

1. Let G be a group. Let $M, N \trianglelefteq G$ with $M \cap N = \{1\}$.

Let $m \in M, n \in N$.

$$mnm^{-1}n^{-1} = (mnm^{-1})n^{-1} \in N \text{ since } N \trianglelefteq G$$

$$= m(nm^{-1}n^{-1}) \in M \text{ since } M \trianglelefteq G.$$

$$M \cap N = \{1\} \text{ so } mnm^{-1}n^{-1} = 1$$

$$mnm^{-1} = n$$

$$mn = nm$$

2. a) $f: \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ by $f([x]_2) = [x]_4$

$$[1]_2 = [3]_2, \quad f([1]_2) = [1]_4, \quad f([3]_2) = [3]_4$$

$[1]_4 \neq [3]_4$ so f is not well-defined.

b) Let $n \in \mathbb{Z}$,

$$\text{If } n = 4k \text{ then } n^2 = 16k^2 = 4m$$

$$\text{If } n = 4k+1 \text{ then } n^2 = 16k^2 + 8k + 1 = 4m+1$$

$$\text{If } n = 4k+2 \text{ then } n^2 = 16k^2 + 16k + 4 = 4m$$

$$\text{If } n = 4k+3 \text{ then } n^2 = 16k^2 + 24k + 9 = 4m+1$$

$$\text{If } [n]_2 = [0]_2 \text{ then } n = 4k \text{ or } 4k+2$$

$$\text{and } n^2 = 4m \text{ so } [n^2]_4 = [0]_4$$

$$\text{If } [n]_2 = [1]_2 \text{ then } n = 4k+1 \text{ or } 4k+3$$

$$\text{and } n^2 = 4m+1 \text{ so } [n^2]_4 = [1]_4$$

Thus g is well-defined.

Let $G \neq \{1\}$, $G = \langle a_1, \dots, a_n \rangle$

3. Let $\mathcal{L} = \{N \trianglelefteq G \mid N \neq G\}$

$\mathcal{L} \neq \emptyset$ since $\{1\} \trianglelefteq G$, $\{1\} \neq G$ so $\{1\} \in \mathcal{L}$

Let \mathcal{C} be a chain in \mathcal{L}

Let $H = \bigcup_{C \in \mathcal{C}} C$.

1) $H \trianglelefteq G$: $1 \in C \forall C \in \mathcal{C}$ so $1 \in H$ and $H \neq \emptyset$

Let $x, y \in H$. $\exists H_x, H_y \in \mathcal{C}$ st $x \in H_x, y \in H_y$.

\mathcal{C} is a chain so H_x and H_y are ordered.

Let $M = \max(H_x, H_y)$. Then $x, y \in M$, $xy^{-1} \in M$

$M \in \mathcal{C}$ so $xy^{-1} \in H = \bigcup C$.

Let $x \in H$, $g \in G$. $\exists H_x \in \mathcal{C}$, $x \in H_x$. $H_x \trianglelefteq G$ so $gxg^{-1} \in H_x$, $gxg^{-1} \in H$
and $H \trianglelefteq G$.

2) $H \neq G$. Suppose $H = G$. Then $\forall i = 1, \dots, n$

$\exists H_i \in \mathcal{C}$ st $a_i \in H_i$. \mathcal{C} is a chain so

H_1, \dots, H_n are ordered. Let H_k be the maximum of H_1, \dots, H_n . Then $H_i \subseteq H_k \forall i = 1, \dots, n$

so $a_i \in H_k$ for $i = 1, \dots, n$. Then $G = \langle a_1, \dots, a_n \rangle \subseteq H_k \subseteq G$

But $H_k \in \mathcal{C} \subseteq \mathcal{L} \Rightarrow H_k \neq G$. Contradiction.

Thus $H \neq G$.

By (1) & (2) $H \in \mathcal{L}$. Thus any chain \mathcal{C} in \mathcal{L} has an upper bound in \mathcal{L} .

By Zorn's Lemma, \mathcal{L} has a maximal element, i.e. $\exists M \in \mathcal{L}$ st $N \in \mathcal{L}$, $M \leq N \Rightarrow M = N$.

Thus $M \trianglelefteq G$ and $M \neq G$ and if $N \trianglelefteq G$, $N \neq G$, $M \leq N$ then $M = N$.

4. a) $\sigma_g(a) = ga \in A$ so $\sigma_g: A \rightarrow A$

$$\sigma_{g^{-1}} \circ \sigma_g(a) = g^{-1}(ga) = (g^{-1}g)a = 1a = a \quad \forall a \in A$$

$$\sigma_g \circ \sigma_{g^{-1}}(a) = g(g^{-1}a) = (gg^{-1})a = 1a = a \quad \forall a \in A$$

so $\sigma_{g^{-1}} \circ \sigma_g = 1_A = \sigma_g \circ \sigma_{g^{-1}}$ and σ_g is a permutation of A .

b) Let $\Sigma: G \rightarrow S_A$ be defined by $\Sigma(g) = \sigma_g$.

$$\begin{aligned} \Sigma(gh)(a) &= \sigma_{gh}(a) = gh a = g(ha) = \sigma_g(\sigma_h(a)) \\ &= \Sigma(g) \Sigma(h)(a) \end{aligned} \quad \forall a \in A$$

so $\Sigma(gh) = \Sigma(g) \Sigma(h)$ and Σ is a group homomorphism.

c) Let $|G| = 343 = 7^3$. I

Let G act on A with $|A| = 6$.

$\Sigma: G \rightarrow S_A$ defined by $\Sigma(g) = \sigma_g$

where $\sigma_g(a) = ga$ is a homomorphism by (b).

$$G/\ker \Sigma \cong \Sigma(G) \leq S_A$$

$$|\Sigma(G)| \mid |S_A| \quad |S_A| = 6! = 720$$

$$|G/\ker \Sigma| \mid |G|, \quad |G/\ker \Sigma| = |\Sigma(G)|$$

$$\text{So } |G/\ker \Sigma| \mid 343 \text{ \& } |G/\ker \Sigma| \mid 720$$

$$\text{GCD}(343, 720) = 1 \text{ so } |G/\ker \Sigma| = 1$$

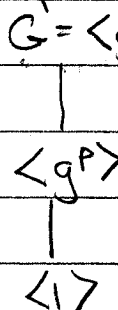
Thus $\ker \Sigma = G$, i.e. $\Sigma(g) = 1_A \quad \forall g \in G$

i.e. $ga = a \quad \forall g \in G, a \in A$.

5. Let p be prime. Let G be an abelian group with $|G| = p^2$. Then $\forall g \in G$

$|g| \mid p^2$, i.e., $|g| \in \{1, p, p^2\}$

If $\exists g' \in G$ st $|g'| = p^2$ then $G = \langle g' \rangle$ is cyclic and the lattice is:

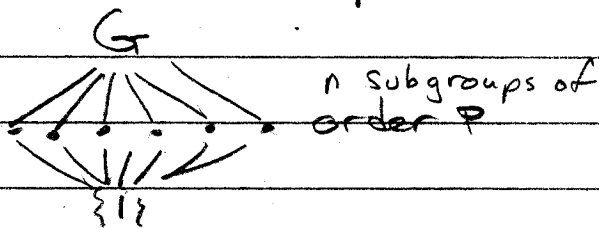


If $\nexists g \in G$ st $|g| = p^2$ then

$\forall g \in G$ st $g \neq 1$

$|g| = p$. Thus the subgroups of G are $\{1\}$, G , and cyclic groups of order p .

Thus the lattice of subgroups of G is:



The only remaining issue is the number n

of subgroups of order p . If $|a| = |b| = p$ then $\langle a \rangle \cap \langle b \rangle = \langle a \rangle$ or $\{1\}$. Each subgroup of order p has $p-1$ elements of order p and two are either the same or have distinct elements of order p .

$$|G| = \sum_{\substack{H \\ |H|=p}} |H| + |1| = n(p-1) + 1$$

$$p^2 - 1 = n(p-1) \quad |H|=p \quad \text{order } p \quad \text{order } 1$$