UH - Math 3330 - Dr. Heier - Spring 2014
HW 7 - Solutions to *Selected* Homework Problems
by Angelynn Alvarez

1. (Section 3.3, Problem 14g) Prove that the following subset H of $M_2(\mathbb{R})$ is a subgroup of the group G of all invertible matrices in $M_2(\mathbb{R})$ under multiplication.

(g)

$$H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc = 1 \right\}$$

Proof. First note that when $a = d = 1$ and$b = c = 0$, the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in H, so $H \neq \emptyset$.

Now let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ be in H. This means that $ad - bc = 1$ and $a'd' - b'c' = 1$. Usual matrix multiplication yields

$$AB = \begin{bmatrix} aa' + bc' & ad' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}$$

Note that $(aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') = (ad - bc)(a'd'b'c') = (1)(1) = 1$. Hence, $AB \in H$ and H is closed under multiplication.

Lastly, for any $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H$, its inverse is $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, where $da - (bc) = 1$, due to the commutativity of the reals. Hence $A^{-1} \in H$. Therefore, H is a subgroup of $M_2(\mathbb{R})$. □

3. (Section 3.3, Problem 17) **(a)** For any group G, the set of all elements that commute with every element of G is called the **center** of G and is denoted by $Z(G)$:

$$Z(G) = \{a \in G \mid ax = xa \text{ for every } x \in G\}$$

Prove that $Z(G)$ is a subgroup of G.

(b) Let R be the equivalence relation on G defined by xRy if and only if there exists an element $a \in G$ such that $y = a^{-1}xa$. If $x \in Z(G)$, find $[x]$, the equivalence class containing x.

Solution.
(a) $Z(G)$ is a subgroup of G.

Proof. First note that $Z(G)$ is nonempty because $e \in Z(G)$. Now let $a, b \in Z(G)$ and let $x \in G$ be arbitrary. Due to the associativity of G and the fact that $ax = xa$ and $bx = xb$, we have

$$(ab)(x) = a(bx) = a(xb) = (ax)(b) = (xa)(b) = x(ab)$$

Thus, $ab \in Z(G)$ and $Z(G)$ is closed under multiplication. Now let a^{-1} be the inverse of $a \in Z(G)$. Then

$$a^{-1}x = a^{-1}xe = a^{-1}x(aa^{-1}) = a^{-1}(xa)a^{-1} = a^{-1}(ax)a^{-1} = (a^{-1})(ax)a^{-1} = xa^{-1}$$

So, $a^{-1} \in Z(G)$ and $Z(G)$ is a subgroup of G. □

(b) Let $a \in Z(G)$. The equivalence class containing x is

$$\begin{aligned}[x] &= \{y \in G \mid y = a^{-1}xa, a \in G\} \\ &= \{y \in G \mid y = a^{-1}ax, a \in G\} \\ &= \{y \in G \mid y = ex, a \in G\} \\ &= \{y \in G \mid y = x\}\end{aligned}$$

Thus, $[x] = \{x\}$.

4. (Section 3.3, Problem 24) Let G be an abelian group. For a fixed positive integer n, let

$$G_n = \{a \in G \mid a = x^n \text{ for some } x \in G\}$$

Prove that G_n is a subgroup of G.

Proof. Since $e = e^1$, $e \in G_n$—so $G \neq \emptyset$. Now assume $a, b \in G_n$. This means that $\exists\ x, y \in G$ such that $a = x^n$ and $b = y^n$. Consider ab^{-1}. Then $ab^{-1} = x^n(y^n)^{-1}$. Because $(x^n)^{-1} = (x^{-1})^n$, we have that $ab^{-1} = x^n(y^n)^{-1}$. Since G is abelian, $ab^{-1} = (xy^{-1})^n$. Thus, $ab^{-1} \in G_n$ and by Theorem 3.10, G_n is a subgroup of G. □

5. (Section 3.4, Problem 23c, d) Let $G = \langle a \rangle$ be a cyclic group of order 24. List all the elements having each of the following orders in G.

Solution.
(c) We want to list the elements which have order **4**. Because G has order 24. we have that $a^{24} = e$. So $(a^6)^4 = a^{24} = e$. Thus, a^6 has order 4. Also, $(a^{18})^4 = a^{72} = (a^{24})^3 = e^3 = e$. Thus, a^{18} has order 4. Hence, the elements $\boxed{a^6 \text{ and } a^{18} \text{ have order } 4}$.

(d) We are asked to list the elements which have order **10**. Because 10 does not divide 24, there is $\boxed{\text{no element in } G \text{ with order } 10}$.

6. (Section 3.4, Problem 33) If G is a cyclic group, then the equation $x^2 = e$ has at most two distinct solutions in G.

Proof. First note that e is a solution to the given equation. If there is no other solution, then we are done. So, suppose b and c are two nontrivial solutions. Because G is cyclic, we know that $\exists\ a \in G$ such that $G = \langle a \rangle$. Thus, $\exists$ integers $k, l \in \mathbb{Z}$ such that $b = a^k$ and $c = a^l$. Because, they are both solutions to the given equation, we know that $(a^k)^2 = e$ and $(a^l)^2 = e$. This means that the order of b is 2 and that the order of c is also 2. Thus, b and c each generate a subgroup of order 2. In particular, $\langle b \rangle = \langle a^k \rangle = \{e, a^k\}$ and $\langle c \rangle = \langle a^l \rangle = \{e, a^l\}$. But because G is cyclic, there is only one subgroup of each order. Thus $\langle b \rangle = \langle c \rangle$, and $a^k = a^l$. Hence, there is at most one nontrivial solution. Thus, the equation $x^2 = e$ has at most two distinct solutions in G. □