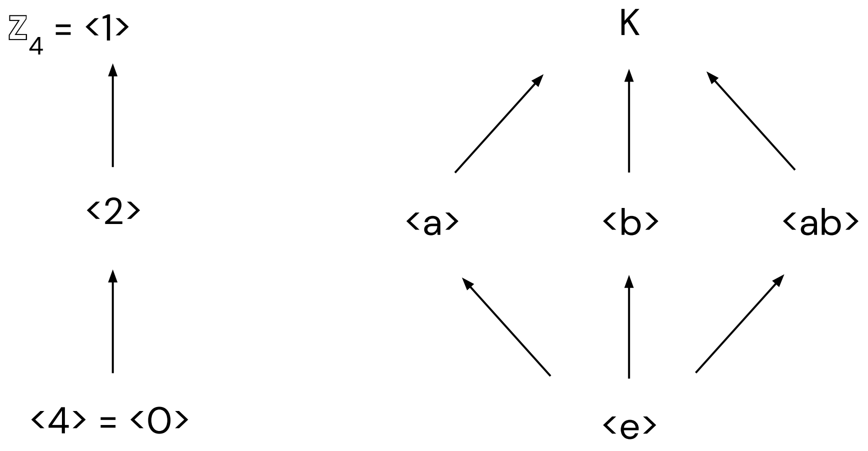


Subgroup Lattice

$\mathbb{Z}_4$ vs Klein four group K

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$
- $\langle 2\rangle = \{0, 2\}$

$K = \{e, a, b, ab\}$
- $\langle a\rangle = \{e, a\}$
- $\langle b\rangle = \{e, b\}$
- $\langle ab\rangle = \{e, ab\}$



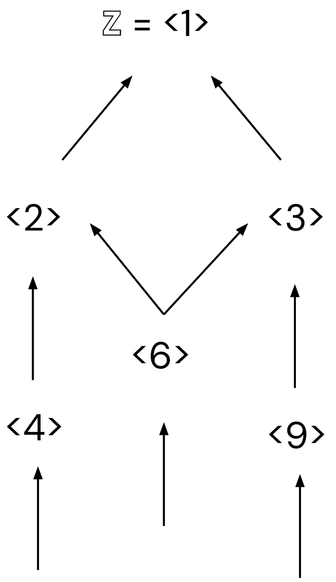
These groups are distinct but both of order 4

Subgroups of infinite cyclic group (integers)

- Every element has infinite order (except 0)

Example $\mathbb{Z}$:

- $\mathbb{Z} = \langle 1 \rangle$
- $\langle 2 \rangle = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}$
- $\langle 3 \rangle = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = 3\mathbb{Z}$
- $\langle m \rangle = \{\ldots, -2m, -m, 0, m, 2m, \ldots\} = m\mathbb{Z}$



Small excerpt of subgroup lattice

Subgroups of integers

We can also look at the subgroup generated by more than one element:

- [multiplicatively] $\langle a, b \rangle = \{1, a, b, ab, ba, a^2, b^2, aba, bab, ab^2, b^2a, \dots$ and all inverses$\}$ = all words formed from a, b, a^{-1}, b^{-1}
- [additively] $\langle a, b \rangle = \{0, a, b, a + b, a - b, b + a, b - a, 2a, 2b, \dots$ and all inverses$\}$

Example: In the integers $\mathbb{Z}$, all subgroups can be generated by a single element

- $\langle 2, 4 \rangle = \langle 2 \rangle$ because $\langle 4 \rangle \leqslant \langle 2 \rangle$
- $\langle 2, 3 \rangle = \mathbb{Z}$ because $3-2 = 1$
- $\langle a, b \rangle = \langle \gcd(a, b) \rangle$
  - (Bezout's theorem) there are n and m such that $\gcd(a, b) = na + mb$

Subgroups of the Symmetric group

- Symmetric groups (permutations) have many subgroups
- $S_k \leqslant S_n$ for all $k \leqslant n$
- [Cayley's theorem] Every finite group of order n is a subgroup of S_n

Subgroup lattice of S_4 (wikipedia)

Cosets and Lagrange’s Theorem

Cosets

The even integers are a subgroup

- $2\mathbb{Z}$ = {2a for all a in Z} = {..., −2, 0, 2, 4, ...} $\leqslant \mathbb{Z}$

What about the odd integers?

- Odds = {..., −3, −1, 1, 3, ...} are not a subgroup, rather a **coset**
- $2\mathbb{Z} + 1$ = {2a + 1 for all a in Z} = Odd integers
- $(2\mathbb{Z}) \cup (2\mathbb{Z} + 1) = \mathbb{Z}$

More generally

- $m\mathbb{Z} + 1, \ldots, m\mathbb{Z} + (m-1)$ are cosets of $m\mathbb{Z}$
- The cosets partition $\mathbb{Z}$ (distinct and cover completely)

Cosets go back to Évariste Galois

Cosets - example

Defn: Let $H \leqslant G$, the cosets of H are formed by g in G

- $gH = \{g * h \mid h \in H\}$
- $g + H = \{g + h \mid h \in H\}$

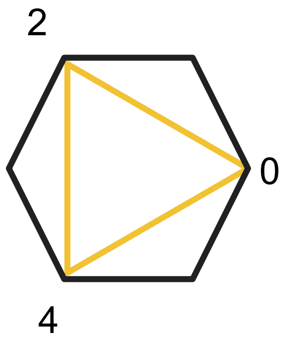
Cosets – example

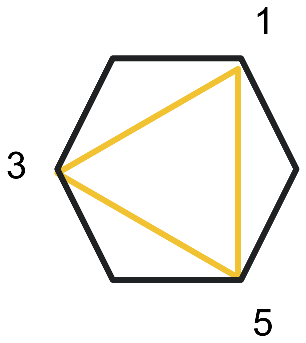
Defn: Let $H \leqslant G$, the cosets of H are formed by g in G

- $gH = \{g * h \mid h \in H\}$
- $g + H = \{g + h \mid h \in H\}$

Cosets of $\langle 2 \rangle \leqslant C_6$:

- $\langle 2 \rangle = \{0, 2, 4\}$
- $\langle 2 \rangle + 1 = \{1, 3, 5\}$
- $\langle 2 \rangle + 2 = \{2, 4, 6 = 0\} = \langle 2 \rangle$
- Generally true that **h + H = H** when **h in H** (subgroup closure)





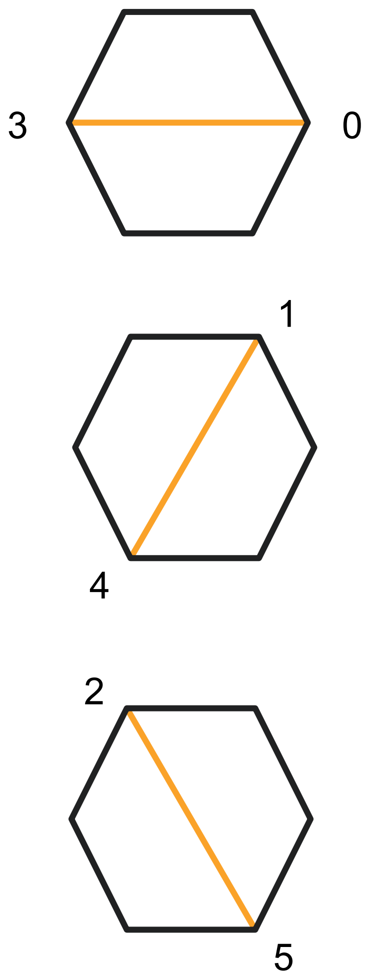
Cosets - example

Defn: Let $H \leqslant G$, the cosets of H are formed by g in G

- $gH = \{g * h \mid h \in H\}$
- $g + H = \{g + h \mid h \in H\}$

Cosets of $\langle 3 \rangle \leqslant C_6$:

- $\langle 3 \rangle = \{0, 3\}$
- $\langle 3 \rangle + 1 = \{0+1, 3+1\} = \{0, 4\}$ (not a subgroup)
- $\langle 3 \rangle + 2 = \{2, 5\}$ (not a subgroup)



Lagrange's Theorem for finite groups

We observed that

- Cosets of a subgroup **H** all have the same size **|H| = |gH|**
- Cosets partition the group: **G = ∪ (gH)** and they are distinct

These are generally true for all groups, and together they prove:

- [Theorem] Order of a subgroup divides the order of the group

Why? All cosets have the same size and partition the group means that
|G| = (number of cosets) * |H|, so |H| divides |G|

Lagrange’s Theorem

- [Theorem] Order of a subgroup divides the order of the group
- [Corollary] for a in G, the order of a divides |G|
  - Apply Lagrange’s Theorem to subgroup <a> and use |<a>| = |a|

With Lagrange’s theorem, we have a limit on the form subgroups of finite groups can take:

- Only subsets where the size is a divisor of G are candidates for subgroups

Theorem has several useful applications in addition to the corollary above

Application: Fermat's little theorem

- Integers mod p (prime) multiplicatively for a cyclic group of size (p–1)
- $\langle a \rangle$ where $|a| = k$ is a subgroup, so by Lagrange k divides (p–1)
- So $nk = (p-1)$ for some positive integer n and we have that
- $a^{p-1} = a^{nk} = (a^k)^n = 1^n = 1 \pmod p$

Example: Let $p = 13$, then $a^{12} = 1 \pmod{13}$ by Fermat's little theorem.

We can then simplify other calculations:

$$\begin{aligned} a^{125} \pmod{13} &= (a^{12})^{10} a^5 \pmod{13} \\ &= 1^{10} * a^5 \pmod{13} \\ &= a^5 \pmod{13} \end{aligned}$$

Cauchy's Theorem

- Based on what we've seen from cyclic groups, you might guess:
  - For any divisor d of the group order |G| that there is a corresponding subgroup order d
  - This would be a converse to Lagrange's theorem
- But we've already seen some counterexamples
  - Klein four group has no element or subgroup of order 4
  - Dihedral group has no element or subgroup of order 2n

However, there are some partial converses:

- [**Cauchy's theorem**] There's an element of order p for every ***prime*** divisor p of the order |G| of the group G
  - So there's a subgroup of order p (generated by the element)
- [**Sylow's first theorem**] If $|G| = p^k m$ where p does not divide m then there are subgroups of size p^k

Example: Groups of order p (prime)

Suppose G is a group and |G| = p for some prime p (not necessarily cyclic)

- [Lagrange] Then G can only have subgroups of size 1 and p
- [Cauchy] Since p is prime and p divides |G|, there is an element a with order p
- Then it must be the case that |G| = <a> since |<a>| = p must be all the elements in the group

So there’s only one “distinct” group of size p. Primality is necessary: for n=4, where there are two distinct groups (cyclic group and Klein four group)

Subgroups – Summary

With these theorems – Lagrange, Cauchy, and Sylow – the subgroups of a smallish finite groups can usually be worked out, and often we can classify all the groups of a certain order

Subgroups – Summary

Despite these and other powerful theorems, the number of groups of a given finite order is still an open question (and very hard!)

- There are 49,487,365,422 groups of order 1024 [source]

Subgroups – Summary

Despite these and other powerful theorems, the number of groups of a given finite order is still an open question (and very hard!)

- There are 49,487,365,422 groups of order 1024 [source]

Group homomorphisms

Homomorphisms

Main idea: symmetries of symmetries – we can learn about groups by studying their structure preserving transformations

What does it mean for a transformation to preserve the structure of a group? The function needs to respect the group operation.

Defn: A function $f: G \to H$ is a **homomorphism** if

- (multiplicative) $f(a *_G b) = f(a) *_H f(b)$
- (additive) $f(a +_G b) = f(a) +_H f(b)$

Homomorphic Encryption

A homomorphic encryption method is one that allows computations to be performed on encrypted data without decrypting

If **f** were some encryption function and the following formula was true:

$$f(a * b) = f(a) * f(b)$$

then we could multiply encrypted values and get the result (encrypted) without decrypting

Very active area of research for privacy-preserving computation.

Homomorphisms

What about the other group structure, like identity and inverses? Those follow from $f(a * b) = f(a) * f(b)$

- A homomorphism always **preserves the identity.**
- Let $f: G \to H$ be a homomorphism. Then:
    - $e_G = e_G * e_G$
    - $f(e_G) = f(e_G) * f(e_G)$
    - $(f(e_G))^{-1} f(e_G) = (f(e_G))^{-1} f(e_G) * f(e_G)$
    - $e_H = f(e_G)$

Homomorphisms

What about the other group structure, like identity and inverses? Those follow from $f(a * b) = f(a) * f(b)$

- A homomorphism always **preserves inverses.**
- Let $f: G \rightarrow H$ be a homomorphism. Then:
  - $e_G = a\ a^{-1} = a^{-1}a$
  - $f(e_G) = f(a\ a^{-1}) = f(a^{-1}a)$
  - $e_H = f(a)\ f(a^{-1}) = f(a^{-1})\ f(a)$
  - Which means that $f(a^{-1})$ is the inverse of $f(a)$ in H

Homomorphism Examples

- $f: \mathbb{Z} \to \mathbb{Z}$, $f(a) = ma$
  - $f(a + b) = m(a+b) = ma + mb = f(a) + f(b)$

- $f: \mathbb{Z} \to \mathbb{Z}_p$, $f(a) = a \bmod (p)$

- Exp and log
  - exp: $(\mathbb{R}, +) \to (\mathbb{R}^+, *)$ $e^{a+b} = e^a e^b$
  - log: $(\mathbb{R}^+, *) \to (\mathbb{R}, +)$ $\log(ab) = \log(a) + \log(b)$

- Determinant: Invertible NxN matrices to non-zero (multiplicative) reals
  - $\det(AB) = \det(A) \det(B)$, also implies that $\det(A^{-1}) = \det(A)^{-1} = 1 / \det(A)$

- Identity map: $f(g) = e$
  - $f(ab) = e = e * e = f(a) f(b)$

Homomorphism Non-Examples

$f: \mathbb{Z} \to \mathbb{Z}$, $f(a) = a + k$ (where $k \neq 0$)

- Doesn't respect group operation (integer addition)
- $f(a + b) = a + b + k \neq (a + k) + (b + k) = f(a) + f(b)$

$f: \mathbb{Z} \to \mathbb{Z}$, $f(a) = a^2$

- Also doesn't respect group operation (integer addition)
- $f(a + b) = (a + b)^2 = a^2 + 2ab + b^2 \neq a^2 + b^2 = f(a) + f(b)$

$f: D_n \to D_n$, $f(r) = s$ and $f(s) = r$

- Doesn't preserve order (unless $n = 2$)
- Doesn't respect the relation $rs = sr^{-1}$

Image of a Homomorphism

The **image of a homomorphism** is defined just like the image of a function:

$f(G) = \{f(g) \text{ for } g \text{ in } G\}$

- The image $f(G)$ is a subgroup of H
  - If $a_1 = f(g_1)$ and $a_2 = f(g_2)$ then $a_1a_2 = f(g_1)f(g_2) = f(g_1g_2)$ is also in the image
  - Lagrange's theorem implies that $|f(G)|$ divides $|G|$ and $|H|$
- More generally, homomorphisms carry subgroups to subgroups
  - If $G' \leqslant G$ then $f(G') \leqslant H$, so subgroup lattices are preserved (or collapsed)
- It's also true that $|f(g)|$ divides $|g|$
  - If $|g| = n$ then $(f(g))^n = f(g^n) = e$, so $|g|$ is a multiple of $|f(g)|$
  - The order of an element can only get smaller

Isomorphisms

An isomorphism is a homomorphism that is also bijective. This means that the two groups are in some sense “the same” abstractly

Examples:

- $\exp(x) = e^x$ and (natural) Log are inverse functions (so bijective) and homomorphisms, so they are isomorphisms between $(\mathbb{R}, +)$ and $(\mathbb{R}+, *)$

- $f(x) = x^3$ and $g(x) = x^{1/3}$ are isomorphisms from $\mathbb{R}$ to $\mathbb{R}$
  - Multiplicatively but not additively

- The cyclic groups $C_n = \langle r \rangle$ and modular integers $\mathbb{Z}_n$ (additively) are iso
  - $f(r) = 1 \bmod (p)$
  - $f(r^m r^n) = m + n \pmod p = f(r^m) + f(r^n) \pmod p$

Kernel of a homomorphism

The kernel of a homomorphism is all the elements that get mapped to the identity: $\ker(f) = \{g \text{ in } G \mid f(g) = e_H\}$

- ker(f) is a subgroup of G
  - Contains identity: $f(e_G) = e_H$
  - Closure: If $f(a) = e_H = f(b)$ then $f(ab) = f(a)f(b) = e_H e_H = e_H$

- [Lagrange's Theorem] |ker G| divides |G|

- Cosets of Ker f partition G and we'll see that
  - $|G| = |\ker f|\,|f(G)|$
  - So $|f(G)|$ also divides $|G|$

Kernels and Injectivity

A homomorphism $f: G \to H$ is injective if and only if $\ker(f) = \{e\}$

- Injective $\to \ker(f) = \{e\}$ since $f(e) = e$
- Suppose $\ker(f) = \{e\}$ and $f(g) = f(h)$
  - Then $f(gh^{-1}) = e$, so gh^{-1} is in the kernel
  - So $gh^{-1} = e$ and so $g = h \to$ injective

More generally, f is a $|\ker(f)|$ to one mapping

- k in $\ker(f) \to f(g) = f(g) + f(k) = f(g + k)$

Example: $f: \mathbb{Z}_{16} \to \mathbb{Z}_4$ given by $f(x) = 4x$ is a 4 : 1 mapping

- $\ker(f) = \{0, 4, 8, 12\}$ $\leftarrow$ any kernel element times 4 is 0 mod (16)

Example: Roots of Unity and the Circle Group

Recall the circle group C: rotation by any angle

$$r_\theta = e^{i\theta}$$

Roots of unity are described by

$$x = e^{\frac{2\pi i}{n}}$$

Example: Roots of Unity and the Circle Group

Recall the circle group C: rotation by any angle

$$r_\theta = e^{i\theta}$$

Roots of unity are described by

$$x = e^{\frac{2\pi i}{n}}$$

Define a homomorphism by f: C → C with $f(x) = x^n$

- ker(f): need $x^n = e^{2\pi i}$ so the kernel consists of the n-th roots of unity
- Shows that n-th roots are a subgroup of C

More Isomorphism Examples

If G abelian, $f: G \to G$ given by $f(g) = g^{-1}$ is a homomorphism

- Recall if G abelian then: $(ab)^{-1} = b^{-1} a^{-1} = a^{-1}b^{-1}$
  - Shows f is a homomorphism $f(ab) = (ab)^{-1} = a^{-1}b^{-1} = f(a)f(b)$
- It's an isomorphism
  - $\mathrm{Ker}(f) = \{e\}$ since $g^{-1} = e \Rightarrow g = e$, so it's injective
  - Onto since every element has a unique inverse

For any group G, $f_h: G \to G$ given by $f_h(g) = hgh^{-1}$ is an isomorphism from G to G

- These are called "inner automorphisms" by conjugation

Homomorphisms Summary

- Homomorphisms preserve group structure
- Image and kernel are subgroups of the domain and codomain
- If bijective, we call it a isomorphism

What’s Next!

Check out these videos on the visual group theory channel

- Cayley Graphs
- Homomorphisms and isomorphisms

Exercises

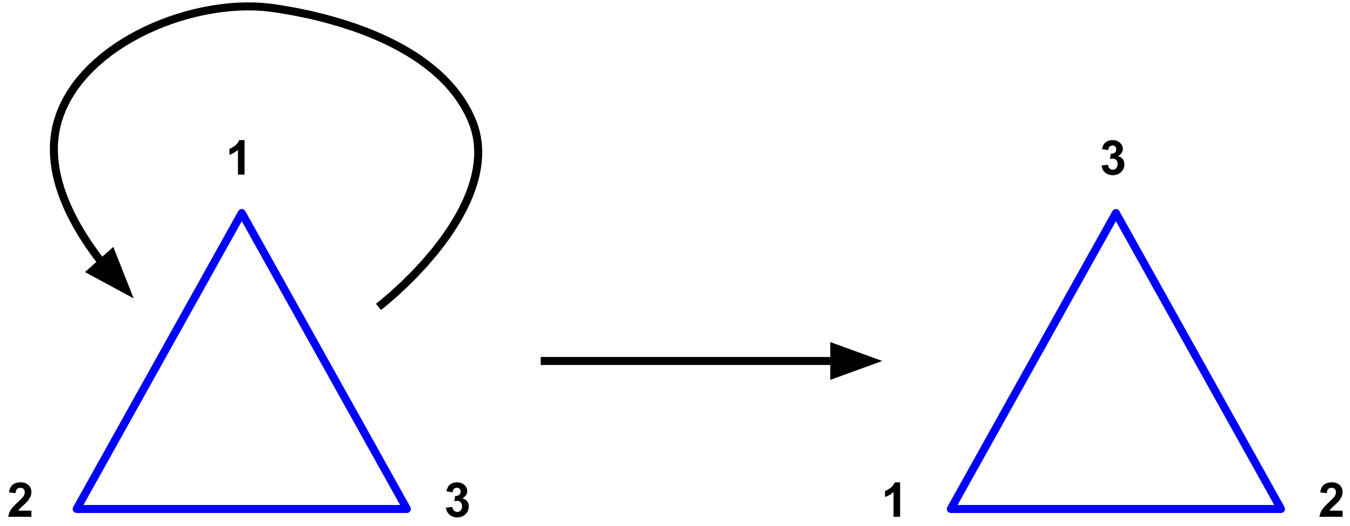
Agenda

- Dihedral groups
  - Basic operations
  - Some interesting subgroups
- Symmetric groups
  - Definition
  - Cycle notation and basic operations
- The Fermat-Euler Theorem
  - Review: Fermat's Little Theorem
  - The Euler totient function
  - The Fermat-Euler Theorem

Dihedral Groups: Symmetries of regular polygons

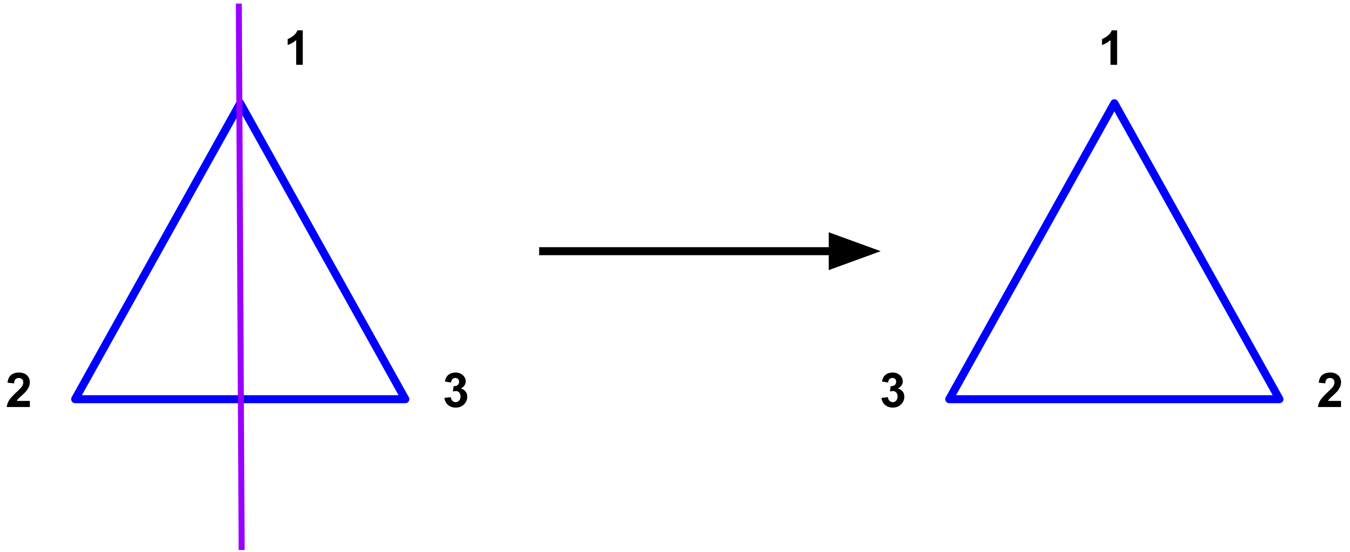
Example: plane symmetries of a regular triangle

Consider an equilateral triangle which lies in the plane. It has some symmetries:
(counterclockwise) Rotation by 120 degrees:



Reflection of a triangle

Reflection across the vertical axis:



Some standard mathematical notation for symmetries of a regular polygon

The group of symmetries of an equilateral triangle is called the **dihedral group with 6 elements**, and is written D_3 (sometimes D_6).

- Rotation by 120 degrees is often named “r” (rotation)
- Reflection across some axis (say the vertical axis) is often named “s”.

This is all naturally generalizable to regular n-gons, and their symmetry group is written D_n.

Exercise: Group operations in D_3

How are r, s related to each other? In particular:

- What happens when you multiply r by itself repeatedly? What about s?
- Convince yourself that $rs \neq sr$. Does $rs = sr^i$ for some value of i? Draw diagrams illustrating how rs vs. sr act on a triangle that show this.

Check that every element of D_3 can be uniquely written in the form $s^i r^j$, where $i = 0$ or 1, $j = 0, 1,$ or 2.

Say you multiply two elements of the above form together. (eg, $(sr) * (sr^2)$) How can you convert this product to the form $s^i r^j$?

Homework exercise

Verify that D_n is a group (at the least, try enumerating elements of symmetries of a square or regular hexagon and convincing yourself they satisfy group axioms).

What are the analogous equations to those on the previous slide for D_n? Can you find an explicit description of every element of D_n as a product of various numbers of r, s?

Exercise: $\mathbb{Z}_n$ inside D_n

Suppose you multiply r by itself repeatedly. You end up with the subset $\{1, r, r^2, \ldots, r^{n-1}\}$ inside of D_n.

Exercise: Verify that this is a subgroup of D_n.

Exercise: Verify that the function $\varphi: \mathbb{Z}_n \to D_n$ given by $\varphi([i]_n) = r^i$ is a homomorphism (recall, this means checking: $\varphi(x + y) = \varphi(x) * \varphi(y)$).

Note that φ is 1-1 (eg $f(x) = f(y)$ implies $x = y$). We call φ an *embedding* of $\mathbb{Z}_n$ into D_n.

Trivia question: Are there any other cyclic groups that are embedded inside of D_n?

Symmetric Group: Permutations of a finite set

Permutations: Definition

Consider a finite set S, which we will just label with positive integers, like {1, 2, ..., n}. A permutation is a rearrangement of the integers in S.

Example: $n = 3$. The rearrangement $1 \to 2$, $2 \to 3$, $3 \to 1$ is a permutation, but the function $1 \to 2$, $2 \to 2$, $3 \to 3$ is not, because both 1 and 2 go to 2.

More formally,

A **permutation** of S is a function $p: S \to S$ which is

- 1 to 1: if $p(x) = p(y)$, then $x = y$. In other words, distinct elements map to distinct elements.
- surjective: for every y, there exists some x such that $p(x) = y$.

Group of Permutations

Suppose n is a fixed positive integer. The set of permutations of $\{1, 2, \ldots, n\}$ is denoted S_n, and form a group under function composition. (Homework: check group axioms!)

Example: S_2 has two elements: the permutations p_1, p_2, where $p_1(1) = 1$, $p_1(2) = 2$, and $p_2(1) = 2$ and $p_2(2) = 1$. p_1 is the identity, and $p_2 \circ p_2 = p_1$.

The group S_n is called the **symmetric group** on n elements.

You can think of a permutation as a “symmetry” of $\{1, 2, \ldots, n\}$, in that a permutation keeps $\{1, 2, \ldots, n\}$ invariant.

Cycle Notation

Cycle notation is a compact way to write down a permutation.

A *cycle* is written as $(a_1\ a_2\ \ldots\ a_k)$, where a_i are distinct integers, and represents the permutation which takes a_i to a_{i+1} and a_k to a_1. Other integers are fixed.

A general permutation can be written as a product of disjoint cycles, essentially uniquely (homework exercise!).

Examples:

- (1 3 5) in S_5 represents the permutation 1 -> 3, 2 -> 2, 3 -> 5, 4 -> 4, and 5 -> 1.
- (1 3)(2 4) in S_4 represents the permutation 1 -> 3, 2 -> 4, 3 -> 1, 4 -> 2.

Basic calculations with cycles

Cycle notation makes it easy to write down inverses: just reverse the order in each cycle.

Example: $(1\ 3\ 2\ 5\ 4)^{-1} = (1\ 4\ 5\ 2\ 3)$.

Products of (non-disjoint) cycles are a little harder to compute. Examples:

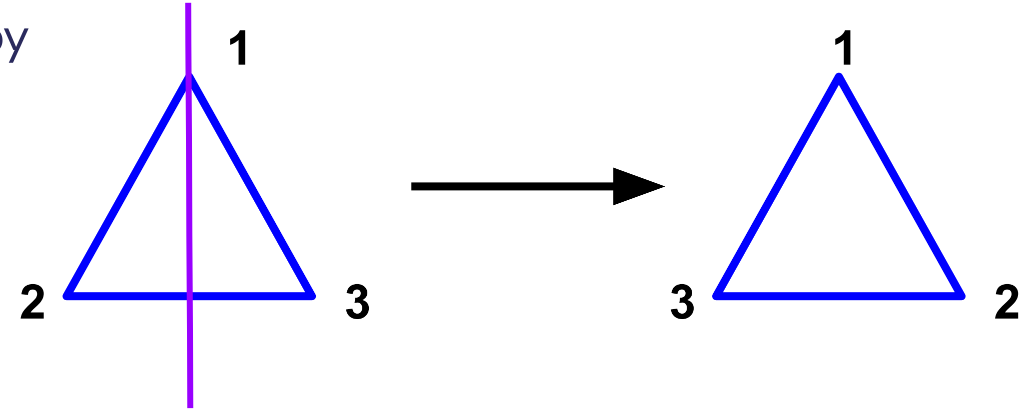
- $(1\ 2)(1\ 3) = (1\ 3\ 2)$. To see this: $(1\ 2)(1\ 3)\ 1 = (1\ 2)\ 3 = 3$, $(1\ 2)(1\ 3)\ 2 = (1\ 2)\ 2 = 1$, $(1\ 2)(1\ 3)\ 3 = (1\ 2)\ 1 = 2$.
- $(1\ 2\ 3)(2\ 4) = (1\ 2\ 4\ 3)$.

Dihedral groups as subgroups of S_n

Think back to D_3, the symmetries of an equilateral triangle.

If we label the vertices of the triangle with 1, 2, 3, then each element of D_3 can be thought of as a permutation of {1, 2, 3}, depending on how the symmetry rearranges the vertices. For example:

the element of D_3 represented by the diagram on the right can be thought of as the permutation swapping 2 and 3 (and keeping 1 fixed).



Exercises: D_3 vs. S_3

Exercise: Show that D_3 and S_3 are identical groups via the identification f in the previous slide. In other words, show that f: $D_3 \rightarrow S_3$ preserves group structure, ie, $f(g*h) = f(g) * f(h)$ for every pair of elements f, $g \in D_3$, and f is bijective.

- What is f(id)?
- Pick some labeling of the vertices of an equilateral triangle. Write down f(r) and f(s) in cycle notation.
- Are there any other maps f which satisfy the above properties? If so, how can you find them?

Exercise: D_n in S_n

- Extend the D_3 map above to a “natural” embedding of D_n in S_n: in other words, find an injective homomorphism f: D_n -> S_n that arises from identifying a symmetry of an n-gon with a permutation on {1, 2, ..., n}. Write down f(r) and f(s) for general D_n in cycle notation.
- It is a fact that there are 3 different subgroups of S_4 which are embeddings of D_4. Can you write them down in cycle notation? That is, can you find three 1-1 homomorphisms f: D_4 -> S_4?

The Fermat–Euler Theorem

Review: Fermat's Little Theorem

Recall from Tuesday's lecture:

> **Fermat's Little Theorem**: Let p be a prime, and let a be an integer not divisible by p. Then $a^{p-1} \equiv 1 \bmod p$.

Sketch of proof: apply Lagrange's Theorem to the subgroup $\langle a \rangle$ sitting inside $\mathbb{Z}_p{}^*$.

The multiplicative group $\mathbb{Z}_n$*.

Recall from last week the exercise about how to make $\mathbb{Z}_n$* a group: remove all elements $[a]_n$ where $\gcd(a, n) > 1$.

Examples:

- $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$
- $\mathbb{Z}_9^* = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$

The Euler totient function

What is the size of $\mathbb{Z}_n^*$? Evidently it is the number of integers in {1, 2, …, n} coprime (that is, gcd(a, n) = 1) to n. We call this number **φ**(n), and **φ** is called the ***Euler totient function***.

How do we compute **φ**(n) without actually going through every integer 1, 2, .., n and checking if they are co-prime to n?

Exercises: Values of the Euler totient function

Exercise: Show that, if p is a prime and n a positive integer, then $\varphi(p^n) = p^n - p^{n-1}$.

Exercise: Now suppose n and m are positive integers with $\gcd(n, m) = 1$. What can you say about the relationship between $\varphi(nm)$ and $\varphi(n)$, $\varphi(m)$? (Try working this out explicitly for small values of n and m, like $n = 3$, $m = 2$, or $n = 3$, $m = 4$, etc.).

Exercise: Compute $\varphi(900)$.

The Fermat-Euler Theorem

Fermat's Little Theorem is generalizable to $(\mathbb{Z}/n\mathbb{Z})^*$. The major changes are:

- $(\mathbb{Z}/n\mathbb{Z})^*$ has size $\boldsymbol{\varphi}(n)$.
- a has to be coprime to n.

Then:

Fermat-Euler Theorem: If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \bmod n$.

(Notice, if $n = p$, we get exactly Fermat's Little Theorem).

One application we will see in two weeks is in a small but critical part of the RSA cryptosystem.