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

Goals

- Regain familiarity with Set Theory
- Investigate the axioms of groups
- Recognize and create sets with a product that are not groups
- Explore the concept of Abelian groups and some of their basic properties
- Distinguish between subgroups and subsets that aren't subgroups

Introduction

Group theory is a very "formal" subject. That is, we will be able to deduce a lot of general results from some very specific "axioms" (ie, rules). The language of much of group theory will be that of Sets: so we will begin with some review of being able to read sets, and make sure we are all comfortable with the notations in set theory. Then we will review the axioms of groups again- and we will investigate why those are the axioms, and give some examples of sets that do not satisfy the axioms. We will finish by investigating a particular type of group, an abelian group. These are special groups that have one further axiom.

1 Set Theory Review

In this course, much of the groups we will be studying will be described using the language of sets. Let us review what a set is and how we read them in English.
A Set is by definition just a collection of objects. The point of set theory notation is to succinctly describe in a formal language these collection of objects. Recall, the way this looks is as follows:

$$\{A : B\}$$

What this means in English is, "The set of A such that B." Let us do some examples where I provide you with a set, and you describe what the collection of objects are in English, without using formal logical symbols.

1. $\{x \in \mathbb{Z} : 2x > x\}$.
   Solution: This set is the collection of all integers such that 2x is greater than x. More succinctly, this is the collection of all positive integers.
2. $\{x \in \mathbb{R} : |x| \geq 1\}$.
   This is the set of all real numbers greater than or equal to 1 and less than or equal to negative 1.
3. $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0\}$
   This is the set of all invertible 2x2 matrices (or, if you forgot that result, is the set of all two by two matrices with nonzero determinant).

Now let us do the reverse: I am going to describe in English a few collection of objects and I want you to write what these collections are using the notation and language of Set Theory. Note: there may be many correct ways to write what these are in set notation.

1. All Real numbers greater than twice pi.
   Solution: $\{x \in \mathbb{R} : x > 2\pi\}$
2. All rational numbers with denominator 2.
   $\{\frac{a}{2} : a \in \mathbb{Z}\}$
3. All two by two matrices with real coefficients that are invertible.
   $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0\}$

2 Axioms of Groups

In this section we are going to review what the "axioms" of groups are. Recall from your textbook that a Group is a Set G, along with a rule to combine two objects in your set which we call a product $*$ such that this product has the following properties:

1. If a,b $\in$ G then $a * b \in$ G (closure axiom)

2. For a,b,c ∈ G we have $a*(b*c) = (a*b)*c$ (associative axiom)
3. There exists an element e ∈ G such that $a*e = e*a = a$ for any a ∈G (identity axiom)
4. For every a ∈ G there exists an element (written a^{-1}) such that $a*a^{-1}$=$a^{-1}*a = e$ (the inverse axiom)

That is, the total data of a group consists of 6 things. First, a set G. Second, a way to combine objects in the set. And then the 4 rules placed on that way to combine objects. The first axiom assures us our rule for combining objects is well defined. The second axiom tells us it doesn't matter how we combine our objects together, so long as the order we combine them remains the same. The third and fourth are a little more subtle- combined they make it so we can "undo" our rule for combining objects in the set.

Let us now recall some examples of groups. For all the following we will write them as (Set, product) In each case write what the identity and inverse elements are.

1. $(\mathbb{Z}, +)$- ie the set of all integers with product being addition
   (a) Identity= 0
   (b) Inverse: Let a ∈ $\mathbb{Z}$. Then $a^{-1} = -a$
2. Let S be any set, and let A(S) be the set of all bijective functions on this set (recall bijective means the function is onto and 1-1). Then (A(S), ∘) is a group where ∘ is function composition.
   (a) Identity= The identity map- the map $i : S \to S$ defined by i(s)=s for all s in S.
   (b) Inverse: Let f ∈ $A(S)$. Then f^{-1} = the inverse function $f^{-1} : S \to S$ defined as $f^{-1}(b) = a$ when f(a)=b.
3. Let $M_{3\times3}(\mathbb{R})$ denote the set of all 3x3 matrices with real coefficients. Then $(M_{3\times3}(\mathbb{R}), +)$ is a group where + is the normal addition of matrices.
   (a) Identity= The so called 0 matrix $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
   (b) Inverse: Let m ∈ $M_{3\times3}(\mathbb{R})$. Then m^{-1} = the matrix where each component is the negative of the corresponding component of m. That is, if $m = (a_{ij})$ them $m^{-1} = (-a_{ij})$
4. $(\mathbb{Q} - \{0\}, \times)$- ie the set of all rational numbers besides 0, with product being multiplication.

(a) Identity= The number 1

(b) Inverse: Let $\frac{a}{b} \in (\mathbb{Q} - \{0\})$. Then $(\frac{a}{b})^{-1} = \frac{b}{a}$

As we will see, there are many many more examples of groups. It is often however, just as illuminating in determining when a given set with a product on it is NOT a group. Let us consider some examples: In each of the following determine why the following set with product is NOT a group. In some cases, there might be more than one reason, if so try to list as many reasons as possible.

1. $(\mathbb{Z}, \times)$.
   Solution: This fails to be a group because, for any integer not equal to ± 1 there is no inverse. For example, $2 \in \mathbb{Z}$ but $2^{-1} \notin \mathbb{Z}$. Notice this example shows why it is required to say what the product on your set is. $\mathbb{Z}$ is a group under addition, but it is NOT a group under multiplication.

2. Let S=the set off all odd integers. Then (S,+) is not a group.
   Solution: (S,+) is not a group because it is not even closed under addition. For example, 3 and 5 are in S, but 3+5=8 is not in S.

3. Let S=$\{m \in M_{2\times 2}(\mathbb{R}) : det(m) = 0\}$ (ie, all 2x2 matrices whose determinant is 0). Then $(S, \times)$ is not a group. (where again, $\times$ is the typical matrix multiplication operation).
   Solution: $(S, \times)$ is not a group because there are no invertible matrix in this set. The condition on the set, det(m)=0 means that m is not invertible.

4. Come up with some other set S and operation on that set that is not a group. Get creative, your set and product can be as funky as you want.
   Solution:
   .....
   .....
   .....

3 Abelian Groups

Note in the rules for groups, we did not require that $a * b = b * a$. In fact, in many cases we do not have such a result. We call a Group that DOES satisfy $a * b = b * a$ for any two objects a,b an Abelian Group. Abelian groups are very "nice" in that they behave more like

addition of numbers in the way we are familiar. Let us consider again the 4 examples of groups we gave above. Decide which of them are abelian and which are not.

1. $(\mathbb{Z}, +)$
   Solution: This is an abelian group. The order in which you add two integers does not matter: x+y=y+x for any two integers x,y.

2. Is $(A(S), \circ)$ an abelian group?
   Solution: A(S) is not an abelian group because function composition is rarely commutative. For example, let $S = \mathbb{R}$ and consider f(x)=x+2 and g(x)=10x. Then $f, g \in A(S)$ but $f \circ g(x)$= f(10x)=10x+2 while $g \circ f(x)$= g(x+2)=10(x+2)=10x+20

3. Is $(M_{3\times 3}(\mathbb{R}), +)$ an abelian group?
   Solution: Yes this is an abelian group- since we defined addition componentwise, and $(\mathbb{R}, +)$ is an abelian group. More concretely, if $m_1 = (a_{ij})$ and $m_2 = (b_{ij})$ we defined the matrix $m_1 + m_2 = (a_{ij} + b_{ij}) = (b_{ij} + a_{ij}) = m_2 + m_1$

4. Is $(\mathbb{Q} - \{0\}, \times)$ an abelian group?
   Solution: Yes, since multiplication of integers is commutative. That is $\frac{a_1}{b_1} \times \frac{a_2}{b_2} = \frac{a_1 \times a_2}{b_1 \times b_2} = \frac{a_2 \times a_1}{b_2 \times b_1} = \frac{a_2}{b_2} \times \frac{a_1}{b_1}$

There is one more example of an abelian group we already have some familiarity of actually. Let V be a real vector space (in fact it is unimportant what "field" you take the vector space over)- then part of the axioms for V require that it is an abelian group under addition. So we have actually studied abelian groups in that context!

I mentioned abelian groups behave more like addition of real numbers. Let us give one example along these lines.

1. Let x,y,z $\in \mathbb{R}$. Assume that x+y=y+Z. Then x=z.

   Solution: First, note that $(\mathbb{R}, +)$ is an abelian group, so we have that y+z=z+y. Thus, since x+y=y+z by assumption, we have that x+y=z+y. Now add $y^{-1} = -y$ on the right to both sides of the equation. This gives us x+y-y=z+y-y. Since y-y=0 is the identity for the group $(\mathbb{R}, +)$ we get x=x+0=z+0=z as desired.

2. Prove or give a counter-example to the following statement: Let $(G, *)$ be a group. Then if $x * y = y * z$ for some objects x,y,z in G we must have x=z.
   Solution: This is false. Consider the group $G = S_3$ and consider x=(12), y=(123) and z=(23)
   Then xy=(13) and yz=(13) yet $x \neq z$

3. Prove or give a counter-example to the following statement: Let $(G, *)$ be an ABELIAN group. Then if $x * y = y * z$ for some objects x,y,z in G we must have x=z.
   Solution: This is true. We can mimick the proof of 1 exactly in this case. The key point is being able to change $y * z = z * y$ so we can multiply on the right to both side y^{-1} to cancel out the y. We could not do that in part 2 for example since S_3 is not abelian.

4 Subgroups

Our goal in this course is to properly understand those sets that can be made to satisfy the axioms of a group. There is a common theme in mathematics that in order to understand an object with a given property, you look at the smaller objects contained in it (that also satisfy the property you are studying) and study those smaller objects with the hope to get some insight into the larger object. This is all rather vague, so let's make this precise with the definition of subgroups.

We have defined a group as a set with an operation $(G, *)$- now remember one can talk about subsets of a set- so a natural question arises: If $S \subset G$ is a subset of G, when is $(S, *)$ also a group? We call such subsets "subgroups." (think back to when you studied vector spaces and "subspaces")

One could of course check the long way, and just make sure all the 4 axioms are satisfied for $(S, *)$- however, it turns out that knowing that S is contained in a a group shortens our work into the following:

Let $(G, *)$ be a group- A subset $H \subset G$ is a subgroup if and only if it is closed under products and inverses (ie, if $x, y \in H$ then both $x * y$ and $x^{-1} \in H$). One of our main goals in the beginning of this course will be to study a couple of particular subgroups that exist for every group. For right now however, let's just gain some familiarity in being able to recognize when subsets are subgroups.

1. Let $2\mathbb{Z}$= the set of all integer multiples of 2 (ie, even numbers). Is $2\mathbb{Z}$ a subgroup of $(\mathbb{Z}, +)$?
   Solution: We just need to show the two conditions listed above. Let x=2l and y=2k for integers l,k. Then x+y=2l+2k=2(k+l) $\in 2\mathbb{Z}$. Now again consider x=2l $\in 2\mathbb{Z}$. Then -2l=2(-l) $\in 2\mathbb{Z}$ as well, and -2l=2(l) x^{-1}. Thus $2\mathbb{Z}$ is a subgroup.

2. Let n be any natural number. Is $n\mathbb{Z}$ a subgroup of $(\mathbb{Z}, +)$?
   Solution: $n\mathbb{Z}$ is a subgroup. Indeed let $x = nk_1$ and $y = nk_2$. Then $x + y = n(k_1 + k_2) \in n\mathbb{Z}$ as required. Also $x^{-1} = -nk_1 = n(-k_1) \in n\mathbb{Z}$

3. Is $\mathbb{N}$ a subgroup of $(\mathbb{Z}, +)$?
   Solution: No, it is not closed under taking inverses. For example, $2 \in \mathbb{N}$ but there is no $2^{-1} \in \mathbb{N}$

4. 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?
   Solution: Yes this is a subgroup. Indeed let $x = a^{i_1}$ and let $y = a^{i_2}$. Then $x * y = a^{i_1+i_2} \in H$. Also we get that $x^{-1} = a^{-i_1} \in H$