Homework 3 Solutions

Sam Mundy

Exercise (I)**.** Write down the Cayley table for the group $\mathbb{Z}/5$. Remember that the group operation is addition. Is your table symmetric?

Solution. The Cayley table for $\mathbb{Z}/5$ is

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The table is symmetric across the diagonal because $\mathbb{Z}/5$ is abelian.

Exercise (Judson, Chapter 3, Exercise 7)**.** Let $S = \mathbb{R}\backslash\{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Solution. The very first thing to check is that this set S is really closed under the operation $*$. We know that given $a, b \in S$ then $a * b$ is always a real number, but we need to see that $a * b \neq -1$. To see this, let us simply write down what it means for $a, b \in S$ to have $a * b = -1$. This means

$$a + b + ab = -1,$$

or equivalently

$$ab + a + b + 1 = 0.$$

But $ab + a + b + 1 = (a + 1)(b + 1)$, so if this is zero, then one of $a + 1$ or $b + 1$ is zero. This is impossible since $a, b \in S$ so neither are -1. Thus S is really closed under $*$.

Now let us check that $*$ is associative. Let $a, b, c \in S$. We have

$$(a * b) * c = (a + b + ab) * c = a + b + ab + c + (a + b + ab)c = a + b + ab + c + ac + bc + abc.$$

We also have

$$a * (b * c) = a * (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc.$$

After rearranging, we see that both expressions are equal. So $*$ is associative.

Now we need to find an identity element. I claim that 0 is an identity element for $(S, *)$. To see this, let $a \in S$. We compute

$$0 * a = 0 + a + 0a = a$$

and

$$a * 0 = a + 0 + a0 = a,$$

so 0 is an identity element.

Next we check for the existence of inverses. This means for every $a \in S$, we need to find an a' such that $a * a' = a' * a = 0$. The formula for a' is $a' = \frac{-a}{a+1}$ which can be derived by solving the equation $a + a' + aa' = 0$. We compute

$$\frac{-a}{a+1} * a = \frac{-a}{a+1} + a - \frac{a^2}{a+1} = a - \frac{a^2 + a}{a+1} = a - a = 0.$$

Similarly, one can compute that $a * a' = 0$ (though, strictly speaking, we do not need to do this since we are about to check that $*$ is commutative!) This completes the verification that $(S, *)$ is a group.

Finally, we check that $(S, *)$ is abelian. Let $a, b \in S$. Then we compute

$$a * b = a + b + ab = b + a + ba = b * a,$$

which shows that $(S, *)$ is abelian. So we are done.

Exercise (Judson, Chapter 3, Exercise 45)**.** Prove that the intersection of two subgroups of a group G is also a subgroup of G.

Solution. Let H, K be two subgroups of G. Let e denote the identity of G. We need to check that $e \in H \cap K$, that $H \cap K$ is closed under the group operation, and that $H \cap K$ has inverses. To see that $e \in H \cap K$, we note that since H and K are subgroups of G, $e \in H$ and $e \in K$. So $e \in H \cap K$.

Now let $g, h \in H \cap K$. Then $g, h \in H$ and $g, h \in K$. Since H and K are subgroups, $gh \in H$ and $gh \in K$. Thus $gh \in H \cap K$. Similarly if $g \in H \cap K$, then $g \in H$ and $g \in K$. Thus $g^{-1} \in H$ and $g^{-1} \in K$, and so $g^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of G.

Exercise (Judson, Chapter 3, Exercise 49)**.** Let a and b be elements of a group G. If $a^4 b = ba$ and $a^3 = e$, prove that $ab = ba$.

Solution. We substitute the second relation into the first: we have $ba = a^4 b = a^3 ab = eab = ab$, which solves the exercise.

Exercise (III)**.** Find all subgroups of the Klein four group V_4. (Don't forget the trivial subgroup and V_4 itself.)

Solution. Recall that $V_4 = \{e, a, b, c\}$ where the elements e, a, b, c are multiplied according to the following Cayley table:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Since every subgroup must contain the identity element e, there are eight sets that may be subgroups:

$$\begin{gathered}\{e\},\\ \{e,a\}, \quad \{e,b\}, \quad \{e,c\},\\ \{e,a,b\}, \quad \{e,a,c\}, \quad \{e,b,c\},\\ \{e,a,b,c\}.\end{gathered}$$

We know that $\{e\}$ and $\{e,a,b,c\}$ are subgroups, but so are the three subsets in the second row. For instance, since $aa = e = ee$, this shows that $\{a,e\}$ has inverses, and since $ee = e = aa$ and $ae = ea = e$, it is also closed. So it is a subgroup, and a similar verification shows $\{e,b\}$ and $\{e,c\}$ are subgroups.

The sets with three element in the third row are not subgroups. Actually, this follows from a theorem we will see later in the course, attributed to Lagrange, that says if H is a subgroup of a finite group G, then the order of H divides the order of G. 3 does not divide 4, so these cannot be subgroups. But this can also be checked directly: $a+b=c$ shows that $\{e,a,b\}$ is not closed, $a+c=b$ shows that $\{e,a,c\}$ is not closed, and $b+c=a$ shows that $\{e,b,c\}$ is not closed. Thus there are five subgroups, namely

$$\{e\}, \quad \{e,a\}, \quad \{e,b\}, \quad \{e,c\}, \quad \{e,a,b,c\}.$$