Groups

Aryan

March 12, 2023

Contents

1 Groups Basics **2**
- 1.1 Binary operations and groups . . . 2
  - 1.1.1 Operations . . . 2
  - 1.1.2 Groups . . . 4
- 1.2 Modular arithmetic and the group $\mathbb{Z}_n$ . . . 5

2 Cyclic Groups **8**

3 Symmetric Groups **11**

4 Subgroups **14**
- 4.0.1 The subgroup test . . . 14
- 4.0.2 Cyclic subgroups . . . 15
- 4.0.3 Cosets and Lagrange's Theorem . . . 15
- 4.1 Normal subgroups . . . 17
- 4.2 Quotient groups . . . 19
  - 4.2.1 The first isomorphism theorem . . . 20
  - 4.2.2 Kernel and image of homomorphism . . . 20
  - 4.2.3 The First Isomorphism Theorem . . . 21

Chapter 1

Groups Basics

1.1 Binary operations and groups

1.1.1 Operations

Say we have the set G, then a binary operation on G is a function

$$\circ : G \times G \to G$$

Examples

Say we have the integers under addition, then the + is a binary operation as it takes in two inputs from the integers and returns something in the integers.

On the other hand say we have subtraction on the natural numbers, this is not a binary operation as we can have 3 - 10 and this does not result in something in the natural numbers.

Point

Binary operations are not necessarily commutative

(Surly this is obvious, say we have matrix multiplication, this is a binary operating but is it not commutative.)

Cayley tables

For some reason we do just skim past this, which is weird cos it is quite useful, but what it is, is a table where you write out all of the possible compositions.

In each row and col you should not have repeats.

Associative

Basically if we have 3 elements g, h, k then:

$$g \circ (h \circ k) = (g \circ h) \circ k$$

For example shit like regular addition and multiplication are associative, but subtraction is not

Commutative

Basically if we have 2 elements g, h then:

$$g \circ h = h \circ g$$

For example shit like regular addition and multiplication are commutative as well , but matrix multiplication is not

Identity

Say we have a group and a operation $\circ$ then there is a identity element e such that

$$g \circ e = g = e \circ g$$

So in other words, there is an element such that any element "binary operated" with that element will return itself.

THE IDENTITY ELEMENT IS UNIQUE - THIS FOLLOW FROM A SIMPLE PROOF:

FSOC assume is is not unique eg there is a e and a e' such that

$$e = e \circ e' = e'$$

So it has to be unique, as they are the same.

Inverse

This one kind of evolves from the inverse.
Under a binary operation there must be a element such that

$$g \circ g^{-}1 = e$$

For example lets say that we have the naturals under multiplication, then apart from one none of them have a inverse as say we take 2, the inverse is 1/2 which is not in the naturals.

The inverse is also unique, and this follow from another easy proof:
FSOC
Say the inverse is not unique therefore take arbitrary h, then h' and h" are both inverses and h' $\neq$ h"

So we can write:

$$h' = h'(hh'') = (h'h)h'' = h'''$$

So they are the same

1.1.2 Groups

A group is a set G with under binary operation $\circ$ such that it is :

- associative
- has an inverse
- has an identity

Order of groups

Say we have group G which has n diffrent elements, then we can write

$$\|G\| = n$$

which means that the order of G is n

If we actually have an n, this means that the group is finite else it is infinite.

Abelian groups

If a group is commutative then it is Abelian.

Applications of the group axioms

Using the group axioms we can prove $(g^-1)^-1 = g$ (the inverse of g^-1 is g).

We know that the inverse is unique.
We also know that

$$g \circ g^-1 = e$$

$$g^-1 \circ (g^-1)^-1 = e$$

So this means that $g = (g^-1)^-1$, as the inverse if unique.

In a similar way, say we wanted to prove that $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$
So again we know that the inverse is unique. So if we show that $(g \circ h) \circ (h^{-1} \circ g^{-1}) = e$ then that suffices to show that is the inverse.

So by associativity we can write

$$g \circ (h \circ h^{-1}) \circ g^{-1} = e$$

$$g \circ g^{-1} = e$$

$$e$$

and as the inverse is unique this suffices as the proof.

Multiple compositions

Say we have g^n, where n is a integer, then

If n = 0, = e
if n ¿ 0, = g ∘ g ∘ g ... n times
if n ¡ 0, = $g^-1 \circ g^-1 \circ g^-1$ ... n times

Now say we have
$g^n * g^m = g^{n+m}$
$(g^n)^m = g^{nm}$

1.2 Modular arithmetic and the group $\mathbb{Z}_n$

Basics

Say we have a, b $\in \mathbb{Z}$. Then we can say

$$a \equiv bmodn$$

Which means that when we divide a by n then the remainder is a.

Equivalence relations

- a $\equiv$ a mod n (reflexivity)
- a $\equiv$ b mod n and b $\equiv$ a mod n (symmetry)
- If a $\equiv$ b mod n and b $\equiv$ c mod n then a $\equiv$ c mod n (transitivity)

Shit to do with mods

Say we have [a], this is just the set;

$$\{b \in \mathbb{Z}, b \equiv amodn\}$$

So we can have say [a] = [a'] iff a and a' are congruent mod n.

So say we have the number n. There there are n equivalences classes, as every integer is congruent to at least one of them mod n. (As in ever integer divided by the number n will return a remainder between 0 and n-1 and this can be seen from Euclid's division lemma.)

So we can then write

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$$

Which is the set of equivalence classes mod n.

Now say we have a, a', b, b' $\in \mathbb{Z}$
and [a] = [a'] and [b] = [b']. Then:

a+b = [a' + b']

ab = [a'b']

And both of these make sense
1. Say we have [a+b]. Say we have a is in the from qr + m and b is in the form qp + c

Then if we add them, then we get:
q(r+p) + (m+c), so the congruence class will be whatever is the class of m+c

In the same way for a' an b' We may have some shit like qw + m and qu + c
Where they will need to have the same remainders as before.
So the classes will be the class of m+c.
So they will be of the same class.

A almost identical proof follows for the multiplication where it will be the class of mc for both.

Quick proof

Say we want to show $(\mathbb{Z}_n, +)$ is a Abelian group:

THEN WE NEED TO SHOW IT ITS A ACTUAL GROUP NOT JUST ABELIAN!

So identity we have the [0]
For inverse say we have [a] then we have [-a]
It is associative
And to show commutative, just use the division lemma and then use the fact that addition is commutative.

Coprimes

Say we have the set [a] and [b] such that [a][b] = 1 iff a is co-prime to n. This is because say we have co-primes. This means that

gcd(a,n) = 1

So we can write ab + nc = 1

So this means that ab $\equiv$ 1 mod n

The set with the star

We define $\mathbb{Z}_n^*$ as the set $\{[a] \in \mathbb{Z}_n : \exists [b] \in \mathbb{Z}_n suchthat [a][b] = [1]$

So basically the set of all of the shit which is coprime to n.

Another quick proof

Say we have the set of $(\mathbb{Z}_n^*$, .), is a finite Abelian group.

Which again make sense:
Start with the finite part:
We know that at max we can have a size of n, therefore it must be finite.
Also if n is a prime then then size of the class is n - 1

Now for the rest of them, it should be easy
It is associative and we can use Euclid's division lemma to show that
It is commutative again by Euclid's division lemma
Inverse and identity are obvious. ([1] is identity and say we have [a] then [b] is the inverse)

Chapter 2

Cyclic Groups

Say we have a group G, with a element g. The the order of g is the smallest integer n such that

$$g^n = e$$

If we do not have such an n, then it is of infinite order.

So say we have G as a finite group. Then every element of G is of finite order.

We can do a quick proof of this :
We know we can have $g, g^2, g^3 ... g^a ...$ and this can keep going for any number. But we also know that these can not be unique, cos then we would have infinitely many elements. Therefore there has to be some b > a such that $g^a = g^b$. This means that $g^{b-a} = e$ So the order will be ATMOST b-a (this is cos we can have scalars which are smaller).

Also very quickly why is $g^{b-a} = e$ true. That is because say we have $g^b = g^b$, We can also write this as:

$g^a * g^{b-a} = g^b$ By power laws.
The we know that $g^a = g^b$, which means in this case g^{b-a} acts as the identity as the identity is unique.

Now say we had the group G and g ∈ G of order n. Then the elements e = $g^0, g, g^2, ..., g^{n-1}$ are all diffrent.
We can do another proof of this.
Say we have $g^i = g^j$. Then we can write j = i+k where we know that k ¡ n.
Now we know we can have

$$g^i g^k = g^j$$

Which means that $g^k = e$
Which we know for a fact is bullshit cos the order of g is n. Therefore we have a contradiction.

Definition of cyclic

A group is cyclic means that there is a g ∈ G such that G = $\{g^n : n \in \mathbb{Z}\}$

And this g is the generator element.

Generators for the mod groups

So for any n, $(\mathbb{Z}_n, +)$ is cyclic and [1] is a generator.

(Which makes sense, cos the [1] will be able to generate all of the elements by adding 1 to the remainders each time)

Cyclic groups are abelian

Say we have h, k which are in the group and the generator g

$hk = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = kh$ And this should make sense, cos it is the commutativity of addition which we know we can use.

But the converse is not true, for example say we have (ℚ, +), this is abelian but not cyclic.

We can prove that by contradiction. (THERE'S A PROOF IN THE LECTURE NOTES BUT I DON'T LIKE IT SO HERE'S A DIFFERENT ONE).

Say we have a generator element g, say g^1 generates some number p and g^2 generates some number q, then there is nothing which will generate $\frac{p+q}{2}$

Therefore we have a contradiction.

A group G of order n is cyclic iff it contains an element of order n.

If G is a finite group and G is cyclic then it has at most one element of order 2.

We can do a proof of this.
First of all what does order two mean
Say we have the group of order n. This means that g^n = e.
It means that we have some element where g ∘ g = e.

Lets rewrite this as $g^i \circ g^i = \text{e}$.
So this means that say n is even we must have $\text{n} = \frac{i}{2}$
And if n is odd then we can have no element of order 2.

Chapter 3

Symmetric Groups

Permutations

A permutation is a bijection:

$$\sigma : \{1, ..., n\} \to \{1, ..., n\}$$

The symmetric group

This is the set of all permutations

Compositions

Say we have the bijection σ and τ
Then we can write $\sigma \circ \tau$ which is also a bijection

Showing it is a group

well obviously:
It is associative, as if we have 3 operations a, b and c, then doing a then (b then c) is the same as doing (a then b) then c.
It has a identity, the map which does nothing
Every operation has an inverse, say we swap (1,2) then the inverse is to again swap (1,2)

Computing what happens

Say we have something like (123)(231)
looking at a small section of it (123), what this means is if we have the number 1 inputted then we get out the number 2, 2 inputted we get out 3 and 3 inputted

we get out 1.

Now to compute what happens in the overall composition what we do is

$$(123)(231) \leftarrow 1 = 3$$
$$(123)(231) \leftarrow 2 = 1$$
$$(123)(231) \leftarrow 3 = 2$$

So basically we are passing in the numbers from the RHS, and then each bracket will do a operation and will then pass into the next bracket.

Size of the group

$|S_n| = n!$
And this makes sense, as this is just the number of permutations.

Cycle notation

A permutation is called a cycle is we have $\sigma(a_1) = a_2, \sigma(a_2) = a_3 ..., \sigma(a_n) = a_1$
And for all other numbers $\sigma(i) = i$

Which makes sense cos that is literally a cycle

The order of a k cycle is k

Well its not gonna be more then k cos common sense ($\sigma^k = Id$).

Now we need to show it will not be less then k. So if it was less then k, that is the same as writing there is some d such that $\sigma^d = Id$ which we know is bullshit.

Disjoint cycles

We can say that the cycles $(a_1, ..., a_k)(b_1, ..., b_m)$ are disjoint is they have no elements in common

Any permutation can be written as a product of disjoint cycles

There is a algorithm to this, but that is obvious, so I will outline it here.
Start by picking some arbitrary value in the set.
Then we look at what that maps to
Repeat

Eventually we will get back to the start element.
At this point we have a cycle
Now if we have exhausted all of the possible elements in the list then we are good.
Else we will pick an element we have not yet looked at and repeat the process
Eventually we will have done this to all of the elements

Cycle types

Lets say we have the cycle (123)(45) this is of cycle type (3,2)

Signs of permutations

In the simplest way, I'm not gonna define an inversion cos it is exactly what you think it is. For the sign of a permutation, if we have a even number of inversions then the sign is positive, if there is a odd number of inversion then the sign is negative.

Any permutation can be written as a product of 2-cycles

And this is something which can be proven by induction.

Chapter 4

Subgroups

Say we have a group G. The a subset H of that group is represented as H $\subseteq$ G and a Subgroup is H $\leq$ G.

A subgroup is defined as

- The subset is closed
- The subset has an inverse in the subset
- The subset has the identity

Also as this is a subset of a group, we can derive the fact that it is associative as the parent group is also associative.

Any group G has two obvious subgroup, itself and the group with one element.

4.0.1 The subgroup test

Say we have (G, $\circ$), and H is a non-empty subset of G, then for any x, y $\in$ H we have x $\circ y^{-}1 \in$ H

Which makes sense cos:
This makes sure for every element it's inverse is in the set
It has an identity
And it is closed under binary operation as:
x $\circ$ y = x $\circ$ $((y^{-1})^{-1})$

This also holds if say we have:
$x^{-1} \circ y \in$ H

4.0.2 Cyclic subgroups

Say we have a group (G, $\circ$) then if we have $\langle g \rangle = \{g^i : i \in (Z)\}$
Basically this is the cyclic subgroup generated by g.

So from this can we show that $\langle g \rangle \leq$ G.

This can be done with the subgroup test. Say we have elements g^i and g^j then we can write

$$g^i \circ (g^j)^{-1}$$

Which is equal to $g^{i-j} \in \langle g \rangle$

Now say we have g has order n, then $\langle g \rangle$ also has order n.

And this is a simple proof to show. We know that all of e, 1, 2 ... n-1 all have to be unique. So we must have at least order n. Now we want to show that we can't have order more then n. Well if this happens we can write it out as g^k s.t k ¿ n. Which we can then write as $g^n * g^p$, where this now tells us that $g^k - g^p$ which is bullshit.

I HAVE NO CLUE WHY THE FUCK THIS IS MENTIONED, BUT IT IS:

Say we have the group ($\mathbb{Z}$, +), n an integer. The $\langle n \rangle$ = n$\mathbb{Z}$

So the order of $[2] \in \mathbb{Z}_6$ is three because $[2]^2 = [4]$ and $[2]^3 = [6] = [0]$.
So the cyclic subgroup generated by $\langle [2] \rangle$ is $\{[0], [2], [4]\} \leq \in \mathbb{Z}_6$

4.0.3 Cosets and Lagrange's Theorem

Cosets

Say we have a group (G, $\circ$) and H is a subgroup of G, then g is a element of G.

The left cost of H by g is gH = $\{g \circ h : h \in H\}$
The right cost of H by g is Hg = $\{h \circ g : h \in H\}$

We write G : H as the set of left cosets of H by elements of G.
Same way H : G is the set of right cosets of H by elements of G.

If g is Abelian then the left cosets equal the right cosets, but the converse does not need to hold.

AND NOW IT MAKES SENSE AFTER LOOKING AT IT FOR A WHILE. THE LEFT COSETS OF gH IS THE SET OF ALL OF THE ELEMENTS WHERE g HAS BEEN COMPOSED WITH THE ELEMENTS FROM THE SET H.

If we have the set H = (1,2,3) then the cyclic subgroup is $\{e, (1,2,3), (1,3,2)\}$

Lagrange's Theorem

Say we have the group (G, $\circ$) and H is the subgroup of G, then for two elements g_1 and g_2, the cosets g_1H and g_2H are the same iff g_2 is a element of g_1H.

From this we can now see that every element of G is in exactly one left coset of H. (This is also a easy proof, we know it is in its own set, and we have just proven if it is in another set, then the two sets are equal)

What this also tells us is that the left cosets are disjoint, and thier union will make up the whole set

If we have a group G and a subgroup H, then all of the left cosets of H have the same size:

$$|gH| = |H|$$

Lagrange's theorme:
If we have G as a finite group and then H as a subgroup then

$$|G| = |H|.|G : H|$$

We know this has to be true from above. We know

$$|gH| = |H|$$

Therefore in this case, the size if G is the number of cosets times the size of H.

Say we have G as a group and H as a subgroup, then the size of the left cosets $|G : H|$ is called the index of H.

If G is a finite group and we have $\langle g \rangle$, then the order of g will divide G

If we have a finite group then

$$g^{|G|} = e$$

In a similar way, if we have G is a finite group of order p, where p is prime, the G is cyclic.

Fermat's last theorem

Say we have an integer a and then p as a prime number then we can write:

$$a^{p-1} \equiv 1 mod p$$

4.1 Normal subgroups

A subgroup is normal is Hg = gH (The notation is H $\trianglelefteq$ G)

So we have seen this before, but if a group is abelian, then all of the subgroups are cyclic so they are all normal.

The center of a group G is the set Z(G) = $\{z \in G : gz = zg \forall g \in G\}$

So let G be a group and H a subgroup of G, then we wan to show there is a bijection between the set of left cosets G:H of H and the set of right cosets.

So first we want to defined a function which goes from the left cosets to the right ones eg:

$$f : (g : H) \to (H : G)$$
$$gH \to Hg^{-1}$$

So we must first show that this function is well defined - well to do so, let us have $g_1H = g_2H$ and we want to show $H(g_2)^{-1} \subseteq H(g_1)^{-1}$ and then by symmetry show $H(g_1)^{-1} \subseteq H(g_2)^{-1}$, so $g_{-1}H = g_{-2}H$ holds.

So first we know that if we have $g_1 \in g_2H$ then $g_1 = g_2h$ for some h (cos g_1 will be in the set g_2H).
So now using that fact we can get to $e = g_2h(g_1)^{-1}$
and inverting again we can get to $(g_2)^-1 = h(g_1)^-1$

Now say we have some x $\in H(g_2)^{-1}$, then we can write that x as h'$(g_2)^{-1}$. Therefore we have x = h'$(g_2)^{-1}$ = h'$(g_1)^{-1} \in H(g_1)^{-1}$

So now we need to check if f is a bijection.
Surjection: Say we have Hg as any right coset.The applying the function above f$(g^{-1}H)$ = Hg, so it is a surjection.

Now to show an injection, if we have f(g_1H) = f(g_2H), that mean we have $H(g_1)^{-1} = H(g_2)^{-1}$, so from this we can get to $g_1H = g_2H$ so that mean that f is injection therefore it is a bijection.

If we have G as a group and H as a subgroup, then If —G:H— = 2 then H is normal.

Well this makes sense. Cos there are 2 left cosets, H and gH. We also know that —H:G— = 2, and as H $\neq$ gH, we know that H and Hg are the only possible right cosets.

Conjugacy Criterion

Let G be a group, H is a subgroup of G. H is normal iff for all g $\in$ G and h $\in$ H then $ghg^{-1} \in H$

So say we have gxg^{-1} this is the called the conjugate of x by g.

From this we can now form a equivalence relation:

$$x_1 \ x_2 iff x_2 = gx_1g^{-1}$$

Also if G is a Abelian group, then there are as many conjugacy classes as there are elements

And that makes sense, cos if we have say,

$$b = gag^{-1}$$

Then this is the same as

$$b = gg^{-1}a$$

And we can write this as

$$b = a$$

So each of the elements are in their own class.

From this we can get the idea that for every symmetric group, the number of conjugacy classes is equal to the number of cycle types

Leading on from this we can write that the conjugacy class of the group G forms a partition of G.

And finally let G be a group, and H is a subgroup of G. The h is normal iff for all of the conjugacy classes C_g of G either $C_g \subseteq H$ or $C_g \cap H = \emptyset$
So using this fact we have a way to find the normal subgroups of G:

1. Compute all of the conjugacy classes inside the group G
2. We know that the size of the subgroups H has to divide the size of G, we can find all of the partitions of H in terms of the conjugacy classes. (Remember the trivial case as well)
3. And check that all of the partitions do form a subgroup.

So the example is quite useful here, say we want to work out all of the normal subgroups of S_4 then what we do is we look at the 5 conjugacy classes and their sizes:
$C_e = 1$
$C_e(i_1, i_2)(i_3, i_4) = 3$
$C_e(i_1, i_2) = 6$
$C_e(i_1, i_2, i_3) = 8$
$C_e(i_1, i_2, i_3, i_4) = 6$

So now from this we can work out the possible subgroups, as they are the groups whose orders will add to a multiple of 24, and will also need to have C_e in it

Conjugate subgroup

Say we have the group G, with a element g and H as a subgroup, then we have the set

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

This is the conjugate subgroup of H by g.

From this we can get for any element g, and H which is a subgroup of G, the set gHg^{-1} is a subgroup of G.

If we have G as a group and then H as a subgroup, then the unique conjugate subgroup of H is the group H itself.

4.2 Quotient groups

The binary operation which sends (gH, g'H) to gH.g'H := gg'H is called coset multiplication.

Say we have a group G and a normal subgroup H, then the set G/H := (G:H, .) is called the quotient group of G by H.

4.2.1 The first isomorphism theorem

Group Homomorphism

Say we have groups (G, $\circ$) and (G', .)
This is a map f from G $\to$ G' such that:

$$f(g_1 \circ g_2) = f(g_1).f(g_2)$$

For all $g_1, g_2 \in$ G

So for example if we have f(x) = e^x then this is a homomorphism

Say we have two subsets S and S', and a map f : S $\to$ S', the the preimage is defined by :

$$f^{-1}(A) = \{s \in S : f(s) \in A\}$$

Now say we have G and G again and f is a homomorphism

1. H $\leq$ G then f(H) $\leq$ G'
   Basically if H is a subgroup of G, then the H under the function f is a subgroup of G'
2. H' $\leq$ G then $f^{-1}(H') \leq$ G'
   This again makes sense, cos if H' is a subgroup of G, and we apply the inverse function then it will be a subgroup of G'
3. If H' is a normal subgroup of G' then $f^{-1}(H')$ is a normal subgroup of G

Now say we have the homomorphism is a bijection, this means that it is a group isomorphism. If there is a isomorphism between G and G' we say G $\cong$ G'

4.2.2 Kernel and image of homomorphism

The kernel of the set f is the set:

$$\{g \in G : f(g) = e_{G'}$$

The image of f is the set

$$\{g' \in G' : f(g) = g', forsomeg \in G$$

If we have f : G $\to$ G' then f is injective iff ker f = $\{e_G\}$

If we have G and G' as groups and then f: G $\to$ G' as a homomorphism, then the kernel of f is a normal subgroup of G and then image is a subgroup of G'.

So the function π is one which will map G $\rightarrow$ G/H.
So the kernel of π is H

This map is important, as it is called the canonical projection of G onto G/H. This is a surjection, but it will only be an injection if H = ker $\pi = \{e_G\}$

4.2.3 The First Isomorphism Theorem

So if we have groups G and G' and we have a group homomorphism, then

$$G/kerf \cong Imf$$

IF we have a homomorphism and G is a finite group, then the size of the Im f divided the size of G.