Tutorial 10

Solution

Q.1 Group or Not?

Is each of the following cases a group?

a) Integers under addition
b) Even numbers under addition
c) Odd numbers under addition
d) Integers under multiplication
e) Multiples of 7 under addition
f) Complex numbers under addition
g) Complex numbers under multiplication
h) 2×2 real matrices under addition
i) 2×2 real matrices under multiplication

Pause and think:
https://www.youtube.com/watch?v=qvx9TnK85bw&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6&index=10

Q.1(Solution)

a) Yes.
b) Yes.
c) No.
   - It violates the Closure property and there is no identity.
d) No.
   - There are no inverses for elements other than 1 or -1.
e) Yes.
f) Yes.
g) No.
   - 0 has no inverse.
h) Yes.
i) No.
   - There are no inverses for matrices with zero determinant.

Q.2 Abelian or not?

- Let G be the set of 2×2 real matrices with non-zero determinant.

a) Is $\langle G, +\rangle$ a group? If so, is it an Abelian group?

b) Is $\langle G, \times\rangle$ a group? If so, is it an Abelian group?

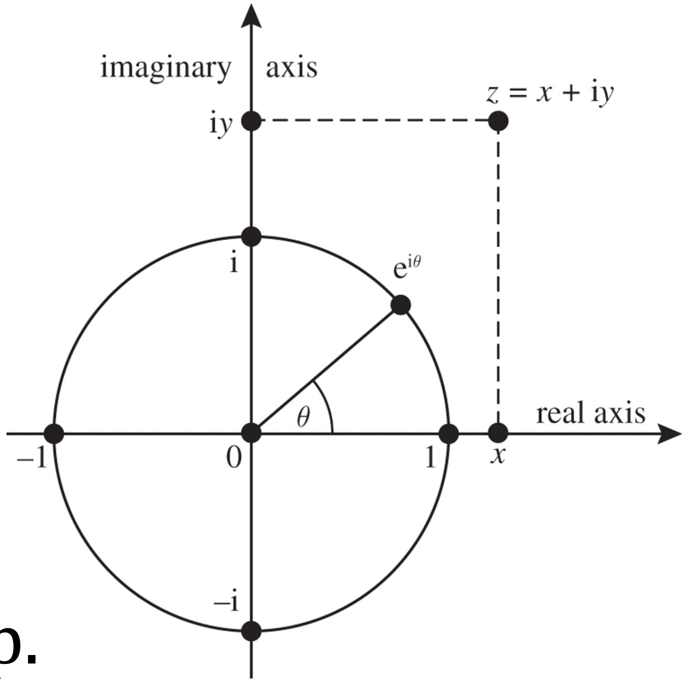
Q.2(Solution)

a) Not a group.
   - It does not satisfy the closure property. For example, $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}+\begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$ has zero determinant, thus not belonging to G.

b) Yes. Non-Abelian.
   - For matrices, $AB \neq BA$ in general.

Q.3 Unit Circle on Complex Plane

- Consider the set of complex numbers on the unit circle:
$$H = \{z \in \mathbb{C}:\ |z| = 1\}.$$
- 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) Does it have a subgroup of order 3? Why?

Q.3 (Solution a)

Each element in H can be represented as $e^{i\theta}$.

We need to check that the four properties hold:

i. Closure:
   - $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)} \in H$

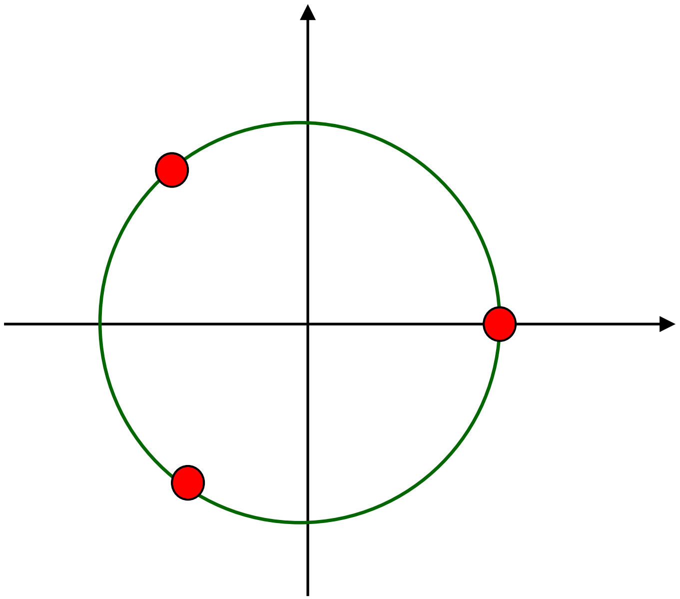
ii. Identity: 1 is the identity element
   - $e^{i\alpha}1 = 1e^{i\alpha} = e^{i\alpha}$

iii. Inverse: $e^{-i\alpha}$ is the inverse of $e^{i\alpha}$.
   - $e^{i\alpha}e^{-i\alpha} = e^{-i\alpha}e^{i\alpha} = 1$

iv. Associativity:
   - $(e^{i\alpha}e^{i\beta})e^{i\gamma} = e^{i\alpha}\left(e^{i\beta}e^{i\gamma}\right) = e^{i(\alpha+\beta+\gamma)}$

Q.3 (Solution b)

- Does it have a subgroup of order 3? Why?



- Yes.
- $\{1, e^{j2\pi/3}, e^{j4\pi/3}\}$

> Think: how about a subgroup of order 8?

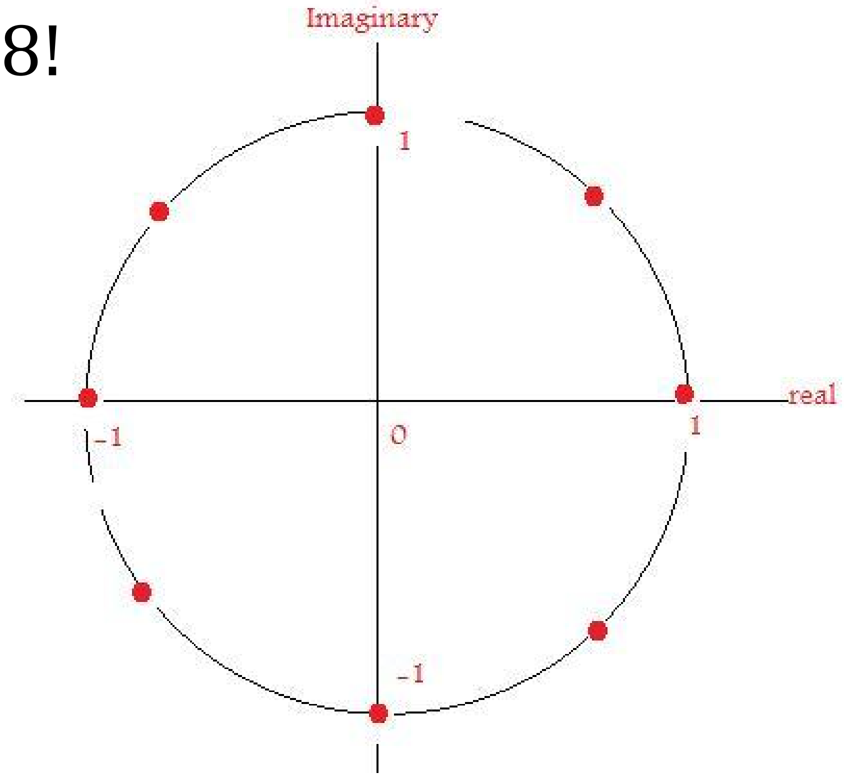
Q.3 (Solution b)

- It has a subgroup of order 8!

- The elements are :

$$\{e^{jk2\pi/8} = e^{jk\pi/4}\},$$

where $k = 0,1,2, \ldots, 7$.



Q.4 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.
- Is C a subgroup of $\mathbb{B}^n$?

Q.4 (Solution)

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