THIS WORKSHEET COVERS MATERIAL SIMILAR TO SOME HOMEWORK 1 PROBLEMS. I RECOMMEND WORKING THROUGH THIS WORKSHEET BEFORE ATTEMPTING THE HW PROBLEMS ON COSETS.

Goals

- Further investigate the concept of subgroups for the integers
- Recall the concepts of equivalence relations and investigate the consequences of equivalence relations
- Gain a working familiarity with modular arithmetic
- Unwind the definition of cosets, and exhibit some familiar examples in the case when the group is $\mathbb{Z}$

Introduction

We finished last weeks worksheet by discussing a little bit about Subgroups. We mentioned that these are particular subsets, typically written H, of a group $(G, *)$ that remain a group under the operation $*$. The goal of this worksheet is to further study some particular subgroups that were defined last week- and to study the concepts of cosets for those particular cases. We will end by defining the "quotient group" for these cosets, and will show that it is a very familiar group.

1 More on subgroups of $\mathbb{Z}$

For this section, we will be considering the group of integers under addition, $(\mathbb{Z}, +)$. We will begin by re-going over a couple of examples of subgroups mentioned from last worksheet.

1. Fix some $n \in \mathbb{Z}$ and let $H = \{x \in \mathbb{Z} : x = nk \text{ for some } k \in \mathbb{Z}\}$. (Ie, H is the set of all integer multiples of n.) Then H is a subgroup of $\mathbb{Z}$

(a) Indeed, from last week we saw that to be a subgroup, you just needed to be closed under the group product and inverses.
Show that H is closed under addition.
Solution: If a=nk and b=nl for some integers k,l are in H, then a+b=n(k+l) is also in H- so H is closed under addition.

(b) Show that H is closed under taking inverses.
Solution. Let $a \in H$. Then a=nk for some k. Now we know $a^{-1} = -nk = n(-k) \in H$ so we are done.

In Worksheet 1, Problem 2 in the section on Subgroups, we denoted this set $H = n\mathbb{Z}$. This is standard notation so from this point on we will call this subgroup of n-multiples $n\mathbb{Z}$ (Note that example 1 from Worksheet 1 on subgroups is the special case $H = 2\mathbb{Z}$, the set of all even integers- we have just generalized that.)

2. In Worksheet 1, problem 4 on the subgroups section we gave the following problem: "Let (G,*) be any group, and let $a \in G$. Consider the subset $H = \{a^i : i \in \mathbb{Z}\}$. (where a^i denotes doing the operation $*$ to a i times.) Is H a subgroup?"

Let us now return to that question in the context where $(G, *) = (\mathbb{Z}, +)$. Let $a \in \mathbb{Z}$.

(a) What is the subset $H = \{a^i : i \in \mathbb{Z}\}$ for this case. That is, describe what the elements of this set are.
Solution: We unwind what a^i means in this case. Recall that we have defined a^i to mean doing the operation of the group to a, i times. In this case, our set $\mathbb{Z}$ is a group under addition. So for example $a^2 = a + a = 2a$ and $a^3 = a + a + a = 3a$ and $a^{-2} = -(a + a) = -2a$. That is, in our context, $a^i = i \times a$ so our subset is all multiples of a.
Finish describing the set H: This set comprises of all multiples of a. In other words, $H = a\mathbb{Z}$

(b) Use your above description of the set H, and problem 1 above to conclude that this set H is a subgroup of $\mathbb{Z}$.
Solution: This cyclic subgroup is just all multiples of a fixed integer, which in part a was shown to be a subgroup.

3. It turns out these subgroups of $\mathbb{Z}$ are the only ones- let us make this precise. Let $H \subset \mathbb{Z}$ be a subgroup of $(\mathbb{Z}, +)$. Then $H = n\mathbb{Z}$ for some integer n. (This example might be beyond what we have learned yet actually- try and think of a proof for it, however do not worry if you can't do it- A proof will be given when we discuss "cyclic groups and cyclic subgroups")
Solution: In your homework you are asked to prove that all subgroups of a cyclic group are cyclic. Since $\mathbb{Z} =< 1 >$ is cyclic every subgroup is also cyclic. We just showed in part b above that cyclic subgroups of $\mathbb{Z}$ are precisely of the form $n\mathbb{Z}$ for some n. Hence we are done.

2 Brief Interlude on Modular Arithmetic

If it is 9:00AM and you have to catch a plane ride in 4 hours (pre-covid, when people actually went outside), what time does your plane take off? At 1:00PM right? Ok, now how did we know that, and what are we really doing?
It is 9:00AM at the beginning, so 4 hours later would be 13- but any time y after 12 is really just the time x such that x+12=y, or put differently, such that x-y=12.
What we are doing in this case, is "modular arithmetic with base 12." In your introductory proof class you hopefully studied modular arithmetic in more detail. I am going to give an extremely brief summary of the definition of modular arithmetic, and give a couple of basic examples.
Let n be a positive integer. Then we say that "a is congruent to b, mod n" and write it like $a \equiv b$ mod n if n divides a-b- that is a-b=nk for some integer k.

1. let n=12. What is 13 congruent to mod 12? (This question is often shortened to what is 13 mod 12)
   Solution: The answer to this is the silly word problem I gave above. It is 1, since 13-1=12 which certainly divides 12.

2. Let n=2. What is 7 mod 2?
   Solution: We have that $7 \equiv 1$ mod 2 since 2 divides 7-1=6

3. Let n=3. Find 1 mod 3, 2 mod 3, 4 mod 3 and 5 mod 3.
   Solution: We have $1 \equiv 1$ mod $3\,, 2 \equiv 2$ mod 3 trivially (all numbers $k < n$ are congruent to themselves mod n.
   Now we also have that $4 \equiv 1$ mod 3 since 3 divides 4-1=3, and we get $5 \equiv 2$ mod 3, since 3 divides 5-2=3

OK, so that's all fine and good but why bring this up now? Well, in some sense the rest of the worksheet is just a massive generalization of this concept! Let me summarize some important facts about modular arithmetic- if any of these are either interesting or unfamiliar to you, please reach out to me!

1. First, one more important notation definition: We write $\mathbb{Z}_n$ to be the set of integers modular n. The elements of this set will be more easily described after the next few points:

2. Congruence is an "equivalence relation", so in particular the equivalence classes "partition" the integers. More on this in the next section

3. Let n be an integer. Then we write [a] or $\overline{a}$ (both are common notations in the literature) to be the equivalence class of a mod n.

   (a) Let n=2. What is $\overline{1}$?
   Solution: By definition, $\overline{1}$ is the equivalence class under the relation congruence mod 2. In other words, $\overline{1} = \{x \in \mathbb{Z} : x \equiv 1 \bmod 2\}$, ie the odd integers.

   (b) Let n=3. What is $\overline{0}$ and what is $\overline{2}$?
   Solution: By definition, $\overline{0}$ is the collection of all integers that are congruent to 0 mod 3. In other words $\overline{0} = \{3z : z \in \mathbb{Z}\} = 3\mathbb{Z}$
   Again, by definition, $\overline{2}$ is the collection of all integers that are congruent to 2 mod 3. In other words, they have remainder 2 when divided by 3, so $\overline{2} = \{3z+2" z \in \mathbb{Z}\}$

4. Combining 2 and 3 gives us that $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$

5. It turns out, one can turn $\mathbb{Z}_n$ into a group under addition by the rule $\overline{a} + \overline{b} = \overline{a+b}$. However, there is one big thing one needs to check in order to make this definition: that this definition is "independent" of choice of representative for the equivalence. Let me explain by means of example, and then we will prove once and for all it is well defined.

   (a) Let n=12: Then $\overline{2} = \overline{14}$ since $14 \equiv 2 \bmod 12$, and $\overline{3} = \overline{15}$ since $15 \equiv 3 \bmod 12$. Let us now compute the following two additions using the rule $\overline{a} + \overline{b} = \overline{a+b}$

      i. Find $\overline{2} + \overline{3}$ (in $\mathbb{Z}_{12}$)
      Solution: Using the rule above we get $\overline{2} + \overline{3} = \overline{5}$.

      ii. Find $\overline{14} + \overline{15}$ again in $\mathbb{Z}_{12}$
      Solution: Again, using the rule we get $\overline{14} + \overline{15} = \overline{29}$

      iii. Compare the two Answers above- what is their relationship?
      Solution: Notice that $29 \equiv 5 \bmod 12$, since 29-5=24 which 12 divides. Therefore we get that $\overline{29} = \overline{5}$. This is reassuring since we started with two inputs that were equal, and if we got a different answer depending on which "representative" from our equivalence class we chose, our rule for addition wouldn't be useful at all.

   (b) Let us now show that addition is well defined in general. Let n be an integer- Define addition in $\mathbb{Z}_n$ by the rule we have been using, $\overline{a} + \overline{b} = \overline{a+b}$ Show this is a well defined operation- ie that it does not change based on your choice of representative for your equivalence class.
   Solution: What we need to show is the following:

      i. Assume $a_1 \equiv a_2 \bmod n$ (ie $\overline{a_1} = \overline{a_2}$)

      ii. Assume $b_1 \equiv b_2 \bmod n$ (ie $\overline{b_1} = \overline{b_2}$)

   Then you must show $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Finish the proof.
   Saying the $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ means that $a_1 + b_1 \equiv a_2 + b_2 \bmod n$. So we show that n divides $a_1 + b_1 - a_2 - b_2$.
   Note that since $a_1 \equiv a_2 \bmod n$ we get that $nk_1 = a_1 - a_2$ for some integer k_1 and

similarly since $b_1 \equiv b_2$ mod n we get that $nk_2 = b_1 - b_2$ for some integer k_2. Thus $a_1 + b_1 - a_2 - b_2 = a_1 - a_2 + b_1 + b_2 = nk_1 + nk_2 = n(k_1 + k_2)$ so we are done.

Thus with this addition in hand it is fairly straightforward to show this is a group. As an exercise figure out what the additive identity and inverse are.
The identity is $\overline{0}$
The inverse is slightly more tricky. Let $a < n$. Then there exists some $b < n$ such that a+b=n. Then the inverse of $\overline{a}$ is $\overline{a}^{-1} = \overline{b}$
For example, if we work in mod 5, the inverse of $\overline{2}$ is $\overline{3}$.

3 Cosets in general

Cosets are a rather abstract concept for an arbitrary group, however for the case when $G = \mathbb{Z}$ and when $H \subset \mathbb{Z}$ is a subgroup, the cosets of H reduce to something more concrete that we should have some familiarity with. We will show that in the next section- first we begin with recalling the general definition of cosets of an arbitrary group

Let H be a subgroup of G and let $a \in G$. Then the set $aH = \{ah : h \in H\}$ is called a left coset of H, and the collection of all left cosets of H is denoted G/H. One important comment to make right away is the following: We mathematicians are often lazy, and this notation "ah" really means $a * h$ where $*$ is the group operation, not necessarily multiplication a times h- this will be important when we discuss additive groups (like, for example $\mathbb{Z}$).

This description of the set aH is a simple way of describing what a left coset "is"- however, it is not a good way of recognizing its importance. For example, why must we demand that H be a subgroup in this definition, why not just any old subset? The following theorem partially explains the importance:

1. First, a preliminary definition. Again let H be a subgroup of G, and let a,b be in G. Then we say that "a is congruent to b" if $a^{-1}b \in H$ and we write it as $a \equiv b$ mod H (why we write it this way and give it this notation will hopefully become clear in the next section- Throughout the rest of this section, keep in mind the previous section on modular arithmetic)

2. It turns out this definition above induces an "equivalence relation." That is one must show the following three things:

   (a) $a \equiv a$ mod H
   Solution: We must show that $a^{-1}a \in H$. However, this is trivial since $a^{-1}a = e$

and the identity element must be in every subgroup. (since H is closed under inverses). Hence proved.

(b) If $a \equiv b$ mod H then $b \equiv a$ mod H
Solution: This will use that H is closed under taking inverses. Indeed, since $a \equiv b$ mod H we get that $a^{-1}b \in H$. Now the element $b^{-1}a = (a^{-1}b)^{-1}$ and since H is closed under inverses, we get that $b^{-1}a \in H$ as desired.

(c) If $a \equiv b$ mod H and $b \equiv c$ mod H then $a \equiv c$ mod H
Solution: This will use that H is closed under products. Indeed we have that $a^{-1}b \in H$ and we have that $b^{-1}c \in H$ so we just have to notice that the element $a^{-1}c = a^{-1}bb^{-1}c$

3. Theorem: Again let $a \in G$ and let H be a subgroup of G. Then the left coset of H, $aH = \{x \in G : x \equiv a \text{ mod H}\}$, ie the equivalence class of a under the above equivalence relation. (Note, this theorem gives us one answer why we demand that H be a subgroup instead of just any old set. The fact that this congruence relation gives an equivalence relation relies on the fact that H is a subgroup.)
Solution: The book proves this for right cosets. Try to change the proof accordingly for this case of left cosets.
We show $aH = \{ah : h \in H\} = \{x \in G : x \equiv a \text{ mod H}\}$.
We first show that $\{ah : h \in H\} \subseteq \{x \in G : x \equiv a \text{ mod H}\}$. Indeed let $ah \in aH$. Then $a^{-1}ah = h \in H$ so $ah \equiv a$ mod H as desired.
Now we show $\{x \in G : x \equiv a \text{ mod H}\} \subseteq \{ah : h \in H\}$. Indeed let x be in G such that $x \equiv a$ mod H. Then we have $a^{-1}x = h$ for some h in H. Multiplying both sides by a gives us x=ah as desired.

Let us unwind why this theorem is useful. When you took Math 100 (or its equivalent Intro to Proofs Course elsewhere) you hopefully covered equivalence relations. One of the main results about equivalence relations on a set is that it "creates a partition of your set". In other words, your set is a disjoint union of the equivalence classes formed under your relation. In our case where the equivalence relation is congruence mod H, the theorem tells us that we get that our set G is a disjoint union of these left cosets. (where recall a disjoint union means the union of all the cosets equals G and the intersection of two different cosets is empty)
The fact that cosets partition the space has immense consequences for us- especially in the case when G is a finite group. We will look more deeply at these consequences of the theorem next week, in particular we will discuss Lagrange's Theorem. However, before we go further and discuss that, let us ground our self a bit by discussing cosets in the more familiar context when $G = \mathbb{Z}$.

4 Cosets of $\mathbb{Z}$ with an eye toward quotient groups

Let $H \subset \mathbb{Z}$ be a subgroup. We want to study left cosets of H in $\mathbb{Z}$ and we want to study the set of all cosets $\mathbb{Z}/H$ in this case as well. We do this first with an example.

1. Let $H = 2\mathbb{Z}$. In our case $\mathbb{Z}$ is a group under addition- so a general left coset of H in $\mathbb{Z}$ looks like $aH = \{a + h : h \in H\}$, and is thus sometimes written as $a + H$ instead of aH.

   (a) We showed in section3 that the cosets aH were actually the equivalence class of a under the equivalence relation of $x \equiv a$ mod H. What is the relationship between this equivalence relation and the equivalence relation defined in Section 2 for modular arithmetic
   Solution: By definition, we say $x \equiv a$ mod $2\mathbb{Z}$ iff $x - a \in 2\mathbb{Z}$. In other words, x-a=2k for some integer k. Note, from section 2 this is saying that $x \equiv a$ mod 2. That is, this notion of congruence up to a subgroup is really just a generalization of congruence that we have seen before.

   (b) Write out the cosets $0 + 2\mathbb{Z}$ and $1 + \mathbb{Z}$ in set notation.
   Solution: As mentioned above, a general coset of H looks like $a + 2\mathbb{Z}$ for some a in $\mathbb{Z}$. Now we always have the trivial coset when a=0, so in this case the coset is just $0 + 2\mathbb{Z} = \{0 + 2z : z \in \mathbb{Z}\} = 2\mathbb{Z}$
   How about when a=1: $1 + 2\mathbb{Z} = \{1 + 2z : z \in \mathbb{Z}\}$

   (c) Are there any other left cosets of $2\mathbb{Z}$? For example is the coset $3 + 2\mathbb{Z}$ distinct from $1 + 2\mathbb{Z}$?
   Solution: We can use the theorem that classified left cosets from Section3. Recall that cosets are actually equivalence classes, so if there is any overlap (ie, intersection) between two cosets they must be the same. Use this to conclude that the two cosets given in part b are the only two cosets of H.
   Note any number not equal to 0 or 1 is congruent to either 0 or 1 mod 2. Hence their equivalence classes will be the same. In particular $3 \equiv 1 mod 2\mathbb{Z}$ so the two cosets are equal.

   (d) Section 3 gave an abstract result about how cosets partitioned our group. Parts b and c above actually show how that manifests itself in a much more familiar case of the integers. Explain what this partition of the integers is.
   Solution: Note the coset $0+2\mathbb{Z}$ is just the collection of even integers and the coset $1 + 2\mathbb{Z}$ is just the collection of odd integers. So part c's result saying those are the only two cosets is really just saying that the integers can be separated into those integers that are even, and those that are odd.

   (e) Write out the set of cosets $\mathbb{Z}/2\mathbb{Z}$- does it look similar to another group?
   The collection of all left cosets of $H = 2\mathbb{Z}$, which we denoted $\mathbb{Z}/2\mathbb{Z}$ is the set

$\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$ Note the similarity between the set $\mathbb{Z}/2\mathbb{Z}$ and the set $\mathbb{Z}_2$ as described in section 2. This similarity is not a coincidence, and it explains the "with an eye towards quotient groups" part of the title of this section. (Namely, I mentioned in Section 2 that $\mathbb{Z}_n$ is a group! Can we turn $\mathbb{Z}/2\mathbb{Z}$ or more generally G/H into a group as well?)

2. Let $H = 3\mathbb{Z}$.

   (a) Find the left cosets 0+H, 1+H and 2+H.
   Solution: $0 + H = 3\mathbb{Z}$
   $1 + H = \{3x + 1 : x \in \mathbb{Z}\}$
   $2 + H = \{3x + 2 : x \in \mathbb{Z}\}$

   (b) Are there any more cosets than these three?
   Soltuion: No for the same reason as in the previous problem.

   (c) Again let $\mathbb{Z}/3\mathbb{Z}$ be the set of all left cosets of $H = 3\mathbb{Z}$. Write out the elements of $\mathbb{Z}/3\mathbb{Z}$.
   Solution: $\mathbb{Z}/3\mathbb{Z} = \{0 + H, 1 + H, 2 + H\}$

3. Let n be an integer and let $H = n\mathbb{Z}$

   (a) Find $\mathbb{Z}/n\mathbb{Z}$ and describe a set it looks familiar to.
   Solution: $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$. This looks very similar to the group $\mathbb{Z}_n$