Homework Assignment 4

Due Friday, February 21

1. Let G be a group. Let $H, K \leq G$ be two subgroups.

   (a) Show that the intersection $H \cap K$ is a subgroup of G.

   Proof. We first must show $H \cap K$ is nonempty, but as H and K are both subgroups, the both contain 1, and therefore so does $H \cap K$. Next we must show that $H \cap K$ has inverses, so fix an member x. As x is in the subgroup H, so is x^{-1}, and we can similarly argue that $x^{-1} \in K$ as well. Therefore $x^{-1} \in H \cap K$. Finally we must show that if $x, y \in H \cap K$, then so is xy. But $x, y \in H$ implies xy is as H is a subgroup, and similarly $xy \in K$. Therefore $xy \in H \cap K$, completing the proof. □

   (b) Give an example to show that the union $H \cup K$ need not be a subgroup of G.

   Proof. The even numbers $2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, 6, \cdots\} \leq \mathbb{Z}$ and the multiples of three $3\mathbb{Z} = \{\cdots, -6, -3, 0, 3, 6, 9\} \leq \mathbb{Z}$ are both subgroups of the integers. Their union $2\mathbb{Z} \cup 3\mathbb{Z}$ consists of integers which are either even or mutliples of 3. Thus it contains both 2 and 3. But their sum $2 + 3 = 5$ is not even or a multiple of 3, thus is not in the union. Therefore the union isn't closed under addition, and therefore is not a subgroup. □

   (c) Show that $H \cup K$ is a subgroup of G if and only if $H \subset K$ or $K \subset H$.

   Proof. If $H \subset K$, then $H \cup K = K$ is a subgroup, and if $K \subset H$ the proof is identical. On the other hand, suppose thaat $H \cup K$ is a subgroup. Suppose for the sake of contradiciton that neither of H or K is contained in the other, so that we can find $h \in H \setminus K$ and $k \in K \setminus H$. As $H \cup K$ is a subgroup that $hk \in H \cup K$, so (without loss of generality) we may assume that $hk \in H$. But then mutliplying by h^{-1} on the left, we have $k \in H$, contrary to our assumption. □

2. Let A be an *abelian* group.

   (a) Let $A^n = \{a^n | a \in A\}$ be the collection of nth powers of elements in A. Show that this is a subgroup of A.

   Proof. It is nonempty as $1^n = 1 \in A^n$. If $x \in A^n$ then $x = a^n$, so that $x^{-1} = a^{-n} = (a^{-1})^n \in A^n$ so that A^n has inverses. If $x, y \in A^n$ then $x = a^n$ and $y = b^n$. Therefore $xy = a^n b^n = (ab)^n \in A^n$. Notice in the last step we used that A is abelian, as in general we dont have $(ab)^n = a^n b^n$ (for instance, if $n = 2$ this says $abab = a^2 b^2$ which requires commuting an n and a b). □

   (b) Let $A[n] = \{a \in A | a^n = 1\}$. Show that $A[n]$ is a subgroup of A. This is often called the *n-torsion* subgroup of A.

   Proof. As $1^n = 1$ then 1 is n-torsion and so $A[n]$ is nonempty. If $x \in A[n]$ then $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$ so that x^{-1} is n-torsion and $A[n]$ has inverses. If $x, y \in A[n]$ then $(xy)^n = x^n y^n = 1 \cdot 1 = 1$ so that xy is n-torsion as well. Notice again here we used that A is abelian. □

(c) Let $A^{\text{tors}} = \{a \in A | \, |a| < \infty\}$. Show that A^{tors} is a subgroup of A. This is often called the *torsion* subgroup of A.

Proof. Notice 1 has order 1 so A^{tors} is nonempty. If $x \in A^{\text{tors}}$ then $|x^{-1}| = |x| < \infty$ so that A^{tors} contains inverses. If $x, y \in A^tors$ then let $n = |x|$ and $m = |y|$. Then

$$(xy)^{mn} = x^{mn}y^{mn} = (x^n)^m(y^m)^n) = 1^m 1^n = 1,$$

so that A^{tors} is closed under multiplication. □

(d) Give an example of a nonabelian group G where G^{tors} is not a subgroup of G. (Note that G must be infinite, as if G were finite every element would have finite order so that we would have $G^{\text{tors}} = G$).

Proof. Note: this takes some creativity as we haven't really defined this group in class. I have the following example in mind, but there are certainly others. Let D_∞ be the infinite dihedral group, which we can define in terms of generators and relations as $\langle r, s | s^2 = 1, rs = sr^{-1} \rangle$. Then $|sr^i| = 2$ for every i (the proof is the same as homework 2 problem 8). Thus, $sr, sr^2 \in D_\infty^{\text{tors}}$. But

$$(sr)(sr^2) = s(rs)r^2 = s(sr^{-1})r^2 = s^2 r = r.$$

As $|r| = \infty$, r is not torsion, so that D_∞^{tors} is not closed under multiplication, and therefore cannot be a subgroup. □

3. Compute the center of the dihedral group. Explicitly, let n be an integer ≥ 3. Compute $Z(D_{2n})$. (Note: you will need to split into the two cases, where n is even or n is odd).

Proof. We first notice that for an element to be in the center of a group, it need only commute with the generators of that group. We record this as a lemma.

Lemma 1. *Let G be a group generated by $g_1, \cdots, g_n$. If $x \in G$ and $g_i x = x g_i$ for all i, then $x \in Z(G)$.*

Proof. First notice that if $xg = gx$ then $xg^i = g^i x$ for all powers of g. For positive powers we pass one by one inductively. To get negative powers notice $xg^{-1} = g^{-1}x$ by multiplying on the left and right by g, and then proceeding inductivly again. As every element of g is an algebraic combination of powers of the g_i, we just pass them by x one by one and observe commutatitivity. □

Therefore, to see if an element $x \in D_{2n}$ is in the center, we need only check if multiplication commutes with r and with s, If $x = sr^i$ we have:

$$xr = sr^{i+1}$$

and

$$rx = rsr^i = sr^{i-1}.$$

Therefore if $xr = rx$ we deduce that $r^2 = 1$, but $n > 3$ so this equality does not hold. Therefore sr^i is never in the center of D_{2n}

If $x = r^i$ (for $0 \leq i < n$) then $xr = rx$. Also notice that

$$sx = sr^i$$

and

$$xs = sr^{-i}.$$

So if $xs = sx$ then we deduce $r^{2i} = 1$. As $0 \leq i < n$ we have $i = 0$ or $i = n/2$. Thus if n is even we have $Z(D_{2n}) = \{1, r^{n/2}\}$ and if n is odd we have $Z(D_{2n}) = \{1\}$ as we cannot take fractional powers of r. □

4. Let G be a group.

(a) Show that if H is a subgroup of G, then $H \leq N_G(H)$.

Proof. Recall that $N_G(H) = \{g \in G : gHg^{-1} = H\}$. Let $h \in H$. Then for every $x \in H$ we have $hxh^{-1} \in H$ as it is the product of three elements of H. Therefore $hHh^{-1} = H$ implying that h is in the normalizer of H. As $h \in H$ was arbitrary we have $H \subseteq N_G(H)$, and as H is already a subgroup of G, it contains inverses and products so in fact $H \leq N_G(H)$. □

(b) Give an example where $A \subset G$ is a a subset (not necessarily a subgroup), and $A \not\subset N_G(A)$.

Proof. Let $G = D_{2n}$ for $n \geq 3$. Notice that if we conjugate r by s we get

$$srs^{-1} = r^{-1}ss^{-1} = r^{-1}.$$

Therefore let $A = \{r, s\}$ (just the two element set, not the subgroup they generate).

$$sAs^{-1} = \{srs^{-1}, sss^{-1}\} = \{r^{-1}, s\} \neq A.$$

Therefore $s \notin N_G(A)$ so that $A \not\subseteq N_G(A)$. □

(c) Show that $H \leq C_G(H)$ if and only if H is abelian.

Proof. We recall that $C_G(H) = \{g \in G : ghg^{-1} = h \text{ for all } h \in H\}$. Suppose $H \leq C_G(H)$ and fix $x, y \in H$. Then $x \in C_G(H)$ so that $xyx^{-1} = y$. Multiplying on the right by x shows that $xy = yx$. Since x and y were abitrary elements of H we conclude that H is abelian.

Conversely, suppose that H is abelian. Fix $h \in H$. Then for every $g\imath H$ we have $gh = hg$. Multilying on the left by g^{-1} shows $ghg^{-1} = h$. Since this holds for each $h \in H$ we conclude $g \in C_G(H)$. As g was arbitrary then $H \subseteq C_G(H)$, and arguing as in the end of 4(a) then $H \leq C_G(H)$. □

5. In class we classified all finite cyclic groups and their generators. In this exercise you take care of the infinite case. Let $H = \langle x \rangle$ be a cyclic group of infinite order.

(a) Show that the map $\varphi : \mathbb{Z} \to H$ defined by the rule $\varphi(a) = x^a$ is an isomorphism.

Proof. We first show that φ is a homomorphism. But this is clear as:

$$\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b).$$

Next we show it is bijective. We will show it is injective and surjective. Surjectivity is easy, as every element of H is of the form x^a for some $a \in \mathbb{Z}$, and is therefore equal to $\varphi(a)$. For injectivity, suppose $\varphi(a) = \varphi(b)$. Then $x^a = x^b$. Therefore $x^{b-a} = 1$. As x has infinite order, this can only happen if $b - a = 0$, so that $a = b$. $\square$

(b) Since H is cyclic every element of H is of the form x^a for some a. Show that x^a generates H if and only if $a = \pm 1$.

Proof. Using the homomorphism φ from part (b) we notice that x^b is a power of x^a if and only if $a|b$. Since 1 and -1 divide every integer, we have x and x^{-1} both generate H. On the other hand, if x^a generates H then in particular it must have a power equal to x. Thus $a|1$ so a must equal ± 1 $\square$

6. In this exercise we study products of finite cyclic groups. Recall that we denote by Z_n the cyclic group of order n (written multiplicatively).

(a) Prove that $Z_2 \times Z_2$ is not a cyclic group.

Proof. Notice that $|Z_2 \times Z_2| = 4$. Therefore if it were cyclic, it would need a generator x of order 4. But notice that if $x = (a, b)$ then $x^2 = (a^2, b^2) = (1, 1)$ since a, b have order ≤ 2 as elements of Z_2. Therefore $|x| \leq 2$ so x cannot generate the entire group. $\square$

(b) Prove that $Z_2 \times Z_3 \cong Z_6$. Conclude that $Z_2 \times Z_3$ is a cyclic group.

Proof. For simplicity we use the identification $Z_n = \mathbb{Z}/n\mathbb{Z}$ and write additively. I claim $(\overline{1}, \overline{1})$ generates $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Indeed, since $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}| = 6$ it suffices to show that $|(\overline{1}, \overline{1})| = 6$. Suppose that for some $n > 0$ we have $n(\overline{1}, \overline{1}) = (\overline{n}, \overline{n}) = (0, 0)$. This implies that $2|n$ and that $3|n$. In particular we have $6|n$. Thus the smallest n can be is 6. As $(\overline{6}, \overline{6}) = (0, 0)$ we have $|(\overline{1}, \overline{1})| = 6$ completing the proof. $\square$

Those two examples really cover all the bases. Use the intuition you gained from them to prove the following classification result.

(c) Show that $Z_n \times Z_m$ is cyclic if and only if $\gcd(n, m) = 1$. (Hint: recall that up to isomorphism there is only one cyclic group of order N for every positive integer N).

Proof. The real heavy lifting here is done because $\gcd(m, n) = 1$ if and only if $\operatorname{lcm}(m, n) = mn$. I will state and prove this here as a lemma, but it is rather well known and elementary so I am ok with it just being used without proof in this instance.

Lemma 2. *Let $a, b \in \mathbb{Z}$ be positive integers. then*

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

In particular, $\gcd(a, b) = 1$ *if and only if* $\operatorname{lcm}(a, b) = ab$.

Proof. By the fundamental theorem of arithmetic we have prime factorizations

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}, \end{aligned}$$

where we allow α_i or β_i to be 0 so that the p_i are the same. Then it is clear that,

$$\begin{aligned} \gcd(a,b) &= p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)} \\ \operatorname{lcm}(a,b) &= p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}. \end{aligned}$$

Thus the product is

$$gcd(a,b) \cdot \operatorname{lcm}(a,b) = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n} = ab,$$

and we win. □

With this in hand we can proof the classification result. As in part b we identify Z_n with $\mathbb{Z}/n\mathbb{Z}$ and write additively. First suppose that $\gcd(n,m) = 1$. Then $(\overline{1}, \overline{1})$ is a generator for $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Indeed, if $a > 0$ and

$$a(\overline{1}, \overline{1}) = (\overline{a}, \overline{a}) = (0,0)$$

then $n|a$ and $m|a$, so that $\operatorname{lcm}(m,n) = mn$ divides a. Thus

$$|(\overline{1}, \overline{1})| = mn = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|,$$

so $(\overline{1}, \overline{1})$ generates the group and so it is cyclic of order mn.
Conversely, suppose that $\gcd(n,m) \neq 1$. Then $l = \operatorname{lcm}(m,n) < mn$. Therefore for any $(\overline{a}, \overline{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, we have $l(\overline{a}, \overline{b}) = (\overline{la}, \overline{lb}) = (0,0)$ so that $|(\overline{a}, \overline{b})| \leq l < mn$ and it cannot be a generater. Therefore $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ cannot be cyclic. □

7. Let $G = S_n$ be the symmetric group equipped with it's natural action on $\Omega_n = \{1, 2, \cdots, n\}$ by permutations. For $i \in \Omega_n$, let $G_i = \{\sigma \in G | \sigma(i) = i\}$ be the stabilizer of i. What is $|G_i|$?

Proof. Reording the elements of Ω_n, we may assume that $i = n$. Then an element of G_n is just a permutation of $1, 2, \cdots, n-1$, keeping n fixed. In fact, we have just described an bijection (in fact an isomorphism) $G_n \to S_{n-1}$. In particular, this implies that for any i, we have

$$|G_i| = |G_n| = |S_{n-1}| = (n-1)!$$

□