Tutorial 10

Groups (with solution)

Q.1 Group or Not?

Is each of the following cases a group? If so, is it an Abelian group?

a) Even numbers under addition
b) Odd numbers under addition
c) Multiples of 7 under addition
d) 2×2 real matrices under addition
e) 2×2 real matrices under multiplication

Q.1

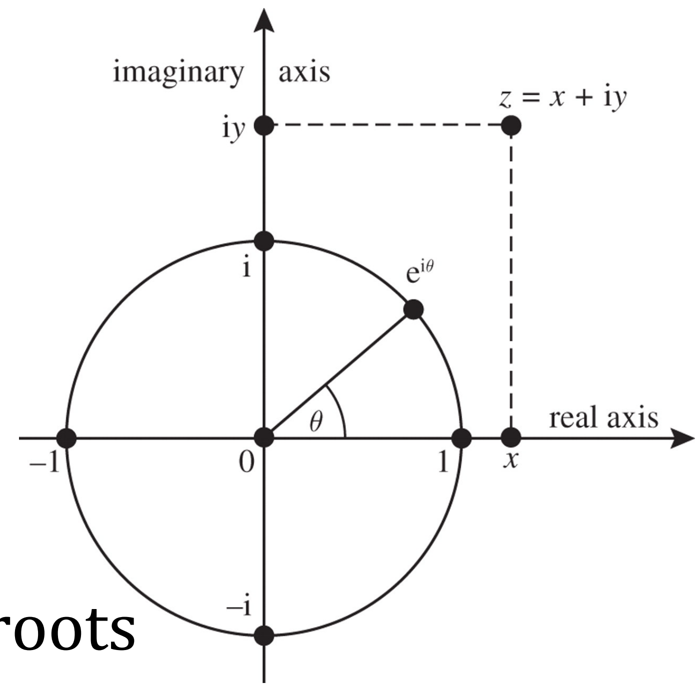
a) Yes. Abelian, addition is commutative.
b) No.
   - It violates the Closure property and there is no identity.
c) Yes. Abelian, addition is commutative.
d) Yes. Abelian, addition is commutative.
e) No. There are no inverses for matrices with zero determinant.

Q.2 Unit Circle on Complex Plane

- Consider the set of complex numbers on the unit circle:

$$H = \{z \in \mathbb{C}\colon\ |z| = 1\}.$$

- Denote multiplication by $\times$.
  - e.g. $(1 + 2i)(3 - i)$
    $= (3 + 2) + (6 - 1)i$
    $= 5 + 5i.$



a) Show that $\langle H, \times \rangle$ forms a group.

b) Find the cube roots of unity, or roots satisfying the equation: $z^3 = 1$, where $z \in \mathbb{C}$. Do the roots form a subgroup of H?

Q.2

a) It is a group.

- Closure
  - $e^{j\theta_1} \times e^{j\theta_2} = e^{j(\theta_1+\theta_2)}$.
- Identity
  - 1 is the identity, since $1 \times e^{j\theta} = e^{j\theta}$ for any $e^{j\theta}$.
- Inverse
  - The inverse of $e^{j\theta}$ is $e^{-j\theta}$, since $e^{-j\theta} \times e^{j\theta} = 1$.
- Associativity
  - $e^{j\theta_1} \times e^{j\theta_2} \times e^{j\theta_3} = e^{j\theta_1} \times (e^{j\theta_2} \times e^{j\theta_3})$

Q.2

b) $z^3 = 1 = e^{j2\pi k}$

- Then the cube roots of unity are given by

$$z = e^{j2\pi k/3}, k = 0,1,2$$

- $\{1, e^{j2\pi/3}, e^{j4\pi/3}\}$ forms a subgroup of H.

Q.2

- *Furthermore, the n-th roots of unity form a subgroup of H of order n*.

Closure

- The product of two nth roots of unity is also nth roots of unity. If $x^n = 1$ and $y^n = 1$, then $(xy)^n = 1$.

Identity

- 1 is the identity

Inverse

- The inverse of one nth roots of unity is also nth roots of unity. If $x^n = 1$, then If $(x^{-1})^n = 1$.

Associativity

- Straightforward.

Q.3 Binary Linear Code

- Recall that a binary linear code C is a subset of $\mathbb{B}^n$.
- It is defined by the encoding function $f: \mathbb{B}^k \to \mathbb{B}^n$, where $f(u) = uG$ and G is the generator matrix.
- It can be checked that $\mathbb{B}^n$ with binary addition is a group.
- Is C a subgroup of $\mathbb{B}^n$?

Q.3

- Yes, it is a subgroup.

a) Closure
  - Consider two codewords, c_u and c_v.
  - $c_u + c_v = uG + vG = (u+v)G$, which is a codeword.

b) Identity
  - 0 is a codeword, since $u = 0$ implies $f(u) = uG = 0$.
  - 0 is the identity, since $c + 0 = c$ for any codeword c.

c) Inverse
  - The inverse of c is c itself, since $c + c = 0$.

d) Associativity
  - $(c_u + c_v) + c_w = c_u + (c_v + c_w)$