Math 417
HW 3
Due 2/8/19

Ungraded:

§1.5 - 21

a) $25\mathbb{Z}, +$: I'd say $0, 25, -25, 50, -50$

~~b) $(\frac{1}{2})^n$; $1, \frac{1}{2}, (\frac{1}{2})^2, (\frac{1}{2})^{-1} = 2, 2^2$~~

c) π^n; $1, \pi, \pi^2, \pi^{-1}, \pi^{-2}$

There is no unique "correct" answer

§1.6 - 17

In $\mathbb{Z}_{30} = \mathbb{Z}/30\mathbb{Z}$

$(25) = ([25]_{30})$: The elements are the multiples of $[25]_{30}$, namely, $[0]_{30}, [25]_{30}, [50]_{30} = [20]_{30}, [75]_{30} = [15]_{30}, [100]_{30} = [10]_{30}, [125]_{30} = [5]_{30}$.

$\gcd(25, 30) = 5$. Order of subgroup is $\frac{30}{\gcd(25,30)} = \frac{30}{5} = 6$: $\{[0], [5], [10], [15], [20], [25]\}$ it checks!

§1.6 - 27

$\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$. Subgroups have order d, where $d | 12$. So there are subgroups of order $1, 2, 3, 4, 6, 12$

1a §1.4 - 29

So let's look at pairs (x, x^{-1}). Notice that $(x^{-1})^{-1} = x$, so if $x \neq x^{-1}$, then it is paired up with something else, but ease.

Suppose G has an even number of elements. Write down the pairs

e

$x_1 \longleftrightarrow x_1^{-1}$

⋮

There has to be some other element paired with itself; that is $x \neq e$ so that $x * x = e$.

What this means is that $\{e, x\}$ is a subgroup of G, so if $|G|$ is even, G has a subgroup of order 2. (Last sentence is a remark, not part to the solution.)

1b. §1.5 - 47

Suppose G is an abelian group and $H = \{x : x^2 = e\}$.

We need to prove that H is a subgroup.

1) Is it closed? $x \in H$, $y \in H \Rightarrow x^2 = e$, $y^2 = e$. What about xy? $(xy)^2 = (xy)(xy) = x(yx)y = x(xy)y = x^2y^2 = e$. ✓

2) Is the identity there? $e^2 = e$ ✓.

3) If $x \in H$, is $x^{-1} \in H$?

$x^2 = e \Rightarrow (x^{-1}) \cdot x^2 = x^{-1} \Rightarrow x = x^{-1}$, so $(x^{-1})^2 = x^2 = e$ ✓.

All conditions are satisfied.

Remark: Note that for the nonabelian group S_3, H ~~might not be a~~ isn't a subgroup: the square of any flip is e, but the product of two different flips is a rotation, which doesn't belong to H.

2. $\mathbb{Z}/14\mathbb{Z}^{\times} = \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$ We saw this on HW1. You showed that this is a cyclic group, with generators $[3]_{14}$ (or $[3]_{14}^{-1} = [5]_{14}$). Since it is cyclic, all subgroups are cyclic

Keeping these in mind, the subgroups are:

$(\mathbb{Z}/14\mathbb{Z})^*$ itself
$= \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$

The identity alone
$\{[1]_{14}\}$.

The factors of 6 are 1, 2, 3, 6, so

$\{[1]_{14}, [9]_{14}, [11]_{14}\}$
(generated by $[9]_{14} = [3]_{14}^2$)

or $\{[1]_{14}, [13]_{14}\}$.
(generated by $[13]_{14} = [3]_{14}^3$)

3. Duplicate-Free Problem

4. $G = \langle a \rangle$, $a^{18} = 1$.
We have a theorem that says that $H = \langle a^k \rangle = \langle a^{\gcd(k,18)} \rangle$ is a subgroup of order $\frac{18}{\gcd(k,18)}$.

(a). $k=12$. $\gcd(12,18)=6$, so $\langle a^{12} \rangle = \langle a^6 \rangle$ is a subgroup of order $\frac{18}{6}=3$. (Check: $\{e, a^{12}, (a^{12})^2 = a^{24} = a^6\}$, $(a^{12})^3 = e$.

b) $k=5$, $\gcd(5,18)=1$, so $\langle a^5 \rangle = \langle a \rangle = G$ is a subgroup of order $\frac{18}{1}=18$. That is, a^5 is also a generator: $e, a^5, a^{10}, a^{15}, a^{20}=a^2, a^7, a^{12}, a^{17}, a^{22}=a^4, a^9, a^{14}, a^{19}=a, a^6, a^{11}, a^{16}, a^{21}=a^3, a^8, a^{13}, a^{18}=e$. Yep, that's all of them.
The point of the theorem is that you don't have to do this!

5a. Φ is an isomorphism, so $\Phi(g *_G h) = \Phi(g) *_H \Phi(h)$ for all $g, h \in G$.

(a). In particular, $\Phi(g *_G e_G) = \Phi(g)$
so $\Phi(g) = \Phi(g *_G e_G) = \Phi(g) *_H \Phi(e_G)$.
In other words, $\Phi(e_G)$ is the identity element in H: $\Phi(e_G) = e_H$.

(b) $g *_G g^{-1} = e_G$ by definition.
Since Φ is an isomorphism,
$\Phi(g *_G g^{-1}) = \Phi(g) *_H \Phi(g^{-1})$
$\Phi(e_G) = e_H$ (by part (a)).
That is, $\Phi(g) *_H \Phi(g^{-1}) = e_H$, so $\Phi(g^{-1})$ satisfies the definition of the inverse.

(c) Note that $\Phi(g*g) = \Phi(g)*\Phi(g)$, so $\Phi(g^2) = (\Phi(g))^2$, etc.
If g has order k, then $\{e_G, g, \ldots, g^{k-1}\}$ are different and $g^k = e_G$.
Look at $\{\Phi(e_H), \Phi(g), \ldots, \Phi(g)^{k-1}\}$.
Since $(\Phi(g))^j = \Phi(g^j)$, these are all different and $\Phi(g)^k = \Phi(g^k) = \Phi(e_G) = e_H$; that is, $\Phi(g)$ has order k.

6. $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

σ^2: $1 \to 2 \to 3$, $2 \to 3 \to 1$, $3 \to 1 \to 2$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ τ^2: $1 \to 1 \to 1$, $2 \to 3 \to 2$, $3 \to 2 \to 3$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\sigma\tau$ (remember, do τ first!)
$1 \to 1 \to 2$
$2 \to 3 \to 1$
$3 \to 2 \to 3$
$\tau \quad \sigma$
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\tau\sigma$ (remember, do σ first!
$1 \to 2 \to 3$
$2 \to 3 \to 2$
$3 \to 1 \to 1$
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Note: Alias, $\sigma = \rho_1$, $\tau = \mu_1$ from the handout