Solution

\( G \) is a finite group, \( \sigma \) an automorphism

\( \text{i.} \ \ \sigma(g) = g \iff g = 1 \)
\( \text{ii.} \ \ \sigma^2 = \text{ID}_G \)

Then \( G \) is abelian

**Claim**: Every element of \( G \) can be written

\[ g = x^{-1} \sigma(x) \]

If \( \text{consider } T : G \rightarrow G, \quad x \mapsto x^{-1} \sigma(x) \)

For \( x, y \in G \)

\[ T(x) = T(y) \]

\[ \iff x^{-1} \sigma(x) = y^{-1} \sigma(y) \]

\[ yx^{-1} = \sigma(y) \sigma(x)^{-1} \]

\[ = \sigma(yx^{-1}) \]

So \( yx^{-1} = 1 \implies x = y \) by \( \text{i.} \)

\( T \) injective, thus \( G \) finite \( \implies \) \( T \) surjective

**Claim**: \( \sigma(g) = g^{-1} \)

Note: \( \sigma(x^{-1} \sigma(x)) = \sigma(x^{-1}) x = (x^{-1} \sigma(x))^{-1} \)

**Claim** follows, since this is true of every element \( g \)

To finish, refer to the proof that \( G \) abelian \( \iff \) \( g \mapsto g^{-1} \) is a homomorphism.

\[ x^{-1} \sigma(x) \text{ is injective } \implies G \text{ finite } \implies x^{-1} \sigma(x) \text{ is surjective} \]

\[ \sigma(x^{-1} \sigma(x)) = \sigma(y^{-1} yx^{-1}) \implies xy^{-1} \sigma(x) = \sigma(y^{-1}) \sigma(y) \]

\[ \sigma(x^{-1} \sigma(x)) = \sigma(x^{-1}) x = (x^{-1} \sigma(x))^{-1} \implies \sigma: g \mapsto g^{-1} \]
§2.4 Let $G$ be a group

Recall $\langle A \rangle$ is a subgroup

$\times$ A subset of $G$
$\times$ $\langle A \rangle = \bigcap H$
$\qquad A \subseteq H \subseteq G$

Remark $\langle \emptyset \rangle = \langle e \rangle = \{e\}$

Since $\emptyset \subset \langle e \rangle \leq G$

Prop Assume $A$ nonempty subset of $G$

Let $\overline{A} = \left\{ a_1^{l_1} a_2^{l_2} \ldots a_n^{l_n} \mid a_1, a_2, \ldots, a_n \in A, \right. \left. l_1, l_2, \ldots \in \mathbb{Z} \right\}$

Then $\langle A \rangle = \overline{A}$

Proof

First $\overline{A} \subseteq G$

to show $A \subseteq \overline{A}$ so $\overline{A} \neq \emptyset$

Next, choose $a_1^{l_1} a_2^{l_2} \ldots a_m^{l_m}$ and $a_{m+1}^{l_{m+1}} \ldots a_n^{l_n}$

both in $\overline{A}$ for $l_1, \ldots, l_n \in \mathbb{Z}$ $a_1, \ldots, a_n \in A$

Then $a_1^{l_1} \ldots a_m^{l_m} \in \overline{A}$, so subgroup of $G$

$\overline{A} \triangleleft G$ so $\langle A \rangle \leq \overline{A}$

$\langle A \rangle$ is the minimal subgroup containing $A$.

$\overline{A} = \left\{ a_1^{l_1} a_2^{l_2} \ldots a_n^{l_n} \mid l_1, \ldots, l_n \in \mathbb{Z}, \right. \left. a_1^{l_1} a_2^{l_2} \ldots a_n^{l_n} \in A \right\}$.

Then $\overline{A} = \langle A \rangle$.
On the other hand if \( A \leq H \leq G \) then

\[
\bar{A} \leq H \quad \text{because} \quad H \text{ closed so}
\]

\[
\bar{A} \leq \bigcap H = \langle A \rangle
\]

**Examples**

1. Cyclic groups are

   \( G = \langle g \rangle \) for some \( g \in G \)

2. \( \mathbb{Q}^x = \langle \mathbb{Z} \setminus \{0\} \rangle \)

3. \( D_{2n} = \langle s, r \rangle \) where \( r \) is rotation, \( s \) reflection

**Finally generated**

Def. When \( G = \langle g_1, \ldots, g_n \rangle \) some \( g_1, \ldots, g_n \in G \)

we say \( G \) is **finally generated**

Some infinite groups are finally generated, e.g. \( \mathbb{Z} = \langle 1 \rangle \)

E.g. \( \mathbb{Q}^x \) is **not** finally generated

**Abelian simple**

Appendix: Additive Notation

\( G \) additive abelian groups

\( A \leq G \quad A \neq \emptyset \)

Then \( \langle A \rangle = \left\{ \sum_{i=1}^{n} l_i g_i \mid l_i \in \mathbb{Z} \right\} \)

further suppose \( G \) finally generated

\( G = \langle g_1, \ldots, g_n \rangle \) some \( g_1, \ldots, g_n \in G \)

Cyclic groups are generated from a single element

\( \mathbb{Q}^x = \langle \mathbb{Z} \setminus \{0\} \rangle \)

\( D_{2n} = \langle s, r \rangle \) where \( r, s \) appropriate rotations, reflections

If \( A \subseteq G \), an abelian additive group, \( \langle A \rangle = \left\{ \sum_{i=1}^{n} l_i a_i \mid l_i \in \mathbb{Z} \right\} \) in fixed order
L(G) set of subgroups

\[ G = \{ l_1 g_1, \ldots, l_m g_m \mid l_i, \ldots, l_m \in \mathbb{Z} \} \]

depends on being abelian

§ 2.5 Briefly

let \( G \) be a group

let \( L(G) = \{ H \mid H \leq G \} \)

let \( H, K \in L(G) \)

\[ \langle H \cup K \rangle = : \langle H, K \rangle \]

is the unique smallest (with inclusion) subgroup of \( G \) containing both \( H \) and \( K \)

Refer to \( \langle H, K \rangle \) as the JOIN of \( H \) and \( K \)

Also \( H \cap K \) is the largest subgroup of \( G \) contained within both \( H \) and \( K \), called the MEET of \( H \) and \( K \)

\( L(G) \) together with \( \cap \) and \( \cup \) is a LATTICE

Example \( \mathbb{Z}/12\mathbb{Z} \)

\[ \mathbb{Z}/12\mathbb{Z} = \langle 1 \rangle \]

"Lattice of subgroups of \( \mathbb{Z}/12\mathbb{Z} \)"

The set of all subgroups \( H \leq G \) is a lattice, with \( \langle H, K \rangle = \langle H \cup K \rangle \)

(minimal group containing both) the JOIN and \( H \cap K \) the MEET of \( H \) and \( K \)
CHAPTER 3

QUOTIENT GROUPS & HOMOMORPHISMS

G a group

Def i. H is a coset subgroup of G and \( g \in G \)
Then \( gH = \{ gh \mid heH \} \)

is the left LEFT COSET of H in G corresponding to \( g \) and

\( Hg = \{ hg \mid heH \} \) is the RIGHT COSET

An element of a (right or left) coset is called a REPRESENTATIVE of that coset

For each \( g \in G \), set

\( gNg^{-1} = \{ gng^{-1} \mid n \in N \} \)

Exercise \( gNg^{-1} \leq G \)

If \( gNg^{-1} = N \) for all \( g \in G \), we say \( N \) is NORMAL in \( G \)
and write \( N \trianglelefteq G \)

If \( H \leq G \) and \( g \in G \), then \( gH \) is the left coset of \( H \) wrt \( g \), and

\( Hg \) the right coset.

If \( gNg^{-1} = N \) for any \( g \in G \), then \( N \) is a normal subgroup of \( G \).
Lemma
A subgroup \( N \) is normal in \( G \) \( \iff \) \( gN = Ng \) for all \( g \in G \)

\[ \iff \]

Proof
\( \Rightarrow \) for all \( g \in G \)
\[ gN = g(g^{-1}Ng) = \{ gg^{-1}n \mid n \in N \} = Ng \]

\( \Leftarrow \) so \( gNg^{-1} = N \)
\[ gNg^{-1} = \{ hg^{-1} \mid h \in gN \} \]
\[ = \{ hg^{-1} \mid h \in Ng \} \]
\[ = \{ nng^{-1} \mid n \in N \} \]
\[ = N \]

Lemma
\( N \leq G \). Then \( N \trianglelefteq G \) \( \iff \) \( gNg^{-1} \subseteq N \) for all \( g \in G \)

Proof
\( \Leftarrow \) immediate
\[ gNg^{-1} \subseteq N \text{ for all } g \in G \text{ if also holds } g^{-1}Ng \subseteq N \text{ for all } g \in G \]
\[ \Rightarrow (gg^{-1})N(gg^{-1}) = g(g^{-1}N)g^{-1} \subseteq g^{-1}Ng \subseteq N \]
\[ \Rightarrow gNg^{-1} \subseteq N \]

We have two equivalent conditions for normality:
\[ \forall g \in G \quad gN = Ng \]
\[ gNg^{-1} \subseteq N \]
Lemma \( \forall N \leq G \) Then

\[ (gN)(hN) = \{ gnhn' \mid n, n' \in N \} \]

= \( (gh)N \)

conversely \( \forall N \leq H \leq G \) if \( \forall a,b \in G \)

(aH \times bH) = (ab)H \quad \text{then} \quad H \leq G

if \( gNg^{-1} \subseteq (gN)(g^{-1}N) \)

\[ \subseteq (gg^{-1}) \]

If for all \( g, h \in G \) then

\[ (gN \times hN) = \{ gnhn' \mid n, n' \in N \} \]

= \( \{ n(gh)n' \mid n, n' \in N \} \)

= \( \{ (gh)nN' \mid n, n' \in N \} \)

= \( \{ (gh)n \mid n \in N \} \)

= \( (gh)N \)

for converse, assume \( H \) has property \( (aH \times bH) = (ab)H \)

for all \( a, b \in G \) then for all \( g \in G \)

\[ gNg^{-1} \subseteq (gN)(g^{-1}N) = (gg')N = N \]
\[ a \quad \textit{a fortiori} \]

\[ a = x^{-1} \delta(x) \]