

- (1) Let G be a group, N be a normal subgroup of G , and g be an element of G . Prove that the order of gN (in G/N) divides the order of g (in G).

Let k be the order of g . Then $(gN)^k = g^k N = eN = N$. By Proposition 3.5, the order of gN must therefore divide k .

- (2) If $f : G \rightarrow H$ is a homomorphism, find a group K , and homomorphisms $g : G \rightarrow K$ and $h : K \rightarrow H$ so that g is surjective, h is injective, and $h \circ g = f$. Further, prove that K is unique up to isomorphism. (I.e. if the same is true for some other K' , then $K \cong K'$.)

Existence: Let K be the image of f . I.e. $K = \{f(x) : x \in G\}$, $g = f$, and h is the identity. Then $h \circ g(x) = id(f(x)) = f(x)$. g is surjective by definition. And h is injective because it's the identity.

Uniqueness: Suppose that K' is another such group, with surjective homomorphism $g' : G \rightarrow K'$ and injective homomorphism $h' : K' \rightarrow H$ so that $f = h' \circ g'$. Then define the map $i : K' \rightarrow K$ by $i(x) = h'(x)$. First we need to check that this always gives a value in K . For any $x \in K'$, $x = g'(y)$ for some $y \in G$. So $i(x) = h'(x) = h'(g'(y)) = f(y)$, so $i(x)$ is in the image of f , which is K . Since h' is an injective homomorphism because, so is i . To see that i is also surjective, consider any $x \in K$. Then $x = f(y)$ for some $y \in G$ since K is just the image of f . Now $i(g'(y)) = h'(g'(y)) = f(y) = x$. So i is an isomorphism as desired.

- (3) Consider the ways of color the corners of a cube either red, blue, or green. Two colorings are the same if there is a rigid motion from one to the other. Use Burnside's Theorem to count the number of such colorings.

Recall that the rigid motions of the cube are just S_4 permuting the diagonals. So we'll look at what each elements of S_4 does to the colors, and count which colorings it fixes. We need to compute X_g for various g . We'll break it down by disjoint cycle decomposition. First note that for any cycle, each diagonal comes back to the same orientation. So although all the diagonals in a cycle must be the same, the ends can be different colors. There are three cases where a diagonal is fixed: the identity, a single transposition or a 3-cycle. For the identity or a 3-cycle, the orientation of a fixed diagonal does not change, so each end can be colored differently. For a transposition, both fixed diagonals swap orientation, so each must have the same color on both ends. So we get

cycle decomposition of g	number of such	$ X_g $
id	1	3^8
$(i j)$	6	3^4
$(i j)(k l)$	3	3^4
$(i j k)$	8	3^4
$(i j k l)$	6	3^2

Thus by Burnside's Theorem, the number of orbits is

$$\frac{1}{|S_4|} \sum X_g = \frac{1}{24} (1 \cdot 3^8 + 6 \cdot 3^4 + 3 \cdot 3^4 + 8 \cdot 3^4 + 6 \cdot 3^2) = 333$$

(4) Do exercise 12.20 in Judson.

Forward: Suppose $a \star x = b \star x$ for every $x \in X$. Then $a^{-1} b \star x = a a^{-1} b \star x = b \star x = x$. So $a^{-1} b$ fixes everything and must be the identity. Then $a = a e = a a^{-1} b = e b = b$.

Backwards: Suppose that if for all x , $a \star x = b \star x$, then $a = b$. If some $g \in G$ fixes all x , then $g \star x = x = e \star x$. So $g = e$. and G acts transitively.

(5) Do exercise 12.24 in Judson.

Since $|G| = p^n$, any subgroup of G has index p^i for some $i \leq n$. In particular, for any x , $[G : G_x]$ has to either be 1 or divisible by p . So \mathcal{O}_x has to have size 1 or be divisible by p . Now if we take the class equation modulo p , all the nontrivial orbits are removed, because their sizes are divisible by p . This leaves $|X| \equiv |X_G| \pmod{p}$.

(6) Let G be a finite group, and p be a prime so that p divides the order of G . Define X to be the p -tuples from G whose product is the identity. I.e.

$$X = \{(g_1, g_2, \dots, g_{p-1}, g_p) : g_1, g_2, \dots, g_{p-1}, g_p \in G \text{ and } g_1 g_2 \dots g_{p-1} g_p = e\}$$

Let σ be $(1 \ 2 \ 3 \ \dots \ p-1 \ p)$ in S_p .

(a) Prove that $|X| = |G|^{p-1}$.

For any $p-1$ elements of G , g_1, g_2, \dots, g_{p-1} , there is exactly one element in X of the form $(g_1, g_2, \dots, g_{p-1}, a)$ for some a . In this case, $g_1 g_2 \dots g_{p-1} a = e$. That is a must be $(g_1 g_2 \dots g_{p-1})^{-1} = g_{p-1}^{-1} g_{p-2}^{-1} \dots g_1^{-1}$.

(b) We will let $\langle \sigma \rangle \leq S_p$ act on X by setting

$$\tau \star (g_1, g_2, \dots, g_{p-1}, g_p) = (g_{\tau(1)}, g_{\tau(2)}, \dots, g_{\tau(p-1)}, g_{\tau(p)})$$

First, prove by induction on i that if $(g_1, g_2, \dots, g_{p-1}, g_p) \in X$ then $\sigma^i \star (g_1, g_2, \dots, g_{p-1}, g_p) \in X$. Then prove that \star is a valid group action.

$\sigma^0 = id$ sends every x to itself, Now assume $\sigma^i \star (g_1, g_2, \dots, g_{p-1}, g_p)$ is in X and consider $\sigma^{i+1} \star (g_1, g_2, \dots, g_{p-1}, g_p)$. We know

$$\begin{aligned} g_{\sigma^i(1)} g_{\sigma^i(2)} \dots g_{\sigma^i(p)} &= e \\ g_{\sigma^i(1)} g_{\sigma^i(2)} \dots g_{\sigma^i(p-1)} &= g_{\sigma^i(p)}^{-1} \\ g_{\sigma^i(p)} g_{\sigma^i(1)} g_{\sigma^i(2)} \dots g_{\sigma^i(p-1)} &= g_{\sigma^i(p)} g_{\sigma^i(p)}^{-1} = e \end{aligned}$$

Since

$$\sigma^{i+1} \star (g_1, g_2, \dots, g_{p-1}, g_p) = (g_{\sigma^i(p)}, g_{\sigma^i(1)}, g_{\sigma^i(2)}, \dots, g_{\sigma^i(p-1)})$$

We know this has product e , so it's in X .

Now since we know we actually get things in X , to check that \star is a valid, we first note that the identity sends everything to itself. Also:

$$\begin{aligned} \tau \star (\nu (g_1, g_2, \dots, g_{p-1}, g_p)) &= \tau \star (g_{\nu(1)}, g_{\nu(2)}, \dots, g_{\nu(p-1)}, g_{\nu(p)}) \\ &= (g_{\tau(\nu(1))}, g_{\tau(\nu(2))}, \dots, g_{\tau(\nu(p-1))}, g_{\tau(\nu(p))}) \\ &= (\tau \circ \nu) \star (g_1, g_2, \dots, g_{p-1}, g_p) \end{aligned}$$

So \star is a valid group action.

(c) Prove that p divides $|X_\sigma|$.

Since the order of $\langle \sigma \rangle$ is p , by problem 5, $|X| \equiv |X_{\langle \sigma \rangle}| \pmod{p}$. Since p divides $|G|$, by part (a), p divides $|X|$. So p divides $|X_{\langle \sigma \rangle}|$.

(d) Use (c) to show that G must have an element of order p .

Since the (e, e, \dots, e) is in $X_{\langle \sigma \rangle}$ and p divides the $|X_{\langle \sigma \rangle}|$, $X_{\langle \sigma \rangle}$ must have some nonidentity element. Call it $\bar{g} = (g_1, g_2, \dots, g_p)$. Since σ fixes \bar{g} , it must be that $g_1 = g_2 = \dots = g_p$. Since \bar{g} is in X , we now know that $g_1 g_1 \dots g_1 = e$. That is, the order of g_1 is divisible by p . Since g_1 is not the identity and p is prime, the order of g_1 must be p .