MATH 430: HW 2

Jacob Lockard

28 January 2026

Exercise 2.10 (Detailed)

> *Let n be a positive integer and let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.*
>
> *a. Show that $\langle n\mathbb{Z}, +\rangle$ is a group.*
>
> *b. Show that $\langle n\mathbb{Z}, +\rangle \simeq \langle \mathbb{Z}, +\rangle$.*

Let n be a positive integer, let pq denote ordinary integer multiplication for any $p, q \in \mathbb{Z}$, let $+$ be the ordinary addition operator on $\mathbb{Z}$, and let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.

(a) We will show that $\langle n\mathbb{Z}, *\rangle$ is a group, where $* : n\mathbb{Z} \to n\mathbb{Z}$ is the function such that $np * nq = p + q$ for all $np, nq \in n\mathbb{Z}$.

Let $np, nq \in n\mathbb{Z}$. By distributivity in $\mathbb{Z}$,

$$np * nq = np + nq = n(p + q)\,.$$

By definition, $p, q \in \mathbb{Z}$, so $p + q \in \mathbb{Z}$, since $+$ is an operator over the integers and thus has a codomain of $\mathbb{Z}$. So, by definition, $np * nq = n(p+q) \in n\mathbb{Z}$. Since np and nq are arbitrary elements of the domain of $*$ and $np * nq$ is an element of its codomain, we conclude that $*$ exists and is well-defined.

Let $np, nq, nr \in n\mathbb{Z}$. By distributivity and additive associativity in $\mathbb{Z}$,

$$\begin{aligned}
(np * nq) * nr &= (np + nq) + nr \\
&= \big(n(p + q)\big) + nr \\
&= n\big((p + q) + r\big) \\
&= n\big(p + (q + r)\big) \\
&= np + \big(n(q + r)\big) \\
&= np + (nq + nr)\,.
\end{aligned}$$

$np, nq, nr \in n\mathbb{Z}$ by assumption, so by definition,

$$(np * nq) * nr = np + (nq + nr) = np * (nq * nr)\,.$$

We conclude that the group associativity axiom holds for $\langle n\mathbb{Z}, *\rangle$.

Let $nm \in n\mathbb{Z}$, and let 0 be the integer additive identity. $0 \in n\mathbb{Z}$, since $0 = n(0)$. $n \in \mathbb{Z}$ by assumption and $m \in \mathbb{Z}$ by definition, so the closure of integer multiplication ensures $nm \in \mathbb{Z}$. By the definition of 0,

$$nm * 0 = nm + 0 = nm = 0 + nm = 0 * nm\,.$$

We conclude that the group identity axiom holds for $\langle n\mathbb{Z}, *\rangle$, with $0 \in \mathbb{Z}$ being the identity.

Let $nm \in n\mathbb{Z}$. As shown above, $nm \in \mathbb{Z}$, so nm has an integer additive inverse $-nm$. The algebraic properties of the integers ensure that $-nm = (-1)nm = n(-1)m = n(-m)$. Since $-m \in \mathbb{Z}$, by definition $-nm = n(-m) \in n\mathbb{Z}$. By the definition of the integer additive inverse,

$$nm * (-nm) = nm + (-nm) = 0 = (-nm) + nm = (-nm) * nm\,.$$

We conclude that the group inverse axiom holds for $\langle n\mathbb{Z}, *\rangle$, with the inverse of any $nm \in n\mathbb{Z}$ being its integer additive inverse $-nm$. $\square$

(b) We will show that $\langle n\mathbb{Z}, *\rangle \simeq \langle \mathbb{Z}, +\rangle$.

Let $f : n\mathbb{Z} \to \mathbb{Z}$ be defined by $f(nm) = m$. Let $x \in n\mathbb{Z}$. By definition, we can write $x = np$ for some $p \in \mathbb{Z}$. If we can also write $x = nq$ for some $q \in \mathbb{Z}$, then since $n \neq 0$ the cancellation law ensures $p = q$. So for any $x \in n\mathbb{Z}$, there's exactly one way to write x as a product of n and an integer. Thus, f exists.

For any $m \in \mathbb{Z}$, by definition $f(nm) = m$, so f is surjective. Let $np, nq \in \mathbb{Z}$. If $f(np) = f(nq)$, then by definition of the function $p = q$ and thus $np = nq$, so f is injective.

Let $np, nq \in \mathbb{Z}$. Then we have:

$$f(np * nq) = f(np + nq) = f\big(n(p + q)\big) = p + q = f(np) + f(nq)\,,$$

which follows from our definitions and from distributivity and closure in $\mathbb{Z}$. $\square$

Exercise 2.11

Let $n \in \mathbb{N}$. We will show that $\langle M, +\rangle$ is a group, where M is the set of all real, diagonal $n \times n$ matrices and $+$ is the ordinary matrix addition operator.

Let $A, B \in M$. For all $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$, we have:

$$(A + B)_{ij} = A_{ij} + B_{ij} = 0 + 0 = 0\,,$$

since A and B are diagonal. Since all the non-diagonal entries are zero, $A + B$ is diagonal, and hence the codomain of $+$ is M.

Let $A, B, C \in M$. For all $i, j \in \{1, 2, \ldots, n\}$, we have:

$$\begin{aligned}\big((A+B)+C\big)_{ij} &= (A+B)_{ij} + C_{ij} \\ &= A_{ij} + B_{ij} + C_{ij} \\ &= A_{ij} + (B+C)_{ij} \\ &= \big(A+(B+C)\big)_{ij}\,,\end{aligned}$$

which follows from the definition of matrix addition and the associativity of the reals. Since corresponding entries of $(A+B)+C$ and $A+(B+C)$ are equal, we conclude that the associativity axiom holds for $\langle M, +\rangle$.

Let $\mathbf{0}$ be the matrix such that $M_{ij} = 0$ for all $i, j \in \{1, 2, \ldots, n\}$. $\mathbf{0} \in M$, since all entries, including the non-diagonal ones, are zero. Let $A \in M$. Then we have:

$$\begin{aligned}(A+\mathbf{0})_{ij} &= A_{ij} + \mathbf{0}_{ijj} = A_{ij} + 0 = A_{ij}\,, \\ (\mathbf{0}+A)_{ij} &= \mathbf{0}_{ijj} + A_{ij} = 0 + A_{ij} = A_{ij}\,,\end{aligned}$$

by the definition of matrix addition and of $0 \in \mathbb{R}$. So $A + \mathbf{0} = A = \mathbf{0} + A$, and $\mathbf{0}$ satisfies the identity axiom for $\langle M, +\rangle$.

Let $A \in M$. Let $-A$ be the matrix such that $A_{ij} = -A_{ij}$ for all $i, j \in \{1, 2, \ldots, n\}$. For all $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$, we have:

$$(-A)_{ij} = -(A)_{ij} = -0 = 0\,,$$

since A is diagonal. So $-A \in M$. We have:

$$\begin{aligned}\big(A+(-A)\big)_{ij} &= A_{ij} + (-A)_{ij} = A_{ij} + (-A_{ij}) = 0\,, \\ \big((-A)+A\big)_{ij} &= (-A)_{ij} + A_{ij} = (-A_{ij}) + A_{ij} = 0\,,\end{aligned}$$

by the definition of matrix addition and of additive inverses in $\mathbb{R}$. So $A + (-A) = \mathbf{0} = (-A) + A$, and we've shown that the inverse axiom holds for $\langle M, +\rangle$. $\square$

Exercise 2.17

Let $n \in \mathbb{N}$. We will show that $\langle M, \times\rangle$ is a group, where M is the set of all real $n \times n$ upper-triangular matrices with determinant 1, and $\times$ is the ordinary matrix multiplication operator. We also denote $A \times B$ like AB for any real $n \times n$ matrices A and B.

Let $A, B \in \mathbb{M}$. Let $i, j \in \{1, 2, \ldots, n\}$ with $i > j$. By the definition of matrix multiplication,

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} = \sum_{k=1}^{i-1} A_{ik} B_{kj} + \sum_{k=i}^{n} A_{ik} B_{kj}\,.$$

If $k \in \{1, 2, \ldots, i-1\}$, then $i > k$ and $A_{ik} = 0$ since A is upper triangular. So the first sum is zero:

$$\sum_{k=1}^{i-1} A_{ik} B_{kj} = \sum_{k=1}^{i-1} 0(B_{kj}) = 0 \, .$$

If $k \in \{i, i+1, \ldots, n\}$, then $k \geq i > j$ and $B_{kj} = 0$ since B is upper triangular. So the second sum is zero:

$$\sum_{k=i}^{n} A_{ik} B_{kj} = \sum_{k=i}^{n} B_{kj}(0) = 0 \, .$$

We've shown that for any $i, j\{1, 2, \ldots, n\}$ with $i > j$, we have $(AB)_{ij} = 0$. So AB is upper triangular. Further, we have:

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1 \, ,$$

so the determinant of AB is 1. We conclude that the codomain of $\times$ is M.

Any introductory linear algebra text will demonstrate that $\times$ is associative over M, and that there exists an identity matrix I for the set of $n \times n$ matrices. This identity is upper triangular and has determinant 1, so we are assured it is in M.

Finally, let $A \in M$. Since $\det A = 1$, we know it is invertible. Denote its inverse A^{-1}. We know $\det A^{-1} = (\det A)^{-1} = 1$, and for the purposes of this proof, we'll assume that A^{-1} is upper triangular. □

Exercise 2.28

> *An element $a \neq e$ in a group is said to have order 2 if $a * a = e$. Prove that if G is a group and $a \in G$ has order 2, then for any $b \in G$, $b' * a * b$ also has order 2.*

Let G be a group. Let $a \in G$ have order 2, and let $b \in G$. We have:

$$\begin{aligned}
(b' * a * b) * (b' * a * b) &= b' * a * (b * b') * a * b && \text{associativity} \\
&= b' * a * e * a * b && \text{inverses} \\
&= b' * a * a * b && \text{associativity, identity} \\
&= b' * e * b && \text{assoc.; since } a \text{ is order 2} \\
&= b' * b && \text{associativity, identity} \\
&= e \, . && \text{identity}
\end{aligned}$$

□

Exercise 2.31

Prove that a group has exactly one idempotent element.

Let $\langle G, * \rangle$ be a group. Let a be an idempotent for $*$ in G. Then,

$$\begin{aligned} a * a &= a \\ a * a * a' &= a * a' \\ a * e &= a * a' \\ a &= e\,. \end{aligned}$$

Since the group identity is unique, the idempotent must also be unique. □

Exercise 2.32

Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian.

Let $a, b \in G$. Then,

$$\begin{aligned} (a * b) * (a * b) &= e \\ a * b * a * b &= e \\ a * a * b * a * b &= a * e \\ b * a * b &= a * e \\ b * b * a * b &= b * a * e \\ a * b &= b * a\,. \end{aligned}$$

□

Exercise 2.33

Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

Let $\langle G, * \rangle$ be an abelian group. For every $n \in \mathbb{Z}^+$, let P_n be the statement that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$. We will show that P_n holds for all $n \in \mathbb{Z}^+$.

P_1 holds, since for all $a, b \in G$,

$$(a * b)^1 = a * b = (a^1) * (b^1)\,.$$

Now assume that P_n holds for some $n \in \mathbb{Z}^+$. We have, for all $a, b \in G$:

$$\begin{aligned}
(a * b)^{n+1} &= (a * b)^n * (a * b) && \text{definition} \\
&= (a^n) * (b^n) * a * b && \text{assumption} \\
&= (a^n) * a * (b^n) * b && \text{abelian} \\
&= (a^{n+1}) * (b^{n+1})\,. && \text{definition}
\end{aligned}$$

We've shown that P_1 holds and that P_n implies P_{n+1} for all $n \in \mathbb{Z}^+$. By induction, we conclude that P_n holds for all $n \in \mathbb{Z}^+$. $\square$

Exercise 2.36

> *Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.*

Let $a \in G$. Let $f : \mathbb{N} \to G$ be defined like $f(n) = a^n$. $\mathbb{N}$ is infinite and G is finite, so $|\mathbb{N}| > |G|$, which means f is not injective. So there exist $n, m \in \mathbb{N}$ such that $a^n = f(n) = f(m) = a^m$ and $n \neq m$. Assume without loss of generality that $m > n$. We have:

$$\begin{aligned}
a^n &= a^m \\
a^n &= a^{(m-n)+n} \\
a^n &= a^{m-n} * a^n \\
a^n * (a^{-1})^n &= a^{m-n} * a^n * (a^{-1})^n \\
(a * a^{-1})^n &= a^{m-n} * (a * a^{-1})^n \\
(e)^n &= a^{m-n} * (e)^n \\
e &= a^{m-n} * e \\
e &= a^{m-n}\,.
\end{aligned}$$

But $m - n > 0$, so $m - n \in \mathbb{Z}^+$. We've thus shown that $m - n$ has the desired properties.

$\square$

Exercise 2.38

> *Let G be a group and let $a, b \in G$. Show that $(a * b)' = a' * b'$ if and only if $a * b = b * a$.*

If $(a * b)' = a' * b'$,

$$\begin{aligned}
(a * b)' * a * b &= e \\
a' * b' * a * b &= e \\
a * b &= b * a\,.
\end{aligned}$$

If $a * b = b * a$,

$$\begin{aligned} (a * b)' * a * b &= e \\ (a * b)' * b * a &= e \\ (a * b)' &= a' * b' \,. \end{aligned}$$

□