Group Theory - Homework 1

Problem 1. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}\setminus\{0\}\}$. Show that G is a group under multiplication.

- Closure: If $a, b \in G \Rightarrow ab \in G$.

  Take $a, b \in G$, so $a^m = b^n = 1$ for some $m, n \in \mathbb{Z}$. Then

  $$(ab)^{mn} = (a^m)^n (b^n)^m = 1. \quad , \ mn \in \mathbb{Z}$$

  Remember to check closure whenever it isn't trivial!

- Identity: $1 \in G$.
- Associativity: Complex multiplication is associative.

Inverses: If $a \in G \Rightarrow a^{-1} \in G$

Take $a \in G$ with $a^n = 1$, then $\underbrace{(a^{-1})^{-n} = a^n = 1}_{a^{-1} \in G.}$, and $-n \in \mathbb{Z}$

Note: Notice G isn't finite! In particular, it contains all roots of unity.

$$\bigcup_{n \in \mathbb{Z}} \{e^{\frac{i2\pi k}{n}} \mid k \in \{0, \dots, n-1\}\} \subset G.$$

Problem 2. Find the order of each element in $\mathbb{Z}/12\mathbb{Z}$.

Let's use abusive notation: $\mathbb{Z}/12\mathbb{Z} = \{0, 1, \dots, 11\}$

Remember the group operation in $\mathbb{Z}/12\mathbb{Z}$ is the sum (mod (12)). Can you check that $\mathbb{Z}/12\mathbb{Z}$ is not a group with respect to multiplication? What would be the multiplicative inverse inverse of 2?

The order of $k \in \mathbb{Z}/12\mathbb{Z}$ is the smallest positive integer $|k|$ such that

$$\underbrace{k + \dots + k}_{|k| \text{ times}} = 0 \pmod{12}, \text{ ie. } |k| \cdot k = 0 \pmod{12}$$

Claim $|k| = \text{lcm}(k, 12)/k \quad (k > 0)$

proof. Note $\dfrac{\text{lcm}(k,12)}{k} \cdot k = \text{lcm}(k, 12) = 0 \pmod{12}$

By contradiction. Suppose $\underbrace{a \cdot k = 0 \pmod{12}}_{\text{So } a \cdot k \text{ is a multiple of } 12}$ and $a < \dfrac{\text{lcm}(12, k)}{k}$

Then $\underbrace{a \cdot k}_{\text{Clearly a multiple of } k\text{, also}} < \text{lcm}(12, k)$, a contradiction ⚡

1

Problem 3. Let G be a group and $u,v \in G$. Show the elements uv and vu have the same order, i.e. $|uv| = |vu|$

This is Ex.22 on p.22 of Dummit & Foote's "Abstract Algebra".

Obs. Note $(uv)^k = \underbrace{uv \cdot uv \cdots uv}_{k \text{ times}} \neq \underbrace{vu \cdot vu \cdots vu}_{k \text{ times}} = (vu)^k$

Remember the group operation is not always commutative!

It is not the case $(uv)^k = u^k v^k = (vk)^k$. To get some perspective:

Claim. $(uv)^k = u^k v^k \ \forall k \in \mathbb{Z}$ iff $uv = vu$.

Claim. G is Abelian iff $(uv)^2 = u^2 v^2 \ \forall u,v \in G$.

Hint for Problem 3 (from D & F): Show that given $x, g \in G$ $|x| = |g^{-1}xg|$, then show $|uv| = |vu|$ for all $u,v \in G$.

Case 1. $|x| = k$ (so finite order)

$$\underbrace{(g^{-1}xg)(g^{-1}xg) \cdots (g^{-1}xg)(g^{-1}xg)}_{k \text{ times}} = g^{-1}x\underbrace{(gg^{-1})}_{e}x\underbrace{(gg^{-1})}_{e}\cdots\underbrace{(gg^{-1})}_{e}x\underbrace{(gg^{-1})}_{e}xg$$

$$= g^{-1}x^k g = e \text{ if } x^k = e.$$

More generally $(g^{-1}xg)^k = g^{-1}x^k g \quad \forall k \in \mathbb{Z}$.

This also follows from $\varphi : G \to G$, $x \xmapsto{\varphi} g^{-1}xg$ being a group homomorphism.

Case 2. $|x|$ is infinite

By contradiction, if $(g^{-1}xg)^k = e$ for some positive k, then

$$e = (g^{-1}xg)^k = g^{-1}x^k g \Rightarrow g(g^{-1}x^k g)g^{-1} = geg^{-1} \Rightarrow x^k = e$$

Now we can finish the problem:

$$|uv| = |u^{-1}(uv)u| = |vu|.$$

Problem 4. Prove that if $x^2 = e$ for all $x \in G$, then G is Abelian.

Take $a,b \in G$, then

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

by assumption, as $(ab)^2 = e$

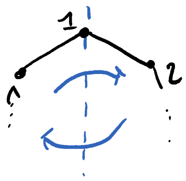
by assumption again, because $a^2 = b^2 = e$

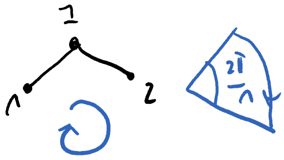
Problem 6. Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = e \rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = rs$.

Recall that D_{2n}: "group of symmetries of the regular n-gon"

s = "reflexion with respect to (w.r.t.) the axis of symmetry going through vertex 1"

r = "clockwise rotation by $2\pi/n$ radians"

$s =$ 

 $= r$

The presentation you saw in class is $D_{2n}\ \langle r, s \mid s^2 = e,\ r^n = e,\ rs = sr^{-1} \rangle$.

You can check these relations are true, but this isn't part of the exercise. (You did it in class, right?)

① $\langle r, s \mid s^2 = e, r^n = e, rs = sr^{-1} \rangle \xRightarrow[a=s,\ b=rs]{} \langle a, b \mid a^2 = b^2 = (ab)^n = e \rangle$

i.e. we want to check the l.h.s relations imply the r.h.s ones.

- $a^2 = s^2 = e$
- $b^2 = (rs)(rs) = (sr^{-1})(rs) = s^2 = e$
- $(ab)^n = (srs)^n = sr^n s = s^2 = e$

We must also prove the converse!

② $\langle a, b \mid a^2 = b^2 = (ab)^n = e \rangle \xRightarrow[a=s,\ b=rs]{} \langle r, s \mid s^2 = e^2, r^n = e, rs = sr^{-1} \rangle$

- $s^2 = a^2 = e$.
- $b^2 = e \Rightarrow (rs)(rs) = e \Rightarrow (rs)^{-1} = rs \Rightarrow s^{-1}r^{-1} = rs \underset{s^2 = e}{\Rightarrow} sr^{-1} = rs$
- $(ab)^n = e \Rightarrow \underbrace{(srs)^n}_{= sr^n s} = e \Rightarrow r^n = e.$

Problem 5. The gist of P5 is that we can weaken the group axioms. As long as we have associativity, we can ask for left-inverses as opposed to two-sided inverses, and for a left identity as opposed to the two-sided identity of the original definition of group.

See Appendix 1 of section I.1 in Zee's "Group Theory in a Nutshell for Physicists" for all the details. It's a nice book!