Nathan Bickel
MATH 546: Section
Professor: Dr. Vraciu
September 21, 2023

MATH 546 Homework 3

Problem 1 Find the order of each of the following elements of $GL_2(\mathbb{R})$. Show work to prove your answer.

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Solution.

For A, we have

$$A^1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, A^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2,$$

so $o(A) = 4$. However, we claim that

$$B^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

We will show this with induction. Clearly the base case is true, since $[B^1]_{1,2} = [B]_{1,2} = 1$. For the induction step, let $n \in \mathbb{N}$, $n > 1$, and suppose that

$$B^{n-1} = \begin{bmatrix} 1 & n-1 \\ 0 & 1 \end{bmatrix}.$$

Then we can write

$$B^n = B(B^{n-1}) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n-1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (n-1)+1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

so the claim holds for all $n \in \mathbb{N}$. Thus $o(B) = \infty$, because

$$B^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

for all $n \in \mathbb{Z}^+$. □

Problem 2 Let n, k be integers, $n \geq 2$. Prove that the order of $[k]_n$ as an element of $\mathbb{Z}_n$ is equal to $n/\gcd(n, k)$.

Solution.

Let $d := \gcd(n, k)$. We first claim that $\frac{n}{d}$ times $[k]_n$ is the identity $[0]_n$. Since $d \mid k$, there exists $\ell \in \mathbb{Z}$ such that $k = d\ell$. So

$$\left[\frac{n}{d}\right]_n \cdot [k]_n = \left[\frac{nk}{d}\right]_n = \left[\frac{nd\ell}{d}\right]_n = [n\ell]_n.$$

Since $n \mid (n\ell - 0)$, we have $n\ell \equiv 0 \pmod{n}$ and thus $[n\ell]_n$ is the identity element $[0]_n$.

We next claim that for any $m \in \mathbb{N}$, $1 \leq m < \frac{n}{d}$, m times $[k]_n$ is not the identity $[0]_n$. Suppose toward contradiction that there exists some $m \in \mathbb{N}$, $1 \leq m < \frac{n}{d}$ such that m times $[k]_n$ is the identity element $[0]_n$. So

$$[m]_n \cdot [k]_n = [mk]_n = [0]_n,$$

and thus $n \mid mk$. Since $m < \frac{n}{d}$, we also have

$$mk < \frac{nk}{\gcd(n,k)} = \operatorname{lcm}(n,k)$$

(we have proved that $ab = \gcd(a,b)\operatorname{lcm}(a,b)$ for $a, b \in \mathbb{N}$). Clearly, mk is a multiple of k, and by our assumption, mk is a multiple of n. But then mk is a common multiple of n and k, a contradiction since it is less than $\operatorname{lcm}(n,k)$. Therefore, we have

$$o([k]_n) = \frac{n}{\gcd(n,k)}.$$

□

Problem 3 Using the result from problem 2, list all the elements of $\mathbb{Z}_{90}$ that have order equal to 6. Explain how you know that the elements on your list have order equal to 6, and also how you know that the list is complete.

Solution.

From problem 2, all elements $[k]_{90}$ with $o([k]_{90}) = 6$ will have $\frac{90}{\gcd(90,k)} = 6$, which implies $\gcd(90,k) = 15$. For $0 < k < 90$, we have $15|k$ if and only if $k \in \{15, 30, 45, 60, 75\}$ ($[0]_{90}$ has order 1, so we won't consider it). We have

$$\gcd(90,15) = 15, \gcd(90,30) = 30, \gcd(90,45) = 45, \gcd(90,60) = 30, \gcd(90,75) = 15,$$

so $[15]_{90}$ and $[75]_{90}$ are the only elements in $\mathbb{Z}_{90}$ with order 6. □

Problem 4 Let $(G,*)$ be a group with the property that $(a*b)^2 = a^2 * b^2$ for all $a, b \in G$. Prove that G is abelian.

Solution.

Let $a, b \in G$. We have

$$\begin{aligned}
(a*b)^2 &= a^2 * b^2 && \text{(property)}\\
\implies (a*b)*(a*b) &= (a*a)*(b*b)\\
\implies a*(b*a)*b &= a*(a*b)*b && \text{(associativity)}\\
\implies (a^{-1}*a)*(b*a)*(b*b^{-1}) &= (a^{-1}*a)*(a*b)*(b*b^{-1})\\
\implies e*(b*a)*e &= e*(a*b)*e\\
\implies b*a &= a*b,
\end{aligned}$$

so for all $a, b \in G$, $a*b = b*a$. Thus, G is commutative and therefore abelian. □

Problem 5 Let $(G,*)$ be a group, and let $a, b \in G$ be elements of G. Assume that $o(a) = 3$, $o(b) = 2$, and $a*b = b*a$. Prove that $o(a*b) = 6$.

We first claim $(a * b)^6 = e$. We have $(a * b)^6 = a^6 * b^6$ because $*$ is commutative, and

$$a^6 * b^6 = a^3 * a^3 * b^2 * b^2 * b^2 = e * e * e * e * e = e$$

because $o(a) = 3, o(b) = 2 \implies a^3 = b^2 = e$.

We next claim $(a * b)^k \neq e$ for some $k \in \{1, 2, 3, 4, 5\}$. Suppose (toward contradiction) there does exist some such k.

Case 1: $(a * b)^1 = e$. Then $a * b^2 = b$, and since $b^2 = e$, we have $a * e = b$ and thus $a = b$. This is a contradiction because $o(a) \neq o(b)$.

Case 2: $(a * b)^2 = e$. Then $a^2 * b^2 = e$, and since $b^2 = e$, we have $a^2 * e = e$ and thus $a^2 = e$, a contradiction because $o(a) = 3 > 2$.

Case 3: $(a * b)^3 = e$. Then $a^3 * b^3 = e$, and since $a^3 = e$, we have $e * b^3 = e$. So $b^3 = e$, thus $b * b^2 = e$, thus $b^1 * e = e$, thus $b = e$, a contradiction because $o(b) = 2 > 1$.

Case 4: $(a * b)^4 = e$. Then $a^4 * b^4 = e \implies a^3 * a * b^2 * b^2 = e$, and since $a^3 = b^2 = e$, we have $e * a * e * e = e \implies a * e$, a contradiction since $o(a) = 3 > 1$.

Case 5: $(a * b)^5 = e$. Then $a^5 * b^5 = e \implies a^3 * a^2 * b^2 * b^2 * b = e \implies e * a^2 * e * e * b = e \implies a^2 * b = e$. Since $b^2 = e$, we have $a^2 * b^2 = b \implies a^2 * e = b \implies a^2 = b$. Since $a^3 = e$, we have $a^2 = b \implies a^3 = ab \implies ab = e$. So $a^{-1} = b$, but this is a contradiction because we have shown $o(a) = o(a^{-1})$, and we have $o(a) \neq o(b)$.

So the least $k > 0$ such that $(a * b)^k = e$ is 6. Thus, $o(a * b) = 6$. □