Homework 3

I encourage you to work on the assignment with other students; remember to name anyone you collaborate with and to write up your final solutions by yourself.

- Lauritzen Chapter 2, Exercises 2, 4, 5, 9, 10
- Problems not from the textbook

1. Prove or disprove that the following are groups:

   (a) even integers under addition

   Solution 0.1. Let G be the set of even integers under addition. We need to check the group axioms:
   Closure: Let $a, b \in G$. Then $a = 2m$ and $b = 2n$ for some integers m and n. Then $a + b = 2m + 2n = 2(m + n)$, which is even. Thus, $a + b \in G$.
   Associativity: Addition of integers is associative, so this holds.
   Identity: The identity element is 0, which is even.
   Inverse: Let $a \in G$. Then $a = 2m$ for some integer m. Then $-a = -2m = 2(-m)$, which is even. Thus, $-a \in G$.
   Thus, G is a group.

   (b) odd integers under addition

   Solution 0.2. Let G be the set of odd integers under addition. We need to check the group axioms:
   Closure: Let $a, b \in G$. Then $a = 2m + 1$ and $b = 2n + 1$ for some integers m and n. Then $a + b = 2m + 1 + 2n + 1 = 2(m + n) + 2 = 2(m + n + 1)$, which is even. Thus, $a + b \notin G$.
   Thus, G is not a group.

   (c) $\{3^n : n \in \mathbb{Z}\}$ under multiplication.

   Solution 0.3. Let $G = \{3^n : n \in \mathbb{Z}\}$ under multiplication. We need to check the group axioms:
   Closure: Let $a, b \in G$. Then $a = 3^m$ and $b = 3^n$ for some integers m and n. Then $a \cdot b = 3^m \cdot 3^n = 3^{m+n}$, which is in G. Thus, $a \cdot b \in G$.
   Associativity: Multiplication of integers is associative, so this holds.
   Identity: The identity element is 1, which is in G.
   Inverse: Let $a \in G$. Then $a = 3^m$ for some integer m. Then $a^{-1} = 3^{-m} = \frac{1}{3^m}$, which is in G.
   Thus, G is a group.

2. Matrix groups are an extremely important class of groups. Assume all matrices in the following statements have entries in $\mathbb{R}$, though it is fun to think about the same questions for matrices with entries in $\mathbb{Z}$ or $\mathbb{C}$! It is also fun to think about the same questions for $n \times n$ matrices. You may assume that matrix addition and matrix multiplication are associative. Prove or disprove that the following are groups:

   (a) 2×2 diagonal matrices under matrix addition

Solution 0.4. Let G be the set of 2×2 diagonal matrices under matrix addition. We need to check the group axioms:
Closure: Let $A, B \in G$. Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ for some real numbers a, b, c, d. Then $A + B = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix}$, which is in G. Thus, $A + B \in G$.
Associativity: Matrix addition is associative, so this holds.
Identity: The identity element is the 2×2 zero matrix, which is in G.
Inverse: Let $A \in G$. Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ for some real numbers a, b. Then $-A = \begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix}$, which is in G.
Thus, G is a group.

(b) 2×2 matrices with determinant 1 under matrix addition

Solution 0.5. Let G be the set of 2×2 matrices with determinant 1 under matrix addition. We need to check the group axioms:
Closure: Let $A, B \in G$. Then $\det(A) = 1$ and $\det(B) = 1$. Then $\det(A + B) = \det(A) + \det(B) = 1 + 1 = 2 \neq 1$. Thus, $A + B \notin G$.
Thus, G is not a group.

(c) 2×2 matrices with determinant 1 under matrix multiplication

Solution 0.6. Let G be the set of 2×2 matrices with determinant 1 under matrix multiplication. We need to check the group axioms:
Closure: Let $A, B \in G$. Then $\det(A) = 1$ and $\det(B) = 1$. Then $\det(A \cdot B) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$. Thus, $A \cdot B \in G$.
Associativity: Matrix multiplication is associative, so this holds.
Identity: The identity element is the 2×2 identity matrix, which is in G.
Inverse: Let $A \in G$. Then $\det(A) = 1$. Then $A^{-1} = \frac{1}{\det(A)} \cdot \operatorname{adj}(A)$, which is in G.
Thus, G is a group.

(d) 2×2 matrices with trace 0 under matrix addition

Solution 0.7. Let G be the set of 2×2 matrices with trace 0 under matrix addition. We need to check the group axioms:
Closure: Let $A, B \in G$. Then $\operatorname{tr}(A) = 0$ and $\operatorname{tr}(B) = 0$. Then $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B) = 0 + 0 = 0$. Thus, $A + B \in G$.
Associativity: Matrix addition is associative, so this holds.
Identity: The identity element is the 2×2 zero matrix, which is in G.
Inverse: Let $A \in G$. Then $\operatorname{tr}(A) = 0$. Then $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$, which is in G.
Thus, G is a group.

(e) 2×2 symmetric matrices (recall that a matrix A is symmetric if $A = A^T$) with nonzero determinant under matrix multiplication

Solution 0.8. Let G be the set of 2×2 symmetric matrices with nonzero determinant under matrix multiplication. We need to check the group axioms:
Closure: Let $A, B \in G$. Then $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ and $B = \begin{pmatrix} d & e \\ e & f \end{pmatrix}$ for some real numbers a, b, c, d, e, f. Then $A \cdot B = \begin{pmatrix} ad + be & ae + bf \\ bd + ce & be + cf \end{pmatrix}$, which is in G. Thus, $A \cdot B \in G$.
Associativity: Matrix multiplication is associative, so this holds.
Identity: The identity element is the 2×2 identity matrix, which is in G.
Inverse: Let $A \in G$. Then $\det(A) \neq 0$. Then $A^{-1} = \frac{1}{\det(A)} \cdot \operatorname{adj}(A)$, which is in G.
Thus, G is a group.

(f) 2×2 orthogonal matrices (recall that a matrix A is orthogonal if $AA^T = I$, where I is the identity matrix) under matrix multplication.

Solution 0.9. Let G be the set of 2×2 orthogonal matrices under matrix multiplication. We need to check the group axioms:
Closure: Let $A, B \in G$. Then $AA^T = I$ and $BB^T = I$. Then $(A \cdot B)(A \cdot B)^T = ABB^TA^T = AIA^T = AA^T = I$. Thus, $A \cdot B \in G$.
Associativity: Matrix multiplication is associative, so this holds.
Identity: The identity element is the 2×2 identity matrix, which is in G.
Inverse: Let $A \in G$. Then $AA^T = I$. Then $A^{-1} = A^T$, which is in G.
Thus, G is a group.

3. Recall Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$. Let n be a positive integer. The complex equation

$$z^n = 1$$

can then be written as $e^{ni\theta} = \cos(n\theta) + \sin(n\theta) = 1$. Notice this has solutions of the form $\theta = \frac{2k\pi}{n}$ where $k \in \mathbb{Z}$. Thus, we see the equation $z^n = 1$ has n distinct solutions,

$$z_k = e^{\frac{2ki\pi}{n}} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right),$$

where $0 \le k < n$. These are called the n^{th} roots of unity. Prove that the set of n^{th} roots of unity under the operation of complex multiplication forms a group. You may assume that complex multiplication is associated. Sketch the n^{th} roots of unity in the complex plane for $n = 2, 3, 4$.

Proof: Let $G_n = \left\{ z_k = e^{\frac{2k\pi i}{n}} : 0 \le k < n \right\}$ be the set of n^{th} roots of unity. We need to prove that $(G_n, \cdot)$ is a group, where $\cdot$ denotes complex multiplication.

(a) **Closure:** For any $z_j, z_k \in G_n$, we need to show that $z_j \cdot z_k \in G_n$.

$$\begin{aligned} z_j \cdot z_k &= e^{\frac{2j\pi i}{n}} \cdot e^{\frac{2k\pi i}{n}} \\ &= e^{\frac{2(j+k)\pi i}{n}} \\ &= e^{\frac{2m\pi i}{n}}, \text{ where } m = (j+k) \mod n \end{aligned}$$

Since $0 \le m < n$, $z_j \cdot z_k \in G_n$.

(b) **Associativity:** This is given in the problem statement.

(c) **Identity Element:** The identity element is $e^0 = 1$, which is in G_n (it's z_0). For any $z_k \in G_n$:

$$z_k \cdot 1 = 1 \cdot z_k = z_k.$$

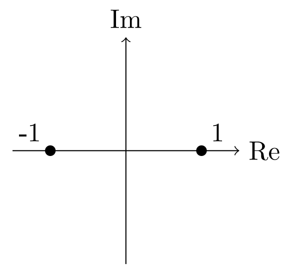
(d) **Inverse Element:** For any $z_k \in G_n$, its inverse is z_{n-k} (or z_0 if $k = 0$).

$$\begin{aligned} z_k \cdot z_{n-k} &= e^{\frac{2k\pi i}{n}} \cdot e^{\frac{2(n-k)\pi i}{n}} \\ &= e^{\frac{2n\pi i}{n}} \\ &= e^{2\pi i} = 1. \end{aligned}$$

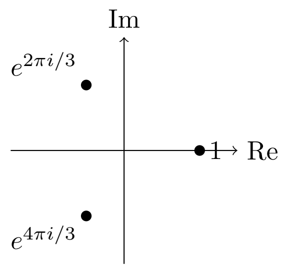
Therefore, $(G_n, \cdot)$ is a group.

Sketches of $n^{\mathbf{th}}$ Roots of Unity:

For $n = 2$ (Square roots of unity):



For $n = 3$ (Cube roots of unity):



For $n = 4$ (Fourth roots of unity):