MATH 31 – HOMEWORK 2 SOLUTIONS!

due Wednesday, July 12

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

1. (a) (4.13) Show that if G is a finite group, then every element of G is of finite order.

   Proof: We will prove the contrapositive by assuming that G has an element of infinite order and prove that G must be an infinite group. Suppose that there exists $x \in G$ such that $o(x) = \infty$. Then, $\langle x \rangle$ is a subgroup of G that contains $\{x, x^2, x^3, \ldots\}$ (and possibly other things). If we can show that x^i and x^j are actually different elements for all positive integers i and j, then we'll be done (but we have to actually show this!).

   Suppose that i and j are two integers such that $i \leq j$. If $x^i = x^j$ then by the cancellation law it follows that $e = x^{j-i}$. Since $j - i \geq 0$ and since $o(x) = \infty$, the only possible values of i and j are $i = j$. Hence if $i \neq j$ then $x^i \neq x^j$. □

   (b) (4.14) Give an example of an infinite group G such that every element of G has finite order.

   Solution: The easiest example that we've seen already is a group from the first homework assignment. Let S be any set. Then we verified that $(\mathcal{P}(S), \triangle)$ is a group. If S is infinite, for example $S = \mathbb{Z}$, then $\mathcal{P}(S)$ is infinite, so $(\mathcal{P}(\mathbb{Z}), \triangle)$ is an infinite group. Moreover, every nonidentity element has order 2 because if $A \subseteq \mathbb{Z}$ then $A \triangle A = \emptyset$.

2. Find all subgroups of $(\mathbb{Z}_{30}, \oplus)$, and draw the subgroup lattice.

   Solution: Since $\mathbb{Z}_{30}$ is cyclic, so are all its subgroups. There are 30 possible cyclic subgroups

   $$\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \ldots, \langle 29 \rangle.$$

   but many may be the same.

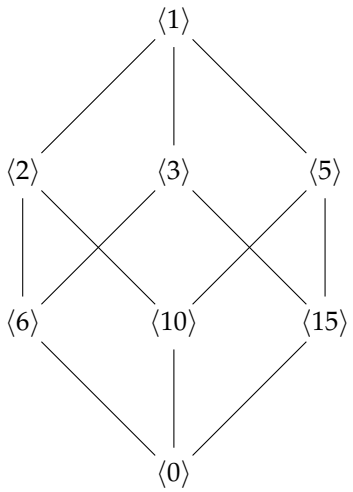
   There's a theorem in the book that is helpful to figure out which subgroups are the same. We didn't directly cover it in class, but you can use it, and if you didn't notice it was there then you might have discovered and proved it as you did this problem. You can also find the answer to this question by just checking which subgroups are the same by hand.

   Theorem 5.5.iii says: Let $G = \langle x \rangle$ be a cyclic subgroup of order n. Then, two powers x^r and x^s generate the same subgroup of G if and only if $\gcd(r, n) = \gcd(s, n)$.

   So, for example, for any s such that $\gcd(s, 30) = \gcd(1, 30) = 1$ we have $\langle s \rangle = \langle 1 \rangle$. We eventually find that the subgroups are

   $$\{\{e\}, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \langle 6 \rangle, \langle 10 \rangle, \langle 15 \rangle\}.$$

   The subgroup lattice is:



3. (5.24) *This exercise proves a condition that helps you test if a subset is a subgroup.* Let G be a group and let H be a nonempty subset of G such that whenever $x, y \in H$ we have $xy^{-1} \in H$. Prove that H is a subgroup of G.

   Proof: This exercise is a very good test of your ability to make logical step-by-step arguments. We assume that H is a nonempty subset of a group G, and that for any pair of elements $x, y \in H$ we are guaranteed that $xy^{-1} \in H$ as well. We will prove that H is a subgroup by using the theorem from class which says that a subset H is a subgroup if (i) H is nonempty, (ii) H is closed under multiplication, (iii) H is closed under inverses.

   Condition (i) is given to us as true. We'll prove condition (iii) next because it will be useful when proving condition (ii). We can't do much until we do the following step: because H is nonempty, it contains at least one element, which we'll call a. By the fact, since $a \in H$ we can set $x = a$ and $y = a$ and be guaranteed that $aa^{-1} \in H$. Since $aa^{-1} = e$, (where e is the identity of G), we now know that H must contain the identity of G. To prove closure under inverses, we suppose that b is an arbitrary element of H and we prove that b^{-1} must be in H. Well, if $b \in H$ then we can apply the fact given to us with $x = e$ and $y = b$ to conclude that $eb^{-1} \in H$. Since $eb^{-1} = b^{-1}$, we've now verified condition (iii) by showing that anything in H must also have its inverse in H.

   Lastly we verify condition (iii). Suppose c and d are any elements of H. Our goal is to show that cd must be in H. By condition (ii), we are guaranteed that $d^{-1} \in H$. Now apply the fact given to us with $x = c$ and $y = d^{-1}$. The result is that $c(d^{-1})^{-1} \in G$. Since $c(d^{-1})^{-1} = cd$, we've proved that $cd \in H$.

   Having verified the three necessary conditions, we can conclude that H is a subgroup of G. □

4. Let G be an abelian group and suppose that G has at least two distinct elements of order 2. Show that G has a subgroup of order 4.

   Solution: You must show this for *all* abelian groups, infinite or finite, cyclic or noncyclic, etc. So, let G be an arbitrary group that has at least two distinct elements of order 2. The only possible next step is to give these elements names.

   By the hypothesis, there exist two elements a and b in G such that $a \neq b$, $o(a) = 2$ and $o(b) = 2$. This means that $a^2 = e$ but $a \neq e$ and $b^2 = e$ but $b \neq e$, where e is the identity of G. We've now summarized the information given to us.

   Our goal is to construct a subgroup of order 4 given these ingredients. There's not much to choose from! Every subgroup contains the identity, so we need to find three more elements. Clearly we want to add a and b as well. This gives a subset with three elements, but it's not a subgroup yet, as it contains a and b, but not ab (it is not closed under multiplication). So, let's just add in ab and see if that works. Now we have a set

   $$S = \{e, a, b, ab\}.$$

To check if S is a subgroup of G, we will again use the theorem that lets us check three conditions.

Clearly S is nonempty. Next we check that all the products of two elements of S are in S. Since G is abelian, we only have to calculate that $ea = a \in S$, $eb = b \in S$, $e(ab) = ab \in S$, $a^2 = e \in S$, $ab \in S$, $a(ab) = a^2b = b \in S$, $b(ab) = ab^2 = a \in S$, and $(ab)(ab) = a^2b^2 = e \in S$.

To check closure under inverses, first note that since $a^2 = e$ it follows that $a = a^{-1}$. Similarly, $b = b^{-1}$. We know as a general rule that $(ab)^{-1} = b^{-1}a^{-1}$ in any group, so in this group $(ab)^{-1} = b^{-1}a^{-1} = ba = ab$. Lastly, as usual, $e^{-1} = e$. So every element of S has an inverse in S.

Having verified the three necessary conditions, we can conclude that S is a subgroup of G. $\square$