Homework Assignment 4

Due Friday, February 18

1. 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. □

   (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. □

   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 being used without proof.

   Lemma 1. *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 generator. Therefore $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ cannot be cyclic. $\square$

2. Let G be a group and H a *nonempty* subset of G. Let's introduce a few tricks to speed up testing if something is a subgroup.

   (a) *(Subgroup Criterion)* Suppose that for all $x, y \in H$, $xy^{-1} \in H$. Show that H is a subgroup of G.

   Proof. H is nonempty by assumption. Suppose $x \in H$. Then by assumption $xx^{-1} = 1 \in H$. Since $1, x \in H$, then $1x^{-1} = x^{-1} \in H$, so H is closed under inversion. Now fix $x, y \in H$. We have already seen H is closed under inversion so that $x, y^{-1} \in H$, and thus $x(y^{-1})^{-1} = xy \in H$. Therefore H is closed under multiplication so we win. $\square$

   (b) *(Finite Subgroup Criterion)* Show that if H is finite and closed under multiplication, then H is a subgroup of G.

   Proof. H is nonempty and closed under multiplication by assumption. All that remains is to show it is closed under inversion. Since H is closed under multiplication, we know that the set $\{x, x^2, x^3, x^4, \cdots\} \subseteq H$. Since H is finite, we know that the list of powers of x cannot go on forever without repeating (else we would be exhibiting infinitely many different elements of H). Therefore there is some $i < j$ with $x^i = x^j$. In particular, $x^{j-i} = 1$, and $x^{-1} = x^{j-i-1} \in \{x, x^2, x^3, \cdots\} \subseteq H$, and therefore H is closed under inversion. (To be completely precise, one could also have $j - i - 1 = 0$, but then $x^{-1} = 1 = x \in H$ so we're ok.) $\square$

3. 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, they 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 also because H is a subgroup, and similarly $xy \in K$. Therefore $xy \in H \cap K$, completing the proof. $\square$

(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. Conversely, suppose that $H \cup K$ 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. □

(d) Adjust your proof from part (a) to show that the intersection of an arbitrary collection of subgroups is a subgroup. That is, let $\mathcal{A}$ be a collection of subgroups of G. Show that

$$\bigcap_{H \in \mathcal{A}} H$$

is a subgroup of G. This completes the proof that the subgroup generated by a subset is in fact a subgroup.

Hint. *For part (d), the proof should be very similar to part (a), with only cosmetic modifications. You won't need to use induction. In fact, since $\mathcal{A}$ is could in principle be uncountable, induction won't work without modifications (think about why this is).*

Proof. We first must show $\mathbb{H} = \bigcap_{H \in \mathcal{A}} H$ is nonempty, but since $1 \in H$ for all H, 1 is in their intersection. Next we must show that $\mathbb{H}$ has inverses, so fix an member x. As x is in each $H \in \mathcal{A}$, so is x^{-1}, so that x^{-1} is in the intersection and thus in $\mathbb{H}$. Finally we must show that if $x, y \in \mathbb{H}$, then so is xy. But for each H we know $x, y \in H$, so that $xy \in H$ as well. Since this holds for each H, xy is in the intersection, which is $\mathbb{H}$. □

4. Given a homomorphism $\varphi : G \to H$, we obtain 2 important subgroups, one of G and one of H. They are called the *kernel of* φ and *image of* φ and are defined by the following rules:

$$\begin{aligned} \ker \varphi &= \{g \in G : \varphi(g) = 1_H\}, \\ \operatorname{im} \varphi &= \{h \in H : h = \varphi(g) \text{ for some } g \in G\}. \end{aligned}$$

(a) Show that $\ker \varphi$ is a subgroup of G.

Proof. We know $1_G \in \ker \varphi$ by HW3 Problem 4(a) so that it is nonempty. If $x \in \ker \varphi$ then applying HW3 Problem 4(b) we have:

$$\varphi(x^{-1}) = \varphi(x)^{-1} = 1_H^{-1} = 1_H.$$

so that $x^{-1} \in \ker \varphi$ also. If $x, y \in \ker \varphi$, then

$$\varphi(xy) = \varphi(x)\varphi(y) = 1_H \cdot 1_H = 1_H,$$

so that xy is too. Thus it is a subgroup. □

(b) Show that $\operatorname{im}\varphi$ is a subgroup of H.

Proof. We must first show it is nonempty, but by HW3 Problem 4(a) it contains 1_H. Next we show it contains inverses, but this follows by HW3 Problem 4(b) as if $x = \varphi(a) \in \operatorname{im}\varphi$ then $x^{-1} = \varphi(a)^{-1} = \varphi(a^{-1})$. Finally, if $x = \varphi(a)$ and $y = \varphi(b)$ are in the image, then $xy = \varphi(a)\varphi(b) = \varphi(ab)$ is in the image as well. □

(c) *Important:* Show that φ is injective if and only if $\ker\varphi = \{1_G\}$. (This is an incredibly useful fact!)

Proof. Suppose φ is injective. If $g \in \ker\varphi$ then $\varphi(g) = 1_H = \varphi(1_G)$ so that by injectivity $g = 1_G$.
Conversely, suppose $\ker\varphi = \{1_G\}$. Fix $x, y \in G$ and suppose $\varphi(x) = \varphi(y) = h$. Then:

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = h \cdot h^{-1} = 1_H.$$

Thus $xy^{-1} = 1_G$. Multiplying on the right by y shows $x = y$ and so φ injects. □

5. The kernel has the following important generalization. For $h \in H$ define the *fiber over* h as

$$\varphi^{-1}(h) = \{g \in G : \varphi(g) = h\}.$$

This is sometimes also called the *preimage of* h. Observe that by definition, the kernel of φ is the fiber over 1.

(a) Show that the fiber over h is a subgroup if and only if $h = 1_H$.

Proof. If $h = 1_H$ then $\varphi^{-1}(h) = \ker\varphi$ which we showed was a subgroup in 4(a). Conversely, suppose $\varphi^{-1}(h)$ is a subgroup. Then in particular it contains 1_G. So that $h = \varphi(1_G) = 1_H$ as desired. □

(b) Show that the *nonempty* fibers of φ form a partition of G. (In particular, if φ is surjective its fibers partition G.)

Proof. First notice we are only considering nonempty fibers so the elements of the partition are by definition nonempty. We must show their union is all of G, but if $g \in G$ then $\varphi(g) = h$ and so $g \in \varphi^{-1}(h)$ as desired. Lastly we must show they have empty intersections. Let $g \in \varphi^{-1}(h) \cap \varphi^{-1}(h')$. Then $h = \varphi(g) = h'$ so they were the same fibers to begin with. □

(c) Show that all nonempty fibers have the same cardinality. (Hint: if $\varphi^{-1}(h)$ is nonempty, build a bijection between it and $\ker\varphi$.) Observe that this generalizes 2(c).

Proof. (Note: in my opinion this is the most difficult problem of the assignment).
It suffices to build a bijection $f : \ker\varphi \to \varphi^{-1}(h)$. Fix some $x \in \varphi^{-1}(h)$. For $g \in \ker\varphi$, define $f(g) = x \cdot g$. Let us begin by first checking that this defines a map to $\varphi^{-1}(h)$, i.e., that the image of f actually lies in the fiber over h. To check this we apply φ to xg and notice that

$$\varphi(xg) = \varphi(x)\varphi(g) = h \cdot 1_H = h,$$

so that $xg \in \varphi^{-1}(h)$ as desired. What remains is to show that f is a bijection. To do this we construct an inverse $f^{-1} : \varphi^{-1}(h) \to \ker\varphi$. As f was multiplication by x then the inverse should be multiplication by x^{-1}. As above, we begin by showing this map actually lands in the kernel, that is, fixing $g' \in \varphi^{-1}(h)$, we must see that $x^{-1}g' \in \ker\varphi$. Applying φ we see

$$\varphi(x^{-1}g') = \varphi(x^{-1})\varphi(g') = \varphi(x)^{-1}\varphi(g') = h^{-1}h = 1_H,$$

so that it is indeed in the kernel. From here it is clear that f^{-1} is an inverse to f, as composition is multiplictation by $x^{-1}x$ or xx^{-1}, i.e., mutliplication by 1_G or the identity map. Thus we have built a bijection between $\ker\varphi$ and $\varphi^{-1}(h)$ and so they must have the same cardinality. Since every nonempty fiber has the same cardinality as $\ker\varphi$ they all have the same cardinality. □

6. Let G be a group and A a set, and suppose we are given homomorphism $\varphi : G \to S_A$. Show that the rule:

$$g \cdot a = \varphi(g)(a) \text{ for all } g \in G \text{ and } a \in A,$$

describes a group action of G on A, and further that the permutation representation of this action is φ itself.

Proof. We first show that the rule given actually defines a group action. There are two conditions:

(a) $1 \cdot a = a$ for all $a \in A$

(b) $g \cdot (h \cdot a) = (gh) \cdot a$ for all $g, h \in G$ and $a \in A$

To show the first we observe that by HW3 Problem 4(a): $\varphi(1) = id_A$. Therefore:

$$1 \cdot a = \varphi(1)(a) = id_A(a) = a,$$

as desired. To show the second condition we compute:

$$g \cdot (h \cdot (a)) = \varphi(g)\left(\varphi(h)(a)\right) = \left(\varphi(g) \circ \varphi(h)\right)(a) = \varphi(gh)(a) = (gh) \cdot a.$$

Here we use that that multiplication in S_A is composition, and φ is a homomorphism, so that $\varphi(g) \circ \varphi(h) = \varphi(gh)$. Therefore we have confirmed that the rule defines an action.

Consider the action defined above, and let $\psi : G \to S_A$ be the permutation representation. That is, $\psi(g) = \sigma_g$ where $\sigma_g(a) = g \cdot a$. We want to confirm that $\varphi = \psi$. This means showing that for every $g \in G$, $\varphi(g)$ and $\psi(g)$ agree as functions on A. To see this we compute:

$$\psi(g)(a) = \sigma_g(a) = g \cdot a = \varphi(g)(a).$$

□

7. Let G be a group acting on a set A. For an element $a \in A$, we define the *stabilizer* of a to be the collection of elements of G that act trivially on a, that is:

$$G_a := \{g \in G : g \cdot a = a\}.$$

The *kernel* of the group action is the collection of elements of G that act trivially on *all of* A, that is:

$$G_0 := \{g \in G : g \cdot a = a \text{ for all } a \in A\}.$$

(a) Prove that G_a and G_0 are subgroups of G.

Proof. Notice that $1 \cdot a = a$, so that $1 \in G_a$. Suppose $g, h \in G_a$. Then:

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a,$$

so that $gh \in G_a$, and therefore it is closed under multiplication. Suppose that $g \in G_a$. Then:

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a,$$

so that $g^{-1} \in G_a$. Therefore G_a is closed under inversion as well, and is therefore a subgroup.

The proof for G_0 is very similar. First that $1 \cdot a = a$ for every a, so that $1 \in G_0$. Suppose $g, h \in G_0$. Then for each $a \in A$:

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a,$$

so that $gh \in G_0$, and therefore it is closed under multiplication. Suppose that $g \in G_0$. Then for every $a \in A$:

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a,$$

so that $g^{-1} \in G_0$. Therefore G_0 is closed under inversion as well, and is therefore a subgroup. □

(b) Prove that G_0 is equal to the kernel of the permutation representation associated to the action of G on A. (cf. Problem 4: This justifies the naming convention).

Proof. Let $\varphi : G \to S_A$ be the permutation representation sending g to the function $\sigma_g(a) = g \cdot a$.

$$\begin{aligned} g \in \ker \varphi \quad &\Leftrightarrow \quad \sigma_g = id_A \\ &\Leftrightarrow \quad \sigma_g(a) = a \text{ for every } a \in A \\ &\Leftrightarrow \quad g \cdot a = a \text{ for every } a \in A \\ &\Leftrightarrow \quad g \in G_0. \end{aligned}$$

□

8. For $n \geq 2$ 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. Describe an isomorphism between G_i and S_{n-1}.

Proof. Reordering 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 particular, this gives an action on $\{1, \cdots, n-1\}$. The permutation representation is then a homomorphism $G_n \to S_{n-1}$. It is surjective as any permutation of $1, \cdots, n-1$ can be extended to a permutation of $1, \cdots, n$ by keeping n fixed. To see injectivity suppose $\sigma \in G_n$ is in the kernel. This means it fixes $1, \cdots, n-1$, and since it is in G_n it fixes n. Therefore σ is the identity permutation, and so the kernel is trivial. By 4(c), the map is injective. □