HW 3 Solutions Due: 24 April 2024

1 Computations

1. Write down every subgroup of $\mathbb{Z}_5$. (You can use "generator" notation. For example, $\langle 1\rangle = \{0,1,2,3,4\}$.)
2. Write down every subgroup of $\mathbb{Z}_{10}$.
3. Write down every subgroup of $\mathbb{Z}_{70}$.
4. Do you have a conjecture about the number of subgroups of cyclic groups?
5. How many surjective functions are there from $\mathbb{Z}_2 \times \mathbb{Z}_2$ to $\mathbb{Z}_2$? How many injective functions?

Solutions.

1. Subgroups are: $\langle 0\rangle$ and $\langle 1\rangle$.
2. Subgroups are: $\langle 0\rangle$, $\langle 5\rangle$, $\langle 2\rangle$, and $\langle 1\rangle$.
3. Subgroups are: $\langle 0\rangle$, $\langle 35\rangle$, $\langle 14\rangle$, $\langle 10\rangle$, $\langle 7\rangle$, $\langle 5\rangle$, $\langle 2\rangle$, and $\langle 1\rangle$.
4. For any positive integer n, the subgroups of $\mathbb{Z}_n$ are in one-to-one correspondence with the (positive integer) divisors of n.
5. There are 14 surjective functions (the only two nonsurjective functions out of the 16 total functions are: the one that maps everything to 0 and the one that maps everything to 1) and 0 injective functions.

□

2 Proofs

(I) Let G, H be groups with identities, e_G, e_H, respectively. Prove that $\{(e_G, h) \mid h \in H\}$ is a subgroup of $G \times H$. (A similar proof shows that $\{(g, e_H) \mid g \in G\}$ is a subgroup of $G \times H$, but you don't need to write this up.)

(II) Let G be a group, and define

$$C = \{g \in G \mid \text{for all } x \in G,\ xg = gx\}.$$

Prove that C is a subgroup of G.

(III) Let G be a group, let H be a subgroup of G, and choose any $g \in G$. Prove that

$$\left\{ghg^{-1} \mid h \in H\right\}$$

is a subgroup of G.

Solutions. (I) Let's write K for $\{(e_G, h) \mid h \in H\}$.

- Since $(e_G, e_H) \in K$, we see $K \neq \varnothing$.
- Choose any $(e_G, h_1), (e_G, h_2) \in K$, then note that

$$(e_G, h_1)(e_G, h_2) = (e_G e_G, h_1 h_2) = (e_G, h_1 h_2) \in K.$$

- Finally, if we choose any $(e_G, h) \in K$, we recall that the inverse of (e_G, h) is $\left(e_G, h^{-1}\right)$; and $\left(e_G, h^{-1}\right)$ is in K by definition of K.

Thus, we see that K is a subgroup of $G \times H$ by the subgroup test.

(II) Let's write e for the identity element of G.

- By the definition of identity element, we know that for any $g \in G$, we have $eg = ge = g$, so that $e \in C$ by definition. In particular, we see $C \neq \varnothing$.
- Choose any $g, h \in C$. To show that $gh \in C$, choose any $x \in C$ and note that associativity and the definition of C tell us:

$$x(gh) = (xg)h = (gx)h = g(xh) = g(hx) = (gh)x,$$

so $gh \in C$.

- Finally choose any $g \in C$. To show $g^{-1} \in C$, we choose any $x \in G$ and use Shoes and Socks and the definition of C to compute

$$xg^{-1} = \left(gx^{-1}\right)^{-1} = \left(x^{-1}g\right)^{-1} = g^{-1}x.$$

Thus, we see $g^{-1} \in C$. Could we have done this without Shoes and Socks? Yes! "Use the fact that G is a group and the definition of C to compute

$$xg^{-1} = e\left(xg^{-1}\right) = \left(g^{-1}g\right)\left(xg^{-1}\right) = g^{-1}(gx)g^{-1} = g^{-1}(xg)g^{-1} = \left(g^{-1}x\right)\left(gg^{-1}\right) = \left(g^{-1}x\right)e = g^{-1}x,$$

so $g^{-1} \in C$."

(III) Like normal, we'll write e for the identity of G and we'll apply the subgroup test. We'll write gHg^{-1} for $\left\{ghg^{-1} \mid h \in H\right\}$

- We know from class that $e \in H$ since H is a subgroup. Then $e = gg^{-1} = geg^{-1} \in gHg^{-1}$ by the definition of gHg^{-1}.
- Suppose that $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$. Since H is a subgroup, we know $h_1h_2 \in H$, so

$$\left(gh_1g^{-1}\right)\left(gh_2g^{-1}\right) = gh_1\left(g^{-1}g\right)h_2g^{-1} = gh_1\left(e\right)h_2g^{-1} = g\left(h_1h_2\right)g^{-1} \in gHg^{-1}.$$

- Finally, choose any $ghg^{-1} \in gHg^{-1}$. Since H is a subgroup, we know $h^{-1} \in H$, so

$$ghg^{-1}\left(gh^{-1}g^{-1}\right) = gh\left(g^{-1}g\right)h^{-1}g^{-1} = g\left(hh^{-1}\right)g^{-1} = g\left(e\right)g^{-1} = gg^{-1} = e,$$

we see that

$$\left(ghg^{-1}\right)^{-1} = gh^{-1}g^{-1} \in gHg^{-1}. \qquad (\dagger)$$

Here we used the fact from class again. That is, we deduced that (†) was true by computing $ghg^{-1}\left(gh^{-1}g^{-1}\right)$ without needing to compute $\left(gh^{-1}g^{-1}\right)ghg^{-1}$.

□