Homework 3: Sections 5 & 6

Algebra

Author

Paul Beggs

BeggsPA@Hendrix.edu

Instructor

Dr. Christopher Camfield, Ph.D.

Due

September 25, 2025

Section 5

In Exercises 12 and 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.
[Hint: Make use of Exercise 44. What must be the image of a generator under an automorphism?]

12. The $n \times n$ matrices with determinant -1 or 1

Solution. Let H be the set of all $n \times n$ matrices with determinant -1 or 1. We will show that H is a subgroup of $GL(n, \mathbb{R})$ by verifying the subgroup criterion:

- **Identity:** The identity matrix I_n has a determinant of 1, so $I_n \in H$.
- **Closure:** Let $A, B \in H$. Then $\det(A) = \pm 1$ and $\det(B) = \pm 1$. The determinant of the product AB is given by:

  $$\det(AB) = \det(A)\det(B) = (\pm 1)(\pm 1) = \pm 1.$$

  Thus, $AB \in H$.
- **Inverses:** Let $A \in H$. Then $\det(A) = \pm 1$. The determinant of the inverse A^{-1} is given by:

  $$\det(A^{-1}) = \frac{1}{\det(A)} = \pm 1.$$

  Thus, $A^{-1} \in H$.

Therefore, we have shown that H contains the identity, is closed under matrix multiplication, and contains inverses. Hence, H is a subgroup of $GL(n, \mathbb{R})$.

13. The set of all $n \times n$ matrices A such that $(A^T)A = I_n$ [These matrices are called **orthogonal**. Recall that A^T, 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 $(AB)^T = (B^T)(A^T)$].

Solution. Let H be the set of all $n \times n$ orthogonal matrices. We will show that H is a subgroup of $GL(n, \mathbb{R})$ by verifying the subgroup criterion:

- **Identity:** Since the identity matrix I_n has the properties $I_n^T = I_n$ and $I_n I_n = I_n$, then $(I_n^T)I_n = I_n$, so $I_n \in H$.
- **Closure:** Let $A, B \in H$. Then $(A^T)A = I_n$ and $(B^T)B = I_n$. We need to show that $((AB)^T)(AB) = I_n$, thereby showing AB is orthogonal. Using the property of transposes and the associativity of matrix multiplication, we have:

$$\begin{aligned}(AB)^T(AB) &= (B^T)(A^T)(AB)\\ &= (B^T)(A^TA)B\\ &= (B^T)(I_n)(B)\\ &= (B^T)B = I_n.\end{aligned}$$

  Hence, $AB \in H$.
- **Inverses:** For each A in the set, the equation $(A^T)A = A(A^T) = I_n$ shows that there exists an inverse A^T. To show that this inverse exists in the set, consider the following:

$$(A^T)^T A^T = AA^T = I_n.$$

  Thus, $A^T \in H$.

Therefore, we have shown that H contains the identity, is closed under matrix multiplication, and contains inverses. Hence, H is a subgroup of $GL(n, \mathbb{R})$.

In Exercise 34, find the order of the cyclic subgroup of the given group generated by the indicated element.

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

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

Solution. If we continuously multiply the matrix by itself until we get the identity matrix, we find:

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4.$$

Therefore, the order is 4.

---

39. Mark each of the following true or false.

______ **a.** The associative law holds in every group.
______ **b.** There may be a group in which the cancellation law fails.
______ **c.** Every group is a subgroup of itself.
______ **d.** Every group has exactly two improper subgroups.
______ **e.** In every cyclic group, every element has a generator.
______ **f.** A cyclic group has a unique generator.
______ **g.** Every set of numbers that is a group under addition is also a group under multiplication.
______ **h.** A subgroup may be defined as a subset of a group.
______ **i.** $\mathbb{Z}_4$ is a cyclic group.
______ **j.** Every subset of every group is a subgroup under the induced operation.

Solution. In response to the above statements:

a. True. The associative law is one of the defining properties of a group.

b. False. The cancellation law holds in every group due to the existence of inverses.

c. True. A group is always a subgroup of itself by definition.

d. False. The trivial group $G = \{e\}$ only has one improper subgroup, which is itself.

e. False. Consider the counterexample of $\mathbb{Z}_6$, which is cyclic but has elements like 2 and 3 that do not generate the entire group.

f. False. For example, in $\mathbb{Z}_6$, both 1 and 5 are generators.

g. False. The set of integers under addition is a group, but under multiplication, it does not have inverses for all elements (e.g., 2 has no multiplicative inverse).

h. False. A subgroup must satisfy the group axioms, not just be a subset.

i. True. $\mathbb{Z}_4$ is generated by 1 and is cyclic.

j. False. For example, the subset $\{1, 2\}$ of $\mathbb{Z}_4$ is not a subgroup since it is not closed (i.e., $1 + 2 = 3$ is not in the subset).

53. Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $ab^{-1} \in H$. Show that $\sim$ is an equivalence relation on G.

Solution. For $\sim$ to be an equivalence relation on G, we need to satisfy the following conditions:

- **Reflexive:** Since H is a subgroup of G, it has an identity element. So, let $a \in G$, then $aa^{-1} = e$, which is in H.
- **Symmetric:** Let $a, b \in G$ and suppose that $a \sim b$. By definition, this means $ab^{-1} \in H$. Since H is a subgroup, it is closed under inverses. Therefore, the inverse of ab^{-1} must also be in H. The inverse is $(ab^{-1})^{-1} = ba^{-1}$. Since $ba^{-1} \in H$, it follows that $b \sim a$.
- **Transitive:** Let $a, b, c \in G$ with $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$, so their product $ab^{-1}bc^{-1} = ac^{-1}$ is also in H since H is closed under the group operation. Thus, $a \sim c$.

Since $\sim$ is reflexive, symmetric, and transitive, it is an equivalence relation on G.

Section 6

In Exercises 17, 18 and 19, find the number of elements in the indicated cyclic group.

17. The cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25

Solution. The cyclic group $\mathbb{Z}_{30}$ generated by 25 contains the elements:

$$\langle 25\rangle = \{0, 25, 20, 15, 10, 5\}.$$

Therefore, the number of elements in the cyclic group is 6.

18. The cyclic subgroup of $\mathbb{Z}_{42}$ generated by 30

Solution. Similarly to the previous problem, the cyclic group $\mathbb{Z}_{42}$ generated by 30 contains the elements:

$$\langle 30\rangle = \{0, 30, 18, 6, 36, 24, 12\}.$$

Therefore, the number of elements is 7.

19. The cyclic subgroup $\langle i\rangle$ of $\mathbb{C}^*$ of nonzero complex numbers under multiplication

Solution. The cyclic subgroup $\langle i\rangle$ generated by i contains the elements:

$$\langle i\rangle = \{1, i, -1, -i\}.$$

Therefore, the number of elements is 4.

In Exercise 23, find all subgroups of the given group, and draw the subgroup diagram for the subgroups.

23. $\mathbb{Z}_{36}$

Solution. The subgroups of $\mathbb{Z}_{36}$ correspond to the divisors of 36. The divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18,$ and 36. The subgroup diagram is as follows:

$$\begin{tikzcd}
 & & \mathbb{Z}_{36} \arrow[dl, dash] \arrow[dr, dash] & & \\
 & \langle 2\rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 3\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 4\rangle \arrow[dr, dash] & & \langle 6\rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 9\rangle \arrow[dl, dash] \\
 & \langle 12\rangle \arrow[dr, dash] & & \langle 18\rangle \arrow[dl, dash] & \\
 & & \langle 0\rangle & &
\end{tikzcd}$$

46. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

Solution. Let the order of ab be n. This means that $(ab)^n = e$, where e is the identity element of the group G, and n is the smallest positive integer for which this holds. We want to show that $(ba)^n = e$. So, we have:

$$(ba)^n = \underbrace{(ba)(ba)\dots(ba)}_{n \text{ times}}$$

Now, notice that we can write ba as $a^{-1}(ab)a$. Thus, we can make the following substitution:

$$(ba)^n = (a^{-1}(ab)a)(a^{-1}(ab)a)\dots(a^{-1}(ab)a).$$

By rearranging the inner terms, we can connect the a and a^{-1} pairings:

$$\begin{aligned}(ba)^n &= a^{-1}(ab)(aa^{-1})(ab)(aa^{-1})\dots(ab)a \\ &= a^{-1}(ab)(e)(ab)(e)\dots(ab)a \\ &= a^{-1}(ab)^n a.\end{aligned}$$

Recall that $(ab)^n = e$. We can make this substitution to reveal:

$$(ba)^n = a^{-1}(ab)^n a = a^{-1}(e)a = a^{-1}a = e.$$

Thus, $ba^n = e$. So, the order of ba must be a divisor n. If we call the order of ba an integer m, then we have just shown that $m \leq n$.

By a symmetrical argument, the roles of a and b (and thus the products ab and ba) are interchangeable. If we assume that ba has order m, the same exact line of reasoning from above would force the order of ab to be less than or equal to m. Since we know the order of ab is n, the symmetric logic implies that $n \leq m$. Thus, since $n \leq m$ and $m \leq n$, the only way for both equalities to be true is if $n = m$. Therefore, the order of ba is also n.