MATH 3311, FALL 2025: HOMEWORK 3

(1) Decide if the following statements are true or false and write down a sentence or two justifying your answer:

(a) If $f : G \to H$ is a group homomorphism, then, for every $g \in G$, we have

$$f(g)^{-1} = f(g^{-1}).$$

True: Note first that $f(e_G *_G g) = f(g) = f(e_G) *_H f(g)$ so via right cancellation, $f(e_G) = e_H$. Now, $f(g *_G g^{-1}) = f(g) *_H f(g^{-1})$ and $f(g *_G g^{-1}) = f(e_G) = e_H$. As such, $f(g) *_H f(g^{-1}) = e_H$, meaning $f(g^{-1}) = f(g)^{-1}$.

(b) The groups $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ are not isomorphic.

False: They are both cyclic groups of order 6. Mapping the generator $1 \in \mathbb{Z}/6\mathbb{Z}$ to the generator $(1, 1) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ yields an isomorphism. The former generator generates every element by the following steps: $[1], [2], [3], [4], [5], [0]$. The latter generates every element by the following steps: $(1, 1), (0, 2), (1, 0), (0, 1), (1, 2), (0, 0)$.

(c) There is only one group of order 17 up to isomorphism.

True: the order is prime, and any group of prime order is cyclic by HW#2 problem 6.

(d) Every homomorphism between groups is an isomorphism.

False: There are non-bijective homomorphisms. Example: $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(a) = 2a$ is a homomorphism as $\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b)$. However, This is not surjective, for odd numbers are not given by this homomorphism.

(e) There is more than one non-abelian group of order 6 up to isomorphism.

False: This is directly given by HW#2 problem 7: they are all isomorphic to D_6.

(f) If $f : G \xrightarrow{\simeq} H$ is an isomorphism, then the function inverse f^{-1} is also an isomorphism.

True: $\forall a, b \in K \exists \tilde{a}, \tilde{b} \in G : \psi(\tilde{a}) = a$ and $\psi(\tilde{b}) = b$. Then, $\psi(\tilde{a} * \tilde{b}) = \psi(\tilde{a}) \cdot \psi(\tilde{b}) = a \cdot b$. Now, we know that $\psi^{-1}(a \cdot b) = \psi^{-1}(a) * \psi^{-1}(b)$ because they both evaluate to $\tilde{a} * \tilde{b}$. We also know f^{-1} is a bijective because it is the inverse of the bijective function (HW#1 problem 9 bullet 4).

(2) Verify that, for any two elements g_1, g_2 in a group G, we have $(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$, and use this to show the following:

(a) The function

$$G \to G$$
$$g \mapsto g^{-1}$$

is a homomorphism if and only if G is abelian.

Lemma 1. *For $g_1, g_2 \in G$, $(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$*

Proof.

$$(g_1 * g_2) * (g_2^{-1} * g_1^{-1}) = g_1 * ((g_2 * g_2^{-1}) * g_1^{-1}) = g_1 * (e * g_1^{-1}) = g_1 * g_1^{-1} = e$$

Therefore, $g_2^{-1} * g_1^{-1}$ is the unique inverse of $g_1 * g_2$.

□

Lemma 2. *$f : G \to G$ given by $f(g) = g^{-1}$ is an isomorphism (if it is a homomorphism).*

Proof. First, $(g^{-1})^{-1} = g$ because $(g^{-1})^{-1} * g^{-1} = e$ and $g * g^{-1} = e$, so $(g^{-1})^{-1} * g^{-1} = g * g^{-1}$. Via right cancellation, we establish equality.
Second, we prove injectivity: $f(g) = f(h) \implies g^{-1} = h^{-1} \implies (g^{-1})^{-1} = (h^{-1})^{-1} \implies g = h$.
For surjectivity, $g \in G$ can be given by $f(g^{-1})$ as $f(g^{-1}) = (g^{-1})^{-1} = g$.
Therefore f is a bijective homomorphism, i.e. an isomorphism.

□

Part 1: First, assume $f : G \to G$ given by $f(g) = g^{-1}$ is a homomorphism. By our lemma, we know f is surjective. so $\forall g, h \in G, \exists \tilde{g}, \tilde{h} \in G : f(\tilde{g}) = g \wedge f(\tilde{h}) = h$. Furthermore, $f(\tilde{g} * \tilde{h}) = f(\tilde{g}) * f(\tilde{h}) = g * h$. We also know that $\tilde{g} = g^{-1}$ because $f(g^{-1}) = (g^{-1})^{-1} = g$, and since f is injective, $\tilde{g}$ is precisely g^{-1}. With the same reasoning, $\tilde{h} = h^{-1}$.

Now,

$$g * h = f(g^{-1}) * f(h^{-1}) = f(g^{-1} * h^{-1}) = (g^{-1} * h^{-1})^{-1} = (h^{-1})^{-1} * (g^{-1})^{-1} = h * g$$

We have thus proven $\forall g, h \in G, gh = hg$. The group G is abelian if the function f is a homomorphism.

Part 2: Assuming G is abelian, we want to prove that $f : G \to G$ given by $f(g) = g^{-1}$ is a homomorphism.

$\forall g, h \in G, f(g * h) = (g * h)^{-1} = h^{-1} * g^{-1} = g^{-1} * h^{-1} = f(g) * f(h)$. The function is also well defined as it outputs the unique inverse of the input. Thus, the described function is a homomorphism.

(b) If H is a group such that every $h \in H$ satisfies $h^2 = e$, then H is abelian.

$\forall j, k \in H, j * k = l$ for some $l \in H$. Then,

$$j * j * k = j * l \implies e * k = j * l \implies k = j * l \implies k * l = j * l * l \implies k * l = j * e$$

$$\implies k * l = j \implies k * k * l = k * j \implies e * l = k * j \implies l = k * j \implies j * k = k * j$$

Thus H is abelian.

An element $g \in G$ in a group has **finite order** if there is some integer $n \geq 1$ such that $g^n = e$. In this case, the **order of** g, denoted $|g|$, is the *smallest* such integer.

(3) Show the following:

(a) If g is a generator for a cyclic group of order n, then $|g| = n$.
First, $|g|$ cannot be infinite. Then, $G = \{g^k : k \in \mathbb{Z}\}$ has infinite size (if two elements are equal in the expanded list, $i > j$, $g^i = g^j \implies g^{i-j} = e$ means the order is finite anyways). Now, by way of contradiction, suppose $|g| = m \neq n$.

Then, $G = \{g^k : k \in \mathbb{Z}\} = \{g^k : k \in \{0, 1, ..., m-1\}\}$ because $\forall k \in \mathbb{Z}$ we may use the Euclidean algorithm to obtain $k = mq + r$ and $g^k = g^{mq+r} = (g^m)^q * g^r = e^q * g^r = e * g^r = g^r$, with $r \in \{0, 1, ..., m-1\}$. Now, no two elements g^i and g^j for $i \neq j$ and $i, j \in \{0, 1, ..., m-1\}$ can be

equal.

Without loss of generality, assume $i > j$. Then, $g^i = g^j \implies g^{i-j} = e$. However, $0 < i - j < m$ but $g^{i-j} = e$. This is a contradiction of m being the order of g. Now, since there are no repeats in $G = \{g^k : k \in \{0, 1, ..., m-1\}\}$, we may find $|G| = m$. But $|G| = n \neq m$. This is a contradiction. Therefore, the generator g must have order n.

(b) If $g \in G$ is an element of order n, then we have $g^m = e$ for some integer m if and only if m is a multiple of n.
Part 1: $g^m = e \implies n \mid m$. We proceed by way of contradiction: assume $g^m = e$ and suppose $n \nmid m$. Then, $\gcd(n, m) < n$, because any factor greater than n cannot divide n, and we supposed n does not divide m. Now, we know that $\exists a, b \in \mathbb{Z} : \gcd(n, m) = an + bm$. Then, $g^{\gcd(n,m)} = g^{an+bm} = (g^n)^a * (g^m)^b = e^a * e^b = e^{a+b} = e$. We see that $\gcd(n, m)$ is a positive number such that $g^{\gcd(n,m)} = e$. However, $\gcd(n, m) < n$, violating the definition that the order is the least positive integer k where $g^k = e$. Therefore, assuming $g^m = e$, we may conclude m is a multiple of n.

Part 2: $n \mid m \implies g^m = e$. Assuming $n \mid m$, $m = kn$ for some integer k. $g^m = g^{kn} = (g^n)^k = e^k = e$. We are done.

(4) Suppose that G is a finite cyclic group of order n and that $g \in G$ is a generator.
(a) Show that, for any integer m, g^m has order $\frac{n}{\gcd(n,m)}$.

Since there is an isomorphism $f : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} G$ satisfying $f(1) = g$, we will first prove that for any integer m, $m[1] = [m]$ has order $\gcd(n, m)$. Given $|g| = n$ by problem 3a, we prove that $(\frac{n}{\gcd(n,m)})[m] = [0]$. Number theoretically, we know $mn = \gcd(m, n)\mathrm{lcm}(m, n)$. Therefore, $(\frac{n}{\gcd(n,m)})[m] = [\mathrm{lcm}(m, n)] = \mathrm{lcm}(m, n)[1] = [0]$ since $n \mid \mathrm{lcm(m, n)}$.

Now we need to demonstrate that for any $0 < k < \frac{n}{\gcd(n,m)}$, $k[m] \neq [0]$. By way of contradiction, suppose $k[m] = [0]$. By Problem 3b, we know that $k[m] = km[1] = [0] \implies n \mid km$.

Then, $km < \frac{n}{\gcd(n,m)}m = \frac{nm}{\gcd(n,m)} = \mathrm{lcm}(n, m)$. However, km is clearly a multiple of both m and n, yet is clearly a positive integer less than $\mathrm{lcm}(n, m)$. Therefore, we now have a lower common multiple. This is a contradiction.

Lemma 3. *If $f : H \to K$ is an isomorphism, $\forall h \in H, |h|_H = |f(h)|_K$.*

Proof. First, we observe that $f(h^k) = f(h)^k$ for any positive integer k. (This holds by induction: $f(h^n) = f(h)^n \implies f(h *_H h^n) = f(h) *_K f(h)^k \implies f(h^{n+1}) = f(h)^n$. We also have the base case of $f(h^1) = f(h) = f(h)^1$.)

Then, $\forall h \in H, f(h^{|h|}) = e_H = f(h)^{|h|}$. Now we need to demonstrate that there are no other positive integers $l < |h|$ for which $f(h)^l = e_H$. By way of contradiction, suppose there is such an l. Then, $f(h)^l = f(h^l) = e_H = f(h^{|h|})$. By injectivity of f, $h^l = h^{|h|} = e_H$. Then, l is a positive integer less than the order that satisfies $h^l = e_H$. This violates the definition of order. Therefore, we have demonstrated that If $f : H \to K$ is an isomorphism, $\forall h \in H, |h|_H = |f(h)|_K$.

□

Now we are ready to prove that for any finite cyclic group G of order n with $g \in G$ as the generator. Let $f : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} G$ satisfying $f(1) = g$. Then, $\forall m \in \mathbb{Z}, |[m]| = |f([m])| = |g^m|$. Also, since $|[m]| = |m[1]| = \frac{n}{\gcd(n,m)}$, it is true that $|g^m| = \frac{n}{\gcd(n,m)}$. Therefore, $\forall m \in \mathbb{Z}, |g^m| = \frac{n}{\gcd(n,m)}$.

(b) Show that, for any integer $d \mid n$, there is a unique subgroup of G of order d, and that this subgroup is cyclic and generated by $g^{n/d}$.

Lemma 4. *Any subgroup of a finite cyclic group G is cyclic.*

Proof. Suppose $|G| = n$ with G generated by $g \in G$. Then as always, $G = \{e, g, g^2, ..., g^{n-1}\}$. Suppose $H \leq G$ is a subgroup with elements of form $g^k : k \in \{0, 1, ..., n-1\}$. We know there must be some g^a with the least power a. Every element must be $g^{j \cdot a}$ for some integer j. Suppose not: $\exists g^b : g^b \neq g^{j \cdot a}$ for some integer j. $0 < \gcd(a, b) < a$ and $\exists s, t \in \mathbb{Z} : as + bt = \gcd(a, b) < a$. Then, $g^{as+bt} \in H$ but $0 < as + bt < a$. This contradicts that we chose a to be the lowest power of g in H.

As demonstrated, $\langle g^a \rangle \subseteq H$. By closure, $H \subseteq \langle g^a \rangle$. Therefore, $H = \langle g^a \rangle$. So for any $H \leq G$, H is a cyclic subgroup.

□

We will now try to find only cyclic subgroups (defined by their generators). By problem 3a, we know that if g^k is a generator of a cyclic subgroup G_k with $|G_k| = d$ of G, then $|g^k| = d$. We now want to find such an element that $|g^k| = d$ (and later confirm this generates what we want). One such element is $g^{n/d}$: $|g^{n/d}| = \frac{n}{\gcd(n, n/d)} = \frac{n}{n/d} = d$. Note that $\gcd(n, n/d) = n/d$ because $n/d \mid n$ as $n/d \cdot d = n$. Additionally note that n/d is an integer because $d \mid n$.

We already know from class that $\langle g^{n/d} \rangle$ is a subgroup. We also know from class that $|\langle g^{n/d} \rangle| = |g^{n/d}| = d$. Now we need to prove that this group is unique.

We demonstrate that for any $g^k \in G$, $|g^k| = d \implies g^k = g^{j \cdot n/d}$ for some $j \in \mathbb{Z}$.

$$|g^k| = \frac{n}{\gcd(n, k)} = d \implies \gcd(n, k) = n/d \implies n/d \mid k \implies k = j \cdot n/d : j \in \mathbb{Z}$$

This proves that $g^k \in \langle g^{n/d} \rangle$, and any cyclic subgroup of $\langle g^{n/d} \rangle$ generated by g^k would be the same as $\langle g^{n/d} \rangle$.

To get a cyclic subgroup of order d is to have an element of order d, but we demonstrated that all such elements are already in $\langle g^{n/d} \rangle$ and would generate the same exact group. Therefore, we have proved that $\forall d \mid n, \exists!$ unique subgroup of G of order d generated by $g^{n/d}$.

Hint: One way to do this is to note that there is an isomorphism $f : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} G$ satisfying $f(1) = g$ (Problem 5 on Homework 2). So you only really have to consider the case $G = \mathbb{Z}/n\mathbb{Z}$ (with addition!) and $g = 1$.

Given two groups G and H, write $\mathrm{Hom}(G, H)$ for the set of homomorphisms from G to H.

(5) Suppose that G is a group and that $g \in G$ is an element.
(a) Show that the function

$$\mathbb{Z} \to G$$
$$a \mapsto g^a$$

is a homomorphism of groups, and use this to construct a bijection between the set $\mathrm{Hom}(\mathbb{Z}, G)$ and the set G.

Let f be such function. First, this function is well defined, as $a = b \implies g^a = g^b$. Now, $\forall a, b \in \mathbb{Z}, f(a + b) = g^{a+b} = g^a * g^b = f(a) * f(b)$. Thus f is a homomorphism.

Moreover, any homomorphism $h : \mathbb{Z} \to G$ must satisfy $h(a) = \tilde{g}^a$ for some $\tilde{g} \in G$. Suppose $h(1) = \tilde{g}$. Then, $\forall a \in \mathbb{Z}, h(a) = h(a1) = h(1)^a = \tilde{g}^a$.

$\varphi : \mathrm{Hom}(\mathbb{Z}, G) \to G$ given by $\varphi(\phi) = \phi(1)$ is a bijection. φ is well defined, as for each $\phi \in \mathrm{Hom}(\mathbb{Z}, G)$, ϕ is well defined, meaning there is only one possible output for $\varphi(\phi) = \phi(1)$.

We now want to prove injectivity: Assume $\varphi(\phi_1) = \varphi(\phi_2)$ (i.e. $\phi_1(1) = \phi_2(1)$). Then, $\forall a \in \mathbb{Z}, \phi_1(a) = \phi_1(a1) = \phi_1(1)^a = \phi_2(1)^a = \phi_2(a1) = \phi_2(a)$. This means $\phi_1 = \phi_2$, as their outputs are equal at each input. We thus successfully demonstrated that $\forall \phi_1, \phi_2 \in \mathrm{Hom}(\mathbb{Z}, G), \varphi(\phi_1) = \varphi(\phi_2) \implies \phi_1 = \phi_2$.

Now we need to demonstrate surjectivity: $\forall g \in G$, we showed that the function $f : \mathbb{Z} \to G$ with $f(a) = g^a$ is a homomorphism. Then, $\phi(f) = f(1) = g^1 = g$. We have found a homomorphism corresponding to each element in G.

Our function $\varphi : \mathrm{Hom}(\mathbb{Z}, G) \to G$ is a bijection.

(b) Suppose that $n \geq 1$ is an integer. When is the function

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\} &\to G \\ a &\mapsto g^a \end{aligned}$$

a homomorphism? Use your answer to naturally identify $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$ with a certain subset of G.

Lemma 5. *The described function (call it h) is a homomorphism if and only if $|g| \mid n$.*

Proof. Assume $|g| \mid n$ meaning $n = |g|k : k \in \mathbb{Z}$. Then, if we have $[a] = [b] \in \mathbb{Z}/n\mathbb{Z}$, we prove that $h([a]) = h([b])$ to prove well-defined ness (i.e. the representative doesn't matter). $[a] = [b] \implies a = q_1 n + r \wedge b = q_2 n + r$. Then, $h([a]) = g^a = g^{q_1 n + r} = g^{q_1 |g| k} * g^r = e^{q_1 k} * g^r = e * g^r = g^r$. In the same way, $h([b])$ yields g^r. This means $h([a]) = h([b])$. We have established that h is well-defined.

Now, $\forall [a], [b] \in \mathbb{Z}/n\mathbb{Z}, f([a] + [b]) = f([a + b]) = g^{a+b} = g^a * g^b = f([a]) * f([b])$. Therefore, h is a homomorphism.

Now assume h is a homomorphism. $[n] = [0]$ because both n and 0 have a remainder of 0 after dividing by n via the Euclidean algorithm. Because h is well-defined, $h([n]) = h([0]) \implies g^n = g^0 = e$. By problem 3b, we know that $|g| \mid n$. We have proved the remaining direction of implication.

□

$\varphi : \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \to \{g \in G : |g| \mid n\}$ given by $\varphi(\phi) = \phi(1)$ is a bijection from $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z})$ to a subset of G. We continue to demonstrate this.

Again, φ is well defined because ϕ is well defined. There is one possible output for $\phi(1)$ and thus $\varphi(\phi)$.

The injectivity argument is also identical to that of 5a: Assume $\varphi(\phi_1) = \varphi(\phi_2)$ (i.e. $\phi_1(1) = \phi_2(1)$). Then, $\forall a \in \mathbb{Z}, \phi_1(a) = \phi_1(a1) = \phi_1(1)^a = \phi_2(1)^a = \phi_2(a1) = \phi_2(a)$. This means $\phi_1 = \phi_2$, as their outputs are equal at each input. We thus successfully demonstrated that $\forall \phi_1, \phi_2 \in \mathrm{Hom}(\mathbb{Z}, G), \varphi(\phi_1) = \varphi(\phi_2) \implies \phi_1 = \phi_2$.

The surjectivity argument is also similar: $\forall g \in \{g \in G : |g| \mid n\}$, we showed that the function $h : \mathbb{Z} \to G$ with $h(a) = g^a$ is a homomorphism. Then, $\phi(h) = h(1) = g^1 = g$. We have found a homomorphism corresponding to each element in $\{g \in G : |g| \mid n\}$.

We have thus constructed a bijection from $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z})$ to a certain subset of G, namely the set of all elements such that their orders divide n.

Remark: The point in the second problem is that the assignment $a \mapsto g^a$ logically depends on the choice of representatives for the equivalence classes. In other words, if $n = 5$, it is logically possible for g^2 and g^7 to be different elements in G, even though $2 \equiv 7 \pmod 5$. You should find that its being a homomorphism is equivalent *to its not depending on the choice of representatives.*

(6) Let $X \subset \{1, 2, \ldots, n\}$ be any non-empty subset, and let

$$H_X = \{\sigma \in S_n : \ \sigma(x) = x, \text{for all } x \in X\}$$

be the subset of permutations that fix every element in X. Show that H_X is a subgroup of S_n. How many elements does it have?

Closure: $\forall \sigma_1, \sigma_2 \in H_X, \forall x \in X, (\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1(x) = x \implies \sigma_1 \circ \sigma_2 \in H_X$

Identity: $\forall a \in \{1, 2, ..., n\}, \mathrm{Id}(a) = a$. Since $X \subset \{1, 2, ..., n\} \implies \forall x \in X, x \in \{1, 2, ..., n\} \wedge \mathrm{Id}(x) = x$. Thus, $\mathrm{Id} \in H_X$.

Inverses: $\forall \sigma \in H_X$, we know $\sigma^{-1} \in S_n$ from the inverse property of S_n. Now, since $\forall x \in X, \sigma(x) = x$, then $\forall x \in X, \sigma^{-1}(x) = \sigma^{-1}(\sigma(x)) = x$. Therefore, $\forall \sigma \in H_X, \sigma^{-1} \in H_X$.

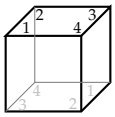
Since $H_X \subseteq S_n$ has the properties of closure, identity, and inverses, $H_X \leq S_n$.

Also, $|H_X| = (n - |X|)!$ where $|X|$ is the cardinality of X (not order of group). This is because when we want to give an output to some $a \in \{1, 2, ..., n\} \setminus X$, there are initially $n - |X|$ choices to keep the permutation injective. When we want to assign another element ($n - |X| - 1$ elements left now) to an output, we have $n - |X| - 1$ choices. This repeats until no elements are left: $(n - |X|)(n - |X| - 1) \cdots (1) = (n - |X|)!$. Note that each permutation obtained is still surjective: if one number isn't "hit" by the permutation, by the pigeonhole principle, one other number must have been assigned to two input, destroying injectivity.

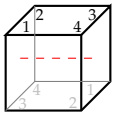
Sometimes, groups like S_n can be viewed as symmetries of things other than the set of n elements. The next problem illustrates this.

(7) Consider the cube in three dimensional space. Show that rotations that preserve the cube form a group that is isomorphic to S_4.

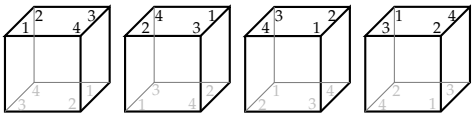
Hint: You need to find a set of 4 elements on which this group of rotations acts. What does a cube have four of?

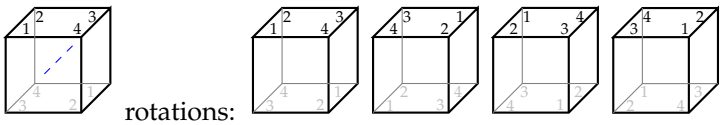


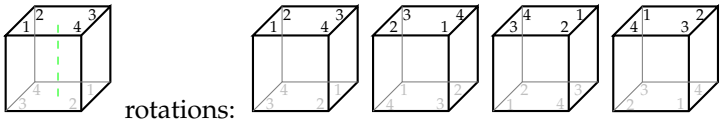
The structure of the labeled pairs of vertices will remain preserved under any rotation. There are thirteen axes of symmetry in a cube: 3 from middle of a face to an opposite one, 4 from one point to the complete opposite point, and 6 from the middle of one edge to the middle of the complete opposite edge.

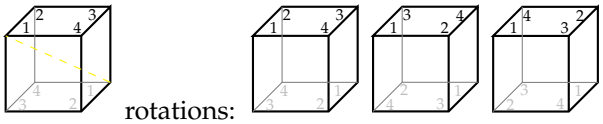


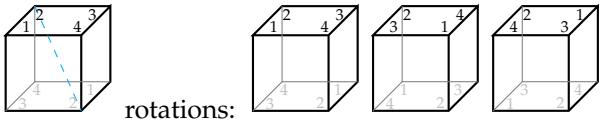
rotations:

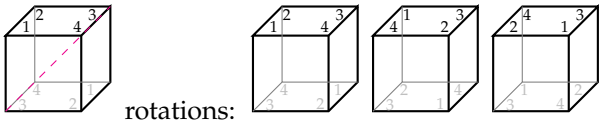


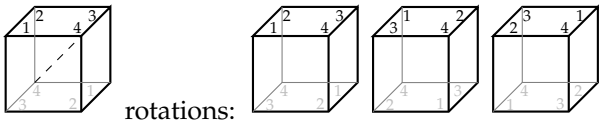

rotations:

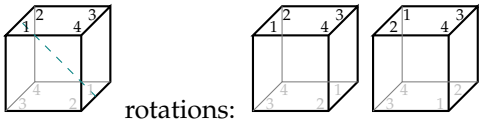

rotations:

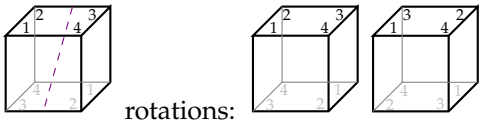

rotations:

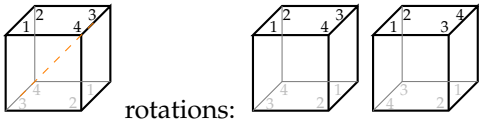

rotations:

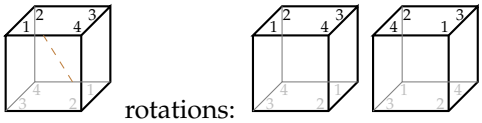

rotations:

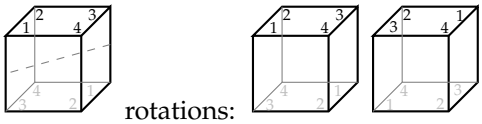

rotations:

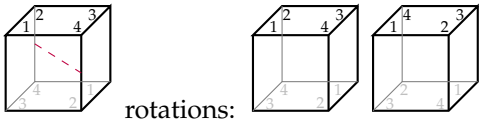

rotations:

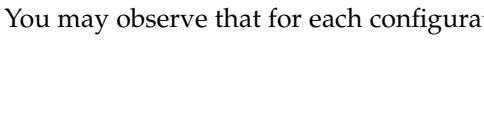

rotations:

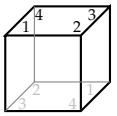

rotations:


rotations:


rotations:

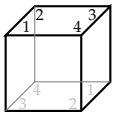

rotations:

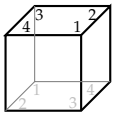

rotations:

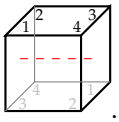
You may observe that for each configuration, the structure of the labeled points are alike. Furthermore, each rotation can be seen as a permutation of $\{1,2,3,4\}$. E.g  is $\left\{\begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 4 \\ 3 \mapsto 3 \\ 4 \mapsto 2 \end{array}\right\}$. This means that each rotation can be mapped to an element of S_4.

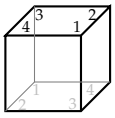
Of course, this set of 24 elements is a group.

Composition of rotations is closed because rotating a rotation gives another rotation of the cube: we have the binary operation.

We have the identity of doing nothing to the cube: 

. Of course, rotating and doing nothing will be that rotation, and doing nothing and then rotating will again be that rotation.
We also have associativity since rotation is basically a function (as seen from each rotation being able to be written as a permutation).
And finally we have inverses: Given any rotation based on an axis, if it is the nth position from the left (indexed from 1) on our list, the inverse is on the nth to last position on the list, unless the rotation is doing nothing, in which case doing nothing is the inverse. For example, 

is the second on the list for the axis 

. The second to last would be 

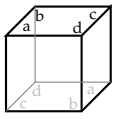
. You can confirm that rotating along the axis twice (180 degrees) and then twice again (180 degrees again) will bring back the identity position.

Therefore, we proved that the rotations that preserve the group, G, forms a group.

The group acts on the four elements of $\{1, 2, 3, 4\}$. so we have the *unique* homomorphism $\rho : G \to S_4$ (from a group action, we get a unique homomorphism that corresponds to the group action).

We just need to show that this homomorphism is bijective.

Injectivity: In our list of rotations, no two different rotations give the same action (besides the identity, but the identity for each rotation is basically doing no rotation, which is the same thing anyways).

Surjectivity: Given an element $\left\{ \begin{array}{l} 1 \mapsto a \\ 2 \mapsto b \\ 3 \mapsto c \\ 4 \mapsto d \end{array} \right\} \in S_4$, as we listed all possibilities of rotations, we know there is a rotation yielding 

for any a, b, c, d that are distinct and are in $\{1, 2, 3, 4\}$. This is the rotation that takes the pair of vertices 1 to a, 2 to b, 3 to c, and 4 to d.

Therefore, $\rho : G \xrightarrow{\simeq} S_4$ is the isomorphism from G to S_4, meaning the rotations that preserve the cube form a group isomorphic to S_4.

Two elements h_1, h_2 in a group G are **conjugate** if there exists $g \in G$ such that $gh_1g^{-1} = h_2$.[1] If $H \leq G$ is a subgroup and $g \in G$, we will set

$$gHg^{-1} = \{ghg^{-1} : \ h \in H\}.$$

[1]We're all adults now, so we will omit the '*' symbol for the group operation, and use concatenation of symbols to denote multiplication in a group.

(8) Suppose that we have a group action of G on a set X. Show that, for any $g \in G$ and $x \in X$, $G_{g\cdot x} = gG_xg^{-1}$. That is, stabilizers of elements in the same orbit are *conjugate*.

$\forall h \in G_{g\cdot x}, h \cdot (g \cdot x) = (hg) \cdot x = g \cdot x \implies g^{-1} \cdot ((hg) \cdot x) = g^{-1} \cdot (g \cdot x) \implies g^{-1}hg \cdot x = x$. This means $g^{-1}hg \in G_x$. This then means $h = g(g^{-1}hg)g^{-1} \in gG_xg^{-1}$. Thus $G_{g\cdot x} \subseteq gG_xg^{-1}$.

$\forall k \in gG_xg^{-1}, k = g\tilde{k}g^{-1}$ for some $\tilde{k} \in G_x$. Then,

$$h \cdot (g \cdot x) = gkg^{-1} \cdot (g \cdot x) = (gkg^{-1}g) \cdot x = (gk) \cdot x = g \cdot (k \cdot x) = g \cdot x \implies h \in G_{g\cdot x}$$

Thus $gG_xg^{-1} \subseteq G_{g\cdot x}$. Because $G_{g\cdot x} \subseteq gG_xg^{-1} \wedge gG_xg^{-1} \subseteq G_{g\cdot x}$, we have proven $G_{g\cdot x} = gG_xg^{-1}$: stabilizers of elements in the same orbit are conjugate.

Let p be a prime. Let Y be any set, and let

$$X = \underbrace{Y \times \cdots \times Y}_{p \text{ times}}$$

be the p-fold Cartesian product of Y with itself. So X consists of p-tuples $(a_1, \ldots, a_p)$, where $a_i \in Y$.

Let $\alpha \in \mathrm{Bij}(X)$ be the cyclic permutation:

$$\alpha \cdot (a_1, \ldots, a_p) = (a_p, a_1, \ldots, a_{p-1}).$$

(9) Let C_p be the cyclic group of order p (this is just $\mathbb{Z}/p\mathbb{Z}$, but we prefer to think of the group operation multiplicatively). Fix a generator $g \in C_p$ (corresponding for instance to $1 \in \mathbb{Z}/p\mathbb{Z}$). Verify that the function

$$\begin{aligned} \rho : C_p &\to \mathrm{Bij}(X) \\ g^r &\mapsto \alpha^r \end{aligned}$$

defines a group action of C_p on X.

Hint: This is essentially a direct application of the definitions and problem 5(b)

We need to prove that ρ is well-defined and also that $\rho(g^ag^b) = \rho(g^a) \circ \rho(g^b)$: For well-defined ness, we need to show that $g^a = g^b \implies \forall x \in X, \alpha^a \cdot x = \alpha^b \cdot x$.

Lemma 6. *If $\phi : G \to H$ is an isomorphism and $\psi : H \to K$ is a homomorphism, then $\psi \circ \phi : G \to K$ is a homomorphism.*

Proof. Firstly, $\psi \circ \phi$ is well-defined, as both ψ and ϕ are well defined. Also, all the inputs of ψ are still elements of H.

$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b)$. Therefore, $\psi \circ \phi$ is a homomorphism.

□

As per problem 5b, $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{Bij}(X)$ given by $\phi([a]) = \alpha^a$ is a homomorphism whenever $|\alpha| \mid p$. We just need to verify that this is the case: We observe that $\forall x \in X, \alpha^p = x$ because cycling each element of a tuple p times will bring it back to its original position. Then, since $\forall x \in X, \alpha^p \cdot x = \mathrm{Id} \cdot x$, we know $\alpha^p = \mathrm{Id}$. By problem 3b, p is a multiple of $|\alpha|$, meaning $|\alpha| \mid p$. Thus ϕ is a homomorphism.

By HW#2 problem 5, $\psi : C_p \to \mathbb{Z}/n\mathbb{Z}$ given by $\psi(g^a) = [a]$ is an isomorphism. By lemma 6, $\psi \circ \phi : C_p \to \mathrm{Bij}(X)$ is a homomorphism. Moreover, $\rho : C_p \to \mathrm{Bij}(X)$ is the same as $\psi \circ \phi : C_p \to \mathrm{Bij}(X)$. We can confirm this by seeing that $\psi \circ \phi$ also sends g^r to α^r: $(\psi \circ \phi)(g^r) = \psi(\phi(g^r)) = \psi([r]) = \alpha^r$.

Therefore, $\rho : C_p \to \mathrm{Bij}(X)$ with $g^r \mapsto \alpha^p$ is a homomorphism. This means that the described function defines a group action of C_p on X.