Math 71: Abstract Algebra

Prishita Dharampal

Credit Statement: Talked to Sair Shaikh'26, Jacob Lehmann Duke, Henry Dorr '28, Kason Sabazan-Chambers '28, Ali Azam '28, and Math Stack Exchange.

Problem 1. Let H be a subgroup of the group G.

1. Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.
2. Show that $H \leq C_G(H)$ if and only if H is abelian.

Solution.

1. The normalizer of H, $N_G(H)$ is defined as:

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

And a subgroup is closed under the group operation and inverses, so $\forall x, y \in H, H \leq G$, $xyx^{-1} \in H \implies \{x \in H \mid xHx^{-1} = H\} \implies H \leq N_G(H)$. This is not necessarily true for all subsets because they are not closed under the group operation and inverses. For instance, let $G = D_6$, $H = \{1, r, s\}$, then,

$$sHs^{-1} = \{1, r^5, s\} \neq H \implies H \not\leq N_G(H).$$

2. To prove

$$H \leq C_G(H) \iff gh = hg, \forall gh \in H$$

Assuming $H \leq C_G(H)$ ($\implies$)
Then for any $g, h \in H$, $ghg^{-1} = h \implies ghg^{-1}g = hg \implies gh = hg$. Thus H is abelian.
Assuming subgroup H is abelian ($\impliedby$).

$$\forall x, y \in H, xyx^{-1} = xx^{-1}y = y$$

By definition of centralizer of H,

$$C_G(H) = \{g \in G \mid ghg^{-1} = h\}$$

But all $x, y \in H$ are $x, y \in G$ (because $H \leq G$). So by definition, $H \leq C_G(H)$. Hence, $H \leq C_G(H)$ if and only if H is abelian.

Problem 2. Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \bar{1} \to x^a$ extend to an isomorphism from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}.

Solution.

$$\varphi_a : \mathbb{Z}/48\mathbb{Z} \to Z_{48}$$
$$\varphi_a : \bar{1} \to x^a$$

For φ_a to be an isomorphism, it has to be injective, surjective, and a homomorphism:

1. Injectivity:
   $\bar{1}$ is a generator of $\mathbb{Z}/48\mathbb{Z}$, i.e. $\bar{1}$ generates 48 elements in $\mathbb{Z}/48\mathbb{Z}$. So the mapping φ_a can only be injective if it maps to an element that generates 48 elements in Z_{48}, i.e, to all $x^a, Z_{48} = \langle x^a \rangle$ ($\mid Z_{48} \mid= 48$).
   To find generators of Z_n we need to find elements $x^a \in Z_n$ such that if $(x^a)^m \equiv 0 \pmod{x^n}$, $m = n$, where m is the order of the element and n is the order of the group. Let $d = gcd(a, n), a = da', n = dn'$. Lets find the order of x^a, by definition the order of an x^a, m is the smallest positive integer such that $(x^a)^m = 1$. We also know that the order of an element divides the order of the group.

   $$(x^a)^m = x^{am} = 1 \implies n \mid am \implies n' \mid a'm$$

   But since $gcd(a', n') = 1$,
   $$n' \mid m \implies m \geq n'$$
   But also,
   $$(x^a)^{n'} = x^{a'dn'} = x^{a'n} \implies n' \geq m$$
   $$m = n' \implies m = \frac{n}{gcd(n, a)}$$
   We can see that $m = n$ will only be true if $gcd(n, a) = 1$. Hence all x^a, where a is relatively prime to n are generators of Z_n.
   Thus, φ_a is an injective for all $x^a, gcd(a, 48) = 1$.

2. Homomorphism:
   For φ_a to be a homomorphism the following needs to be true:

   $$\varphi_a(xy) = \varphi(x)\varphi(y)$$

Z_{48} is a cyclic group, and all cyclic groups are abelian:

$$\begin{aligned}\varphi_a(xy) &= (xy)^a \\ &= \underbrace{(xy)(xy)...(xy)}_{a-times} \\ &= (x)^a(y)^a \\ &= x^a y^a \\ &= \varphi_a(x)\varphi_a(y)\end{aligned}$$

Hence, φ_a is a homomorphism.

3. The order of Z_{48} is 48, i.e. Z_{48} is finite. From (1) and (2) we know that φ_a is an injective homomorphism. And it is obvious that all injective homomorphism on finite groups are surjective.

Thus, the homomorphism $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to Z_{48}$ is injective and surjective for all $x^a \in Z_{48}$ such that $gcd(a, 48) = 1$.

Problem 3. Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 (\text{mod } p^n)$ but $(1+p)^{p^{n-2}} \not\equiv 1 (\text{mod } p^n)$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution.

1. Showing $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$:

   p prime, $p \neq 2$, $n \in \mathbb{Z}^+$. The binomial theorem says,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

   For $(1+p)^{p^{n-1}}$ this means,

$$(1+p)^{p^{n-1}} = \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} 1^{p^{n-1}-k} p^k$$

   We can see that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ using induction.
   Base case, $n = 1$.

$$(1+p)^{p^{1-1}} = (1+p)^{p^0} = 1+p$$

   And,

$$1+p \equiv 1 \pmod{p^1}$$

   Inductive hypothesis, assume that the claim holds for $n = k$,

$$(1+p)^{p^{k-1}} \equiv 1 \pmod{p^k} \iff (1+p)^{p^{k-1}} = 1 + ap^k$$

   where a is an integer. Then for the inductive case, $n = k+1$,

$$(1+p)^{p^{k+1-1}} = (1+p)^{p^k} = ((1+p)^{p^{k-1}})^p$$

   Substituting the inductive hypothesis,

$$\begin{aligned}(1+p)^{p^{k+1-1}} &= (1+ap^k)^p \\ &= 1 + \sum_{j=1}^{p} \binom{p}{j} (ap^k)^j\end{aligned}$$

But for $j = 1$, $\frac{p!}{(p-1)!1!} ap^k = ap^{k+1}$, then we can say that,

$$\begin{aligned}(1+p)^{p^{k+1-1}} &= 1 + ap^{k+1} + \sum_{j=2}^{p} \binom{p}{j} (ap^k)^j \\ &= 1 + ap^{k+1} + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj}\end{aligned}$$

Because $j \geq 2$, we can factor out p^{k+1} from all terms in the summation,

$$(1+p)^{p^{k+1-1}} = 1 + ap^{k+1}(1 + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj-k-1})$$

$$1 + ap^{k+1}(1 + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj-k-1}) \equiv 1 \pmod{p^{k+1}}$$

Hence, $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ holds for all $n \geq 1$.

2. Showing $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$:
   To show this, we can induct with a stronger condition, $p \nmid a$. Checking this condition for the base case:
   Base case, n =1.
   From part 1 we know that $(1+p)^{p^{n-1}} = 1 + ap^n$,

$$(1+p)^{p^0} = (1+p)^1 = 1 + ap^n = 1 + 1 \cdot p^1 \implies p \nmid 1 \implies p \nmid a$$

Assuming that this condition holds for the inductive hypothesis,

$$(1+p)^{p^{k-1}} \equiv 1 \pmod{p^k} \iff (1+p)^{p^{k-1}} = 1 + ap^k \iff p \nmid a$$

Then for the inductive case, $n = k+1$,

$$(1+p)^{p^k} \equiv 1 \pmod{p^{k+1}} \iff (1+p)^{p^k} = 1 + ap^{k+1}$$

$$\begin{aligned}(1+p)^{p^{k-1}} &= 1 + ap^{k+1} = (1+ap^k)^p \\ &= 1 + ap^{k+1}\left(1 + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj-k-1}\right)\end{aligned}$$

We want to show that $p \nmid a\left(1 + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj-k-1}\right)$

(i dont know why the summation notation is rendering weirdly, sorry!)

We already know that $p \nmid a$ from the inductive hypothesis.
Let $x = \left(1 + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj-k-1}\right)$ For $2 \leq j \leq p$, the terms look like $\binom{p}{j} a^j p^{kj-k-1}$, where $p^{kj-k-1} \geq p$, so p divides the term, i.e. $x = 1 + gp$, for some $g \in \mathbb{Z}$.

$$\implies p \nmid x \implies p \nmid a \left(1 + \sum_{j=2}^{p} \binom{p}{j} a^j p^{kj-k-1}\right)$$

So the induction hypothesis holds.
We know that $(1+p)^{n-2} = 1 + ap^{n-1} \equiv 1 \pmod{p^{n-1}}$.
If $(1+p)^{n-2} \equiv 1 \pmod{p^n}$ then,
$(1+p)^{n-2} \equiv 1 \pmod{p^n} \iff 1 + ap^{n-1} \equiv 1 \pmod{p^n} \iff ap^{n-1} \equiv 0 \pmod{p^n}$
But $p \nmid a$, and $p^n \nmid p^{n-1}$, so
$(1+p)^{n-2} \not\equiv 1 \pmod{p^n} \iff 1 + ap^{n-1} \not\equiv 1 \pmod{p^n} \iff ap^{n-1} \not\equiv 0 \pmod{p^n}$

3. For the order of $(1+p) \in (\mathbb{Z}/p^n\mathbb{Z})^{\times}$,
From the last subpart, we can see that because $p \nmid a$, and for any integer k p is raised to, $(1+p)^{p^k}$ we can only factor out $ap^k + 1$ from the summation. So if $k < n-1$, $ap^{k+1} < p^n \implies p^n \nmid ap^{k+1} \implies (1+p)^{p^{k-1}} \not\equiv 1 \pmod{p^n}$. So the smallest integer x for which $(1+p)^x \equiv 1 \pmod{p^n}$ is p^{n-1}.

Problem 4. Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \text{ by } \sigma_a(x) = x^a \text{ for all } x \in Z_n$$

1. Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).
2. Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.
3. Prove that every automorphism of Z_n is equal to σ_a for some integer a.
4. Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\bar{a} \to \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $Aut(Z_n)$ is an abelian group of order $\varphi(n)$).

Solution.

1. To show that σ_a is an automorphism on Z_n, we need to show that σ_a is an injective or surjective homomorphism from $Z_n \to Z_n$:
   (a) Homomorphism:
   $\forall x, y \in Z_n$,
   $$\begin{aligned} \sigma_a(xy) &= (xy)^a \\ &= x^a y^a \qquad \text{(cyclic groups are abelian)} \\ &= \sigma_a(x)\sigma_a(y) \end{aligned}$$
   Hence, σ_a is a homomorphism from $Z_n \to Z_n$.
   (b) Surjectivity:
   Let $x^a \in Z_n$, we know that the $\mid x \mid = n \implies \mid x^a \mid = \frac{n}{gcd(n,a)} = k, k \leq n$. We also know that $Z_n = \langle x \rangle$, where elements of Z_n are generated by the first n powers of x. Under the homomorphism, this would look like the first n powers of x^a. If $gcd(a, n) \neq 1$, then $\exists k < n : \mid x^a \mid = k$, i.e.,
   $$\sigma_a(x^0) \to (x^0)^a = e$$
   $$\sigma_a(x^k) \to (x^k)^a = e$$
   Thus, the kernel of σ_a is not trivial if $gcd(a, n) \neq 1$, and hence σ_a is not surjective. But if $gcd(a, n) = 1$, then it is easy to see that $\nexists k < n, (x^a)^k = e$. Or, the kernel of σ_a is trivial and σ_a is surjective.

   All surjective homomorphisms are injective. Thus,σ_a is an automorphism of Z_n if and only if $gcd(a, n) = 1$.

2. Assuming $a \not\equiv b \pmod{n}$ ($\implies$):

$$\begin{aligned}
&a \equiv b \pmod{n} \\
&\implies a = nk + p \\
&\implies b = nm + q \\
\text{where } p \neq q& \\
&\implies \sigma_a(x) = x^a = x^{nk+p} = x^{nk}x^p = x^p \\
&\implies \sigma_b(x) = x^b = x^{nm+q} = x^{nm}x^q = x^q \\
&\implies \sigma_a(x) \neq \sigma_b(x)
\end{aligned}$$

Assuming $a \equiv b \pmod{n}$ ($\impliedby$):

$$\begin{aligned}
&a \equiv b \pmod{n} \\
&\implies a = nk + p \\
&\implies b = nm + p \\
&\implies \sigma_a(x) = x^a = x^{nk+p} = x^{nk}x^p = x^p \\
&\implies \sigma_b(x) = x^b = x^{nm+p} = x^{nm}x^p = x^p \\
&\implies \sigma_a(x) = \sigma_b(x)
\end{aligned}$$

Thus, $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.

3. All automorphisms of Z_n are isomorphisms from Z_n to itself. Because isomorphisms are surjective, we need to map x to an $x^a \in Z_n$ such that $Z_n = \langle x \rangle = \langle x^a \rangle$. But we know that, for all x^a in Z_n, x^a is a positive integer power of x. Thus, $\exists a, 0 < a \leq n$, for all automorphic maps σ_a.

4. Proving $\sigma_a \circ \sigma_b(x) = \sigma_{ab}(x)$:

$$\begin{aligned}
\sigma_a \circ \sigma_b(x) &= \sigma_a(\sigma_b(x)) \\
&= \sigma_a(x^b) \\
&= (x^b)^a = x^{ba} = x^{ab} \text{ (cyclic groups are abelian)} \\
&= \sigma_{ab}(x)
\end{aligned}$$

Hence $\sigma_a \circ \sigma_b(x) = \sigma_{ab}(x)$.
Define the map $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to Aut(Z_n)$ such that $\varphi(\bar{a}) = \sigma_a$. To show that φ is an isomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ to $Aut(Z_n)$ we need to show that it is an injective or surjective homomorphism (since all injective homomorphisms on cyclic groups are surjective and vice versa.):

(a) Homomorphism:
Using what we just proved,

$$\varphi(\bar{a}\bar{b}) = \sigma_{ab} = \sigma_a \circ \sigma_b = \varphi(\bar{a}) \circ \varphi(\bar{b})$$

Thus, φ is a homomorphism.

(b) Surjectivity:
From (1) we know that σ_a is an automorphism of Z_n only if $gcd(a, n) = 1$, and from (3) we know that there exists an a for all σ_a in $Aut(Z_n)$. From (2) we know that $\sigma_a = \sigma_b$ if $a \equiv b \pmod{n}$. Hence there are a finite number of $a \leq n, gcd(a, n) = 1$ that represent all automorphisms of Z_n. The group $(\mathbb{Z}/n\mathbb{Z})^{\times}$ by definition is the group of all $a \leq n$ such that $gcd(a, n) = 1$, i.e φ is surjective.

(c) Injectivity:
Again from (2) we know that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$. Then for $a, b \leq n$, $\sigma_a \neq \sigma_b$. Thus φ is injective.

Thus, the map $\bar{a} \to \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ onto the automorphism group of Z_n. Because $Aut(Z_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\times}$ it has the same properties as $(\mathbb{Z}/n\mathbb{Z})^{\times}$. So we can say that $Aut(Z_n)$ is abelian and has order $\varphi(n)$.

Problem 5. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2].

Solution.

Consider the element $2^n - 1 \in (\mathbb{Z}/n\mathbb{Z})^\times$:

$$(2^n - 1)^2 = (2^n)^2 - 2.2^n + 1 = 2^n 2^n - 2^n 2 + 1$$

Taking mod 2^n,

$$(2^n - 1)^2 \equiv 0 - 0 + 1 \equiv 1 \pmod{2^n}$$

The elements $\{1, 2^n - 1\}$ form a subgroup (closed under inverses $(2^n - 1)^{-1} = 2^n - 1$ and multiplication $(2^n - 1)^m$ results in either 1 or $2^n - 1$) of order 2.

Now consider the element $2^{n-1} - 1 \in (\mathbb{Z}/n\mathbb{Z})^\times$:

$$(2^{n-1} - 1)^2 = (2^{n-1})^2 - 2.2^{n-1} + 1 = 2^n 2^n 2^{-2} - 2^n + 1$$

Taking mod 2^n,

$$(2^{n-1} - 1)^2 \equiv 0 - 0 + 1 \equiv 1 \pmod{2^n}$$

The elements $\{1, 2^{n-1} - 1\}$ also form a subgroup (closed under inverses $(2^{n-1} - 1)^{-1} = 2^{n-1} - 1$ and multiplication $(2^{n-1} - 1)^m$ results in either 1 or $2^{n-1} - 1$) of order 2.

By theorem 7, we know that for every a dividing the order of the group, there exists a unique subgroup of order a, but we have at least 2 subgroups in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ of order 2 (order of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is $2^n/2 = 2^{n-1}$, which is divisible by 2) which means that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ for $n \geq 3$ is not cyclic.

Problem 6. Prove that the subgroup of S_4 generated by (12) and (12)(34) is a noncyclic group of order 4. (Show that it is isomorphic to Klein Four).

Solution.

Let A be the subgroup generated by (12) and (12)(34) Define a map $\varphi : V_4 \to A$ such that:

1. $\varphi(e) = e$
2. $\varphi(a) = (12)$
3. $\varphi(b) = (12)(34)$

To see if this is an homomorphism we check the relations in the presentation of Klein Four (V_4) and see if they hold:

$$V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$$

1. $a^2 = b^2 = e$
   $a^2 \implies (12)(12) = (1)(2) = e \implies |\ (12)\ |= 2$
   $b^2 \implies (12)(34)(12)(34) = (1)(2)(3)(4) = e \implies |\ (12)(34)\ |= 2$
   $\implies ((12))^2 = ((12)(34))^2 = e$

2. $ab = ba$
   $(12)(12)(34) = (34)$
   $(12)(34)(12) = (34)$
   $\implies (12)(34)(12) = (12)(12)(34)$

The relations of V_4 hold in A, so φ is a homomorphism. The distinct elements in A are generated by the generators raised to powers 1 and 0 (both the generators have order 2). Let $x = (12), y = (12)(34)$:

1. $x^0y^0 = x^2y^2 = x^0y^2 = x^2y^0 = e$
2. $x^1y^0 = (12)$
3. $x^0y^1 = (12)(34)$
4. $x^1y^1 = (12)(34)(12) = (34)$

Hence, $|\ A\ |= 4$. Also, φ is a surjective homomorphism from a group of order 4 to a subgroup of order 4, and hence is an isomorphism. And because there exist 3 elements of A with order two, it is not cyclic.

Problem 7. Prove that the subgroup of S_4 generated by (12) and (13)(24) is isomorphic to the dihedral group of order 8.

Solution.

Let A be the subgroup generated by $(12), (13)(24)$, and let $a = (12)$, $b = (13)(24)$, and $c = ab = (1324)$. The order of these elements is $2, 2, 4$ respectively (order of disjoint m-cycles is equal to the lcm of their lengths).
Then we can write a partial presentation of A as follows:

$$A = \langle a, c \mid a^2 = c^4 = e \rangle$$

This looks awfully similar to the presentation of D_8.

$$D_8 = \langle s, r \mid s^2 = r^4 = e, rs = sr^{-1} \rangle$$

If we can show that the relation $rs = sr^{-1}$ holds in A for a, c, we can define a homomorphism between the two. Checking,
$ac^{-1} = (12)(4231) = (14)(23)$, and $ca = (1324)(12) = (14)(23) \implies ca = ac^{-1}$.
The relation holds.

$$A = \langle a, c \mid a^2 = c^4 = e, ca = ac^{-1} \rangle$$

Now we can define $\varphi : D_8 \to A$, such that $\varphi(s) = a, \varphi(r) = b \implies$ we can map the generators of D_8 to the generators of A, this gives us a surjective homomorphism (any product of s, r is the image of the corresponding product of a, c).

Elements in A look like $a^x c^y, x = 0, 1$ and $y = 0, 1, 2, 3$. There are 8 such combinations, $A = \{e, a, ac, ac^2, ac^3, c, c^2, c^3\} \implies \mid A \mid = 8$. We also know that the order of D_8 is 8. A surjective homomorphism between groups of the same order is also injective. Hence, the subgroup A is isomorphic to D_8.

Problem 8. A group H is called finitely generated if there is a finite set A such that $H = \langle A \rangle$.

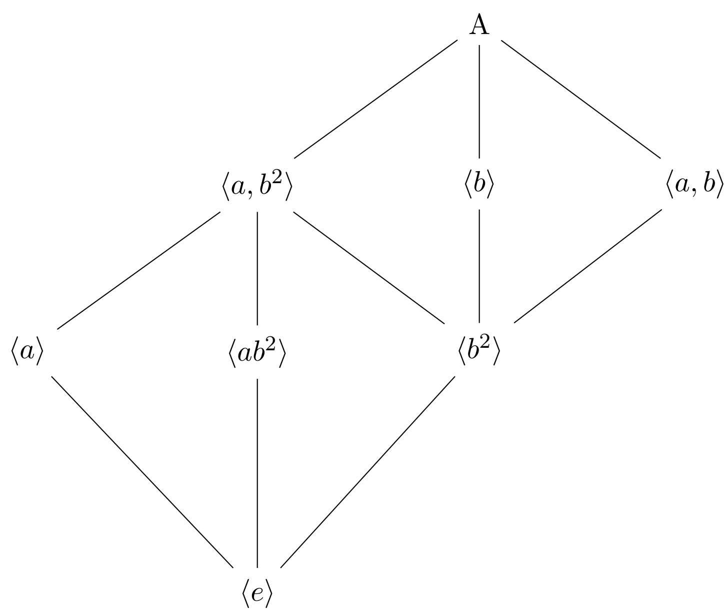
1. Prove that every finite group is finitely generated.
2. Prove that $\mathbb{Z}$ is finitely generated.
3. Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$, where k is the product of all the denominators which appear in a set of generators for H.]
4. Prove that $\mathbb{Q}$ is not finitely generated

Solution.

1. If G is a finite group that acts over the finite set H, then by definition we can generate the finite group from the set H.
$$G = \langle H \rangle$$
2. $\mathbb{Z}$ is a cyclic group of infinite order generated by $\mathbb{Z} = \langle 1 \rangle$,
i.e. $\forall n \in \mathbb{Z}, n = \underbrace{1 + 1 + \ldots + 1}_{n-times} = n * 1$
3. Let A be any finitely generated subgroup of the additive group $\mathbb{Q}$, then we can represent A as:
$$A = \left\langle \frac{a_1}{d_1}, \frac{a_2}{d_2}, \ldots, \frac{a_m}{d_m} \right\rangle$$
Where $\frac{a_1}{d_1}, \frac{a_2}{d_2}, \ldots, \frac{a_m}{d_m}$ are generators of A in their lowest forms. Then we can find a fraction $\frac{1}{q}$ such that $q = lcm(d_1, d_2, \ldots, d_m)$. Let this be a generator for a subgroup B of $\mathbb{Q}$: $B = \left\langle \frac{1}{q} \right\rangle$ Because q is a multiple of any product of the denominators of A we can multiply an integer n such that $\frac{n}{q} = \frac{a}{d}$ for any element in A. So we can say that $A \subseteq B$. We also know (from the question) that A is a finitely generated subgroup, we know that A is closed under multiplication and inverses. Then, $A \leq B$, and all subgroups of cyclic groups are cyclic. Hence, every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.
4. Assume $\mathbb{Q}$ is finitely generated, then it must be finitely cyclically generated according to part 3. Let $\mathbb{Q} = \left\langle \frac{p}{q} \right\rangle$ for some relatively prime p, q. Since $\frac{p}{q}$ is a generator, there must exist an x, such that $x\frac{p}{q} = \frac{1}{r}$ for some r that is relatively prime to q. Then, $q = xpr \implies r \mid q$. This contradicts our original assumption that r, q are co-prime, and hence shows that $\mathbb{Q}$ cannot be finitely generated.

Problem 9. The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$ has order 8 and has three subgroups of order $4 : \langle a, b^2 \rangle \cong V_4, \langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.

Solution.



Problem 10. Let M be the group of order 16 with the following presentation:

$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5\rangle$$

(sometimes called the modular group of order 16). It has three subgroups of order 8: $\langle u, v^2\rangle, \langle v\rangle$, and $\langle uv\rangle$ and every proper subgroup is contained in one of these three. Prove that $\langle u, v^2\rangle \cong Z_2 \times Z_4, \langle v\rangle \cong Z_8$ and $\langle uv\rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

Solution.

1. $\langle v\rangle \cong Z_8$
   Z_8 and $\langle v\rangle$ are both cyclic group of order 8 (from question). And we know that all cyclic groups of the same order are isomorphic (Theorem 7). So we can say, $\langle v\rangle \cong Z_8$.

2. $\langle uv\rangle \cong Z_8$
   Similar to the case above, we know that $\mid \langle uv\rangle \mid= 8 =\mid Z_8 \mid$. And from Theorem 7, we can say that $\langle uv\rangle \cong Z_8$.

3. $\langle u, v^2\rangle \cong Z_2 \times Z_4$
   Let x be the generator of the cyclic group Z_2, and y be the generator of Z_4, then elements in $Z_2 \times Z_4$ look like (x^a, y^b), where $a \in \{0, 1\}, b \in \{0, 1, 2, 3\}$. Then we can define a map $\varphi : Z_2 \times Z_4 \to \langle u, v^2\rangle$ such that $\varphi((x^a, y^b) = u^a(v^2)^b$. Then to check if φ is a homomorphism, we take any $(x^a, y^b), (x^c, y^d) \in Z_2 \times Z_4$ and map them.

   $$\varphi((x^a, y^b) \cdot (x^c, y^d)) = \varphi((x^{a+c}, y^{b+d})) = u^{a+c}(v^2)^{b+d}$$

   Checking if u, v^2 commute,

   $$vu = uv^5 \implies vvu = vuv^5 \implies v^2u = uv^5v^5 = uv^{10} = uv^2 \implies v^2u = uv^2$$

   They do! The subgroup $\langle u, v^2\rangle$ is abelian. Going back to proving the homomorphism.

   $$\begin{aligned}\varphi((x^a, y^b) \cdot (x^c, y^d)) &= u^{a+c}(v^2)^{b+d}\\ &= u^a u^c(v^2)^b(v^2)^d\\ &= u^a(v^2)^b u^c(v^2)^d\\ &= (u^a(v^2)^b)(u^c(v^2)^d)\\ &= \varphi((x^a, y^b))\varphi((x^c, y^d))\end{aligned}$$

   Thus, the map φ is homomorphic. The kernel of φ is,

   $$ker(\varphi) = \{(x^a, y^b) \mid u^a(v^2)^b = 1\}$$

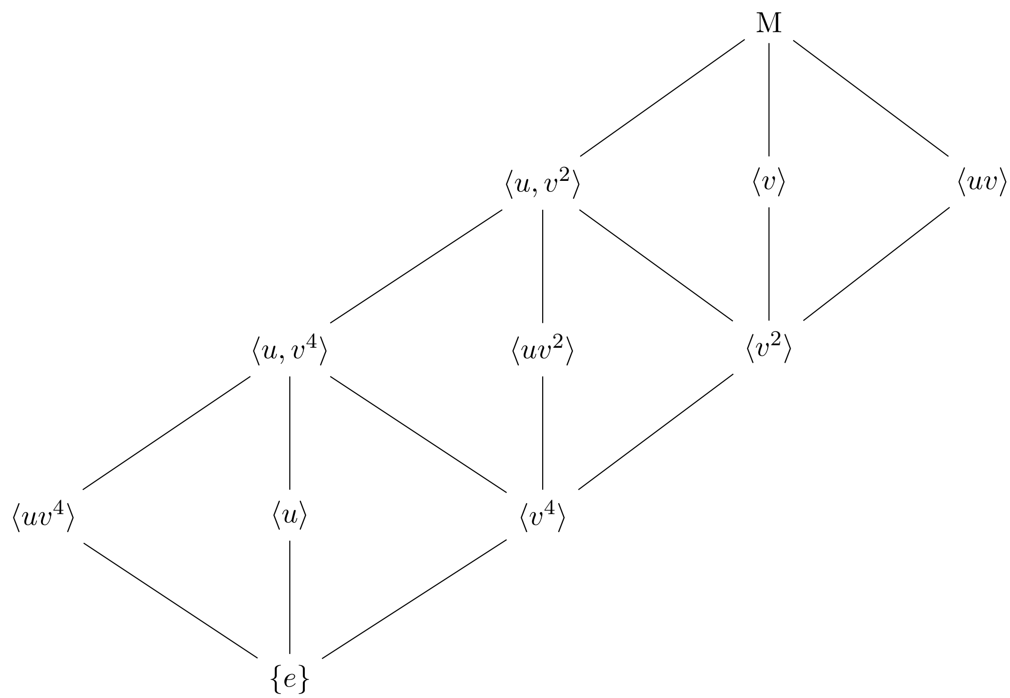
   Checking cases:

(a) $a = 0 \implies v^{2b} = 1 \implies 2b = 8 \implies b = 4 \implies b \equiv 0 \pmod 4$.

(b) $a = 1 \implies u(v^2)^b = 1 \implies u = (v^2)^{-b} \implies 1 = u^2 = (v^2)^{-2b}$ But order of v^2 cannot be negative, and neither can b (by definition), so this case is not feasible.

Hence, the kernel is trivial $\iff$ the map is injective. But we also know that $\mid \langle u, v^2 \rangle \mid = \mid Z_2 \times Z_4 \mid = 8$. Injective homomorphism between groups of equal order is surjective. Hence, φ is an isomorphism.

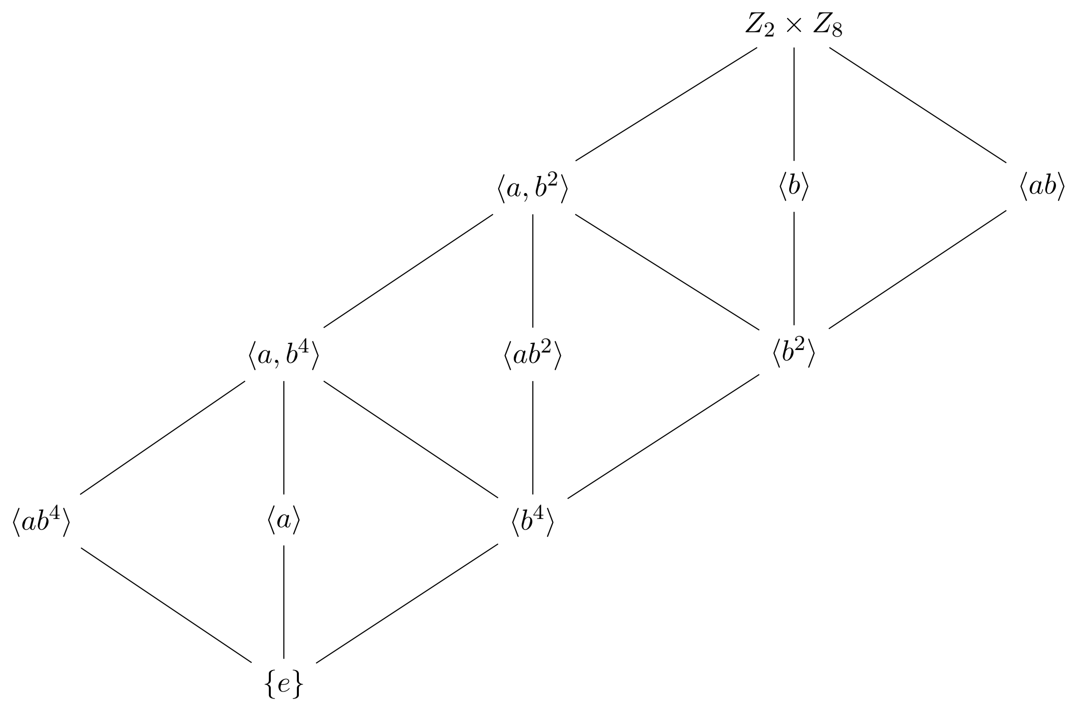
4. $M = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$



Lattice of M

For $Z_2 \times Z_8$, let $a = (1, 0)$ and $b = (0, 1)$ be the generators (Z_2, Z_8 are cyclic groups, so elements co-prime with the order of the group can act as generators) of the group. Then,

$$Z_2 \times Z_8 = \langle a, b \mid a^2 = b^8 = 0, ab = ba \rangle$$



Lattice of $Z_2 \times Z_8$

From presentation of the groups, we know that M is not abelian, where as $Z_2 \times Z_8$ is, so the two groups cannot be isomorphic.

Problem 11. Prove Euler's Theorem: If a and n are relatively prime integers, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. Hint. Use Lagrange's theorem on the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Solution.

We know that the order of $\mid (\mathbb{Z}/n\mathbb{Z})^\times \mid = \varphi(n)$, we also know that $gcd(a, n) = 1 \implies a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then by Lagrange's Theorem, $|\langle a \rangle| \Big| |(\mathbb{Z}/n\mathbb{Z})^\times|$.

We also know that $|a| \Big| |\langle a \rangle| \implies |a| \Big| |(\mathbb{Z}/n\mathbb{Z})^\times| \implies |a| \Big| |\varphi(n)|$. a raised to any multiple of its order will also give the identity $\implies a^{\varphi(n)} \equiv 1 \pmod{n}$.

Problem 12. Show that for all $n, m \geq 1$, the group S_{n+m} contains a subgroup isomorphic to $S_n \times S_m$. Conclude that $n!m!$ divides $(n+m)!$.

Solution.

Let A be the set that S_{n+m} acts on, $A = \{1, \ldots, n, n+1, \ldots, m\}$. Then we can partition A into two disjoint sets, $B = \{1, \ldots, n\}, C = \{n+1, \ldots, m\}$, with n and m elements respectively. Also, S_n acts on a set with n elements and S_m acts on a set with m elements. We can then define a map $\varphi : S_n \times S_m \to S_{n+m}$ such that

$$\varphi((\sigma, e)) = \alpha(1 \ldots n)$$
$$\varphi((e, \tau)) = \alpha(n+1 \ldots m)$$

, where σ is any permutation in S_n, τ is any permutation in S_m, and α is any permutation in S_{n+m}. To show that φ is a homomorphism we need to show that

$$\varphi((\sigma_1, \tau_1)(\sigma_2, \tau_2)) = \varphi((\sigma_1, \tau_1))\varphi((\sigma_2, \tau_2))$$

$$\begin{aligned}
\varphi((\sigma_1, \tau_1)(\sigma_2, \tau_2)) &= \varphi((\sigma_1\sigma_2)(\tau_1\tau_2)) \\
&= \alpha_1(1 \ldots n)\alpha_2(1 \ldots n)\alpha_1(n+1 \ldots m)\alpha_2(n+1 \ldots m) \\
&= \alpha_1(1 \ldots n)\alpha_1(n+1 \ldots m)\alpha_2(1 \ldots n)\alpha_2(n+1 \ldots m) \text{ (disjoint cycles commute)} \\
&= \varphi((\sigma_1, \tau_1))\varphi((\sigma_2, \tau_2))
\end{aligned}$$

φ is a homomorphism, and there exists a subgroup in S_{n+m} that φ maps onto. $ker(\varphi) = \{(\sigma, \tau) | \varphi(\sigma, \tau) = e\}$ When $\varphi(\sigma, \tau) = e$ the elements in the cycle stay constant, but since σ and τ are disjoint cycles $\varphi(\sigma, \tau) = \varphi(\sigma, e)\varphi(e, \tau)$ i.e when the $\{1 \ldots n\}$ elements are constant and $\{n+1 \ldots m\}$ elements are constant. So, $\varphi(\sigma, \tau) = e \iff \sigma = e, \tau = e$. Hence, the kernel is trivial, and the homomorphism φ is injective.
All maps are surjective onto their images (by definition). Hence, φ is an isomorphism and we can say that S_{n+m} contains a subgroup isomorphic to $S_n \times S_m$.
$| S_{n+m} | = (n+m)!$, $| S_n \times S_m | = n!m!$, and let Z be the subgroup in S_{n+m} it is isomorphic to. Then by Lagrange's Theorem, $| Z | \Big| \, | S_{n+m} | \implies n!m! \mid (n+m)!$.

Problem 13. Tricks with Euler's theorem. You can only use pencil and paper!

1. Prove that every element of $(\mathbb{Z}/72\mathbb{Z})^\times$ has order dividing 12. (Hint: This is better than what a straight application of Euler's theorem will give you! Try applying Euler's theorem to a pair of relatively prime divisors of 72.)

2. Prove that if n is a positive integer, then n and n^5 have the same last digit. Now Google "Fifth root trick" and watch the Numberphile video.

3. Find the last two digits of the huge number $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ where there are 2025 threes appearing! (Hint: Do nested applications of Euler's theorem.)

Solution.

1. We know the following 2 properties of Euler's totient function:

$$\varphi(ab) = \varphi(a)\varphi(b), (a, b) = 1$$

$$\varphi(p^x) = (p^{x-1})(p-1)$$

   Then we can write $\varphi(72) = \varphi(9)\varphi(8)$. $\varphi(9) = \varphi(3^2) = 3(2) = 6$, and $\varphi(8) = \varphi(2^3) = 4(1) = 4$.

$$\varphi(72) = \varphi(8)\varphi(9) = 6 \cdot 4 = 24$$

   From Problem 11 and the statements above, we know that $\forall a \in (\mathbb{Z}/72\mathbb{Z})^\times$, $a^{\varphi(9)} \equiv 1 \pmod 9 \implies a^6 \equiv 1 \pmod 9$, and $a^{\varphi(8)} \equiv 1 \pmod 8 \implies a^4 \equiv 1 \pmod 8$. Then the following is also trivially true,

$$(a^4)^3 = a^{12} \equiv 1 \pmod 8 \qquad (a^6)^2 = a^{12} \equiv 1 \pmod 8$$

   But if something is equivalent to 1 (mod 8), and (mod 9), then it is equivalent to 1 (mod 72) because $8, 9$ are coprime and $8 \cdot 9 = 72$.

$$a^{12} \equiv 1 \pmod{72}$$

2. The last digit of n^5 is $n^5 \pmod{10}$. We need to show that $n^5 \equiv n \pmod{10}$. Using part 1, we can equivalently show $n^5 \equiv n \pmod 5$ and $n^5 \equiv n \pmod 2$.

   (a) $n^5 \equiv n \pmod 2$
   If $n \equiv 1 \pmod 2$, then $n^5 \equiv 1 \pmod 2$ (all powers of an odd number are odd.

$$\implies n^5 \equiv n \pmod 2$$

   If $n \equiv 0 \pmod 2$, then $n^5 \equiv 0 \pmod 2$ (all powers of an even number are even.

$$\implies n^5 \equiv n \pmod 2$$

(b) $n^5 \equiv n \pmod 5$
$\varphi(5) = 4 \implies a^4 \equiv 1 \pmod 5$

$$\begin{aligned} n^5 &\equiv n \pmod 5 \\ n^4 n &\equiv n \pmod 5 \\ n &\equiv n (\text{mod } 5) \end{aligned}$$

So, $n^5 \equiv n \pmod 2$ and $n^5 \equiv n \pmod 5 \implies n^5 \equiv n \pmod{10}$. Hence, n and n^5 have the same last digit.

3. The last two digits of $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ is $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}} \pmod{100}$. Let $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$, where there are 2025 3s, be P.

$$\varphi(100) = 40 \text{ so } 3^{P \text{ (mod 40)}} \equiv 1$$

Let $P \pmod{40} = Q$. Using the $\varphi(100) = 40, \varphi(40) = 16, \varphi(16) = 8, \varphi(8) = 4, \varphi(4) = 2, \varphi(2) = 1$,

$$\begin{aligned} Q &\equiv Q_1 \pmod{16} \\ Q_1 \pmod{16} &\equiv Q_2 \pmod 8 \\ Q_2 \pmod 8 &\equiv Q_3 \pmod 4 \\ Q_3 \pmod 4 &\equiv Q_4 \pmod 2 \end{aligned}$$

$$\begin{aligned} 3 \pmod 2 &\equiv 1 = Q_4 \\ 3^{Q_4} \pmod 4 = 3^1 \pmod 4 &\equiv 3 = Q_3 \\ 3^{Q_3} \pmod 8 = 3^3 \pmod 8 &\equiv 3 = Q_2 \\ 3^{Q_2} \pmod{16} = 3^3 \pmod{16} &\equiv 11 = Q_1 \end{aligned}$$

We know $3^4 = 81 \equiv 1 \pmod{40}$

$$\begin{aligned} 3^{Q_1} \pmod{40} &= 3^{11} \pmod{40} = 3^3 \equiv 27 = Q \\ 3^Q \pmod{100} &= 3^{27} \pmod{100} \end{aligned}$$

$$\begin{aligned} &3^5 = 243 \equiv 43 \pmod{100} \\ &3^{10} \equiv (43)^2 \pmod{100} \equiv 1849 \pmod{100} \equiv 49 \pmod{100} \\ &3^{20} \equiv (49)^2 \pmod{100} \equiv 2401 \pmod{100} \equiv 01 \pmod{100} \\ \implies &3^{27} = 3^{20}3^5 3^2 = 1 \cdot 43 \cdot 9 = 387 \equiv 87 \pmod{100} \end{aligned}$$

Last two digits of $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ are 87.