1. Suppose x is an element of a finite group G. Show that

   (a) x has finite order (denote it k),

   (b) $x^n = e$ if and only if k divides n,

   (c) $x^{|G|} = e$.

(a) By the pigeonhole principle x^n, $n=0,1,\ldots$ are not all distinct, so $\exists\, m>n$ $\quad x^m = x^n$

Then $m-n>0$ and $x^{m-n}=e$, so x has finite order.

(b) Let $S=\{n>0 : x^n=e\}$. Then $k=|x|=\min S$.

If $k \mid n$ $\exists\, j$ $\quad n=kj$ so $x^n=(x^k)^j=e^j=e$.

Conversely suppose $x^n=e$. By the division algorithm

$\exists!\, q,r \quad n=kq+r \quad 0\le r<k$

Then $x^n=x^{kq+r}=(x^k)^q x^r=e^q x^r=x^r$, so $x^r=e$

If $r>0$, $r\in S$ ☹ $\therefore r=0$ so $k \mid n$ ☺

(c) By Langrange's theorem $k=|x|=|\langle x\rangle|$ divides $|G|$.

Thus, by (b) $x^{|G|}=e$.

2. Sketch the subgroup lattice for $\mathbf{Z}_{12}$. For each subgroup, list all the elements and indicate all possible generators of the subgroup.

Divisors of 12: 1, 2, 3, 4, 6, 12

Subgroups: $\mathbb{Z}_{12} = \{0, \underline{1}, 2, 3, 4, \underline{5}, 6, \underline{7}, 8, 9, 10, \underline{11}\}$

$2\mathbb{Z}_{12} = \{0, \underline{2}, 4, 6, 8, \underline{10}\}$

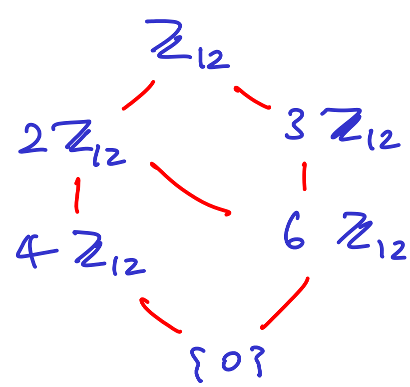
Possible generators underlined.

$3\mathbb{Z}_{12} = \{0, \underline{3}, 6, \underline{9}\}$

$4\mathbb{Z}_{12} = \{0, \underline{4}, \underline{8}\}$

$6\mathbb{Z}_{12} = \{0, \underline{6}\}$

$12\mathbb{Z}_{12} = \{0\}$



3. Define a function from the integers to the multiplicative group of nonzero complex numbers $\varphi\colon \mathbf{Z} \to \mathbf{C}^*$ by $\varphi(k) = e^{2k\pi i/5}$.

   (a) Prove that φ is a group homomorphism.

   (b) What subgroup of $\mathbf{Z}$ is the kernel of φ?

   (c) Sketch the image of φ.

   (d) What does the first isomorphism theorem tell you about fifth roots of unity?

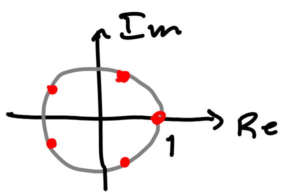
(a) $\varphi(j+k) = e^{2(j+k)\pi i/5} = e^{2j\pi i/5 + 2k\pi i/5}$

$= e^{2j\pi i/5} \cdot e^{2k\pi i/5} = \varphi(j)\cdot\varphi(k)$ ☺

(b) $k \in \ker\varphi \iff \varphi(k) = 1 \iff e^{2k\pi i/5} = 1$

$\iff \exists n \in \mathbb{Z}\ \ 2k\pi/5 = 2n\pi \iff \exists n \in \mathbb{Z}\ \ k = 5n$

$\iff k \in 5\mathbb{Z}$ $\therefore$ $\ker\varphi = 5\mathbb{Z} = \{0, \pm 5, \pm 10, \dots\}$

(c) 

$\text{image}(\varphi) = H = \{ z \in \mathbb{C} : z^5 = 1 \}$

$= \{ e^{2k\pi i} : k = 0,1,2,3,4 \}$

(d) $\dfrac{\mathbb{Z}}{\ker\varphi} \cong \text{image}(\varphi)$ $\therefore$ $\dfrac{\mathbb{Z}}{5\mathbb{Z}} \cong H$ $\therefore$ $H \cong \mathbb{Z}_5$

4. Suppose an element x of the dihedral group D_n is a composition (in an arbitrary order) of j rotations and k reflections (flips). [Example: $x = r_3 f_2 r_1 r_2 f_1$ with $j = 3$ and $k = 2$] Under what conditions on j and k is x a rotation? A reflection? Explain.

If k is even x is orientation preserving (a rotation).

If k is odd x is orientation reversing (a flip).

5. Let $\alpha = (1, 2, 5, 4)(2, 6, 3)(5, 6, 3, 2, 1)$ be a permutation (in cycle notation). Express α as a product of disjoint cycles. What is the order of α? Simplify α^{61}.

$\alpha = (1,4)(3,6,5)$ Parity odd + even = odd

By Ruffini's theorem $|\alpha| = \text{lcm}(2,3) = 6$

$61 = 1 + 2\cdot 30 = 1 + 3\cdot 20$

Since disjoint cycles commute, $\alpha^{61} = (1,4)^{61}(3,6,5)^{61}$

$= (1,4)^{1+2\cdot 30}(3,6,5)^{1+3\cdot 20}$

$= (1,4)(\underbrace{(1,4)^2}_{\varepsilon})^{30}(3,6,5)(\underbrace{(3,6,5)^3}_{\varepsilon})^{20} = (1,4)(3,6,5) = \alpha$

6. Prove that the set A_n of all even permutations in the symmetric group S_n is a normal subgroup. What can you say about the quotient group S_n/A_n? Give a concrete example of a subgroup of S_3 that is not normal. Explain.

$A_n = \ker \varphi$, where $\varphi : S_n \to \mathbb{Z}_2$ is the homomorphism

given by $\varphi(\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ is even} \\ 1 & \text{if } \alpha \text{ is odd} \end{cases}$

$\therefore A_n \triangleleft S_n$ ☺

Alt: Since $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$,

the only option for a nontrivial coset (right or left) of A_n is $S_n \setminus A_n$ ☺

Since there are 2 cosets of A_n, $\frac{S_n}{A_n} \cong \mathbb{Z}_2$

Also: Since φ is onto, 1^{st} iso. thm says ↑

Let $H = \{\varepsilon, (1,2)\} < S_3$

Then $(1,3)H = \{(1,3), (1,2,3)\}$

$H(1,3) = \{(1,3), (1,3,2)\}$

are not equal so $H \ntriangleleft S_3$

7. How many group homomorphisms from $\mathbf{Z}_{12}$ to $\mathbf{Z}_3 \oplus \mathbf{Z}_4$ are there? How many of them are isomorphisms? If φ is such an isomorphism with $\varphi(2) = [1, 3]$, what is $\varphi(1)$?

A hom $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4$ is uniquely determined by $\varphi(1)$. In $\mathbb{Z}_{12}$ 1 has order 12, but by by Lagrange's theorem any element of $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ has order that divides $|\mathbb{Z}_3 \oplus \mathbb{Z}_4| = 12$, so the choice of $\varphi(1)$ is free.

$\therefore$ there are 12 homomorphisms $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4$

For φ to be an isomorphism, $\varphi(1)$ must be a generator of $\mathbb{Z}_3 \oplus \mathbb{Z}_4$, so the components of $\varphi(1)$ must be generators of $\mathbb{Z}_3$ and $\mathbb{Z}_4$

Choices: $\mathbb{Z}_3$: 1, 2 $\quad$ $\mathbb{Z}_4$: 1, 3 $\quad$ Total: $2 \cdot 2 = 4$

If $\varphi(2) = [1, 3]$, then since $[1, 3]$ generates $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ and 2 does not generate $\mathbb{Z}_{12}$ φ cannot be an isomorphism.

8. Suppose R is a commutative ring with unity. Show that the set of all units (elements that have a mutliplicative identity) in R is a multiplicative group under the same multiplication as R.

Let $U(R) = \{ x \in R : x \text{ is a unit} \}$

Since $1 \cdot 1 = 1$, $1 \in U(R)$

Suppose $x, y \in U(R)$, then $xy^{-1} y x^{-1} = 1$

so $xy^{-1} \in U(R)$:)