Alternating group A_n, $n \geq 2$.

(see 5.1 of AATA).

S_n is the symmetric group

= group all permutations of n objects, labelled $1, \ldots, n$

1-1 and onto (bijective) function $\{1, \ldots, n\} \to \{1, \ldots, n\}$

where the group operation is composition of these functions.

eg. $\sigma\mu$ will mean "σ after μ"

The preferred notation for a permutation σ is to express σ as a product/composition of its disjoint cycles. using cycle notation.

"Transposition" is a technical term for 2-cycles eg. $(1\ 2)$, $(2\ 3)$

Any cycle can be written as a product of transpositions. using

$$(a_1\ a_2\ \ldots\ a_n) = \overbrace{(a_1\ a_n) \cdots (a_1\ a_4)(a_1\ a_3)(a_1\ a_2)}^{n-1 \text{ transposition}}$$

$$a_j \longmapsto a_{j+1}$$

Using this any permutation can be written as a product of transpositions.

but these expressions are <u>not unique</u>

eg.

$$(16)(253) = (16)(23)(25)$$

$$= (16)(45)(23)(45)(25)$$

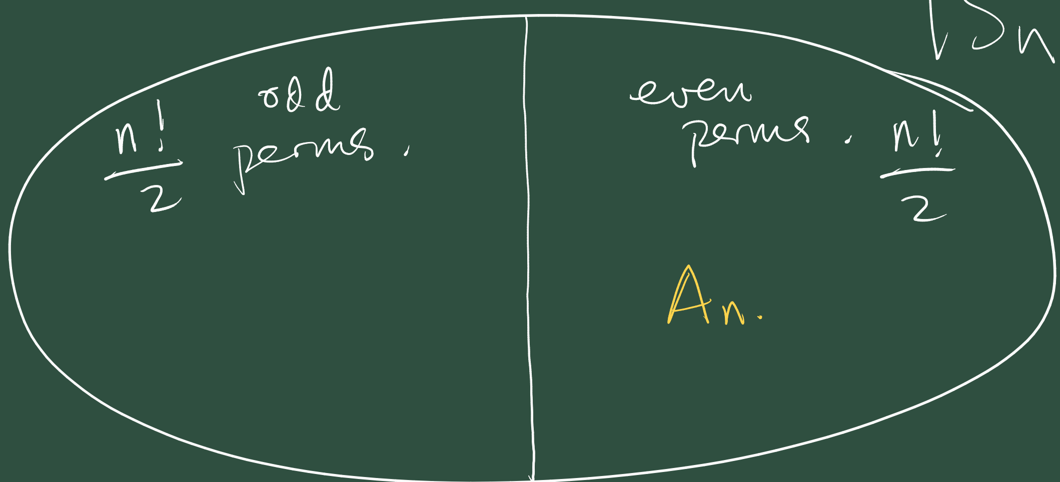
$$= \ldots$$

$$= \ldots$$

will always require an odd number

from Lemma 5.14, Theorem 5.15

$|S_n| = n!$



Theorem 5.16 $A_n :=$ even perms of S_n.

A_n is a subgroup of S_n.

Recall, the symmetric groups S_n, for $n \geq 3$ are non-abelian.

Proof When $n \geq 3$, the transpositions $(1\ 2)$, $(2\ 3)$ can be regarded as elements of S_n.

These do not commute

for
$$(1\ 2)(2\ 3) = (1\ 2\ 3)$$

$$(2\ 3)(1\ 2) = (3\ 2\ 1)$$

and $(1\ 2\ 3) \neq (1\ 3\ 2)$

Therefore S_n is non-abelian.

Trivially S_1, S_2 are abelian.

$$S_1 = \{e\}$$

$$S_2 = \{e, (1\ 2)\}$$

$$|S_4| = 4! = 24.$$

For instance.

A_4 , $|A_4| = 12$.

$$A_4 = \{ e, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\;2)(3\;4), (1\;4)(3\;2), (1\;3)(2\;4) \}.$$

$$(1\,2\,3)(1\,3\,2) = (1)(2)(3) = e.$$

which we expected since $(1\,2\,3)^{-1} = (1\,3\,2)$

Mock Exam.

Q4.

(a). Solving $45x \equiv 15 \pmod{125}$. (*)

By the theorem on linear congruences. solutions to (*) exist if and only if.

$d \mid 15$ where $d = \gcd(\underset{5 \cdot 3^2}{45}, \underset{5^3}{125})$

$= 5$.

and indeed $5 \mid 15$

So the theorem says there 5 solutions to (*) which will be generated by the unique solution t to the reduced congruence

$$\boxed{9x \equiv 3 \bmod 25} \quad (**)$$

and given:

$$(***) \quad \boxed{x \equiv t + i \cdot 25, \quad i = 0, 1, 2, 3, 4}$$

Solving (**).

The solution here is given by

$$t \equiv 9^{-1} \cdot 3 \pmod{25}.$$

$9^{-1} \bmod 25$ can be determined from the extended Euclidean algorithm.

$$25 = 2\cdot 9 + 7.$$
$$9 = 1\cdot 7 + 2.$$
$$7 = 3\cdot 2 + \underline{\underline{1}}$$

Then obtain Bezout's identity for 9, 25

$$\boxed{1} = 7 - 3\cdot 2.$$
$$= 7 - 3\cdot(9-7).$$
$$= 4\cdot 7 - 3\cdot 9.$$
$$= 4\cdot(25 - 2\cdot 9) - 3\cdot 9.$$
$$= 4\cdot 25 \; \underbrace{-11}_{\equiv\, 9^{-1} \bmod 25}\cdot 9.$$

$\Rightarrow$

So $9^{-1} \equiv -11 \equiv 14. \pmod{25}.$

So $\boxed{t = 14\cdot 3} \pmod{25}$
$$\equiv 42$$
$$\equiv \boxed{17} \pmod{25}.$$

So now generate all the solutions to (*) using (***)

$x \equiv 17, 42, 67, 92, 117 \pmod{125}$

(b) Bookwork.

(c) Consider $x^2 \equiv 547 \pmod{631}$

(547, 631 both prime).

Solutions exist if and only if 547 is a quadratic residue modulo 631.

i.e. $(547 | 631) = +1$.

The question suggests there are no solutions, i.e. that $\boxed{(547|631) = -1}$. ✓

$$\boxed{(547|631)} = -(631|547)$$

, by quadratic reciprocity, since $631 \equiv 3 \pmod 4$ and $547 \equiv 3 \pmod 4$.

$= -(84 | 547)$, since $631 \equiv 84 \pmod{547}$ and if $a \equiv b \pmod p$ then $(a|p) = (b|p)$.

$= -(2^2 \cdot 3 \cdot 7 / 547)$

$= -(2|547)^2 (3|547)(7|547)$

, by multiplicative property of $(\cdot \mid p)$

$= -(3 \mid 547)(7 \mid 547)$, since $(2 \mid 547) = \pm 1$ and so $(2 \mid 547)^2 = +1$.

$= -(-(547 \mid 3))(-(547 \mid 7))$, by reciprocity and $547 \equiv 3 \equiv 7 \bmod (4)$

$= -(1 \mid 3)(1 \mid 7)$, by reduction since $547 \equiv 1 \pmod 3$ and $547 \equiv 1 \pmod 7$.

$\boxed{= -1}$

since $(1 \mid 3) = (1 \mid 7) = +1$ since $1^2 \equiv 1 \bmod p$

So 547 is not a quadratic residue modulo 631 and so there are no solutions to $x^2 \equiv 547 \pmod{631}$.

FACTORIZE → FLIP → REDUCE

d). Solutions exist to

$x^2 \equiv a \bmod 631$

(for $a \not\equiv 0 \mod 631$)

Iff a is a quadratic residue modulo 631.

A result from the unit proved there are $\frac{p-1}{2}$ quadratic residues modulo p.

So there are 315 quadratic residues modulo 631

so with the addition of the $a \equiv 0$ case there 316 a for which there are solutions.

Section B.

Q5

a).

1. $(G, *)$ must have an <u>identity element</u>, which is an element $e \in G$ such that for all $g \in G$ $g*e = e*g = g$

and in $(\mathbb{R}\setminus\{0\}, \times)$, $e = 1$.

2. Associativity.

For all $g_1, g_2, g_3 \in G$.

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$$

so in other words, brackets are not needed in triple products and products of more factors.

This is a familiar property of $(\mathbb{R}\setminus\{0\}, \times)$, eg.

$$2 \times (3 \times 4) = 24$$
$$= (2 \times 3) \times 4$$

3. Existence of inverses.

G contains inverses for all its elements.

ie. for all $g \in G$ there exists $g^{-1} \in G$ such that

$$g * g^{-1} = g^{-1} * g = e.$$

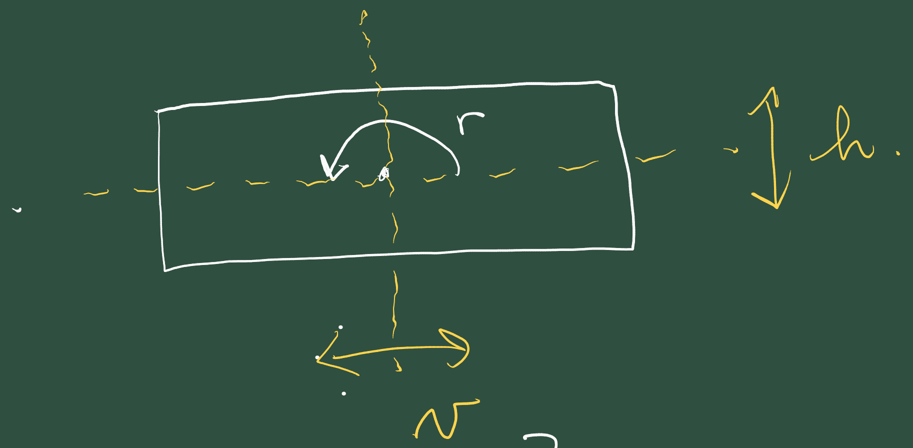
In $(\mathbb{R}\setminus\{0\}, \times)$ the inverses are the reciprocals.

i.e. $\boxed{x^{-1} = \frac{1}{x}}$

as in

$$2^{-1} = \frac{1}{2}, \quad 2 \cdot \frac{1}{2} = 1.$$

(b)



$V = \{ e, r, h, v \}$, $\mathbb{Z}_4 = \{ 0, 1, 2, 3 \}$

Cayley tables are (i)

V	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(ii) From the presence, or absence, of identity on the diagonal we see that $x^2 = e$ for all x in V.

but this is not so for $\mathbb{Z}_4$.
This aspect of their structure is different.

<u>OR</u> $\mathbb{Z}_4$ is cyclic, $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$

But V is not cyclic.

(c). A <u>subset</u> H of a group G is a subgroup of G if H is itself a group under the operation from G.

(d) We'll use the result that a subset H is a subgroup <u>if and only if</u>

1. $e \in H$
2. for all $h_1, h_2 \in H$ $h_1 h_2 = H$.
3. for all $h \in H$ $h^{-1} \in H$.

Let H, K be subgroups of G.

$\Rightarrow e \in H$ and $e \in K$ (from 1)

$\Rightarrow e \in H \cap K$.

Let $x, y \in H \cap K$.

$\Rightarrow x, y \in H$ and $x, y \in K$.

$\Rightarrow xy \in H$ and $xy \in K$ (from 2)

$\Rightarrow xy \in H \cap K$.

Let $x \in H \cap K$

$\Rightarrow x \in H$ and $x \in K$.

$\Rightarrow x^{-1} \in H$ and $x^{-1} \in K$ (from 3)

$\Rightarrow x^{-1} \in H \cap K$

This proves 1–3 for $H \cap K$, so by the result $H \cap K$ is a subgroup of G.

(e). For a group G.

$$Z(G) = \{x \in G : \forall g \in G \ \ gx = xg\}$$

"the centre of G"

Claim. $Z(G)$ is a subgroup of G.

<u>Proof</u>: Use the result from (d)

Firstly, $e \in Z(G)$ ✓ since for all $g \in G$.
the identity has the property that

$$\boxed{ge = g = eg}$$

Secondly, let $x, y \in Z(G)$.
Consider. $g \in G$.

$$xyg = xgy \text{, since } y \in Z(G) \text{ and } yg = gy$$

$$= gxy \text{, since } x \in Z(G) \text{ and } xg = gx.$$

So this shows that

$$(xy)g = g(xy)$$

and so $xy \in Z(G)$.

Thirdly, let $\boxed{x \in Z(G)}$.
let $\boxed{g \in G}$.

we know. $x g^{-1} = g^{-1} x$.

since $x \in Z(G)$.

$$\Rightarrow (x g^{-1})^{-1} = (g^{-1} x)^{-1}$$

$$\Rightarrow (g^{-1})^{-1} x^{-1} = x^{-1} (g^{-1})^{-1}$$

$$\Rightarrow \boxed{g x^{-1} = x^{-1} g.}$$

$$\Rightarrow x^{-1} \in Z(G).$$

This proves 1-3 for $Z(G)$

so $Z(G)$ is a subgroup of G.