Algebra: Chapter 0 Exercises

Chapter 2, Section 1

David Melendez

May 5, 2017

Problem 1.3. Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements g, h of a group G.

Proof. We have (by associativity) that $(gh)(g^{-1}h^{-1}) = e$. But $(gh)(gh)^{-1} = e$, so by cancellation $(gh)^{-1} = h^{-1}g^{-1}$. □

Problem 1.4. Suupose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

Proof. $gh = ghe = gh(hg)^2 = ghhghg = gghg = hg$ □

Problem 1.5. Prove that ever row and every column of the 'multiplication table' of a group contains all elemtns of the group exactly once.

Solution. That every row of a group G's multiplication table is 'sudoku complete' (if you will) is equivalent to the following:

Proposition. For every $g, h \in G$ $g \neq h$, there exists a unique $x \in G$ such that $gx = h$.

Proof. Putting $x = g^{-1}h$, we have $gx = gg^{-1}h = h$. If any y satisfies this property, we have

$$\begin{aligned} gx = h = gy &\implies gx = gy \\ &\implies g^{-1}x = g^{-1}y \\ &\implies x = y \end{aligned}$$

□

The proof for columns is entirely analogous. ■

Problem 1.6. Prove that there is only *one* possible multiplication table for G if G has exactly $1, 2$, or 3 elements. Analyze the possible multiplication tables for groups with exactly 4 elements, and show that there are *two* distinct tables, up to reordering the elements of G.

Solution. .

1. The proof for $|G| = 1$ is trivial.
2. For $|G| = 2$ and $e, a \in G$, we have $ee = e$, $ea = a$, and $ae = e$. Since each element of a group must have an inverse, we must also have $a = a^{-1}$ (since $e \neq a^{-1}$), so $a^2 = e$.
3. For $|G| = 3$, consider the table:

$\cdot$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

We can complete the table like a sudoku puzzle using problem 1.5. Since $ea = a$, we cannot have $a^2 = a$. Since $eb = b$, we can't have $a^2 = e$ since that would force $ab = b$. Hence, $a^2 = b$.

$\cdot$	e	a	b
e	e	a	b
a	a	b	?
b	b	?	?

The rest of the table is forced by problem 1.5.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. Consider the table for $|G| = 4$:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	?	?	?
b	b	?	?	?
c	c	?	?	?

For this table we have two distinct cases: where $a^2 = e$ and where $a^2 = b$. The case where $a^2 = c$ is the same as where $a^2 = b$ up to reordering.
First consider $a^2 = e$:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	?	?
c	c	?	?	?

We can complete the rest of the table using problem 1.5:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Notice that we can also fill the table out this way:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

As it turns out, this is equivalent to the case where $a^2 = b$, but with b and a switched (that is, up to reordering):

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

■

Problem 1.8. Let G be a finite abelian group, with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$.

Proof. Since every element of G has an inverse and the order of composition doesn't matter (since G is abelian), we have, with each $g_j \in G$,

$$\begin{aligned}\prod_{g \in G} g &= e \cdot f \cdot (g_1 \cdot g_1^{-1}) \cdot (g_2 \cdot g_2^{-1}) \cdots (g_n \cdot g_n^{-1}) \\ &= e \cdot f \cdot (e)(e) \cdots (e) \\ &= f\end{aligned}$$

where $n = |G| - 2$ □

Problem 1.9. Let G be a finite group of order n and let m be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd.

Proof. We can divide the elements of G into three classes: elements of order 1, elements of order 2, and elements of order greater than 2:

1. The only group element of order 1 is the identity e.

2. We have assumed that there are m elements of order 2.
3. Note that for every element g with $|g| > 2$, we also have a distinct g^{-1}, meaning that there are an even number of these elements.

Taking these three classes into consideration, we have $|G| = n = 1 + m + 2j$ where j is a nonnegative integer. Hence $n - m = 2j + 1$ as desired. □

Problem 1.10. Suppose the order of g is odd. What can you say about the order of g^2?

Solution. $|g^2| = \frac{\text{lcm}(2,|g|)}{2} = |g|$ ■

Problem 1.11. Prove that for all g, h in a group G, $|gh| = |hg|$.

Solution. Since $gh = h(gh)h^{-1}$, we just need to prove that $|aga^{-1}| = |g|$ for $a, g \in G$ (as is given in the problem as a hint).

Proof. Note that, with $n = |g|$,

$$\begin{aligned}(aga^{-1})^n &= ag(a^{-1}a)g(a^{-1}a)\cdots ga^{-1} \\ &= a(g^n)a^{-1} \\ &= aa^{-1} \\ &= e\end{aligned}$$

Since n is the smallest positive integer that makes the g's vanish like this, we have $|aga^{-1}| = n = |g|$. □

■

Problem 1.12. In the group of 2×2 matrices, consider

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad , \qquad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Verify that $|g| = 4$, $|h| = 3$, and $|gh| = \infty$.

Solution. The first two are a trivial application of matrix multiplication.
Consider the product $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We will work with its corresponding linear map

Proposition. $|gh| = \infty$

Proof. Consider the corresponding linear map $T \in \mathcal{L}(\mathbb{R}^2)$. Let x, y be a basis of $\mathbb{R}^2$. We then have, from the matrix, that

$$\begin{aligned}Tx &= x \\ Ty &= x + y\end{aligned}$$

(This is enough to define T since T is linear).
It then follows that T^n is as follows:

$$\begin{aligned}
T^n x &= x \\
T^n y &= nx + y
\end{aligned}$$

Finding the order of gh then boils down to solving $T^n = I$ for n. Since $T^n x = x$, we just need to solve $T^n y = y$.

$$\begin{aligned}
T^n y &= y \\
\implies nx + y &= y \\
\implies \quad nx &= 0 \\
\implies \quad n &= 0
\end{aligned}$$

Since no integer other than 0 gives $T^n = (gh)^n = e$, we have $|gh| = \infty$. ■

■

Problem 1.13. Give an example showing that $|gh|$ is not necessarily $\text{lcm}(|g|, |h|)$ even if g and h commute.

Solution. Let $h = g^{-1}$ and $g \neq e$. Then clearly g and h commute, but
$\text{lcm}(|g|, |h|) = |g| \neq |gh| = 1$. ■

Problem 1.14. As a counterpoint to Exercise 1.13, prove that if g and h commute, and $\gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$. (Hint: let $N = |gh|$; then $g^N = (h^{-1})^N$. What can you say about this element?)

Proof. We will prove, with $|gh| = N, |g| = m, |h| = n$, that $N|mn$ and $mn|N$.
Note that since g and h commute, $(gh)^{mn} = g^{nm}h^{mn} = e$. Hence, $N|mn$.
Now, consider $(gh)^N$. Note that since $(gh)^N = e$, we have $g^N = (h^N)^{-1} = (h^{-1})^N$. Then, since $(g^N)^n \left((h^{-1})^N\right)^n = h^{-Nn} = e$, we have $m|Nn$. Similarly, $n|Nm$. It then follows, since $\gcd(m, n) = 1$, that $m|N$ and $n|N$. Finally, since m and n are coprime, it follows from this that N must be a product of the prime factors of n, the prime factors of m, and some other positive integer, showing that $mn|N$, as desired. □

¡++¿