1.(1) $H < G$. describe $\langle G \setminus H \rangle$

Let $S = G \setminus H$

1°. claim, $\forall g \in S$, $h \in H$, $g^{-1}, gh \notin H$

If $g^{-1} \in H$, then since $H < G$, $g \in H$ but $g \in S$, $S \cap H = \emptyset$. ↯

If $gh \in H$, then $\exists h_1 \in H$ s.t $gh = h_1$, i.e $g = h_1 h^{-1} \in H$, ↯

2°. From 1°, $\forall h \in H$, $\exists g^{-1}, gh \in S$ s.t $g^{-1}gh = h$

Since $g^{-1}gh \in \langle S \rangle$, it shows $H < \langle S \rangle$

3° thus, $\langle S \rangle = \langle S, H \rangle = \langle G \rangle = G$

(2). if G fin. $S \subseteq G$ $|S| > n/2$. $\forall g \in G$. $\exists$ $a.b \in S$, $g = ab$.

$\forall g \in G$, $|gS^{-1}| > n/2$, hence $gS^{-1} \cap S \neq \emptyset$

which means that $\exists$ $a.b \in S$ s.t $gb^{-1} = a \Rightarrow g = ab$

2. G fin. only one max. subgrp. show $|G| = p^k$. G cyclic.

Let $H \underset{max}{<} G$ Consider $g \in G \setminus H$, then $G = \langle g \rangle$

if not, $\langle g \rangle < G$ shows that $\langle g \rangle \leq H$, ↯ $g \notin H$

Hence G is cyclic.

Now suppose $|G| = n$ where $p \neq q$, $p | n$, $q | n$, p, q are primes

Then $\langle g^p \rangle, \langle g^q \rangle < G \Rightarrow \langle g^p \rangle, \langle g^q \rangle \leq H$

since $(p.q) = 1$, $\exists$ l, k s.t $lp + kq = 1$

$\Rightarrow \quad g = g^{lp+kq} \in H \Rightarrow H = G$ ↯

3. A. fin abel. p prime.

$A^p = \{a^p \mid a \in A\} \qquad A_p = \{x \mid x^p = 1\}$.

(a) $A/A^p \simeq A_p$.

Consider $\sigma: A \to A^p$ since A is an abelian group
$x \mapsto x^p$ (also epi.)

σ is a group homomorphism, and $\ker\sigma = A_p$

thus $A/A_p \simeq A^p$, we have $|A| = |A_p| \cdot |A^p|$

also we have $\dfrac{|A|}{|A^p|} = |A_p|$

$A^p \leq A$, furthermore, $A^p \trianglelefteq A$

and A/A^p, A_p are both elementary abelian group

and they have the same order shows $A/A^p \simeq A_p$

(b). Prove subgrps of A of order $p \xleftrightarrow{1:1}$ subgrps of A of index p

from (a). $A/A^p \simeq A_p \simeq \underbrace{\mathbb{Z}_p \times \cdots \mathbb{Z}_p}_{n}$ for some n.

Consider any subgroup H of A with index p. $\forall a \in A$ the coset aH satisfies that $a^p \in H$, thus $A^p \trianglelefteq H$

Thus $\dfrac{|A/A^p|}{|H/A^p|} = |A|/|H| = p$

and $A/A^p \cong A_p$ by (a) shows:

1 $\{$the subgrps H of A with index $p\} \xleftrightarrow{1:1}$

$\{$the subgrps $\bar{H}$ of A/A^p with index $p\} \xleftrightarrow{1:1}$

$\{$the subgrps K of A_p with index $p\}$

and 2 $\{$the number of subgrps of A of order $p\} \xleftrightarrow{1:1}$

$\{$the number of subgrps of A_p of order $p\} \xleftrightarrow{1:1}$

$\{$the number of distinct elements of order p in $A_p\} / p-1$

So we just need to count twice to see if 1 and 2 are coinside.

for 1 $A_p \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$ $K \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n-1}$

the number of distinct K is

$$\frac{\prod_{i=0}^{n-2} p^n - p^i}{\prod_{i=0}^{n-2} p^{n-1} - p^i} = \frac{p^n - 1}{p-1}$$

for ② you know that it is $\frac{p^n-1}{p-1}$

1(c). Let $A = \mathbb{Z}_{60}\times\mathbb{Z}_{45}\times\mathbb{Z}_{12}\times\mathbb{Z}_{36}$.

find the number of elements of order 2 and subgroups of index 2.

$A = \mathbb{Z}_{60}\times\mathbb{Z}_{45}\times\mathbb{Z}_{12}\times\mathbb{Z}_{36}$

$A_2 = \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$

distinct generators of order 2: $2^3-1=7$

$7 =$ the number of subgrpss of order 2 in A_2

= the number of subgups of index 2 in A_2

= the number of subgups of index 2 in A.

4. $H \trianglelefteq G$, $[G:H]=p$. $\forall K\leq G$

$K\leq H$ or $G=HK$ and $[K:K\cap H]=p$.

Since $H\trianglelefteq G$, $K\leq G$, we have $HK\leq G$ and $H\trianglelefteq HK$

Then $|G:H| = |G:HK|\,|HK:H| = p$

1°. $|G:HK|=1$, then $G=HK$ and

Since $HK/H \cong K/H\cap K$

$|K:H\cap K| = |HK:H| = p$

2° $|HK:H|=1 \Rightarrow K\leq H$.

5. If $|G| = n$, n odd. then $\forall x \neq 1$, $x \in G$

we have x, x^{-1} are not conjugate.

If x, x^{-1} are conjugate, then $\exists g \in G$ s.t

$g^{-1} x g = x^{-1}$

1° $g = e$, $x = x^{-1} \Rightarrow o(x) = 2 \Rightarrow o(x) \mid |G|$

$\Rightarrow |G|$ even, contradiction!

2° if $g \neq e$,

$g^{-2} x g^2 = g^{-1}(g^{-1} x g) g = g^{-1} x^{-1} g = (g^{-1} x g)^{-1} = (x^{-1})^{-1} = x$

shows $g^2 \in C_G(x)$

(i). if $g \in \langle g^2 \rangle$, it shows $xg = gx$, since $g^{-1} x g = x^{-1}$

$\Rightarrow x^2 = 1 \Rightarrow o(x) = 2$, $o(x) \mid |G|$

$\Rightarrow |G|$ even. contradiction!

(ii) if $g \notin \langle g^2 \rangle$, it shows $|\langle g \rangle|$ even

and $\langle g \rangle \leq G$ shows $|G|$ even. contradiction!

6. $|G| = n$, $a_1 \cdots a_n$ arbitrary n elements in G.

$\exists$ p, q s.t $a_p a_{p+1} \cdots a_q = 1$.

Let $S = \{a_1, a_1 a_2, \cdots, a_1 a_2 \cdots a_n\}$

if $1 \in S$. then it's done

if $1 \notin S$, since $|G|=n$, $\exists$ two elements in G

$a_1 \cdots a_i = a_1 \cdots a_j$, WLOG let $i<j$

then $a_{i+1} a_{i+2} \cdots a_j = 1$ Let $p=i+1$, $q=j$.

7. if σ has no fixed point, $\sigma^2=1$. then G is abelian with odd order.

Let $H = \{ g^{-1}\alpha(g) \mid g \in G \}$. claim $H = G$

Let map: $\varphi: G \longrightarrow H$

$g \longmapsto g^{-1}\alpha(g)$

Check: φ is bijective.

if $g, h \in G$, $g \neq h$. then $g^{-1}\alpha(g) \neq h^{-1}\alpha(h)$

if not, $g^{-1}\alpha(g) = h^{-1}\alpha(h) \Rightarrow hg^{-1} = \alpha(h)(\alpha(g))^{-1} = \alpha(hg^{-1})$

$\Rightarrow hg^{-1}$ is fixed point of σ, contradiction!

$\Rightarrow \varphi$ is injective and surjective is obvious $\Rightarrow \varphi$ bijective.

Therefore, $\forall a \in G$, $a = g^{-1}\alpha(g)$ for some $g \in G$

$\alpha^2 = 1$ shows $a^{-1} = \alpha(g^{-1})\, g = \alpha(a)$

$\Rightarrow \forall a, b \in G$, $\alpha(ab) = (ab)^{-1} = b^{-1}a^{-1} = \alpha(b)\alpha(a) = \alpha(ba)$

$\Rightarrow ab = ba \Rightarrow G$ is abelian

Since $a^{-1} = \alpha(a) \neq a$, $\forall a \in G \Rightarrow |G|$ is odd.

8. $aba = ba^2b$. $a^3=1$ $b^{2n-1}=1$ $\Rightarrow b=1$

$ab^2a = aba^3ba = (aba)a^2ba = ba^2ba^2ba = ba^2abaa = b^2a^2$

$\Rightarrow ab^2 = b^2a$ suppose $ab^{2k-2} = b^{2k-2}a$, $ab^{2k} = ab^{2k-2}b^2 = b^{2k-2}ab^2 = b^{2k}a$

$\Rightarrow$ for all $n \in \mathbb{Z}_{\geq 1}$. $ab^{2n} = b^{2n}a$, since for some n $b^{2n-1}=1$

$\Rightarrow \exists n$, $ab=ba \Rightarrow ba^2 = aba = ba^2b \Rightarrow b=1$

9. $A \leq G$. $C_GC_GC_G(A) = C_G(A)$

$\forall a \in A$. $\forall b \in C_G(A)$

$ab=ba$

it shows $a \in C_GC_G(A)$

Then $A \leq C_GC_G(A)$

$\Rightarrow C_GC_GC_G(A) \leq C_G(A)$

On the other hand

$\forall x \in C_G(A)$ x commutes with all elements in $C_GC_G(A)$

it shows $x \in C_GC_GC_G(A)$

$\Rightarrow C_G(A) \leq C_GC_GC_G(A)$

$\Rightarrow C_G(A) = C_GC_GC_G(A)$

10. $|G|=n$. odd. $\alpha \in Aut(G)$ $\alpha^2=1$

$G_1 = \{g \in G \mid \alpha(g)=g\}$ $G_{-1} = \{g \in G \mid \alpha(g) = g^{-1}\}$

Prove $G = G_1G_{-1}$ and $G_1 \cap G_{-1} = 1$

1°. $\forall x \in G$, $|\langle x \rangle|$ must odd $\Rightarrow \exists y \in G \quad y^2 = x$

2°. $\forall g \in G$ Let $g^{-1}\alpha(g) = x^2$

since $\alpha(x^2) = \alpha(g^{-1}\alpha(g)) = (\alpha(g))^{-1} g$

$= (g^{-1}\alpha(g))^{-1} = x^{-2} = \alpha(x)^2$

since $o(x) = o(\alpha(x))$ and it odd

$\Rightarrow \alpha(x) = x^{-1} \Rightarrow x \in G_{-1}$

$\alpha(gx) = \alpha(g)\alpha(x) = \alpha(g)x^{-1} = gx^2x^{-1} = gx$

$\Rightarrow gx \in G_1$

$\Rightarrow g = gxx^{-1} \in G_1 G_{-1} \Rightarrow G = G_1 G_{-1}$

Let $g \in G_1 \cap G_{-1} \Rightarrow \alpha(g) = g = g^{-1} \Rightarrow g^2 = 1$

but $|G|$ odd $\Rightarrow g = 1$