Homework 2 solutions.

Problem 4.4. Let g be an element of the group G. Keep g fixed and let x vary through G. Prove that the products gx are all distinct and fill out G. Do the same for the products xg.

Proof. Let $g \in G$. Let $x_1 \neq x_2 \in G$. We need to show that $gx_1 \neq gx_2$.

Suppose for contradiction that $gx_1 = gx_2$. Since G is a group, $g^{-1} \in G$. So this means that $g^{-1}(gx_1) = g^{-1}(gx_2)$. By associativity, this means that $(g^{-1}g)x_1 = (g^{-1}g)x_2$. This simplifies to $ex_1 = ex_2$, where e is the identity. Finally, by the property of the identity, we get that $x_1 = x_2$. But this contradicts the assumption that $x_1 \neq x_2$. So we have shown that if $x_1 \neq x_2$ then $gx_1 \neq gx_1$. Thus all the elements of the form gx are distinct.

Similarly, we have to show that if $x_1 \neq x_2 \in G$ then $x_1 g \neq x_2 g$. Again, suppose not. That is, suppose that $x_1 g = x_2 g$. But then when we multiply both sides by g^{-1} on the right, and use the same group properties as above, we get that $x_1 = x_1$. Again, this is a contradiction, so we must have that all elements of the form xg are distinct.

Next we have to show that the sets $S = \{gx | x \in G\}$ and $S' = \{xg | x \in G\}$ fill out G. That is, for each element $h \in G$, we need to find elements $x, x' \in G$ s.t. $xg = gx' = h$. So let $x = hg^{-1}$ and let $x' = g^{-1}h$. We know that x, x' are in G since $g^{-1} \in G$ by the inverse property, and the products are in G as G is closed under multiplication.

Now we just compute:

$$\begin{aligned} xg &= (hg^{-1})g \\ &= h(g^{-1}g) \\ &= he \\ &= h, \end{aligned}$$

and similarly we can compute that $gx' = g(g^{-1}h)$ is just h after using all three of the group properties.

So for each element $h \in G$, we have found x, x' s.t. $xg = gx' = h$. Therefore the sets S and S' fill out G. □

Problem 4.5. An element $x \in G$ satisfies $x^2 = e$ precisely when $x = x^{-1}$. Use this observation to show that a group of even order must contain an odd number of elements of order 2.

Proof. Let G be a group of even order. Let $|G|$ denote the order of G. So we can write $|G| = 2n$ for some $n \in \mathbb{Z}$. Let S be the set of elements of G that have order greater than 2. Since only elements of order 2 and the identity satisfy $x^2 = e$, we can write $S = \{x \in G | x^2 \neq e\}$. We want to show that S has an even number of elements. We use the idea that if an element has order bigger than 2, it is distinct from its inverse, so elements of S come in pairs. To make this precise, write S as the following union:

$$S = \bigcup_{x \in S} \{x, x^{-1}\}.$$

We show later that the order of x is the same as the order of x^{-1} so this union is indeed S. Since $x^2 \neq e$ for $x \in S$, we have that $x \neq x^{-1}$, so each set in this union has two distinct elements. Since inverses are unique, two sets of the form

$\{x_1, x_1^{-1}\}, \{x_2, x_2^{-1}\}$ are either equal or disjoint. So we can write S as the disjoint union of sets with 2 elements each. Therefore S has an even number of elements. Let $2m$ be the number of elements of S, for some $m \in \mathbb{Z}$.

Let T be the set of elements in G of order 2. Let k be the number of elements of T. Since G is the disjoint union of T, S and $\{e\}$, the number of elements of G is the number of elements of T plus the number of elements in S plus 1. That is, $2n = 2m + k + 1$. Solving for k we get $k = 2(n - m) - 1$. Since $n, m \in \mathbb{Z}$, we get that k is odd. So we have shown that there is an odd number of elements of order 2. □

Problem 4.8. Let x and g be elements of a group G. Show that x and gxg^{-1} have the same order. Now prove that xy and yx have the same order for any two elements x, y of G.

Proof. Let G be a group, and let $x, y, g \in G$. Denote the order of an element x by $|x|$. Suppose $|x| = n$, and $|gxg^{-1}| = m$. We need to show that $n = m$. Recall that the order of an element x is the smallest number n s.t. $x^n = e$. First we will show that the order of gxg^{-1} is at most n. You can use group properties to show that $gxg^{-1} \cdot gxg^{-1} = gx^2g^{-1}$. So we can do the following calculation:

$$\begin{aligned}(gxg^{-1})^n &= \underbrace{gxg^{-1}gxg^{-1}\cdots gxg^{-1}}_{\text{n times}}\\ &= gx^ng^{-1}\\ &= gg^{-1} \text{ since } x^n = e, \text{ as the order of } x \text{ is n}\\ &= e\end{aligned}$$

We have just shown that $(gxg^{-1})^n = e$, so $|gxg^{-1}| \leq |x|$. Since this is true for arbitrary x and g, let $x' = gxg^{-1}$ and let $g' = g^{-1}$. By what we have just shown, $|g'x'g'^{-1}| \leq |x'|$. But since $g'^{-1} = g$, we know that $g'x'g'^{-1} = g^{-1}(gxg^{-1})g = x$. Therefore, $|g'x'g'^{-1}| \leq |x'|$ just means that $|x| \leq |gxg^{-1}|$. Thus $|gxg^{-1}| = |x|$.

Now we will show that $|xy| = |yx|$. Suppose $|xy| = n$. Then,

$$\underbrace{xy\cdots xy}_{\text{n times}} = e$$

Multiplying both sides by y^{-1} on the right, we get

$$\begin{aligned}&xy\cdots xyy^{-1} = ey^{-1} = y^{-1} \text{ i.e.}\\ &\underbrace{xy\cdots xy}_{\text{n-1 times}}\, x = y^{-1}\end{aligned}$$

Now multiplying by y on the left, we get

$$y\,\underbrace{xy\cdots xy}_{\text{n-1 times}}\, x = yy^{-1} = e$$

Note that in the last line, we really have yx multiplied by itself n times. Thus $|yx| \leq |xy|$. Since this is true for arbitrary x and y, we can switch the role of x and y. So we see that $|xy| \leq |yx|$ as well. Therefore, $|xy| = |yx|$.

How this relates to last week's bonus problem: Suppose R and S are rotations of the sphere, and RS has finite order. Since rotations of the sphere form a group, the above statement shows that SR has the same order as RS. If RS is a rotation of order n, then it must rotate by the angle $2\pi/n$. Thus SR rotates by $2\pi/n$ as well. Therefore, if RS has finite order then both RS and SR are rotations through the same angle. Note that there are plenty of rotations that are not finite order, however. Consider, for example, a rotation of the sphere through any axis by angle $\pi/\sqrt{2}$. □

Problem 5.1. Find all the subgroups of each of the groups $\mathbb{Z}_4$, $\mathbb{Z}_7$, $\mathbb{Z}_{12}$, D_4 and D_5.

Answer. We start with a general remark that will make this problem easier.

Remark. Let G by a group, and let $g \in G$ have finite order. Then g^{-1} is a power of g. This is because there is some n s.t. $g^n = e$. So $g \cdot g^{n-1} = e$ meaning $g^{-1} = g^{n-1}$.

In all of these groups, each element has finite order so this remark applies.

We will write $G =< g_1, \ldots, g_n >$ for a group generated by $g_1, \ldots, g_n$. In the following examples, we will find lists of subgroups by choosing subsets of each group to be generators. Note that the above remark means that $< g >=< g^{-1} >$ for all elements g of finite order.

- $\mathbb{Z}_4$: First of all 1 and 3 generate $\mathbb{Z}_4$, so if they were in any generating set we would get all of $\mathbb{Z}_4$ back. On the other hand, the only multiples of 2 are 0 and 2 itself. So the three subgroups are $\{e\}$, $< 2 >= \{0, 2\}$ and $\mathbb{Z}_4$.
- $\mathbb{Z}_7$: All the non-zero elements n of $\mathbb{Z}_7$ generate $\mathbb{Z}_7$. So the only two subgroups are $\{0\}$ and $\mathbb{Z}_7$.
- $\mathbb{Z}_{12}$: The elements $1, 5, 7$ and 11 generate $\mathbb{Z}_{12}$. Since 10 is the additive inverse of 2, $< 2 >=< 10 >$ by the remark at the start of the solution. Similarly, $< 3 >=< 9 >$ and $< 4 >=< 8 >$. 6 is its own inverse so $< 6 >$ isn't paired with anyone.

  Next, we look at subgroups with more than one generator. By the above, including 1,5,7 or 11 in a generating set yields all of $\mathbb{Z}_{12}$. If both 2 and 3 are generators of a subgroup, then 5 is in that subgroup, so including both 2 and 3 in a generating set yields all of $\mathbb{Z}_{12}$. Likewise, including 3 and 4 means 7 will be in the subgroup, so you get all of $\mathbb{Z}_{12}$ again. Since $< 4 >$ is a subset of $< 2 >$, including both 2 and 4 in a generating set is the same as including just 2. So $< 2, 4 >=< 2 >$. Likewise, $< 2, 6 >=< 2 >$. Finally, including 4 and 6 in a generating set means 2 will be in your subgroup, so you may as well have just included 2. That is, $< 4, 6 >=< 2 >$.

  Therefore the subgroups of $\mathbb{Z}_{12}$ are $\{0\}, < 2 >= \{0, 2, 4, 6, 8, 10\}, < 3 >= \{0, 3, 6, 9\}$, $< 4 >= \{0, 4, 8\}$, $< 6 >= \{0, 6\}$ and $\mathbb{Z}_{12}$.
- $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$: The one-generator subgroups of D_4 are $\{e\}$, rotation subgroups $< r >= \{e, r, r^2, r^3\}, < r^2 >= \{e, r^2\}$ and reflection subgroups $< rs >= \{e, rs\}, < r^2s >= \{e, r^2s\}$ and $< r^3s >= \{e, r^3s\}$.

  To get more subgroups we can add generators. Adding a rotation to a rotation subgroup doesn't yield anything new. Adding any reflection to $< r >$ gives us a subgroup with both r and s, meaning we get D_4 back. But we can add a reflection to the subgroup $< r^2 >$. We get $< r^2, s >= \{e, r^2, s, r^2s\}$, and $< r^2, rs >= \{e, r^2, rs, r^3s\}$. Adding any more generators to these two subgroups gives us all of D_4.

  Putting another reflection in a reflection subgroup means that subgroup will have a rotation, and we have just listed all the subgroups with a rotation and a reflection. So the only subgroups are the ones listed above and all of D_4.

- $D_5 =< e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s >$: The one-generator subgroups are: Rotations :$\{e\}, < r >= \{e, r, r^2, r^3, r^4\}$, Reflections: $< s >= \{e, s\}, < rs >= \{e, rs\}, < r^2s >= \{e, r^2s\}, < r^3s >= \{e, r^3s\}$ and $< r^4s >= \{e, r^4s\}$. We cannot add any reflections to the subgroup generated by r since then we would get r and s in the subgroup, giving us the whole group back. Putting adding a reflection to a reflection subgroup will give a rotation, and as we have just said, a subgroup with a rotation and a reflection is the whole group. So the only subgroups are the ones listed above, and D_5 itself.

□

Problem 5.4. Find the subgroup of D_n generated by r^2 and r^2s, distinguishing carefully between the cases n odd and n even.

Answer. Let $G =< r^2, r^2s >$. The elements of G are of the form $(r^2)^{a_1} \cdot (r^2s)^{b_1} \cdots (r^2)^{a_k} \cdot (r^2s)^{b_k}$ where $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$. One can check that $r^2s \cdot r^2 = s$ and $r^2s \cdot r^2s = e$. So the expression above simplifies to an expression of the form $r^{2l}s$ for some $l \in \mathbb{Z}$.

Suppose n is even. Then $n = 2m$ for some $m \in \mathbb{Z}$. Thus $r^n = (r^2)^m = e$, so the powers of r^2 are all the even powers of r up to $2(m-1)$. Thus $G = \{e, r^2, \ldots, r^{2(m-1)}, r^2s, \ldots, r^{2(m-1)}s\}$.

Now suppose n is odd. Then $n = 2m+1$ for some $m \in \mathbb{Z}$, and $r^{2m+1} = e$. Since r^{2m+2} is a power of r^2 and $r^{2m+2} = r$, we have that r is in G. And since $r^2s \cdot r^2 = s$, $s \in G$. But r and s generate all of D_n, so $G = D_n$. □

Problem 5.5. Suppose H is a *finite* non-empty subset of a group G. Prove that H is a subgroup of G iff xy belongs to H whenever x and y belong to H.

Proof. Let G be a group, and H a finite subset of G.

Suppose xy belongs to H whenever x and y belong to H. This means that H is closed under the group operation. And since H is a subset of G, it is associative. So we only need to show that the identity is in H and elements of H have inverses also in H.

Since H is non-empty, we can choose an arbitrary element $x \in H$. Consider the set $S = \{x, x^2, x^3, \ldots, x^n, \ldots\}$. By the assumption, this whole set is in H since every element of S is just x multiplied by the previous element. But H is a finite set. So S must also be a finite set. Which means that elements of S must repeat. That is, there are numbers $i \neq j$ s.t. $x^i = x^j$. Multiplying both sides by x^{-i}, we get the equation $e = x^{j-i}$. But x^{i-j} is in S. Thus, the identity is in H, and moreover the identity is a power of x. Write $n = j - i$. Since $x^n = e$, then $x \cdot x^{n-1} = e$. So $x^{n-1} = x^{-1}$. Since $x^{n-1} \in H$, the inverse of x is in H. Since x was chosen arbitrarily, every element of H has an inverse. So H is a subgroup of G.

Now suppose H is a subgroup of G. Then H is closed under group multiplication, so for any x and y in H, xy is also in H. Therefore, when H is a finite subset of G, H is closed under multiplication if and only if it is a subgroup. □

Problem 5.7. Let G be an *abelian* group and let H consist of those elements of G which have finite order. Prove that H is a subgroup of G.

Proof. Since H is a subset of G it already has the associativity property. Also the identity has order 1, so $e \in H$. So we just need to show it is closed under multiplication and has inverses.

Let $x, y \in H$. Let $|x| = n, |y| = m$ for $n, m \in \mathbb{Z}$. Since G is abelian, $(xy)^{nm} = x^{nm}y^{nm}$. But $x^{nm} = (x^n)^m = e^m$ and $y^{nm} = (x^m)^n = e^n$. So $(xy)^{nm} = e$. Thus the order of xy is at most nm, so $xy \in H$. Therefore H is closed under multiplication.

Let $x \in H$ with $|x| = n$. Then $x^n = e$, so multiplying both sides by x^{-n} we get $e = x^{-n} = (x^{-1})^n$. So the order of x^{-1} is at most n. (In fact, it is n, since we can reverse the roles of x and x^{-1}. Therefore, $x^{-1} \in H$.

So we have shown that H is a subgroup of G. □

Problem 5.11. Show $\mathbb{Q}$ is not cyclic. Even better, prove that $\mathbb{Q}$ cannot be generated by a finite number of elements.

Proof. First we show that $\mathbb{Q}$ is not cyclic. We will do this by contradiction, so suppose it is cyclic. Then it would be generated by a rational number of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$. The set $< \frac{a}{b} >$ consists of all integer multiples of $\frac{a}{b}$. So if $\mathbb{Q} =< \frac{a}{b} >$ then $\frac{a}{2b}$ must be an integer multiple of $\frac{a}{b}$. But if

$$c\frac{a}{b} = \frac{a}{2b}$$

then $c = 1/2$ which is not an integer. Therefore $\mathbb{Q}$ cannot be generated by a single rational number, so $\mathbb{Q}$ is not cyclic.

Now we show that $\mathbb{Q}$ cannot be generated by a finite set of rational numbers. Suppose for contradiction that $\mathbb{Q} =< \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} >$. Since the number $\frac{1}{2b_1 \cdots b_n} \in \mathbb{Q}$, there must be integers $c_1, \dots, c_n$ s.t.

$$c_1\frac{a_1}{b_1} + \cdots + c_n\frac{a_n}{b_n} = \frac{1}{2b_1 \cdots b_n}$$

By adding together the fractions on the left hand side, we get

$$c_1\frac{a_1}{b_1} + \cdots + c_n\frac{a_n}{b_n} = \frac{A_1 + \dots A_n}{b_1 \cdots b_n}$$

where $A_i = c_i a_i b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. Write $A = A_1 + \dots A_n$ to simplify notation. Note that since the A_i are integers, A must be an integer. So we claim that

$$\frac{A}{b_1 \cdots b_n} = \frac{1}{2b_1 \cdots b_n}$$

This can only happen if $A = 1/2$. But A was supposed to be an integer, so we have arrived at a contradiction. Thus $\mathbb{Q}$ cannot be generated by a finite set of rational numbers. □