Review

Reminder: CAPE!

1. Exactly 1.

Between any two groups, always have the "trivial map" which sends everything in domain to identity elt of codomain.

Say $\varphi: D_5 \to \mathbb{Z}_3$ is a homomorphism. Let $H = \operatorname{im}\varphi$. H is a subgroup of $\mathbb{Z}_3$, and $|\mathbb{Z}_3| = 3$, so by Lagrange, either $|H|=1$ or $|H|=3$.

image of any homomorphism is always a subgroup.

If $|H|=1$, then $H=\{0\}$ and φ is trivial map.

If $|H|=3$... By first isomorphism theorem, $D_5/\ker\varphi \approx H$, so

$$\left|D_5/\ker\varphi\right| = |H|$$

$$\frac{10}{|\ker\varphi|} = 3$$

3 is not a divisor of 10, so this can't happen! So $|H|=3$ is impossible.

2. $\mathbb{R}^* = \mathbb{R}^+ \times \{1,-1\}$

internal product

- $\mathbb{R}^+$ is a subgroup of $\mathbb{R}^*$, and is normal since $\mathbb{R}^*$ is abelian.
- $\{1,-1\}$ is also a normal subgroup.
- $\mathbb{R}^+ \cap \{1,-1\} = \{1\}$ is trivial
- Anything in $\mathbb{R}^*$ can be written as $1\cdot a$ for $a \in \mathbb{R}^+$ or $-1\cdot a$ for $a \in \mathbb{R}^+$, so $\mathbb{R}^* = \mathbb{R}^+\{1,-1\}$.

So all conditions to be an internal product are satisfied.

So $\underbrace{\mathbb{R}^* \approx \mathbb{R}^+ \oplus \{1,-1\}}$

elements here are pairs like $(17,1)$ or $(3,-1)$, or $(1,-1)$...

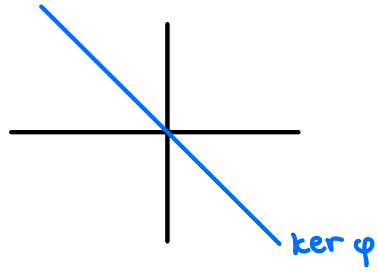
3. $\varphi: \mathbb{R}\oplus\mathbb{R} \to \mathbb{R}^*$
$\varphi(x,y) = e^{x+y}$

$\varphi((x,y)+(x',y')) = \varphi(x+x', y+y') = e^{(x+x')+(y+y')}$
$\varphi(x,y)\varphi(x',y') = e^{x+y}e^{x'+y'} = e^{x+y+x'+y'}$

these are the same!

$\ker\varphi = \{(x,y) \mid \varphi(x,y) = 1\}$

$= \{(x,y) \mid e^{x+y} = 1\}$
$= \{(x,y) \mid x+y=0\}$
$= \{(x,-x) \mid x \in \mathbb{R}\}$



4. $\mathbb{R}$ is abelian group under $+$.
$\mathbb{Z}$ is normal subgroup.

$\mathbb{R}/\mathbb{Z}$ is a group, identity element is $0+\mathbb{Z}$.

Any element of $\mathbb{R}/\mathbb{Z}$ is of the form $a+\mathbb{Z}$ for some $a \in \mathbb{R}$.

and $n(a+\mathbb{Z}) = na + \mathbb{Z} = \mathbb{Z}$ iff $na \in \mathbb{Z}$.

consider $\frac{1}{n}+\mathbb{Z}$. Then $n(\frac{1}{n}+\mathbb{Z}) = 1+\mathbb{Z} = \mathbb{Z}$, so order of $\frac{1}{n}+\mathbb{Z}$ is at most n. But for any $k<n$,

$$k\left(\frac{1}{n}+\mathbb{Z}\right) = \frac{k}{n}+\mathbb{Z} \neq \mathbb{Z}$$

so $\frac{1}{n}+\mathbb{Z}$ has order n.

[$\mathbb{R}$ equiv. reln $\sim$ where $x \sim y$ means $x-y \in \mathbb{Z}$. The equivalence classes for $\sim$ are exactly the cosets of $\mathbb{Z}$ inside $\mathbb{R}$.]

5. $G = \mathbb{Z}_6 \oplus \mathbb{Z}_3$ $\quad H = \langle (2,0) \rangle$.

$|H| = |\langle(2,0)\rangle| = |(2,0)| = \text{lcm}(|2|,|0|) = \text{lcm}(3,1) = 3$

$H = \{(0,0), (2,0), (4,0)\}$

G/H has order 6 because $|G/H| = \frac{|G|}{|H|} = \frac{|\mathbb{Z}_6 \oplus \mathbb{Z}_3|}{3} = \frac{6 \cdot 3}{3} = 6$.

By Lagrange, any element has order 1, 2, 3, or 6 — and G/H is cyclic precisely if there is an element of order 6.

$(1,1)+H \neq H$ since $(1,1) \notin H$.

$2((1,1)+H) = (2,2)+H \neq H$ since $(2,2) \notin H$

$3((1,1)+H) = (3,3)+H \neq H$ since $(3,3) \notin H$.

$\Big\}$ can't use lcm formulas that works in G but not in G/H.

So $(1,1)+H$ doesn't have order 1, 2, or 3, so must have order 6 and $G/H = \langle (1,1)+H \rangle$, ie, $(1,1)+H$ is a generator.

$G = H \times K$

- H, K both normal subgroups of G
- $H \cap K = \{e\}$
- $G = HK$, ie, every element of g can be written as hk for some $h \in H$ & $k \in K$.

$G = H + K$.

could have $h+k$ $h \in K$ if G is additive

$G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$H = \mathbb{Z}_2 \oplus \{0\} \oplus \{0\}$

$K = \{0\} \oplus \mathbb{Z}_2 \oplus \{0\}$

$$\begin{array}{r} (1,0,0) \\ + \ (0,1,0) \\ \hline = (1,1,0) \end{array}$$

But $G \neq H \times K$ because $(0,0,1)$ can't be written as a sum of something in H & something in K.

$H = \langle (1\ 2\ 3) \rangle$

$|H| = |\langle (1\ 2\ 3) \rangle| = |(1\ 2\ 3)| = 3$

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

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

H is normal iff $xHx^{-1} \subseteq H$ for all $x \in S_4$.

In S_4, everything can be written as a product of 2-cycles, so if $xHx^{-1} \subseteq H$ is true for all 2-cycles x, it would be true for all $x \in S_4$ also.

For a 2-cycle, $x^{-1} = x$.

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

$(1\ 4)(1\ 2\ 3)(1\ 4) = (1)(2\ 3\ 4) \notin H$

so H is not normal!

7. Yes, it is a subgroup.

Strategy 1: check 3 criteria for being a subgroup.

- check identity $(0,0)$ is in H
- Check H is stable under addition
- check H is stable under negation.

Strategy 2:

$$H = \{(a,b) \mid 2a+3b=0\} \leq \mathbb{R}\oplus\mathbb{R}.$$

Let $\varphi: \mathbb{R}\oplus\mathbb{R} \longrightarrow \mathbb{R}$ be function $\varphi(a,b) = 2a+3b$. Check that this is a homomorphism

$$\begin{aligned}
\varphi(a,b)+\varphi(a',b') &= (2a+3b)+(2a'+3b') \\
&= 2(a+a')+3(b+b') \\
&= \varphi(a+a', b+b') \\
&= \varphi((a,b)+(a',b'))
\end{aligned}$$

And clearly $H = \ker\varphi$. So H is a subgroup!

8. Bad question...!

$|H| = 4$ $\quad H = \{(1), (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$

$$(1\,2)(1\,2\,3\,4)(1\,2)^{-1} = (1\,3\,4\,2)$$

so H is not normal, so S_4/H is not a group.

If H were normal... $|S_4/H| = \frac{4!}{4} = 3! = 6$, so if S_4/H is isomorphic to one of the groups, it would be isomorphic to $\mathbb{Z}_6$ iff it was cyclic, ie, had an element of order 6.

$S_4/\text{anything}$ can't have an element of order 6

In S_4, can only have order 1, 2, 3, 4.

identity 2-cycle or 2 disjoint 2-cycles 3-cycle 4-cycle.

and order in quotient can only be smaller.

9. $U(5)$

$1 \rightsquigarrow 1$
$2 \quad 2^2=4 \quad 2^3=3 \quad 2^4=1 \quad \rightsquigarrow 4$
3
$4 \quad 4^2=16 \rightsquigarrow 2$

$U(4)$

$1 \rightsquigarrow 1$

$3 \quad 3^2=1 \rightsquigarrow 2.$

$\gcd(n-1,n)=1$ because
$1=(-1)\cdot(n-1)+1\cdot n$
so 1 is a linear combination of $n-1$ & n.

$n-1$ is always in $U(n)$.
$(n-1)^2 \bmod n = n^2-2n+1 \bmod n = 1$
so $n-1$ has order 2 in $U(n)$.

10. $n=2$

$S_2=\{(1),(1\ 2)\} \quad Z(S_2)=S_2 \ni (1\ 2).$

$n=3$

Know: disjoint cycles commute

$(1\ 2)(1\ 3)=(1\ 3\ 2)$
$(1\ 3)(1\ 2)=(1\ 2\ 3)$ so $(1\ 2)\notin Z(S_3)$.

$n>4$

Same thing: $(1\ 3)\in S_4$ also!
In fact, $(1\ 3)\in S_n$ for all $n\geq 3$, so $(1\ 2)\notin S_n$ for all $n\geq 3$.

So just one such integer n—namely, $n=2$.

11. Is a subgroup.
(1) The identity $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ is in H because this of the form $\begin{bmatrix}a&0\\0&a^{-1}\end{bmatrix}$ for $a=1$.

(2) Check that H is stable under multiplication.

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} a' & 0 \\ 0 & a'^{-1} \end{bmatrix} = \begin{bmatrix} aa' & 0 \\ 0 & a^{-1}a'^{-1} \end{bmatrix} \quad \text{(first form).}$$

$$\begin{bmatrix} 0 & -b \\ b^{-1} & 0 \end{bmatrix}\begin{bmatrix} 0 & -b' \\ b'^{-1} & 0 \end{bmatrix} = \begin{bmatrix} & \cdots & \end{bmatrix} \quad \text{(first form)}$$

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} 0 & -b \\ b^{-1} & 0 \end{bmatrix} = \begin{bmatrix} 0 & -ab \\ a^{-1}b^{-1} & 0 \end{bmatrix} \quad \text{(second form)}$$

$$\begin{bmatrix} 0 & -b \\ b^{-1} & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} & \cdots & \end{bmatrix} \quad \text{(second form)}$$

(3) Check that H is stable under inversion.

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} & \cdots & \end{bmatrix} \quad \text{(first form)}$$

$$\begin{bmatrix} 0 & -b \\ b^{-1} & 0 \end{bmatrix}^{-1} = \begin{bmatrix} & \cdots & \end{bmatrix} \quad \text{(second form).}$$

12. $G = \mathbb{Z}$ $\quad H = \langle 2 \rangle = \{\text{even integers}\}$

H is a proper subgroup of G and it is true that $H \cong G$.

Let $\varphi: G \to H$ be function $\varphi(x) = 2x$.

Check that φ is an isomorphism:

- Check it is a homomorphism:

$$\varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y).$$

- Check it's injective:

$\varphi(x) = 0$ iff $x = 0$, so $\ker\varphi = \{0\}$, so injective.

- Check it's surjective:

For any $x \in H$, $x/2 \in \mathbb{Z}$ and $\varphi(x/2) = x$.
so φ is surjective.

Thus $G \cong H$.

[There can be no counterexample with G finite because any proper subgroup would have strictly smaller order, and isomorphisms preserve order.]