1. Let $\alpha = (3,5,1)(4,2,1,3)$ be a permutation (in cycle notation). Express α as a product of disjoint cycles. What are the order and the parity of α? Explain. Simplify α^{11}.

$\underline{\alpha = (1\ 5)(2\ 3\ 4)}$

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

Parity of α : odd + even $= \underline{\text{odd}}$

$11 = 1 + 2\cdot 5 = 2 + 3\cdot 3$

$\alpha^{11} = (1\ 5)^{11}(2\ 3\ 4)^{11}$ (because disjoint cycles commute)

$= (1\ 5)^{1+2\cdot 5}(2\ 3\ 4)^{2+3\cdot 3}$

$= (1\ 5)^1(\underbrace{(1\ 5)^2}_{\varepsilon})^5(2\ 3\ 4)^2(\underbrace{(2\ 3\ 4)^3}_{\varepsilon})^3$

$= (1\ 5)(2\ 3\ 4)^2 = \underline{(1\ 5)(2\ 4\ 3)}$

2. Prove that the set of all rotations in the dihedral group D_n is a normal subgroup. What can you say about the quotient group?

(i) $\det : D_n \to \{1,-1\}$ is a group hom since det is multiplicative.

$\{\text{all rotations}\} = \det^{*}(\{1\}) = \ker(\det)$

$(\{1\} < \{1,-1\})$

Also, note $\{1\} \triangleleft \{1,-1\}$ (because $\{1,-1\}$ is Abelian

(or because $\{1\}$ is always normal)

$\therefore \{\text{all rotations}\} \triangleleft D_n$

$1^{\underline{st}}$ isomorphism theorem: $\dfrac{D_n}{\ker(\det)} \cong \text{image}(\det) = \{1,-1\} \cong \mathbb{Z}_2$

3. Suppose $\varphi\colon \mathbf{Z}_{15} \to \mathbf{Z}_3 \oplus \mathbf{Z}_5$ is a group isomorphism. If $\varphi(2) = [2, 3]$, what is $\varphi(1)$?

Since $16 \equiv 1 \bmod 15$ $\quad \varphi(1) = \varphi(16)$

$= \varphi(8 \cdot 2) = 8\,\varphi(2) = 8\,[2, 3] = [16, 24] = \underline{[1, 4]}$

Check: $2[1, 4] = [2, 8] = [2, 3]$:)

Alternate method: $\varphi(2) = \varphi(2 \cdot 1) = 2\,\varphi(1)$

$2\varphi(1) = [2, 3] = [2, 8] = 2\,\underline{[1, 4]}$

4. Suppose S is a ring with p elements, where p is prime.

(a) Show that as an additive group (ignoring multiplication for the moment), S is cyclic.
Hint: Consider the subgroup generated by a nonzero element of S.

(b) Show that S is a commutative ring.
Hint: Use part (a).

a) Since $p > 1$ S is non-trivial, so let $a \in S \setminus \{0\}$

Then $|\langle a \rangle|$ divides p (by Lagrange's theorem)

and > 1, so $|\langle a \rangle| = p$

$\therefore$ $S = \langle a \rangle = \{na : n \in \mathbb{Z}\}$

Alt.: By the classification theorem for finite Abelian groups

$S \cong \mathbb{Z}_p$

b) Let $ia, ja \in S$.

$ia \cdot ja = ij \cdot a^2 = ja \cdot ia$

For example $(3a)(-2a) =$

$= (a+a+a)(-a-a) = -a^2 - a^2 - a^2 - a^2 - a^2 - a^2$

$= -6a^2$

Similarly: $(-2a)(3a) = \ldots = -6a^2$ ☺

$=$ ☺