ZAD. 1.

Let $g \in G$ *be of order* n*. Show that for each* $m \in \mathbb{Z}$ *we have:*

$$g^m = e \iff n|m.$$

$\Longleftarrow$

We know that there exists $k \in \mathbb{Z}$ such that $m = nk$. That means

$$g^m = g^{nk} = (g^n)^k = e^k = e$$

$\Longrightarrow$

Proof by contraposition. Let us assume that $n \nmid m$. So $m = nk + r$. Then $r \in \{1, \dots, n-1\}$. So we have

$$g^m = g^{nk+r} = g^{nk}g^r = eg^r \neq e$$

ZAD. 2.

Let $N \leq G$*. Show that the following conditions are equivalent.*

(a) $N \triangleleft G$

$N \triangleleft G \implies (\forall\, g \in G)\; gNg^{-1} = N$

Take any $g \in G$. Take any $x \in gNg^{-1}$. Then $x = gng^{-1}$ for some $n \in N$. We have

$$x = gng^{-1} = (gn)g^{-1} = (n'g)g^{-1} = n' \in N$$

because $gn \in gN = Ng$ so we took n' such that $gn = n'g$.

Take any $n \in N$. Then

$$n = ngg^{-1} = (ng)g^{-1} = (gn')g^{-1} = gn'g^{-1} \in gNg^{-1}.$$

(b) $\implies$ (c)

Take any $g \in G$ and any $n \in N$. We want to show that then $gng^{-1} \in N$.

$$gng^{-1} \in gNg^{-1} = N.$$

(c) $\implies$ (a)

Take any $g \in G$. We want to show that $gN = Ng$. Take any $x \in gN$. It means, that for some $n \in N$ we have

$$x = gn$$

which we can multiply on both sides by g^{-1} from right and get

$$xg^{-1} = gng^{-1} \in N.$$

So if we multiply it from right by g we would get

$$xg^{-1}g = x \in Ng.$$

The other inclusion is analogous.

Or, if we want to be more fancy, we could write:

$$gN \subseteq Ng$$

for any g, so in particular for g^{-1}

$$g^{-1}N \subseteq Ng^{-1}$$
$$gg^{-1}Ng \subseteq gNg^{-1}g$$
$$Ng \subseteq gN$$

and the end! Only one inclusion written meticulously.

ZAD. 3.

Let $g \in G$ *be of order 2. Show that*

$$g \in Z(G) \iff \{e, g\} \triangleleft G$$

(we should also prove that $\{e, g\}$ is a subgroup but whooo caaareees)

$\implies$

Here we just want to prove that $kgk^{-1} \in \{e, g\}$ for every k. Since g is commutative, we have

$$(kg)k^{-1} = gkk^{-1} = g \in \{e, g\}$$

$\impliedby$

We know that $kgk^{-1} \in \{e, g\}$ for every k. We want to show that g is in Z(G). We have two possibilities:

$$kgk^{-1} = g \implies kg = gk$$

and this is what we wanted.

$$kgk^{-1} = e \implies kg = k \implies g = e$$

which cannot be because g is of order 2 and e is of order 1.

ZAD. 4.

Let $g \in G$ *be a unique element of order 2 in* G. *Show that* $g \in Z(G)$.

$g \in G$ such that $ord(g) = 2$ only for g. Let us take any other $h \in G$. We should observe that $hgh^{-1}hgh^{-1} = hggh^{-1} = hg(hg^{-1})^{-1} = (hg)(hg)^{-1} = e$. So it is either that ghg^{-1} is of order 1 or order 2.

If it is of order 1, then

$$e = hgh^{-1} \implies h = hg \implies 2 = g$$

and this cannot be!

If it is of order 2, then we have

$$hgh^{-1} = g \implies hg = gh$$

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

What if g is a unique element of order k? (show that then $g \in Z(G)$)

ZAD. 5.

Using the fundamental theorem on group homomorphism, show the following

$$(\mathbb{R}*, \cdot)/\{1, -1\} \simeq (\mathbb{R}_{>0}, \cdot)$$

$f : L \to R$ such that $f(x) = x^2$. We will prove that this is indeed a homomorphism.

$$f(xy) = (xy)^2 = xyxy = x^2y^2 = f(x)f(y).$$

$$(\mathbb{C}, +)/\mathbb{Z} \simeq (\mathbb{C}*, \cdot)$$

$f : L \to R$ such that $f(z) = e^{2\pi iz}$ jeees

$$f(x + y) = e^{2\pi i(x+y)} = e^{\pi ix}e^{\pi iy} = f(x)f(y).$$

Shit I have no clue what is happening now. "We got the pie!!!!"

$$(\mathbb{C}*, \cdot)/\langle e^{2\pi i\frac{1}{n}}\rangle \simeq (\mathbb{C}*, \cdot)$$

$$f(z) = z^n$$

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

ZAD. 6.

Let p *be a prime number and assume that* $|G| = p^2$. *Show that:*

$$G \simeq \mathbb{Z}_{p^2} \text{ or } G \simeq \mathbb{Z}_p \times \mathbb{Z}_p.$$

By Lagrange theorem we know, that for any $g \in G$ $\operatorname{ord}(g) = p$ or $\operatorname{ord}(g) = p^2$ (because each such element generates a cyclic subgroup of G). So we have two possibilities:
1. There exists an element g that has order p^2. So $G = \langle g \rangle$ and it is obvious that such a group is isomorphic with $\mathbb{Z}_{p^2}$.
2. There are no elements of order p^2, then all its elements have order p. So we have $g, h \in G$ such that $g \neq h$ such that $\langle g \rangle \cap \langle h \rangle = \{e\}$ and so they add up to the whole G. Ok so now let us consider a group

$$H = \langle g \rangle \times \langle h \rangle$$

It has order p^2. Because $\langle g \rangle \simeq \mathbb{Z}_p$ and the same goes for $\langle h \rangle$, let ϕ_g, ϕ_h be those two isomorphisms. We want to show that

$$f(x, y) = (\phi_g(x), \phi_h(y))$$

is a homomorphism $H \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. It is quite simple. Now to show that actually $G \simeq H$. Which would be

$$f(x) = \begin{cases} (x, e) & x \in \langle g \rangle \\ (e, x) & x \in \langle h \rangle \\ (q, p) & \text{if} x = qp, q \in \langle g \rangle, p \in \langle h \rangle \end{cases}$$

Ok, but what if i take f(gh)?

ZAD. 7.

Let $\phi : \mathbb{Z}_2 \to \operatorname{Aut}(\mathbb{Z}_n)$ *be the group action from Problem 2 of List 5. Show that*

$$D_n \simeq \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$$

Ok, I really have to learn what on earth does semidirect product mean.
Let

$$N = \{R \in D_n \ : \ R \text{ - rotation}\}$$

and

$$H = \{id, S\}.$$

Then $H \cap N = \{id\}$. It is clear that $N \simeq \mathbb{Z}_n$. Then we can decide weather or not we will invert a rotation by symmetry, so we have that $H \simeq \mathbb{Z}_2$. AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA