1. (a) Associativity of the group operation is from function composition being associative, and the binary operation maps back into the set since compositions of bijections are bijections, and the domain is equal to the codomain. The function $1 := (x \mapsto x)$ is clearly bijective since it is its own inverse, moreover for any $f \in S_\Omega$ we have $f1(x) = f(x)$, and $1f(x) = f(x)$, so that this is an identity. The set theoretic inverse of a bijection $\Omega \to \Omega$ is also a bijection $\Omega \to \Omega$, and satisfies $ff^{-1} = f^{-1}f = 1$, so inverses exist.

(b) Consider the cyclic group (x), if $o(x) = \infty$, then $x^n \mapsto n$ is a homomorphism (well defined since if $x^n = x^m$ for $n \neq m$, then $x^{n-m} = 1$ so that $o(x) \neq \infty$) $(x) \to \mathbb{Z}$, which is clearly surjective, and is injective since if x^n, x^m map to the same element, then $n = m$. Now let $o(x) = n$, then consider the map into $\mathbb{Z}/(n)$, $x^j \mapsto j$. This is well defined since if $x^j = x^k$, then by long division write $j = q_j n + r_j$, $k = q_k n + r_k$ where $0 \leq r_j, r_k < n$, so that $1^{q_j}x^{r_j} = 1^{q_k}x^{r_k}$, and hence $j \equiv k \ \ (r)$. It is also clearly surjective, and is injective since if $x^j \mapsto r_j$ and $x^k \mapsto r_k$, then $j \equiv k \ \ (r)$ and hence $j = qn + k$, so that $x^j = 1^q x^k = x^k$.

This reduces the problem to showing a subgroup of a cyclic group is cyclic. Assume that $H \subset G = (x)$, and k is the smallest power such that $x^k \in H$, then $H = (x^k)$, otherwise there is some $(x^r) \in H \setminus (x^k)$, so that $k \nmid r$, then by long division $r = qk + c$ for $0 \leq c < k$ hence $x^r x^{-qk} = x^c \in H$ which contradicts k being the smallest exponent.

(c) let $x \in N \cap N'$ and $g \in G$, then $gxg^{-1} \in N$ since N is normal, and similarly for N', hence $gxg^{-1} \in N \cap N'$.

(d) $f \circ g(xy) = f(g(x)g(y)) = (f \circ g(x))(f \circ g(y))$.

(e) $f(1) = f(11) = f(1)f(1)$, applying $f(1)^{-1}$ to both sides, $1 = f(1)$. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, applying $f(x)^{-1}$ to the left on both sides yields $f(x)^{-1} = f(x^{-1})$

(f) Let $x, y \in \ker f$, then $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 11^{-1} = 1$, so that $xy^{-1} \in \ker f$. If $u = f(x), v = f(y)$, then $uv^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$ is in $\operatorname{Im} f$.

2. If G is abelian, then $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$. If the inversion map is a homomorphism, then for any $x, y \in G$, $yx = (x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1} = xy$, so G is abelian.

3. (a) $\mathrm{GL}_2(\mathbf{F}_p)$ is a subset of $S_{\mathbf{F}_p^2}$ (as defined in problem 1), so we need only check the subgroup criterion, but this is strightforward since the composition of matrices is a matrix from matrix multiplication, and the inverse is a matrix from Cramer's rule.

(b) An invertible matrix must have a nonzero first column, but any other column can give rise to an invertible matrix, so that there are $p^2 - 1$ choices for the first column by excluding the zero column. For a fixed first column, the second column can be any non-scalar multiple of the first, so that there are $p^2 - p$ choices for the second column. Putting this together, $\#\mathrm{GL}_2(\mathbf{F}_p) = (p^2 - 1)(p^2 - p)$

(c)

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad k \notin (p), \text{ have order } p$$

as well as any matrix conjugate to a matrix of this form. It is not too hard to see that there is more than one such subgroup (e.g.) lower diagonal matrices, and since these subgroups have order p they are cyclic and generated by any nontrivial element, so that if $A, B \in \mathrm{GL}_2(\mathbf{F}_p)$ each with order p, then $(A) \cap (B) = 1$. Hence the number of order p elements is the number of order p subgroups times $p - 1$, we know that any matrix in the stabilizer for the subgroup $\left\{\begin{pmatrix} 1 & k; & 0 & 1 \end{pmatrix}\right\}$ must be upper triangular by computing the conjugation action, moreover conjugation by an upper triangular matrix fixes the subgroup so that the normalizer of the sylow-p subgroup $\left\{\begin{pmatrix} 1 & k; & 0 & 1 \end{pmatrix}\right\}$ is exactly the invertible upper triangular matrices. Since the Sylow-p subgroups are all conjugate, we have by orbit stabilizer that the number of Sylow-p subgroups is $\#G/\#N(P)$, where the normalizer is invertible upper triangular matrices, of which there are $(p-1)^2 p$, so that the number of sylow P subgroups is $p+1$, giving $(p+1)(p-1)$ elements of order p.

Alternatively, we can avoid using Sylow's theorems by using linear algebra. If $A \in \mathrm{GL}_2(\mathbf{F}_p)$ has order p, its minimal polynomial divides $X^p - 1 = (X-1)^p$, this implies that the jordan form of A is $\begin{pmatrix} 1 & 1; & 0 & 1 \end{pmatrix}$, note A is conjugate to its jordan form since all the roots lie in $\mathbf{F}_p$. This means that every matrix having order p is conjugate to $\begin{pmatrix} 1 & 1; & 0 & 1 \end{pmatrix}$, so it suffices to count the orbit of $\begin{pmatrix} 1 & 1; & 0 & 1 \end{pmatrix}$

under conjugation by $\mathrm{GL}_2(\mathbf{F}_p)$. Note that as before, a matrix conjugates $\left(\begin{smallmatrix}1 & 1;\\ 0 & 1\end{smallmatrix}\right)$ to an upper triangular matrix if and only if it is upper triangular, then

$$\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}^{-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}=\begin{pmatrix}1 & da^{-1}\\ 0 & 1\end{pmatrix}$$

It follows that an element of the stabilizer has p choices for b, then $p-1$ choices for a and no choices for d. So the stabilizer of $\left(\begin{smallmatrix}1 & 1;\\ 0 & 1\end{smallmatrix}\right)$ has order $p(p-1)$, which means by orbit stabilizer that there are $(p^2-1)(p^2-p)/p(p-1)=(p-1)(p+1)$ elements of order p.

(d)

$$\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$$

(e) I will prove one exists, I dont think I can write it explicitly for arbitrary p, because the method should be to put it into rational canonical form, but then by the same idea used in the proof provided below this is actually equivalent to finding an explicit element of $\mathbf{F}_p^2$ having order $p+1$. We know that $\mathbf{F}_{p^2}/\mathbf{F}_p$ is an algebraic extension, since the former is the splitting field of $x^{p^2-1}-1$, since $\mathbf{F}_{p^2}^\times$ is cyclic, we can choose a generator α, the minimal polynomial of α will have degree 2 over $\mathbf{F}_p$, so that $\alpha^2=a\alpha+b$, this means we have a copy of $\mathbf{F}_{p^2}^\times$ in $\mathrm{GL}_2(\mathbf{F}_p)$, namely the cyclic subgroup

$$(A)\qquad\qquad A=\begin{pmatrix}0 & b\\ 1 & a\end{pmatrix}$$

This element has the same multiplicative order as α, being p^2-1, it follows that A^{p-1} has order $p+1=(p^2-1,p-1)$.

We can be a little more explicit than this using the idea from the rational canonical form that if $\alpha\in\mathbf{F}_p^2$ has order $p+1$, then the other root to its minimal polynomial is $\Phi_p(\alpha)=\alpha^p$, so that the minimal polynomial is actually $x^2-(\alpha+\alpha^p)x+1$, so the matrix should look like

$$\begin{pmatrix}0 & -1\\ 1 & \alpha+\alpha^p\end{pmatrix}$$

4. A subgroup of S_p having order p must be cyclic, and by cycle types it is generated by a p-cycle. Furthermore, if $H=(\sigma)$, then $H=(\sigma^j)$ for $1\le j<p$ are all p-cycles. Hence the number of subgroups of order p is equal to the number of p-cycles divided by $p-1$. To count all the p-cycles, there are $p-1$ choices of where 1 should go, $p-2$ choices of where 2 should go, etc. So that there are $(p-2)!=\frac{(p-1)!}{p-1}$ such subgroups.

5. (a) If $z_1^n=1$ and $z_2^m=1$, then $(z_1z_2)^{m+n}=1$, and if $z^n=1$, then $(z^{-1})^n=1$, so that indeed it is a subgroup.

(b) That $\sim$ is an equivalence relation follows directly from $=$ being an equivalence relation.

(c) This is not true for the set $\{z\in\mathbb{C}^*\mid\exists n,\ z^n=1\}$, this should be clear since $1,e^{\frac{2}{3}\pi i}$ and $e^{\frac{1}{8}\pi i}$ are all not equivalent, this is also not true if n is arbitrary, i.e. $n=16$, then $e^{\frac{2\pi i}{16}},1,e^{\frac{2\pi i}{32}}$ are all in different equivalence classes.

6. (a) If $z^n=1$, then $(z^{-1})^n=z^{-n}=(z^n)^{-1}=1$, so H is closed under inverses. If $z^n=w^n=1$, then $(zw)^n=z^nw^n=11=1$, so its a subgroup.

(b) $m=kn$, then for any $x\in U_n$ we have $x^m=x^{kn}=(x^n)^k=1^k=1$.

(c) One inclusion follows from (b). For the other inclusion, suppose that $x^n=x^m=1$, then by bezout's identity there are a,b such that $an+bm=d=(n,m)$, it follows that $1=(x^n)^a(x^m)^b=x^{an+bm}=x^d$.

(d) $f(n+m)=e^{(n+m)i\frac{2\pi}{5}}=e^{ni\frac{2\pi}{5}}e^{mi\frac{2\pi}{5}}=f(n)f(m)$. U_5 has at most 5 elements since they all satisfy x^5-1, since $e^{ki\frac{2\pi}{5}}$ all satisfy the polynomial for $k=0,\dots,4$ $U_5=\{e^{ki\frac{2\pi}{5}}\}_1^4$, we can also see by the first isomorphism theorem that $\ker f=5\mathbb{Z}$, so that $U_5\cong\mathbb{Z}/5\mathbb{Z}$.

7. **(a)** $gh \mapsto (x \mapsto (gh)x(gh)^{-1}) = (x \mapsto g(hxh^{-1})g^{-1}) = (x \mapsto gxg^{-1}) \circ (x \mapsto hxh^{-1})$.

(b) If $g \in Z(G)$, then for any x, $gx = xg$ or equivalently $gxg^{-1} = x$, furthermore if $g \notin Z(G)$, then for some x we have $gx \neq xg$ so that $gxg^{-1} \neq x$. This shows that the kernel is precisely $Z(G)$. Thus the natural map can be taken to be the induced map from the first isomorphism theorem (i.e. conjugating by an element of the equivalence class).

(c) Let $\phi \in \mathrm{Aut}G$, then for any y,

$$\phi(x \mapsto gxg^{-1})\phi^{-1}(y) = \phi(g\phi^{-1}(y)g^{-1}) = \phi(g)y\phi(g)^{-1}$$

So that $\phi(x \mapsto gxg^{-1})\phi^{-1} = (x \mapsto \phi(g)x\phi(g)^{-1})$.

(d) Take $\mathbb{Z}/3\mathbb{Z}$, then since this is abelian the map $x \mapsto x^{-1}$ is a homomorphism (also note in this case it is nontrivial). So $\#\mathrm{Aut}(G) \geq \#\{1, (x \mapsto x^{-1})\} = 2$ and $1 = \#G/Z(G) = \#\mathrm{Inn}\, G$, and hence $\#\mathrm{Out}\, G \geq 2/1 = 2$. □