171 — 3

RJ Acuna

(862079740)

Section 4

40 Let $\langle G, \cdot \rangle$ be a group. Consider the binary operation $*$ on the set G defined by

$$a * b = b \cdot a$$

for $a, b \in G$. Show that $\langle G, * \rangle$ is a group, and that $\langle G, * \rangle$ is actually isomorphic to $\langle G, \cdot \rangle$. [Hint: consider the map ϕ with $\phi(a) = a'$ for $a \in G$]

pf.

By hint, consider $\phi : G \to G; a \mapsto a'$.

Suppose $\exists a, b \in G : \phi(a) = \phi(b)$

$$\phi(a) = \phi(b) \implies a' = b' \implies a' * b = b' * b \implies b \cdot a' = b \cdot b' \implies b \cdot a' = e \implies b = (a')' \implies b = a \ .$$

So, ϕ is injective.

Let $c \in G$, we want to show $\exists x \in G : \phi(x) = c$,

Since G is a group $c' \in G$, then $\phi(c') = (c')'$

$$\phi(c') = (c')' \implies \phi(c') * c' = (c')' * c' \implies \phi(c') * c' = e \implies \phi(c') = c \ .$$

So, ϕ is surjective. So,ϕ is a bijection.

We want to show $\forall x, y \in G : \phi(x \cdot y) = x * y$.

$$\phi(x \cdot y) = (x \cdot y)' = y' \cdot x' = \phi(y) \cdot \phi(x) = \phi(x) * \phi(y) \ .$$

So $\langle G, \cdot \rangle$ and $\langle G, * \rangle$ are isomorphic binary structures.

Now to show $\langle G, * \rangle$ is a group note:

Let $z \in G$, then compute $z * e = e \cdot z = z = z \cdot e = e * z$. So, e is the identity element of $\langle G, * \rangle$. This follows from $\langle G, * \rangle$ being a binary structure, if it has an identity element it must be unique.

Let $a, b, c \in G$, then compute

$$(a * b) * c = (b \cdot a) * c = c \cdot (a \cdot b) = (c \cdot a) \cdot b = (a * c) \cdot b = b * (a * c) \ .$$

Which holds since $\langle G, \cdot \rangle$ is a group.

Let $w \in G$, then compute

$$w * w' = w' \cdot w = e$$

So, w' is the inverse of w with respect to $*$, and it exists and is in G, since $\langle G, \cdot \rangle$ is a group.

So, $\langle G, * \rangle$ is a group, and $\langle G, \cdot \rangle \simeq \langle G, * \rangle$ ■

alt. pf. Note, $\phi \circ \phi = 1_G$, so ϕ is a bijection. Prove the homomorphism property as above. So ϕ is an isomorphism. Then note $\langle G, * \rangle$ is a group since isomorphisms preserve the algebraic structure. ■

Section 5

In exercises 8 through 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

8 The $n \times n$ matrices with determinant 2

slu.

No, $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ have determinant 2.

But, $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$, has determinant 4. So, the $n \times n$ matrices with determinant 2 is not closed under matrix multiplication $\lozenge$

13 The set of all $n \times n$ matrices A such that $A^T A = I_n$. [These matrices are called **orthogonal**. Recall A^T, is called the *transpose* of A, is the matrix whose jth column is the jth row of A for $1 \leq j \leq n$, and that the transpose operation has the property $(AB)^T = B^T A^T$.]

pf.

$O(n) := \{X \in GL(n, \mathbb{R}) | X^T X = I_n\}$, denote $I := I_n$.

Let $A, B \in O(n)$

$$(AB)^T AB = B^T A^T AB = B^T IB = B^T B = I \implies AB \in O(n) \ .$$

So, $O(n)$ is closed under multiplication.

$$I^T I = (II^T)^T = (I^T)^T = I \ .$$

So, $I \in O(n)$.

$$\forall X \in O(n), \quad XI = X = IX \ .$$

So, I is the identity element of $O(n)$.

The associativity of $O(n)$ is inherited from $GL(n, \mathbb{R})$.

Since $\forall A \in O(n), A^T A = I$, it follows that $A^T = A^{-1}$ $\square$

In exercises 22 through 25, describe all the elements in $GL(2, \mathbb{R})$ generated by the given 2×2 matrix.

22 $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$

slu.

$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, so $\langle \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \rangle = \{I, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\}$ $\blacklozenge$

23 slu.

Let $M_{23} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$$\begin{aligned} \langle M_{23} \rangle &= \left\{ \ldots, \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, \ldots \right\} \\ &= \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} | n \in \mathbb{Z} \right\} \quad \blacklozenge \end{aligned}$$

24 $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$

I'm a fucking idiot. So I did this one and I didn't have to. slu.

Let $M_{24} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$

$$\langle M_{24} \rangle = \left\{ \dots, \begin{bmatrix} \frac{1}{27} & 0 \\ 0 & \frac{1}{8} \end{bmatrix}, \begin{bmatrix} \frac{1}{9} & 0 \\ 0 & \frac{1}{4} \end{bmatrix}, \begin{bmatrix} \frac{1}{3} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 9 & 0 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 27 & 0 \\ 0 & 8 \end{bmatrix}, \dots \right\}$$
$$= \left\{ \begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix} | n \in \mathbb{Z} \right\} \quad \blacklozenge$$

In Exercises 27 through 35, find the order of the cyclic subgroup of the given subgroup generated by the indicated element.

35 The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

Let $M_{35} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

$$\langle M_{35} \rangle = \{ M_{35}, M_{35}^2, M_{35}^3, M_{35}^4, \dots \}$$
$$= \left\{ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \right\}$$
$$\implies |\langle M_{35} \rangle| = 3 \quad \blacklozenge$$

45 Show that a non-empty subset H of a group G if and only if $ab^{-1} \in H$ for all $a, b \in H$. (This is one of the *more compact criteria* referred to prior Theorem 5.14)

pf.

Let $H \subset G$ and $H \neq \emptyset$. Let $a, b \in H$.

($\implies$) Ass. $H \leq G$.

$H \leq G \implies b^{-1} \in H$ and H is closed $\implies ab^{-1} \in H$.

($\impliedby$) Ass. $\forall a, b \in H$, $ab^{-1} \in H$.

$\forall a, b, c \in H, a(bc) = (ab)c$, since it is also an equation in G.

$\forall a, b \in H \implies ab^{-1} \in H$ and $ba^{-1} \in H$

$\implies aa^{-1} = e = a^{-1}a \in H$. So the identity is in H.

$\implies a^{-1}a(ba^{-1})^{-1} = a^{-1}ab^{-1}a = b^{-1}a \in H$

$\implies b^{-1}aa^{-1} = b^{-1}e = b^{-1} \in H$

Similarly, $a^{-1} \in H$, so inverses are in H.

Also, $ab^{-1}(b^{-1})^{-1} \in H$, and $ab^{-1}(b^{-1})^{-1}(b^{-1})^{-1} = ab \in H$, so H is closed.

$\implies H \leq G \quad \blacksquare$

54 Show that the intersection $H \cup K$ of subgroups H and K of a group G is a subgroup of G.

pf.

$H \leq G$ and $K \leq G \implies e \in H \cup K$. And that for any three elements in both associativity holds as it is inherited from G.

Furthermore, $a \in H$ and $a \in K$, implies $a^{-1} \in H$, and $a^{-1} \in K$, so a^{-1} is in the intersection.

■

57 Show that a group with no proper non trivial subgroups is cyclic.

pf. Let G be a group.

If $a, b \in G, a \neq e, b \neq e$, then G is not cyclic if there is no power of a that you can raise it to get b. If G is not cyclic with that hypothesis, then $< b >$ must be a non trivial subgroup of G, which is a contradiction ■

Section 8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$$

2 $\tau^2\sigma$

slu.

$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix}$$

$$\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix} \quad \blacklozenge$$

5 $\sigma^{-1}\tau\sigma$

This is just stacking the powers of σ.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \\ 4 & 3 & 5 & 6 & 2 & 1 \\ 5 & 4 & 6 & 2 & 1 & 3 \\ 6 & 5 & 2 & 1 & 3 & 4 \\ 2 & 6 & 1 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}$$

So, $\sigma^6 = \iota \implies \sigma^5 = \sigma^{-1}$.

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$$\begin{bmatrix} \iota & 1 & 2 & 3 & 4 & 5 & 6 \\ \sigma & 3 & 1 & 4 & 5 & 6 & 2 \\ \tau & 2 & 4 & 1 & 3 & 6 & 5 \\ \tau\sigma & 1 & 2 & 3 & 6 & 5 & 4 \\ \sigma^{-1} & 2 & 6 & 1 & 3 & 4 & 5 \\ \sigma^{-1}\tau\sigma & 2 & 6 & 1 & 5 & 4 & 3 \end{bmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix} \quad \blacklozenge$$

6 $|\langle\sigma\rangle|$

slu. $|\langle\sigma\rangle| = 6$, because by the computation above it is the smallest power of σ needed to get ι ♦

7 $|\langle\tau^2\rangle|$

slu.

$$\begin{bmatrix} \iota & 1 & 2 & 3 & 4 & 5 & 6 \\ \tau^2 & 4 & 3 & 2 & 1 & 5 & 6 \\ (\tau^2)^2 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}$$

So,$|\langle\tau^2\rangle| = 2$