Math 3310H: Assignment II

Jeremy Favro (0805980)
Trent University, Peterborough, ON, Canada

October 24, 2025

Problem 1. Complete the following Cayley table (for a group). (Justify your results.)

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			
6	6	5	7	8		1		
7	7	8	5	6			1	
8	8	7	6	5				1

Solution 1. The strategy I settled on for this is to use the existing information in the table (obviously) and to break down the unknown entries using the known entries. I found it easiest to look for combinations that gave the identity, like in the case of $8 * 7$ we'll look for some way to make 8 which is the $*$ of something and 7 as $7 * 7 = 1$ which is the identity in this case. We see that $8 = 2 * 7 \implies 8 * 7 = 2 * 7 * 7 = 2 * 1 = 2$. Repeating this process for $8 * 5$ we get $8 * 5 = 3 * 5 * 5 = 3 * 1 = 3$. Using the Sudoku theorem we can automatically fill in the $8 * 6$ spot with a 4 as that is the only element we haven't used.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			3
6	6	5	7	8		1		4
7	7	8	5	6			1	2
8	8	7	6	5				1

Now we can start on the 8 row. Beginning with $5 * 8 = 4 * 8 * 8 = 4 * 1 = 4$. Now $6 * 8 = 3 * 8 * 8 = 3 * 1 = 3$. Then using the Sudoku theorem $7 * 8$ must be 2

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			3
6	6	5	7	8		1		4
7	7	8	5	6			1	2
8	8	7	6	5	4	3	2	1

Now if we just fill in the $5 * 6$ position with $5 * 6 = 2 * 6 * 6 = 2 * 1 = 2$ we obtain that $7 * 6$ must be 3 by Sudoku, then that $7 * 5$ must be 4, then that $6 * 5$ must be 2, then that $6 * 7$ must 4, and $5 * 7$ must be 3.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1	2	4	3
6	6	5	7	8	2	1	3	4
7	7	8	5	6	3	4	1	2
8	8	7	6	5	4	3	2	1

I think this is sufficient because we've only used the already known-to-be-a-group elements and Sudoku theorem so the new elements should preserve associativity. Not entirely sure but pretty confident.

Problem 2. Determine whether the given subset H is a subgroup of the group G.

(a) Let
$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}) \middle| a+b+c+d = 0 \right\}$$
and $G = (\mathcal{M}_{2\times 2}, +)$.

(b) Let $H = \left\{ \frac{1+2m}{1+2n} \middle| m, n \in \mathbb{Z} \right\}$ and $G = (\mathbb{Q} \setminus \{0\}, \cdot)$

(c) Let $H = \{(0,0), (1,9), (2,6), (3,3)\}$ and $G = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +)$

Solution 2.

(a) Here we need:

(i) Closure: Let
$$A, B \in S; \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$
Then
$$A + B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$
and so
$$(a+e) + (b+f) + (c+g) + (d+h) = (a+b+c+d) + (e+f+g+h) = 0 + 0 = 0.$$
Therefore H is closed under $+$.

(ii) H must contain the identity: The identity for matrix addition is just the zero matrix which is obviously contained in H as its elements will sum to zero.

(iii) H must contain inverses: For some
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
the inverse of A is $-A$ whose elements sum to zero as their sum will just be the negative of the sum of the elements of A, which is zero by definition.

As all of the subgroup criterion are satisfied, H is a subgroup of G.

(b) Again we need the following:

(i) Closure: Let $a = \frac{1+2m}{1+2n}$ and $b = \frac{1+2k}{1+2q}$. Then
$$a \cdot b = \frac{1+2m}{1+2n} \cdot \frac{1+2k}{1+2q} = \frac{1+2m+2k+4mk}{1+2n+2q+4nq} = \frac{1+2(m+k+2mk)}{1+2(n+q+2nq)}.$$
Because both $m+k+2mk$ and $n+q+2nq$ will still be integers, $a \cdot b \in H$ and H is therefore closed under $\cdot$.

(ii) H must contain the identity: The identity for multiplication is

$$1 = \frac{1}{1} = \frac{1+2\cdot 0}{1+2\cdot 0} \in H.$$

(iii) H must contain inverses: For any element $a = \frac{1+2m}{1+2n}$, $a^{-1} = \frac{1+2n}{1+2m} \in H$.

As all subgroup criterion are satisfied, H is a subgroup of G.

(c) Again we need the following:

(i) H must contain inverses:

$$\begin{aligned}(1,9)+(3,3)&=(0,0)\\(2,6)+(2,6)&=(0,0)\\(3,3)+(1,9)&=(0,0).\end{aligned}$$

(ii) The identity here is obviously $(0,0)$ as the operation is addition.

(iii) Closure: Here we need to check that repeated addition of each element is closed and that adding each element to another element is closed (recursively). First for $n \in \mathbb{Z}$,

$$\begin{array}{rlll} & n=2 & n=3 & n=4 \\ n(1,9)= & (2,6), & (3,3), & (0,0) \\ n(3,3)= & (2,6), & (1,9), & (0,0) \\ n(2,6)= & (0,0) & & \end{array}.$$

Then for addition of individual elements there are several we don't need to check because they are inverses and the operation here is commutative, all we need is:

$$(1,9)+(2,6)=(3,3)$$

and

$$(2,6)+(3,3)=(1,9).$$

These actually come up in checking the repeated addition but I find this a little more clear.

Problem 3. Prove that any nonabelian group contains nontrivial subgroups.

Solution 3. Any nonabelian group $G \neq \{e\}$ as the trivial group is abelian. This means that there exists some $a \in G$ with $a \neq e$ which means that there exists a subgroup $H = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

Problem 4. Let G be an abelian group. Show that the elements of finite order in G form a subgroup.

Solution 4. Let H be the potential subgroup we are considering here. Following the subgroup criterion:

1. Identity: the identity, e, (whatever the operation may be) will have order 1 and therefore will be in H.
2. Closure: Let $a, b \in H$. Then $|a| = n$ and $|b| = m$ for some positive $n, m \in \mathbb{Z}$. Then, by definition $a^n = e$ and $b^m = e$. We also have that, because G is abelian, $(ab)^k = a^k b^k$ for all k. So, $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e \implies |ab| \leq nm$ and so $ab \in H$.
3. Inverses: Let $a \in H$. Then $|a| = n$ and $a^n = e$ for some positive $n \in \mathbb{Z}$. $a^{-1} \in H$ because

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$$

which means that a^{-1} has finite order $\left|a^{-1}\right| \leq n$ and therefore belongs to H.

Problem 5. For $n \in \mathbb{N}$ define

$$\mathcal{U}(n) = \{x \in \mathbb{Z}_n \,|\, \gcd(x,n) = 1\}.$$

Find the order of the groups

(a) $\mathcal{U}(10)$

(b) $\mathcal{U}(19)$

(c) $\mathcal{U}(20)$

(d) $\mathcal{U}(36)$

Solution 5.

(a) This is the group of all integers coprime with 10. These are 9, 8, 7, 6, 4, 3, and 1. Therefore $|\mathcal{U}(10)| = 7$

(b) 19 is prime so $\mathcal{U}(19)$ will be the group of all $n \in \mathbb{Z}$, $0 < n < 19$. These are

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$$

so $|\mathcal{U}(19)| = 18$.

(c) The set of $n \in \mathbb{Z}$ which satisfy $\gcd(x, 20) = 1$ is $\{1, 3, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$ so $|\mathcal{U}(20)| = 15$

(d) While looking up coprime numbers to see if there's anything interesting about them (there is), I found out you can calculate the number of numbers coprime to another number using Euler's (of course) "totient function":

$$n \prod_{p|n} (1 - \frac{1}{p})$$

where n is the number whose count of coprimes we want to know and the product runs over the prime numbers p which divide n. In this case the prime factorization of 36 is $2^2 3^3$ so the product is

$$36 \left[\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \right] = 12 \implies |\mathcal{U}(36)| = 12.$$

Problem 6. Let G be a group and $a, b \in G$ such that $ab \neq ba$. Prove that $aba \neq e$.

Solution 6. Assume, by way of contradiction, that $aba = e$. Then if we multiply $aba = e$ by a^{-1} on the right we get $ab = a^{-1}$. But if we multiply by a^{-1} on the left we get $ba = a^{-1} \implies ba = ab$ which is in contradiction with our original statement. Therefore $aba \neq e$ if $ab \neq ba$.