Goals

- Investigate the subgroup lattice of group
- Determine how the subgroup lattice of a group relates to its quotient groups
- Investigate what happens when you have a group isomorphism onto itself
- Investigate the connections between the above items.

Introduction

Last week, we proved the very important "First Isomorphism Theorem" which gave us a way to describe up to isomorphism the quotient group G/N for any normal subgroup N. This isomorphism theorem can be viewed as the go to tool in the toolbox for actually determining the structure of quotient groups. A couple of natural questions arise however:

1. Why do we want to determine the structure of the quotient group? How can we actually use quotient groups?
2. Are the "structure" of the groups G and G/N related in any way?
3. Why is this theorem called the "First Isomorphism Theorem?" Are there other isomorphism theorems? If so, what are they, and how are they related to normal subgroups, and group homomorphisms?
4. What about when we have a group homomorphism from a group to itself $\psi : G \to G$? Is there anything unique we can say in this case?

The answer (or at least the first taste of an answer) for questions 1 and 2 will take up the first two sections. We finish the worksheet by examining in detail a certain type of so called group automorphisms. These, a priori, distinct homomorphisms actually have much to do with our discussion of normal subgroups and quotient groups. In fact, they lead nicely into an introduction on some stronger subgroups than normal subgroups, called Characteristic subgroups.

1 Quotient Groups and The Lattice of Subgroups

Recall from Worksheet 3, that if G is abelian, and $N \subseteq G$ then N is automatically normal, so we can form the quotient group G/N- but moreover, we have that G/N is abelian! That is, the abelian structure of G is forced onto any quotient structure G/N.

1. Is this an if and only if? In other words is a group abelian if and only if the quotient G/N is abelian for some normal subgroup of N? (Hint- take your favorite non-abelian group and play around with some normal subgroups of it. Can you form an abelian group out of it?)
   Solution: This is false. As a counter-example, take $G = S_3$ and take $N = \langle(1, 2, 3)\rangle$ the subgroup generated by the 3-cycle 1,2,3. This has order 3 (as you can check) so is Normal, being a subgroup of index 2. Hence the quotient group $G/\langle(1, 2, 3)\rangle$ is abelian (being of order 2, it is in fact cyclic) but S_3 is not abelian.

2. In HW 3, you are asked to prove that the center of a group Z(G) is always normal- so one can always form the quotient G/Z(G). This quotient is rather useful, and can be used to determine if G is abelian. More specifically prove: **If G/Z(G) is cyclic then G is abelian.**
   Solution: In fact, one only needs $N \subseteq Z(G)$ for this to be true. Let $\overline{x}$ be a generator for $G/Z(G)$. Then, let $a \in G$. Then we have $aZ(G) = (xZ(G))^n = x^n Z(G)$ for some n (since it is cyclic). Thus we get that $ax^{-n} \in Z(G)$ (remember what it means for two cosets to be equal!), so $a = x^n z_1$ for some $z_1 \in Z(G)$. Since a was arbitrary, an exact same argument applies to show that $b = x^m z_2$ for some m and $z_2 \in Z(G)$. Hence $(ab) = (x^n z_1)(x^m z_2) = x^n x^m z_1 z_2 = x^m x^n z_2 z_1 = x^m z_2 x^n z_1 = (ba)$

3. Now every cyclic group is in particular abelian, so one could wonder, can we loosen our requirements above and ask only that G/Z(G) be abelian? In other words, **prove or disprove the following claim. If G/Z(G) is abelian then G is abelian.**
   Solution: This is false: Consider D_8 the dihedral group of order $8 = 2^3$. This a non-abelian group, so we know that the center cannot be of order 2^3 trivially. However, by the last problem we know the center of G can't be of order 2^2 either, since then $G/Z(G)$ would be cyclic of order 2, forcing G itself to be abelian, a contradiction. Hence, the center must be of order p, and the corresponding quotient group has order 2^2. Now in your homework this week you are asked to prove every group of order p^2 is abelian- hence we have exhibited a non-abelian group whose quotient by the center is Abelain.

4. Here is an application of the above. Suppose G is a group of order o(G)=pq for some distinct primes p and q. Suppose Z(G) is non trivial. Then prove G is abelian. (in fact, one doesn't even need the condition on the center, but we don't have the tools to show that yet).
   Solution: If the order of $Z(G) = pq$ then we are done trivially. So assume that the order

of $Z(G)$ is less than pq. We are assuming that it is non-trivial, so it must be of order p or q. Either way, when we quotient by Z(G) we get a group of prime order, and hence cyclic- conclude by number 2.

Ok cool, so much of the information about the commutivity of the group product is encoded in the quotient group, and vice-versa. Now if you think back to worksheet 1 and 2- one of the first topics we investigated after discussing abelian groups was subgroups. In particular we described a criteria for determining if a given subset of a group is itself a group. Now that we have built up this new group G/N from the group G, a reasonable question to ask is, are the subgroups of G/N in any way related to the subgroups of G? Throughout the next few problems, let G be a group, $N \trianglelefteq G$ and recall the natural projection map $\pi : G \to G/N$.

1. Let $H \leqslant G$ be a subgroup containing N. ($N \subseteq H$). Prove that the image of H $\pi(H) \subseteq G/N$ is a subgroup of G/N.
   Solution: This is a restatement of the product structure in G/N. Indeed, let $h_1N, h_2N \in \pi(H)$. Then $(h_1N)(h_2N)^{-1} = (h_1N)(h_2^{-1}N) = (h_1h_2^{-1}N)$ where $h_1h_2^{-1} \in H$ since H is a subgroup. Hence we are done.

2. Now let $\overline{H} \leqslant G/N$ be a subgroup of G/N, and let $H = \{g \in G : \pi(g) \in \overline{H}\} = \pi^{-1}(\overline{H})$. Show that H is a subgroup of G that contains N.
   The fact that H contains N is rather trivial. Indeed, for all $n \in N, \pi(n) \in N$ which is the trivial coset contained in every subgroup of G/N. Hence $\pi(n) \in \overline{H}$.
   Thus we must only show that H is a subgroup. Again, this is a rephrasing of old results. Let $h_1, h_2 \in H$. Then by definition $\pi(h_1), \pi(h_2) \in \overline{H}$. Therefore, $\pi(h_1h_2^{-1} = \pi(h_1)\pi(h_2)^{-1} \in \overline{H}$ since $\overline{H}$ is a subgroup and π is a group homomorphism. Thus, $h_1h_2^{-1} \in H$ and we are done.

3. Show that the above two problems give a (mutually inverse) bijection

$$\{H \leqslant G : N \subseteq H\} \longleftrightarrow \{\overline{H} \leqslant G/N\}$$

   That is, there is a bijection (1-1 correspondence) between the subgroups of G that contain N and all of the subgroups of G/N.

   (a) Start with a subgroup H that contains N and consider $\pi(H) \leqslant G/N$. Then you must show that $\pi^{-1}(\pi(H)) = H$
   (b) Conversely, start with a subgroup $\overline{H} \leqslant G/N$ and consider the subgroup of G, $\pi^{-1}(\overline{H})$. You must then show that $\pi(\pi^{-1}(\overline{H})) = \overline{H}$.

   I leave the details of this to you- come to my office hours or email me if you want to see it worked through!

4. The book expresses this in a different way. Remember, the first isomorphism theorem tells us that, if we're given a surjective group homomorphism $f : G \to G'$ then we get an isomorphism $G/ker(f) \cong G'$. Also remember (from last worksheet for example) that kernals of group homomorphisms and normal subgroups are the same thing. So classifying subgroups of G' (as the book does) is the same thing as classifying subgroups of $G/ker(f)$ (or equivalently G/N for any normal subgroup) that we have just done above.

It is hard to overstate the importance of this result above. One of the main tasks in understanding a group is to understand all possible subgroups of our group. This result above tells us that our determining the subgroups of G can be made easier by finding the subgroups of G/N for some normal subgroup, and vice-versa. In words, given a normal subgroup of N, rather than finding all subgroups that contain N, one must only find the subgroups of G/N (which is often much simpler as G/N is literally a smaller group). It turns out this correspondence above preserves even more "structure" than just the amount of subgroups:

The following points are the content of the so called "4th Isomorphism Thrm" (see the next section for the 2nd and 3rd isomorphism Thrm).
Fix G a group, $N \trianglelefteq G$ and let $A, B \leqslant G$ with $N \subseteq A, N \subseteq B$. Denote $\overline{A} = A/N, \overline{B} = B/N$ as in the correspondence above. Then

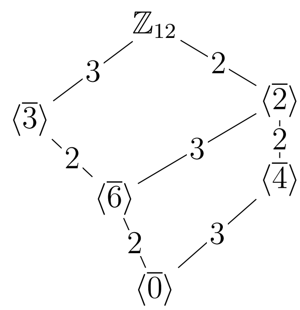
1. $A \leqslant B$ if and only if $\overline{A} \leqslant \overline{B}$
2. If $A \leqslant B$ then [B:A]=[$\overline{B} : \overline{A}$]. In particular (if B=G) $[G : A] = [\overline{G} : \overline{A}]$
3. $\overline{A \cap B} = \overline{A} \cap \overline{B}$
4. $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$

Let us see this in action with the following so called subgroup diagram or lattice of $\mathbb{Z}_{12}$. The way to read this diagram is as follows:

1. The top of the diagram is the whole group
2. The very bottom of the diagram is just the identity
3. Everything in between represents subgroups of G. If there is a line from one subgroup UP to another subgroup that means the subgroup below is contained in the one above it.

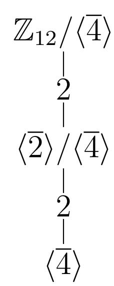
4. The numbers in between the groups represent the index of the below subgroup inside the larger subgroup.

Ok, so recall that $\mathbb{Z}_{12}$ is a cyclic group of order 12, so we know there is precisely one subgroup for every integer that divides 12. Hence there will be precisely one subgroup of order 1,2,3,4,6,12. Let us draw this below.



In words, we have the subgroups generated by $\overline{2}$ (of order 6), $\overline{3}$ (of order 4) , $\overline{4}$, (of order 3), and $\overline{6}$ (of order 2) respectively. The numbers in between the subgroups again represent the index: for example the subgroup $\langle\overline{6}\rangle$ has index 3 inside $\langle\overline{2}\rangle$ (use LaGrange's thrm if you don't believe me).

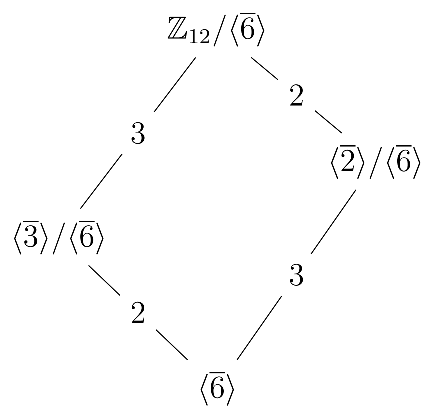
Now, we have that $\mathbb{Z}_{12}$ is an abelian group, so every subgroup is normal. In particular let us take the subgroup $\langle\overline{4}\rangle \trianglelefteq \mathbb{Z}_{12}$ and consider the quotient group $\mathbb{Z}_{12}/\langle\overline{4}\rangle$. Now the point is, the theorem tells us exactly what the subgroups of $\mathbb{Z}_{12}/\langle\overline{4}\rangle$ are! They will be precisely those subgroups that contain $\overline{4}$. From the perspective of the diagram, all we need to do is "look above $\langle\overline{4}\rangle$" and see what subgroups lie above it. Using this, we can draw the entire subgroup diagram of $\mathbb{Z}_{12}/\langle\overline{4}\rangle$.



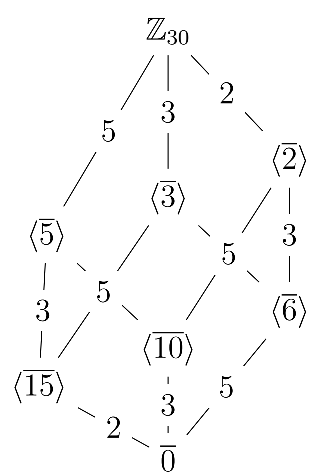
The only non-trivial subgroup of $\mathbb{Z}_{12}/\langle\overline{4}\rangle$ is $\langle\overline{2}\rangle/\langle\overline{4}\rangle$ since the only subgroup that contains $\langle\overline{4}\rangle$ is $\langle\overline{2}\rangle$!

The other important fact to note is that the index of the subgroups did not change! Indeed this is part 2 of the theorem above!
Ok, now it is your turn!

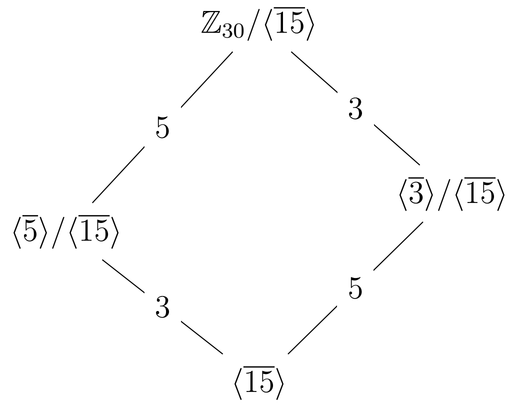
1. Draw the subgroup diagram for $\mathbb{Z}_{12}/\langle\overline{6}\rangle$ and include the index of each subgroup.
   Solution:



2. Draw the subgroup diagram now for $\mathbb{Z}_{30}$. You can mimic what I did for drawing the subgroup diagram for $\mathbb{Z}_{12}$. (Think of all the integers that divide 30- there will be exactly 1 subgroup of that order for each integer). Make sure to include the index of each subgroup.
   Solution: I will start it off for you- fill in the rest.



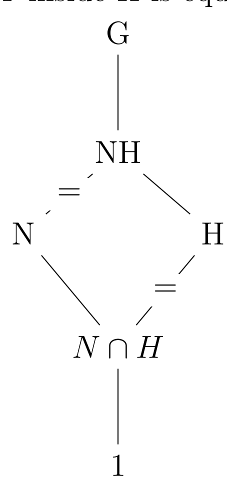
3. Use the subgroup diagram you made above for $\mathbb{Z}_{30}$ to find all subgroups (and the index of each subgroup in the other) for the quotient group $\mathbb{Z}_{30}/\langle\overline{15}\rangle$.



2 The Second and Third Isomorphism Theorems

Last week we investigated the so called "First Isomorphism Theorem" and worked through some of its consequences. The section above demonstrates the powerful "Fourth Isomorphism Theorem" So what gives? What about the second and third you ask? Well- you are actually asked to Prove the Second Isomorphism Theorem for your homework- let me state it here:

Second (or Diamond) Isomorphism Theorem: Let $N \trianglelefteq G$ and $H \leqslant G$ any subgroup. Then we have $N \trianglelefteq NH, N \cap H \trianglelefteq H$ and we have an isomorphism $NH/N \cong H/(N \cap H)$. It has the name diamond isomorphism theorem because of the following diagram. (as the theorem implies that the index of $N \cap H$ inside H is equal to the index of N inside NH)



I will not say much about this theorem since it is slightly unrelated to the topics at hand now, but needless to say it will make an appearance again at some point for us. I want to address the 3rd isomorphism theorem however, because that has some connections to the discussion in the previous section.

1. Look back to the 4 points of the 4th iso theorem I mentioned on page 3. Specifically, focus on point number 4.
2. This says that if $K \trianglelefteq G$ is some normal subgroup of G then $\overline{K} \trianglelefteq \overline{G}$ (recall $\overline{K} = K/N$)
3. Now- any time we have a normal subgroup, we should try and take the quotient of it. So, given a normal subgroup $N \subseteq K \trianglelefteq G$ we can take the following two quotients
   (a) G/K and
   (b) $\overline{G}/\overline{K}$
4. Do you think there is any relationship between the two quotient groups above??
   Solution: Oh ya! We have that $G/K \cong \overline{G}/\overline{K}$ (that is, $G/K \cong (G/N)/(K/N)$)
5. The third isomorphism theorem is a slight generalization of the above: Rather than state it here, let me set it up and let's see if you can guess what the statement of the theorem is.
   Solution: Let $H \trianglelefteq G$ and $K \trianglelefteq G$ with $H \subseteq K$. Then the third isomorphism theorem tells us the following 2 things:
   (a) Fill in first part of it here
   Solution: Well, since K contains a normal subgroup we can quotient by it. Also, by assumption, remember K is normal in G. The first claim is that the quotient remains normal, $K/H \trianglelefteq G/H$
   (b) Fill in second part of it here
   Solution: Well, we have a bunch of normal subgroups to quotient by. By the above, we can form the quotient $(G/H)/(K/H)$, and since $K \trianglelefteq G$ we can also form the quotient G/K. The second claim of the theorem is these groups are isomorphic, $G/K \cong (G/H)/(K/H)$

3 Group Automorphisms

One of the first groups we considered was the collection of all bijective functions on a set S, A(S). Now we have a more "sophisticated" notion of what the functions we should be studying are in this case- namely group homomorphisms! So we should like to define the collection of bijective group homomorphisms of a group onto itself- the goal is to then show this actually forms a group, and investigate what information it tells us about the underlining group itself.

1. Let G be a group. Then denote $Aut(G) = \{\phi : G \to G : \phi \text{ is a group isomorphism}\}$. (We call a group isomorphism from a group back to itself a group automorphism, hence the name Aut(G))

   (a) Show that Aut(G) is a group! I haven't told you even the group product- what do you think the product should be that makes this into a group?
   Solution: The product is function composition! We showed function composition turns a set into a group before- the only new thing is knowing that the composite of 2 automorphisms remains an automorphism! Check that yourself if you are doubtful!

   (b) Great so Aut(G) is always(!) a group, regardless of what the group G is. But if we didn't have any systematic way of determining what the elements of Aut(G) are, then it would be a pretty useless group. Luckily for us, we have already seen a huge class of group automorphisms.

      i. Let G be a group of order larger than 2, and let $h \in G$ not equal to the identity. Define a function $f_h : G \to G$ by $f_h(g) = hgh^{-1}$. Show that this function is :

         A. A group homomorphism.
         Solution: We have $f_h(g_1g_2) = hg_1g_2h^{-1} = (hg_1h^{-1})(hg_2h^{-1}) = f_h(g_1)f_h(g_2)$ where we are sneaky and multiply by $e_G = h^{-1}h$ in the middle there.

         B. An injective homomorphism
         Solution: Indeed, $g \in ker(f_h) \iff hgh^{-1} = e \iff hg = h \iff g = e$

         C. A surjective homomorphism!(hint- the h is fixed, and you want to show f_h maps onto any element g in G. Pick a clever $g' \in G$ such that $f_h(g') = g$)
         Solution: The clever choice of g' is given by $g' = h^{-1}gh$. Indeed, $f_h(g') = h(h^{-1}gh)h^{-1} = g$

      ii. This automorphism above is called conjugation by element h and it turns up everywhere! Think about the condition on H being a normal subgroup for example- or think back to Matrices being similar if you like Linear Algebra.

      iii. Let us now investigate what happens if we try and conjugate for different elements g. (A priori, we get a different function f_g for any different choice of g. Do you think that actually is the case?)

         A. Let G now be an abelian group. What is the function f_h for any choice of h?
         Solution: If G is abelian, then $hgh^{-1} = ghh^{-1} = g$ for all h,g. Thus the function f_h is the identity function.

         B. Let G again be any group (not necessarily abelian), and remember the center of the group is defined to be all the commuting elements of G,

$Z(G) = \{h \in G : hg = gh \text{ for all } g \in G\}$. Now let $y \in Z(G)$. What is the function f_y?
Solution: By the exact same argument as above, $f_y = id$ for y in Z(G).

(c) Let us now combine everything we have learned with this one last, really cool, problem!

i. Let G be any group (of order greater than 2). Let $Inn(G) = \{f_h : h \in G\} \subseteq Aut(G)$ (where f_h is the conjugation function defined above). Prove that $Inn(G) \leqslant Aut(G)$ is a subgroup. (We call the set of all conjugations Inner automorphisms- explaining the notation Inn(G))
First note that $(f_h)^{-1} = f_{h^{-1}}$ (indeed, the proof of surjectivity for f_h showed this!) so Inn(G) is closed under inverses.
Now let $f_h, f_k \in Inn(G)$. Then we want to show $f_h \circ f_k \in Inn(G)$. Indeed $f_h(f_k)(g)) = f_h(kgk^{-1})) = hkgk^{-1}h^{-1} = f_{hk}$

ii. Define a function $\psi : G \to Inn(G)$ as $\psi(g) = f_g$ (the output is again a function, it's a little weird). Show

A. This map $\psi : G \to Inn(G)$ is actually a group homomorphism! (hint, show that $f_{gh} = f_g \circ f_h$)
That this is a group homomorphism is rephrasing the above work showing Inn(G) is a subgroup.

B. What is the image of this homomorphism?
Solution: The image of this is the subgroup $Inn(G)$ by construction.

C. What is the kernal of this homomorphism?
We have $z \in ker(\psi) \iff f_z = id \iff z(g)z^{-1} = g \forall g \in G \iff z \in Z(G)$. Therefore, the kernal of this map is Z(G).

D. Use the 1st isomorphism theorem to determine what $G/ker(\psi)$ is isomorphic to.
By the first isomorphism theorem, we have that $G/Z(G) \cong Inn(G)$

E. **Look back at the work on page 2, problem 2 and 3. (I told you everything in this class is connected!)** In fact, we can now prove an even stronger claim. As a challenge problem prove that if Aut(G) is a cyclic group, then G is abelian! (hint, use subgroups of cyclic groups are cyclic, and problem 2 on page 2)
Suppose Aut(G) is a cyclic group. Then $Inn(G) \leqslant Aut(G)$ is also cyclic. By the above problem we have $Inn(G) \cong G/Z(G)$ any by problem 2 on Pg 3 we showed that any group whose quotient by the center is cyclic is abelian. Therefore we are done.

2. We are now in a position where we can define the second important class of subgroups of a group G. We shall see they are very much connected to Normal subgroups, and will play a star role in the next few weeks with our discussion of the Sylow Theorems.

(a) Let us first clear up a common misconception about Normal subgroups. **Prove or give a counter example to the following claim:** Let $H, K \leqslant G$ be subgroups

of G such that $H \trianglelefteq K \trianglelefteq G$ (H is normal in K and K is normal in G). Then H is normal in G.
This is false! Take $G = D_8$ the group of symetries of a square, $H = \langle s \rangle, K = \langle s, r^2 \rangle$. Then $H \trianglelefteq K \trianglelefteq G$ but H is not normal in G. (where s=reflection about the diagonal, r=rotation 90 degrees)

(b) We bring up the above for a reason. First, we can now define this second class of important subgroups. **We say a subgroup $H \leqslant G$ is a Characteristic Subgroup of G if H is fixed by every automorphism of G. (That is, given $\psi \in Aut(G), \psi(H) = H$).** We denote such an H by H char G. This looks like a funky definition. Let us show that this is a fairly natural consideration.

i. Let H char G. Show that H is a normal subgroup of G. (Hint, think about the defining characterization on being normal- what did we just show about that in the above discussion?)
Solution: H is normal iff $gHg^{-1} = H \; \forall g$. That is, H is normal iff $f_g(H) = H$ for all g. Now, if H is fixed by all automorphisms, in particular it is fixed by all inner automorphisms. Hence $f_g(H) = H \; \forall g$ proving the claim.

ii. Is the reverse true? Are all normal subgroups characteristic subgroups? What do you think?
Solution: No! Consider the normal subgroup $N = \{(x, 0) : x \in R\} \trianglelefteq \mathbb{R}^2$ from a previous worksheet. Then N is normal but the automorphism $\sigma(x, y) = (y, x)$ does not fix N.

iii. The importance of these subgroups is partially explained in the following. In words, the following states that characteristic subgroups fix the lack of transitiveness of normal subgroups.
Show that if H char K char G then H char G. As a consequence, if $K \trianglelefteq G$ and H char K then $H \trianglelefteq G$.
Solution: We show that if $K \trianglelefteq G, HcharK$ then $H \trianglelefteq G$. Indeed, since K is normal in G, we have that $f_g(K) = K$ for all g. That is, $f_g \in Aut(K)$ for all g. Now since H is char in K, this means that all automorphisms of K fix H. In particular, we have that conjugation is an automorphism of K, so it must fix H. That is, $f_g(H) = H$ for all g, which is exactly what we wanted to show.