1.

1.

G is cyclic. Hence, there is a generator g such that $G = \{g^k : k \in \mathbb{Z}\}$.
Since f is homomorphism, we have that $g' \in G : \exists k \in \mathbb{Z} : g' = g^k$ and therefore, $f(g') = f(g^k) = (f(g))^k$. $f(g)$. f is surjective therefore, $f(g)$ is the genarator of H. Hence, H is also a cyclic group.

2.

If any group G is isomorphic to a cyclic group H, there is a surjective isormorphism function that maps the cyclic group H to G. Hence, it is also a cyclic group.

3.

Supppose N is a normal subgroup of G. Then $(g^k \cdot N) = (g \cdot N)^k$, hence $g \cdot N$ is the genarator of G/N. Which means that any quotient of a cyclic group is again cyclic.

2.

1.

From the Langrange's Theorem, we know that every subgroup of D_8 must have 1,2,4 or 8 elements.
1 elements: $\{1\}$
2 elements: since 1 must be included, the other element inverse is itself.
Every element in D_8 can be written in the form $s^i r^j$ where $i \in \{0,1\}$ and $j \in \{0,1,2,3\}$.
If $s = 0$ then the only element not 1 that is an inverse of itself is r^2.
If $s = 1$ then $sr^j sr^j = sr^j r^{4-j} s = sr^4 s = s^2 = 1$.
Hence, the subgroup having 2 elements are $\{1, r^2\}, \{1, s\}, \{1, sr\}, \{1, sr^2\}, \{1, sr^3\}$.
4 elements: 1 is an element of the subgroup.
If there is zero elements of the form sr^i then we have that $\{1, r, r^2, r^3\}$ is a subgroup. If there is one elements of the form sr^i then there is an element of the form r^j where $1 \leq j \leq 3$, which means that $sr^i \cdot r^j = sr^{i+j} \neq sr^i$ and hence not in the set which means there is no subgroup in this case.
If there is two or three elements of the form sr^i then let 2 of them be sr^i and sr^j, we have that $sr^i sr^j = sr^i r^{4-j} s = sr^{4-j+i} s = ssr^{4-(4-j+i)} = r^{j-i}$. r^{j-i} must also be an inverse of itself which means that $j - i = 2$.
Hence, the subgroup in this case is $\{1, s, r^2, sr^2\}, \{1, sr, r^2, sr^3\}$.
Therefore the subgroup having 4 elements are $\{1, r, r^2, r^3\}, \{1, s, r^2, sr^2\}, \{1, sr, r^2, sr^3\}$.
8 elements: itself

2.

From the Langrange's Theorem, we know that every subgroup of S_3 must have 1,2,3 or 6 elements.
1 elements: $\{()\}$ 2 elements: since 1 is in any subgroup, the othere element is an inverse of itself. Hence, the subgroups are $\{(), (12)\}, \{(), (23)\}, \{(), (13)\}$
3 elements: length 2 length 3 cant, 2 length 2 cant, 2 length 3 only 1 case 6 elements: itself

3.

1 elements: $\{1\}$
2 elements: since 1 is in any subgroup, the othere element is an inverse of itself. Hence, the subgroups is $\{1, -1\}$ 4 elements: since 1 is in any subgroup, order 4 so one elements must be an inverse of itself so -1 must also be in the subgroup. As -1 is in the subgroup if i is in the subgroup then so does -i, similar to j and -j, k and -k. Hence the subgroups are $\{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}$ 8 elements: itself

3.

1.

Since $\varphi_k(g) = g^k$, $\forall g^i \in G : \varphi_k(g^i) = (\varphi_k(g))^i = (g^k)^i = g^k i$. Hence, the function is unique as every element is mapped to a predeterimend element in G. $\forall g^i, g^j \in G : \varphi_k(g^i) \cdot \varphi_k(g^j) = g^{ik} \cdot g^{kj} = g^{k(j+i)} = \varphi_k(g^{i+j})$. Hence, φ_k is a homomorphism.

2.

If $\gcd(k, n) \neq 1$, then $\exists m \in \mathbb{Z} : mn = k$ or $mk = n$.
If $mn = k$, then $\forall g^i \in G : \varphi_k(g^i) = g^{ik} = g^{imn} = 1$. Which means the function is not surjective and therefore does not have an inverse hence not an automorphism.
If $mk = n$, then $\varphi_k(g^m) = g^{mk} = 1 = \varphi_k(1)$. Hence, φ_k is not injective and therefore do not have an inverrse hence not an automorphism.
If $\gcd(k, n) = 1$, then let $k = an + b$ where $a, b \in \mathbb{Z}, 0 \leq b < n$.
$\forall g^i \in G : \varphi_{n-b}(g^i) \cdot \varphi_k(g^i) = g^{i(n-b)} \cdot g^{i(an+b)} = 1$. Therefore φ_k has an inverse and is automorphism.

3.

It is obvious that $\forall g^i \in G :$

$$(\varphi_a \circ \varphi_b)(g^i) = ((g^i)^b)^a = g^{iba} = (g^i)^{ab} = \varphi_{a \cdot b}(g^i)$$

4.

$\forall a, b \in \mathbb{Z}$ such that $a \equiv b (\text{mod } n) : \exists t \in \mathbb{Z} : a = b + tn$
$\forall g^i \in G : \varphi_a(g^i) = g^{i(b+tn)} = g^{ib} = \varphi_b(g^i)$. Hence, $\varphi_a = \varphi_b$ and therefore the function is well-defined.
If we restrict $\{a \text{ mod } n\}$ to $\{a \text{ mod } n | \gcd(a, n) = 1\}$. Then we know that φ_a is an automorphism hence we can restrict the original function to a bijection

$$f : (\mathbb{Z}/n)^\times \cong \text{Aut}(G), \qquad (a \text{ mod } n) \to \varphi_a \text{ with } \gcd(a, n) = 1$$

because every function $\varphi_k = f(k)$ and if $\varphi_k = \varphi_l$ then $k \equiv l \pmod n$

5.

$$f(ab) = \varphi_{ab} = \varphi_a \cdot \varphi_b = f(a) \cdot f(b)$$

Hence it is isormorphic.

6.

If H is an infinite cyclic group with generator g, then consider

$$\varphi : \mathbb{Z} \to H, \qquad a \to g^a$$

The function is surjective. It is injective as if $g^a = g^b$ then g has order $a - b$ or $b - a$ which is finite. We also have that

$$\forall a, b \in \mathbb{Z} : \varphi(a \cdot b) = g^{a \cdot b} = g^a \cdot g^b = \varphi(a) \cdot \varphi(b)$$

Hence, φ is in isomorphic. Hence, $\mathrm{Aut}(\mathbb{Z})$ is isoromorphic to $\mathrm{Aut}(H)$. Consider the group action:

$$\psi : \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z})$$

$\forall f \in \mathrm{Aut}(\mathbb{Z})\ f(0) = 0, f(n) = f(-n), f(n) = nf(1)$.
If $|f(1)| \geq 2$ then $\nexists n : f(n) = 1$, which is a contradiction.
If $f(1) = 1$ then let $g \in \mathrm{Aut}(\mathbb{Z})$ such that $g(1) = -1$. Then $\forall a \in \mathbb{Z}$: $f(g(a)) = f(-a) = a$.
If $f(1) = 0$ then $\forall a \in \mathbb{Z} : f(a) = 0$ and hence leads to a contradiction. Hence, H also have two automorphisms, one maps g^a to g^a and the other maps g^a to g^{-a}

4.

1.

If $\forall g \in \ker(\pi) : \pi(g) = 1$ therefore $\psi(g) = \delta(\pi(g)) = \delta(1) = 1$. Hence, $g \in \ker(\psi)$ and hence $\ker(\pi) \subset \ker(\psi)$.

2.

Since, $\ker(\pi) \subseteq \ker(\psi)$. We can create a function δ such that $\forall g \in G : \pi(g) = h, \psi(g) = k$, then let $\delta(h) = k$ hence $\psi = \delta \circ \pi$.
$\forall g_1, g_2 \in G$: let $\pi(g_1) = h_1$, $\pi(g_2) = h_2$, $\psi(g_1) = k_1$, $\psi(g_2) = k_2$, $\delta(h_1) = k_1$, $\delta(h_2) = k_2$. We have:
$\delta(h_1 \cdot h_2) = \delta(\pi(g_1) \cdot \pi(g_2)) = \delta(\pi(g_1 \cdot g_2)) = \psi(g_1 \cdot g_2) = \psi(g_1) \cdot \psi(g_2) = \delta(\pi(g_1)) \cdot \delta(\pi(g_2)) = \delta(h_1) \cdot \delta(h_2)$. Hence, δ is homomorphic.
If there is a function δ such that $\delta(h_1) = k_2$ then $k_1 = \psi(g_1) = \delta(\pi(g_1)) = \delta(h_1) = k_2$. Therefore, the function is unique.

3.

Let $\pi : G \to G/\ker(\varphi)$
First, let restrict φ to a surjective function: $\varphi' : G \to \mathrm{im}(\varphi)$.
We know that $\ker(\varphi') = \ker(\varphi)$ are normal subgroups of G. Hence, from the universal property of quotients,
there exsists a unique homomorphism $\overline{\varphi} : G/\ker(\varphi') \to \mathrm{im}(\varphi')$ satisfies $\overline{\varphi} \circ \pi = \varphi'$ and since $\forall g \in G : \varphi'(g) = \varphi(g)$, $\ker(\varphi') = \ker(\varphi)$, $\mathrm{im}(\varphi') = \mathrm{im}(\varphi)$.
We can rewrite it as $\overline{\varphi} : G/\ker(\varphi) \to \mathrm{im}(\varphi)$ satisfies $\overline{\varphi} \circ \pi = \varphi$.
The kernel of $\overline{\varphi}$ consists of cosets of the form $g \cdot \ker(\varphi)$ with $\varphi(g) = 1$, equivalently, $g \in \ker(\varphi)$. Since $g \cdot \ker(\varphi) = \ker(\varphi) \iff g \in \ker(\varphi)$. Hence, $\overline{\varphi}$ is injective.
φ is surjective, hence so does $\overline{\varphi}$.
Therefore, $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.
As a result, if φ is surjective, that is if $H = \mathrm{im}(\varphi)$ then $G/\ker(\varphi)$ is isomorphic to H.

5.

Since the size of is 2. One coset is $1 \cdot H = H$ and the other is $G \backslash H$.
Pick $x \in G$
If $x \in H$ then obviously, $\forall h \in H : xhx^{-1} \in H$.
If $x \notin H$ then as right cosets are also $H \cdot 1 = H$ and hence $G \backslash H$. Hence, as $xH \neq H, xH = G \backslash H$ and $Hx \neq H, Hx = G \backslash H$ and therefore $xH = Hx$.
In both cases, H is proven normal.
Consider $G = S_3$ and its subgroup $H = \{(), (12)\}$.
$[G : H] = 3$ as $() \cdot H = H$, $(23) \cdot H = \{(23), (123)\}$, $(13) \cdot H = \{(13), (321)\}$ but $(23)(12)(23) = (13) \notin H$.

6.

1.

From definition $Z(G)$ is normal in G as it is a subgroup of G and $\forall g' \in Z(G) : \forall g \in G : gg' = g'g$.

2.

(a) $\iff$ (b): already proven in homework 3
(b) $\iff$ (d): directly, we have that $G/Z(G)$ is trivial if and only if $Z(G) = 1 \cdot Z(G) = G$
(c) $\implies$ (a): $\exists G' \in G/Z(G) : G/Z(G) = \langle G' \rangle$. Since G' is a cosets, $\exists g \in G : G' = tZ(G)$. Hence each cosets is equals to $(G')^n = (tZ(G))^n = t^n Z(G)$.
For arbitary $x, y \in G : \exists i, j : x \in t^i Z(G)$ and $y \in t^j Z(G)$ and hence $\exists z_1, z_2 \in Z(G) : x = t^i z_1$ and $y = t^j z_2$.

$$
\begin{aligned}
xy &= t^i z_1 t^j z_2 \\
&= t^i t^j z_1 z_2 \\
&= t^j t^i z_2 z_1 \\
&= t^j z_2 t^i z_1 \\
&= yx
\end{aligned}
$$

and hence G is abelian.
(d) $\implies$ (c): $G/Z(G)$ is trivial hence cyclic.

3.

G is a finite group of order $p \cdot q$ where p and q are primes. Hence $Z(G)$, subgroup of G, must have $1, p, q$ or pq elements.
If the number of elements in $Z(G)$ is either p or q then $Z(G)$ is cyclic hence G is abelian.
If $Z(G)$ has pq elements then $Z(G) = G$ and hence G is abelian.
If $Z(G)$ has 1 element then it is trivial.

4.

Consider the map

$$\rho : G \to \mathrm{Aut}(G), \qquad \rho(g)(h) = g \cdot h \cdot g^{-1}$$

We have that:
$\ker(\rho) = \{g : \forall h \in G : \rho(g)(h) = h\} = \{g : \forall h \in G : gh = hg\} = Z(G)$. Hence, $G/\ker(\rho) = G/Z(G) \cong \mathrm{im}(\rho) = \mathrm{Inn}(G)$. As $\mathrm{Inn}(G)$ is a normal subgroup of $Z(G)$ and $Z(G)$ is cyclic, $G/Z(G)$ is also cyclic and hence G is abelian.