Practice Midterm

Michael Pham

Fall 2024

Problems

0 Problem 0

Problem 0.1. Give a definition of a group.

Solution. We define a group $(G, *)$ to be a set G with binary operation $* : G \times G \to G$ which satisfies the following:

1. Identity: $\exists e_G \in G$ such that $\forall g \in G, e_G * g = g = g * e_G$.
2. Inverse: $\forall g \in G, \exists g^{-1} \in G$ such that $g * g^{-1} = e_G = g^{-1} * g$.
3. Associativity: $\forall a, b, c \in G$, we have that $a * (b * c) = (a * b) * c$.

■

Problem 0.2. Let G be a group. What is $|G|$? Give an example of G and its $|G|$.

Solution. For a group G, we say that $|G|$ is its order. That is, how many elements is in G. For example, let $G = \mathbb{Z}/2\mathbb{Z}$. Then, we see that $|G| = 2$. ■

Problem 0.3. Give a definition and example of a cyclic group.

Solution. For a group G, we say that G is cyclic if there exists some element $g \in G$ such that $\{g^k : k \in \mathbb{Z}\} = G$. An example would be $G = \mathbb{Z}/2\mathbb{Z}$. ■

1 Problem 1A

Problem 1.1. Compute the order of permutation $(1\,5\,2) = (1\,5\,2)(3)(4) \in S_5$ written in cyclic notation.

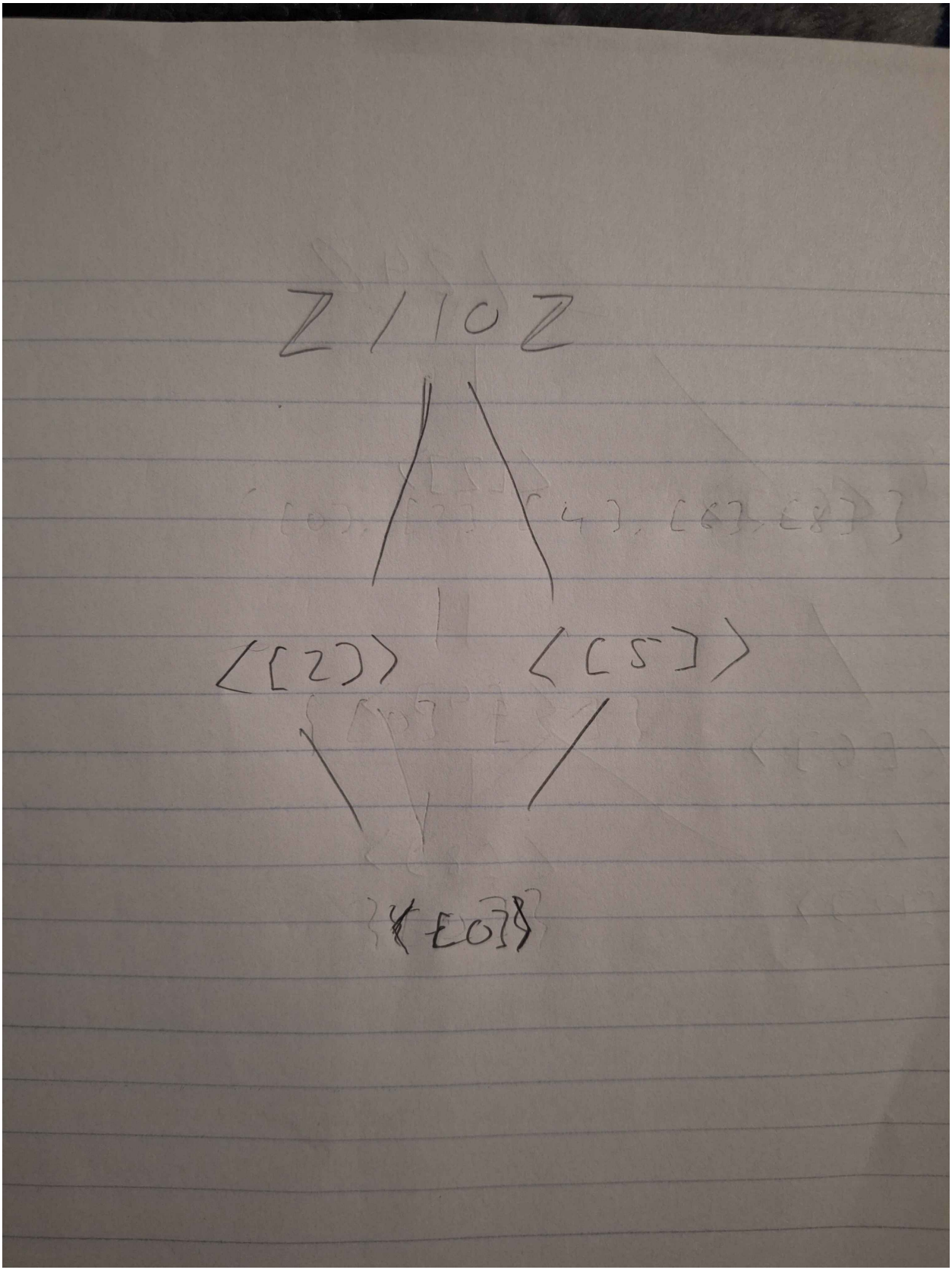
Solution. Looking at the permutation, we note that it contains a three-cycle and then send 3 and 4 to themselves respectively. Then, this means that the order of the given cycle is simply 3. ■

Problem 1.2. Let G be an infinite cyclic group. Prove that G has exactly two generators.

Solution. First, we note that since G is an infinite cyclic group, it is isomorphic to $\mathbb{Z}$. Now, with this in mind, we note that $\mathbb{Z}$ has two generators: -1 and 1. Thus, we see that G has exactly two generators as well. ■

Problem 1.3. Draw the subgroup diagram for the cyclic group $(\mathbb{Z}/10\mathbb{Z}, +)$. Make sure to explain/prove your conclusions.

Solution. We have the following subgroup diagram:



We note that this is because $1, 3, 7$ are all relatively prime to 10 and thus will generate it. Then, with that in

mind, our non-trivial subgroups (i.e. ones that aren't just the identity and the group itself) must not contain these elements or else it'll just be $\mathbb{Z}/10\mathbb{Z}$ itself. Then, using closure property, we can then derive the non-trivial subgroups. ■

Problem 1.4. Prove that the isomorphism $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Solution. We observe that $15 = 3 \times 5$.

Now, we observe first that if we let $H = \{[0], [5], [10]\} = \langle [5] \rangle$, we have a subgroup. Note then that this group is in fact isomorphic to $\mathbb{Z}/3\mathbb{Z}$: since it has order 3 and is cyclic, we note then that $\langle [5] \rangle \cong \mathbb{Z}/3\mathbb{Z}$.

Next, let us consider $K = \{[0], [3], [6], [9], [12]\} = \langle [3] \rangle$. We see then that this is also a subgroup of G. Note that this is in fact isomorphic to $\mathbb{Z}/5\mathbb{Z}$ as $\langle [3] \rangle$ has order 5 and is cyclic (it is generated by 3).

Now, we observe that $[1] = [10] + [6]$, $[2] = [5] + [12]$, $[4] = [10] + [9]$, $[7] = [10] + [12]$, $[8] = [5] + [3]$, $[11] = [5] + [6]$, $[13] = [10] + [3]$, and $[14] = [5] + [9]$.

Furthermore, note that the intersection of H and K is only the identity $[0]$.

Finally, note that $hk = kh$ by virtue of H, K being abelian groups.

Then, we see that G can be written as an internal product of H and K. But then we see that $G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, as desired. ■

1 Problem 1B

Problem 1.1. Compute the order of $[5]$ in $(\mathbb{Z}/3\mathbb{Z}^\times, \times)$

Solution. We note that $[5] \equiv [2]$. Then, we see that since $\gcd(2, 3) = 1$, this is in fact a generator of $\mathbb{Z}/3\mathbb{Z}^\times$. Note that the group contains elements $[1], [2]$, so the order is 2. ■

Problem 1.2. Given $n \in \mathbb{N}$. Prove that there exists a finite cyclic group G with more than n generators.

Solution. We proceed by induction on n.

For $n = 1$, note that $\mathbb{Z}/3\mathbb{Z}$ has two generators: 1 and 2 (under addition).

For $n = k$, we suppose that there exists some prime p such that $\mathbb{Z}/p\mathbb{Z}$ has at least $k + 1$ generators.

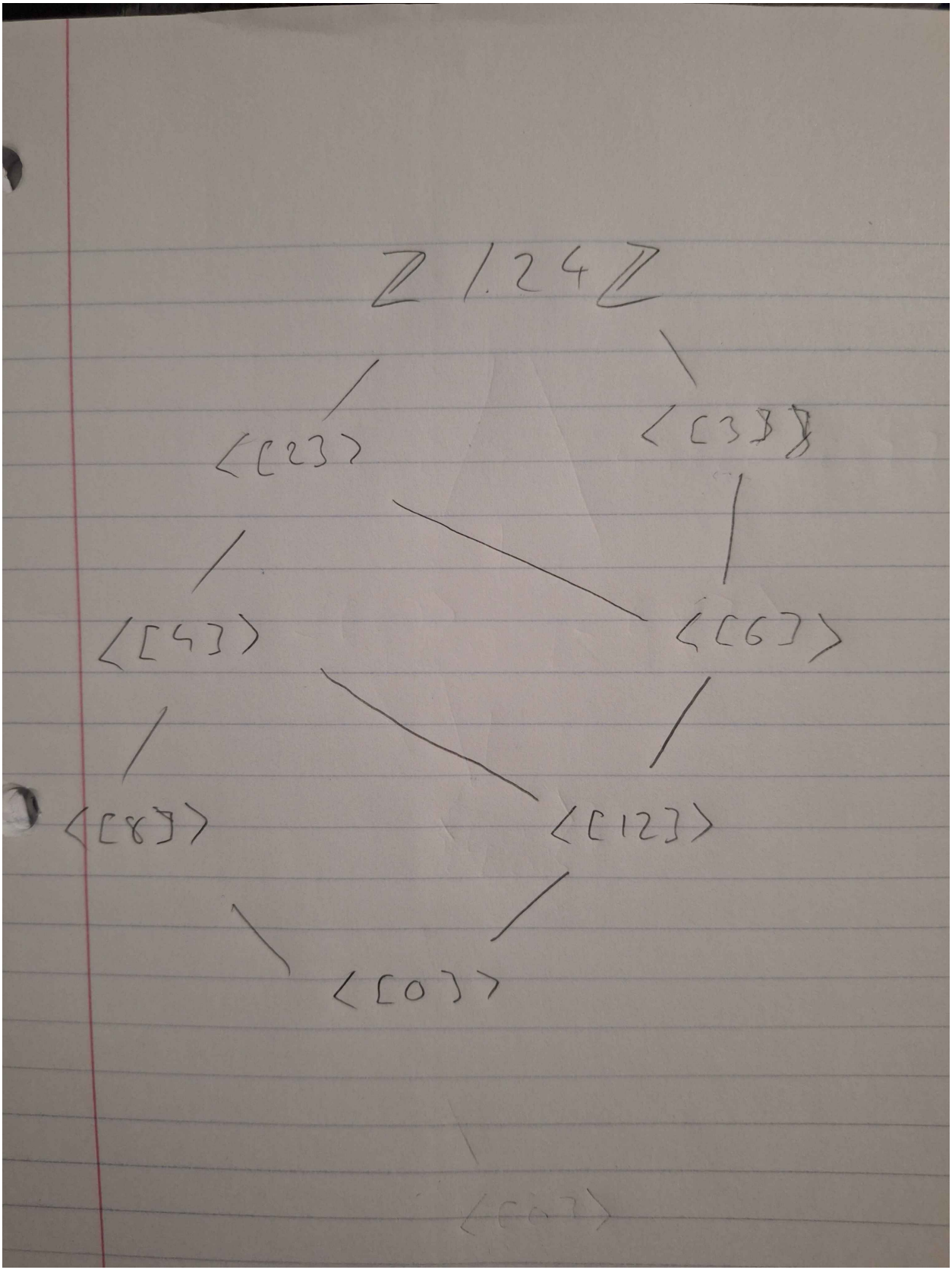
Now, we consider $n = k + 1$. Let us now take the next prime p' after p. We observe that by our induction hypothesis, we know that $\mathbb{Z}/p\mathbb{Z}$ has at least $k + 1$ generators. In the case where $\mathbb{Z}/p\mathbb{Z}$ has $k + 2$ or more generators, we can in fact use the same group $\mathbb{Z}/p\mathbb{Z}$ and we're done.

On the other hand, if $\mathbb{Z}/p\mathbb{Z}$ has $k + 1$ generators, we look at p'. We note then that all of these generators of $\mathbb{Z}/p\mathbb{Z}$ must be relatively prime to p' by definition of p' being prime. Then, we note that since p' is the next prime after p, $\gcd(p, p') = 1$. Then, we note that $[p]$ will in fact be a generator of $\mathbb{Z}/p'\mathbb{Z}$, and thus it has at least $k + 2$ generators.

Therefore, we conclude that the claim holds as desired. ■

Problem 1.3. Draw the subgroup diagram for the cyclic group $(\mathbb{Z}/24\mathbb{Z}, +)$. Make sure to explain/prove your conclusions.

Solution. We have the following subgroup diagram:



We note that for 24, we have that $1, 5, 7, 9, 10, 11, 13, 15, 17, 19$ are all relatively prime to it, so they would

generate the entire group. Then, we want our subgroups to exclude these elements.

From here, we can simply ensure that we have closure for the elements picked and see that we have the diagram given above. ■

Problem 1.4. Prove the isomorphism $\mathbb{Z}/14\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Solution. We observe that if we let $H = \langle [7] \rangle$, note that this is a cyclic subgroup, and that it has order 2. Thus, it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. And $K = \langle [2] \rangle$ is a cyclic subgroup and has order 7, thus being isomorphic to $\mathbb{Z}/7\mathbb{Z}$.

Now, we observe that:

- $[0] = [0] + [0]$
- $[1] = [7] + [8]$
- $[2] = [0] + [2]$
- $[3] = [7] + [10]$
- $[4] = [0] + [4]$
- $[5] = [7] + [12]$
- $[6] = [0] + [6]$
- $[7] = [7] + [0]$
- $[8] = [0] + [8]$
- $[9] = [7] + [2]$
- $[10] = [0] + [10]$
- $[11] = [7] + [4]$
- $[12] = [0] + [12]$
- $[13] = [7] + [6]$

Thus, indeed, we can write G as a direct internal product of H, K. And then, we see then that since that is the case, we have that $\mathbb{Z}/14\mathbb{Z} = HK \cong H \times K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. ■

2 Problem 2A

Problem 2.1. Prove that if G has p elements, where p is prime, then G is cyclic.

Solution. We observe that for such a group G, we have that $|G| = p$. Now, let us consider the cyclic subgroup $H = \langle g \rangle$, where $g \in G$ and $g \neq e_G$.

Now, we observe that by Lagrange's Theorem, we know that $|G|$ must be divisible by $|H|$. But, we know that since $|G|$ is prime, the only numbers that can divide its order is either 1 or p.

Now, we note that since we stated that $g \neq e_G$, we must have that $|H| \neq 1$. But then this means that $|H| = |\langle g \rangle| = p$. Or, in other words, we have that $\langle g \rangle = G$ itself, and thus we see that G is indeed cyclic. ■

Problem 2.2. Let G be a group. Consider the set of all automorphisms of G, denoted by $\mathrm{Aut}(G)$. Prove that this is a group under composition of functions.

Solution. We denote $H = \mathrm{Aut}(G)$ so it's less painful to type out.

First, we check for the identity.

Proof. Note that the identity map $\varphi : G \to G$ is in fact an automorphism, as it maps each element of G to itself.

Then, we observe that for all $\psi \in H$, and for all $g \in G$, we have:

$$\begin{aligned}(\psi \circ \varphi)(g) &= \psi(\varphi(g)) \\ &= \psi(g) \\ &= \varphi(\psi(g)) \\ &= (\varphi \circ \psi)(g)\end{aligned}$$

Thus, we have the identity element in H as desired. □

Next, inverses.

Proof. We note that for any $\varphi \in H$, since it is an isomorphism by virtue of being an automorphism, there exists then an inverse $\varphi^{-1} : G \to G$ such that for all $g \in G$, we have that $(\varphi \circ \varphi^{-1})(g) = \varphi(\varphi^{-1}(g)) = g$, and that $(\varphi^{-1} \circ \varphi)(g) = \varphi^{-1}(\varphi(g)) = g$.

And we note that φ^{-1} is also an automorphism as it is an isomorphism and maps from G to itself, and thus lives in H.

Therefore, for any $\varphi \in G$, there exists an inverse as well. □

Finally, for associativity, we note that this follows from the associativity of composition of functions.

Thus, since all three properties have been satisfied, we observe then that, indeed, H is a group as desired. ■

2 Problem 2B

Problem 2.1. How many non-isomorphic abelian groups of order 39 are there? Prove/explain this.

Solution. We observe that $\mathbb{Z}/39\mathbb{Z}$. We note then that $39 = 3 * 13$. Then, we see that, by the Fundamental Theorem of Finite Abelian Groups, we have that there's only one non-isomorphic abelian group of order 39. ■

Problem 2.2. Let G be a group and $g \in G$ be a fixed element. Define $\psi : G \to G$ by

$$\psi(x) = gxg^{-1}.$$

Prove that $\psi(x)$ is an isomorphism.

Solution. First, we prove that it is a homomorphism. Observe for $x, y \in G$, we have the following:

$$\begin{aligned}\psi(xy) = gxyg^{-1} & \\ &= gxeyg^{-1} \\ &= gx(g^{-1}g)yg^{-1} \\ &= (gxg^{-1})(gyg^{-1}) \\ &= \psi(x)\psi(y).\end{aligned}$$

Thus, we have a homomorphism.

Next, we prove that this is an injection. Observe that for $x = y$, we have that:

$$\begin{aligned}x &= y \\ gx &= gy \\ gxg^{-1} &= gyg^{-1} \\ \psi(x) &= \psi(y)\end{aligned}$$

Thus, we have an injection.

Now, to check for surjectivity, we note that for every $gxg^{-1} \in G$, we have that gxg^{-1} is being mapped to by precisely $x \in G$. Thus, we have a surjection as well.

Therefore, we see that it is a bijective homomorphism; i.e., an isomorphism as desired. ■