Math 103 HW 4 Solutions to Selected Problems

2. **Let Q be the group of rational numbers under addition and let Q^* be the group of nonzero rational numbers under multiplication. In Q, list the elements in $< \frac{1}{2} >$. In Q^*, list the elements in $< \frac{1}{2} >$.**

   Solution: In Q, $< \frac{1}{2} >$ is just all rationals that are of the form

$$\pm(\underbrace{\frac{1}{2} + \cdots + \frac{1}{2}}_{n\text{-times}})$$

   (since the operation here is addition, the inverse of $\frac{1}{2}$ is $-\frac{1}{2}$) for some integer n. Of course, this is just the set $\{\frac{n}{2} | n \in \mathbb{Z}\}$.

   In Q^*, the operation is multiplication, so $< \frac{1}{2} >$ is rationals of the form

$$\underbrace{\frac{1}{2} \cdot \frac{1}{2} \cdot \cdots \cdot \frac{1}{2}}_{n\text{-times}}$$

   in other words the set $\{\frac{1}{2^n} | n \in \mathbb{Z}\}$.

4. **Prove that in any group, an element and its inverse have the same order.**

   Solution: Let n be the order of a. We know (by induction, for example, or just multiplying by a^d and cancelling each term one by one) that $(a^d)^{-1} = (a^{-1})^d$ for an positive integer d. But then

$$\begin{aligned} e &= a^n(a^{-1})^n \\ &= e(a^{-1})^n \\ &= (a^{-1})^n \end{aligned}$$

   so we know that least that a^{-1} has order $\leq n$. But the same argument with a^{-1} replacing a shows that if $(a^{-1})^d = e$, then $((a^{-1})^{-1})^d = a^d = e$ also. Therefore, the order of a^{-1} is at least the order of a, so it must equal n.

25. **Let n be a positive even integer and let H be a subgoup of Z_n of odd order. Prove that every member of H is an even integer.**

Solution: A clue to this problem comes from problem 24 in the book, which claims that if H is any subgroup of Z_n (with n even still), then either every member of H is even (what we want) or exactly half of the members of H are even. This gives our desired result immediately, since if half the members of H are even, then must H have order twice that number, so $|H|$ is even, and we assumed $|H|$ to be odd at the start.

How to prove this claim? <u>Method 1:</u>
We need to show that if H has any odd elements, then half the members of H are even. Let H_O and H_E be the odd and even elements, respectively, of H. Every integer is either even or odd, so we see that $H = H_O \cup H_E$ is a disjoint union, which means that $|H| = |H_O| + |H_E|$. This tells us that it's enough to prove $|H_O| = |H_E|$ if H has an odd element. So suppose H does, and let m be an odd element of H. One way to show two sets are the same size is to exhibit a bijection between the two. We claim that $f(x) = x + m$, where the addition is being done in H (that is, mod n), is a bijective function from H_O to H_E. This is true because m is odd, so if $x \in H_O$, so the integer $x+m$ (with addition being done in $\mathbb{Z}$) will certainly be even before we take the remainder mod n. But n is even, and we get the remainder mod n (or anything congruent mod n, which is what "$x+m$" means in H) by adding a multiple of n to $x+m$, so it will be even as well. Thus f has the correct codomain. A similar argument shows that $g(x) = x - m$ is a well defined function from H_E to H_O, and these are clearly inverses, meaning f is bijective. This implies that $|H_O| = |H_E|$, so we are done.

<u>Method 2:</u> Since Z_n is cyclic, so is any of its subgroups; in particular, H. Let h be a generator of H. If h is even, then $m \cdot h$ is even for any $m \in \mathbb{Z}$. Since n is even, this means that $m \cdot h$ is even in Z_n, hence in H, so in that case H only has even elements. If h is odd, then every odd multiple will be odd, and every even multiple will be even. This means—again because n is even—that in order for $m \cdot h$ to be zero mod n, m must be evens. But this forces the order of h to be even, which since h is a generator of H means that $|H|$ must be even. This being the case, we see that H_O and H_E (which are just the odd multiples and the even multiples of h, respectively) have the same size.

34. **If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G.**

Solution: $H \cap K$ is nonempty, since it contains the identity e (which is in any subgroup of G). Suppose x and y are in $H \cap K$. Then by definition x and y are both in H, so y^{-1}, and hence gh^{-1} is in H too. Since x and y are both in K as well, and K is also a subgroup, then $xy^{-1} \in K$ by the above argument. By definition, this means $xy^{-1} \in H \cap K$, and by the "One-Step Subgroup Test", we conclude $H \cap K$ is a subgroup.

44. **If H is a subgroup of G, then by the *centralizer* $C(H)$ of H we mean the set $\{x \in G | xh = hx$ for all $h \in H\}$. Prove that $C(H)$ is a subgroup.**

Solution: The identity e is in $C(H)$ because $eh = he = h$ for all $h \in H$. Now let a, b be in $C(H)$. Then

$$\begin{aligned} abh &= ahb \\ &= hab \end{aligned}$$

for any $h \in H$, so $ab \in C(H)$. On the other hand, multiplying the equation $ah = ha$ by a^{-1} on both the right and the left yields $ha^{-1} = a^{-1}h$ for all $h \in H$, so a^{-1} is in $C(H)$ too, and $C(H)$ is indeed a subgroup of G.

52. **Give an example of elements a and b from a group such that a has finite order, b has infinite order and ab has finite order.**

Solution: This will definitely not be possible if the group we choose is Abelian, because if $a^n = e = (ab)^m$, then

$$\begin{aligned} e &= ((ab)^m)^n \\ &= (ab)^{nm} \\ &= a^{nm}b^{nm} \\ &= (a^n)^m b^{nm} \\ &= e^m b^{nm} \\ &= b^{nm} \end{aligned}$$

meaning b has finite order if a and ab do. Thus, we our example must come from an infinite non-Abelian group. We haven't learned about many of these so far, but there is at least one: $GL_2(\mathbb{R})$. The way problem 50 in the book is phrased suggests that we should look at the matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Notice that

$$\begin{aligned} A^2 &= \begin{pmatrix} 0-1 & 0+0 \\ 0+0 & -1\cdot -1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

which means that $A^4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^2 = I$. Meanwhile,

$$C^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

and C has determinant 1, so by a well known formula for the inverse of a 2×2 matrix, $C^2 = C^{-1}$. This implies that $C^3 = I$.

However,

$$AC = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and there has infinite order since

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

meaning

$$(AC)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

which cannot be the identity matrix for any postive n. Thus letting $a = A^{-1}$ (which has finite order because A does, as we showed in a previous problem), and $b = AC$, then $ab = C$ has finite order.

54. **For any positive integer n and any angle θ, show that in the group $SL(2, \mathbb{R})$,**

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}^n = \begin{pmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{pmatrix}.$$

Use this formula to find the order of

$$\begin{pmatrix} \cos(60^\circ) & -\sin(60^\circ) \\ \sin(60^\circ) & \cos(60^\circ) \end{pmatrix} \textbf{ and } \begin{pmatrix} \cos(\sqrt{2}^\circ) & -\sin(\sqrt{2}^\circ) \\ \sin(\sqrt{2}^\circ) & \cos(\sqrt{2}^\circ) \end{pmatrix}.$$

Solution: If $n = 1$ then there is nothing to prove, so suppose this is true for some $n \geq 1$. Then (letting $M_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$) we have

$$\begin{aligned} M_\theta^{n+1} &= M_\theta^n \cdot M_\theta \\ &= M_{n\theta} \cdot M_\theta \end{aligned}$$

Let α, β be any angles. Then the angle addition identities from trigonometry tell us that

$$\begin{aligned} M_\alpha \cdot M_\beta &= \begin{pmatrix} \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) & \cos(\beta)\sin(\alpha) + \cos(\alpha)\sin(\beta) \\ \cos(\alpha)\sin(\beta) + \cos(\beta)\sin(\alpha) & -\cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\ &= M_{\alpha+\beta} \end{aligned}$$

In particular, $M_{n\theta} \cdot M_\theta = M_{(n+1)\theta}$, so the identity holds for all $n \geq 1$ by induction.

The θ such that $\cos(\theta) = 1$ and $\sin(\theta) = 0$ are the multiples $360k^\circ$ for $k \in \mathbb{Z}$, so $M_\theta^n = I$ if and only if $\theta = \frac{360k}{n}^\circ$ for some k. $\sqrt{2}$ is not even rational, so it cannot have this form for any n, and $M_{\sqrt{2}}$ has infinite order. Meanwhile, we can check that the smallest $n \geq 1$ such that $60n = 360k$ is 6, meaning M_{60} has order 6.

70. **Let** $H = \{a + bi | a, b \in \mathbb{R}, ab \geq 0\}$**. Prove or disprove that** H **is a subgroup of** $\mathbb{C}$ **under addition.**

Solution: H is not a subgroup: $x = 2i$ and $y = -1 - i$ are both in H, but $x + y = -1 + i$ is not.