Homework 6

Due: June 5th (Friday), 11:59 pm

- Please submit your work on Blackboard.
- You are required to submit your work as a single pdf.
- Please make sure your handwriting is clear enough to read. Thanks.
- No late work will be accepted.
- There are five randomly picked questions (2 pts for each) that will be graded. (2), (3), (7), (8), (11)

---

(1) Finish the proof of Lemma 13 in Lecture Slides_§3.5.

Lemma 13: If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$.

Let $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by

$$\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)), \text{ for all } (x_1, x_2) \in G_1 \times G_2.$$

Claim: ϕ is a group isomorphism.

(i) well-defined: Trivial since $\theta_1(x_1) \in H_1$ and $\theta_2(x_2) \in H_2$.

(ii) ϕ respects the two operations: For any $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$

$$\begin{aligned}\phi((x_1, x_2)(y_1, y_2)) =& \phi((x_1y_1, x_2y_2)) \\ =& (\theta_1(x_1y_1), \theta_2(x_2y_2)) \\ =& (\theta_1(x_1)\theta_1(y_1), \theta_2(x_2)\theta_2(y_2)) \\ =& (\theta_1(x_1), \theta_2(x_2))(\theta_1(y_1), \theta_2(y_2)) \\ =& \phi((x_1, x_2))\phi((y_1, y_2))\end{aligned}$$

(iii) one-to-one: If $\phi((x_1, x_2)) = (\theta_1(x_1), \theta_2(x_2)) = (e_{H_1}, e_{H_2})$, then

$$\theta_1(x_1) = e_{H_1} \Rightarrow x_1 = e_{G_1}$$
$$\theta_2(x_2) = e_{H_2} \Rightarrow x_2 = e_{G_2}$$

and so $(x_1, x_2) = (e_{G_1}, e_{G_2}) = e_{G_1 \times G_2}$.

(iv) onto: Trivial since θ_1 and θ_2 are two groups isomorphisms. In particular, for any element $(h_1, h_2) \in H_1 \times H_2$, we can always find $x_1 \in G_1$ and $x_2 \in G_2$ such that $\theta_1(x_1) = h_1$ and $\theta_2(x_2) = h_2$, and so $\phi((x_1, x_2)) = (h_1, h_2)$.

(2) Let G be a group and let $a \in G$ be an element of order 30. List the powers of a that have order 2, order 3 or order 5.

Since $o(a) = 30 = |\langle a \rangle|$, then we have $\langle a \rangle \cong \mathbf{Z}_{30}$ by Theorem 2. In particular, you can think about the cyclic subgroup $\langle a \rangle$ generated by $a \in G$ is the "multiplicative version" of the additive group $\mathbf{Z}_{30}$. Thus, we have

$$\langle a^j \rangle = \langle a^d \rangle, \text{ where } d = (j, 30) \text{ and so } o(a^j) = |\langle a^j \rangle| = |\langle a^d \rangle| = \frac{30}{d}.$$

(i) $o(a^j) = 2 = \dfrac{30}{d} \Rightarrow d = (j, 30) = 15 \Rightarrow j = 15.$

(ii) $o(a^j) = 3 = \dfrac{30}{d} \Rightarrow d = (j, 30) = 10 \Rightarrow j = 10, 20.$

(iii) $o(a^j) = 5 = \dfrac{30}{d} \Rightarrow d = (j, 30) = 6 \Rightarrow j = 6, 12, 18, 24.$

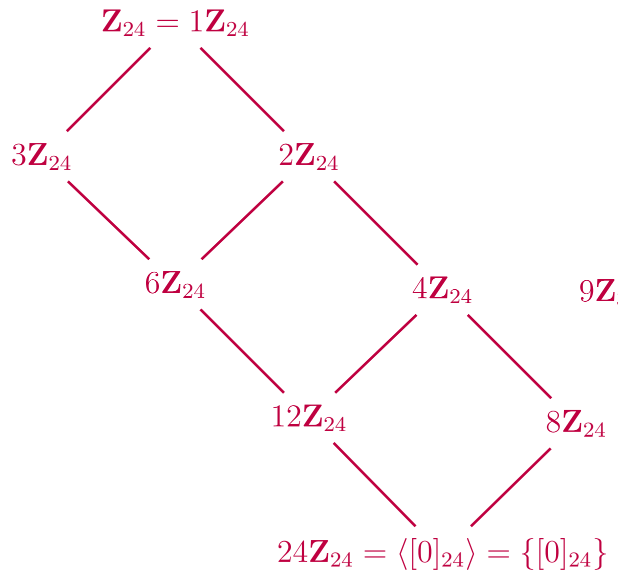
(3) Give the subgroup diagrams of the following groups.

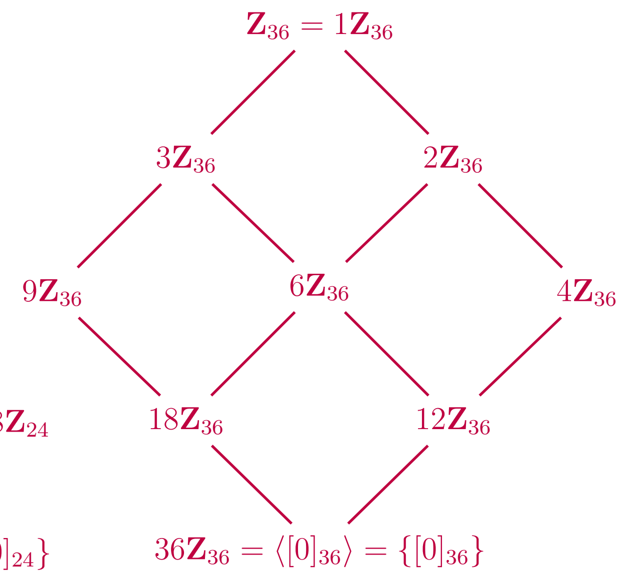
(a) $\mathbf{Z}_{24}$

(b) $\mathbf{Z}_{36}$

$24 = 2^3 3^1$: Any divisor $d = 2^i 3^j$, where $i = 0, 1, 2, 3$ and $j = 0, 1$.

$36 = 2^2 3^2$: Any divisor $d = 2^i 3^j$, where $i = 0, 1, 2$ and $j = 0, 1, 2$.





(4) Which of $\mathbf{Z}_{18}^{\times}, \mathbf{Z}_{20}^{\times}$ are cyclic? (*Do not use Primitive Root Theorem.*)

(a) Check $\mathbf{Z}_{18}^{\times} : \varphi(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6$

$$\mathbf{Z}_{18}^{\times} = \{[1], [5], [7], [11], [13], [17]\} = \{\pm[1], \pm[5], \pm[7]\}$$

(i) $[5]^2 = [25] = [7], [5]^3 = [35] = [-1]$, so $o([5]) = 6$ (Lagrange's Thm).

This implies that $\mathbf{Z}_{18}^{\times} = \langle [5] \rangle$, and so $\mathbf{Z}_{18}^{\times}$ is cyclic.

(b) Check $\mathbf{Z}_{20}^{\times} : \varphi(20) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 8$

$$\mathbf{Z}_{20}^{\times} = \{[1], [3], [7], [9], [11], [13], [17], [19]\} = \{\pm[1], \pm[3], \pm[7], \pm[9]\}$$

(i) $[3]^2 = [9], [3]^3 = [27] = [7], [3]^4 = [21] = [1]$, so $o([3]) = 4$.

(ii) There is no need to try $[7], [9]$ since $[7], [9] \in \langle [3] \rangle$.

(iii) $[11] = [-9], [11]^2 = [-9]^2 = 1$, so $o([11]) = 2$.

(iv) $[13] = [-7], [13]^2 = [-7]^2 = [9], [13]^4 = [9]^2 = [1]$, so $o([13]) = 4$.[1]

(v) $[17] = [-3], [17]^4 = [-3]^4 = 1$, so $o([17]) \leq 4$ since $o([17]) | 4$.

(vi) $[19] = [-1], [19]^2 = [-1]^2 = 1$, so $o([19]) = 2$.

This implies that there is no element of order 8, and so $\mathbf{Z}_{20}^{\times}$ is not cyclic.

[1] Why $o([13]) \neq 3$? Think about Lagrange's Theorem!

(5) Find all cyclic subgroups of $\mathbf{Z}_6 \times \mathbf{Z}_3$.

(a)
- $\langle([0]_6,[0]_3)\rangle = \{([0]_6,[0]_3)\}$.
- $\langle([1]_6,[0]_3)\rangle = \langle([5]_6,[0]_3)\rangle = \{([a]_6,[0]_3) \mid [a]_6 \in \mathbf{Z}_6\}$
- $\langle([2]_6,[0]_3)\rangle = \langle([4]_6,[0]_3)\rangle = \{([0]_6,[0]_3),([2]_6,[0]_3),([4]_6,[0]_3)\}$
- $\langle([3]_6,[0]_3)\rangle = \{([0]_6,[0]_3),([3]_6,[0]_3)\}$

(b)
- $\langle([0]_6,[1]_3)\rangle = \{([0]_6,[0]_3),([0]_6,[1]_3),([0]_6,[2]_3)\}$.
- $\langle([1]_6,[1]_3)\rangle = \{([0]_6,[0]_3),([1]_6,[1]_3),([2]_6,[2]_3),([3]_6,[0]_3),([4]_6,[1]_3),([5]_6,[2]_3)\}$.
- $\langle([2]_6,[1]_3)\rangle = \{([0]_6,[0]_3),([2]_6,[1]_3),([4]_6,[2]_3)\}$.
- $\langle([3]_6,[1]_3)\rangle = \{([0]_6,[0]_3),([3]_6,[1]_3),([0]_6,[2]_3),([3]_6,[0]_3),([0]_6,[1]_3),([3]_6,[2]_3)\}$.
- $\langle([4]_6,[1]_3)\rangle = \{([0]_6,[0]_3),([4]_6,[1]_3),([2]_6,[2]_3)\}$.
- $\langle([5]_6,[1]_3)\rangle = \{([0]_6,[0]_3),([5]_6,[1]_3),([4]_6,[2]_3),([3]_6,[0]_3),([2]_6,[1]_3),([1]_6,[2]_3)\}$.

(c)
- $\langle([0]_6,[2]_3)\rangle = \langle-([0]_6,[2]_3)\rangle = \langle([0]_6,[1]_3)\rangle$.
- $\langle([1]_6,[2]_3)\rangle = \langle-([1]_6,[2]_3)\rangle = \langle([5]_6,[1]_3)\rangle$.
- $\langle([2]_6,[2]_3)\rangle = \langle-([2]_6,[2]_3)\rangle = \langle([4]_6,[1]_3)\rangle$.
- $\langle([3]_6,[2]_3)\rangle = \langle-([3]_6,[2]_3)\rangle = \langle([3]_6,[1]_3)\rangle$.
- $\langle([4]_6,[2]_3)\rangle = \langle-([4]_6,[2]_3)\rangle = \langle([2]_6,[1]_3)\rangle$.
- $\langle([5]_6,[2]_3)\rangle = \langle-([5]_6,[2]_3)\rangle = \langle([1]_6,[1]_3)\rangle$.

(6) Prove that $\mathbf{Z}_{10}^\times$ is not isomorphic to $\mathbf{Z}_{12}^\times$. (*Do not use Primitive Root Theorem.*)

(a) Check $\mathbf{Z}_{10}^\times : \varphi(10) = 10(1-\frac{1}{2})(1-\frac{1}{5}) = 4$

$$\mathbf{Z}_{10}^\times = \{[1],[3],[7],[9]\} = \{\pm[1],\pm[3]\}$$

(i) $[3]^2 = [9]$, so $o([3]) = 4$ (Lagrange's Thm).

This implies that $\mathbf{Z}_{10}^\times = \langle[3]\rangle$, and so $\mathbf{Z}_{10}^\times$ is cyclic.

(b) Check $\mathbf{Z}_{12}^\times : \varphi(12) = 12(1-\frac{1}{2})(1-\frac{1}{3}) = 4$

$$\mathbf{Z}_{12}^\times = \{[1],[5],[7],[11]\} = \{\pm[1],\pm[5]\}$$

$$[5]^2 = [7]^2 = [11]^2 = [1]$$

This implies that there is no element of order 4, and so $\mathbf{Z}_{12}^\times$ is not cyclic.

By Proposition 3 (c) in §3.4, we have $\mathbf{Z}_{10}^\times \not\cong \mathbf{Z}_{12}^\times$.

(7) You need to show work to support your conclusions.

(a) Is $\mathbf{Z}_3 \times \mathbf{Z}_{30}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{15}$? Yes!

By Question (1) or Lemma 13 in §3.5, we get $\mathbf{Z}_3 \times \mathbf{Z}_{30} \cong \mathbf{Z}_3 \times \mathbf{Z}_6 \times \mathbf{Z}_5$ [2] and $\mathbf{Z}_6 \times \mathbf{Z}_{15} \cong \mathbf{Z}_6 \times \mathbf{Z}_3 \times \mathbf{Z}_5$.[3]
Consider the function $\phi : \mathbf{Z}_3 \times \mathbf{Z}_6 \times \mathbf{Z}_5 \to \mathbf{Z}_6 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ [4] by

$$\phi(([x_1]_3, [x_2]_6, [x_3]_5)) = ([x_2]_6, [x_1]_3, [x_3]_5)$$

for any element $([x_1]_3, [x_2]_6, [x_3]_5) \in \mathbf{Z}_3 \times \mathbf{Z}_6 \times \mathbf{Z}_5$. It is obvious that ϕ is an isomorphism. Thus, we prove that $\mathbf{Z}_3 \times \mathbf{Z}_{30} \cong \mathbf{Z}_6 \times \mathbf{Z}_{15}$.

(b) Is $\mathbf{Z}_9 \times \mathbf{Z}_{14}$ isomorphic to $\mathbf{Z}_6 \times \mathbf{Z}_{21}$? No!

By Question (1) or Lemma 13 in §3.5, we get $\mathbf{Z}_9 \times \mathbf{Z}_{14} \cong \mathbf{Z}_9 \times \mathbf{Z}_2 \times \mathbf{Z}_7$ and $\mathbf{Z}_6 \times \mathbf{Z}_{21} \cong \mathbf{Z}_6 \times \mathbf{Z}_3 \times \mathbf{Z}_7 \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_7$.
It shows that the first has an element of order 9, while the second has none. By Proposition 3 (a) in §3.4, we have $\mathbf{Z}_9 \times \mathbf{Z}_{14} \ncong \mathbf{Z}_6 \times \mathbf{Z}_{21}$.

(8) Prove that any cyclic group with more than two elements has at least two different generators.

Proof by contradiction: Let $|G| > 2$ and $G = \langle a \rangle$ for some element $a \neq e$. Suppose that a is the only generator of the group G. However, we also know that $G = \langle a^{-1} \rangle$. By assumption, we have

$$a = a^{-1} \Rightarrow a^2 = e \Rightarrow o(a) = |\langle a \rangle| = |G| = 2 \text{ since } a \neq e, \text{ a contradiction.}$$

Thus, G has at least two different generators.

(9) Prove that any finite cyclic group with more than two elements has an even number of distinct generators.

Let G be a finite cyclic group and $|G| = n > 2$. By Theorem 2 (b), we have $G \cong \mathbf{Z}_n$. Consider the prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, where $p_1 < p_2 < \ldots < p_m$. And the number of distinct generators is equal to

$$|\mathbf{Z}_n^\times| = \varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

If one of $p_1, p_2, \ldots, p_m$ is an odd prime, then it is easy to see that $\varphi(n)$ is even. Otherwise, $n = 2^k$ for some positive integer $k > 2$, then $\varphi(n) = \varphi(2^k) = 2^k \cdot (1 - \frac{1}{2}) = 2^{k-1}$ is again a even number since $k - 1 > 1$. □

(10) Let G be the set of all 3×3 matrices of the form $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}$.

(a) Show that if $a, b, c \in \mathbf{Z}_3$, then G is a group with exponent 3.

[2] Or you can write $\mathbf{Z}_3 \times \mathbf{Z}_{30} \cong \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

[3] Or you can write $\mathbf{Z}_6 \times \mathbf{Z}_{15} \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

[4] Or you can consider $\phi : \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \to \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ by …

For any $a, b, c \in \mathbf{Z}_3$, we have

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2a & 1 & 0 \\ 2b+ac & 2c & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 2a & 1 & 0 \\ 2b+ac & 2c & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 3a & 1 & 0 \\ 3b+3ac & 3c & 1 \end{bmatrix} = I_3$$

(b) Show that if $a, b, c \in \mathbf{Z}_2$, then G is a group with exponent 4.

For any $a, b, c \in \mathbf{Z}_2$, we have

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2a & 1 & 0 \\ 2b+ac & 2c & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ ac & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ ac & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ ac & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ ac & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2ac & 0 & 1 \end{bmatrix} = I_3$$

(11) Let G be any group with no proper, nontrivial subgroups, and assume that $|G| > 1$. Prove that G must be isomorphic to $\mathbf{Z}_p$ for some prime p.

Assume that the only subgroups of G are the trivial subgroup $\{e\}$ and itself.

Since $|G| > 1$, there exists a non-identity element $a \in G$. Then we have $G = \langle a \rangle$ since $\langle a \rangle$ is a subgroup of G but not $\{e\}$, and so G is cyclic.

Moreover, G is a finite cyclic group. Otherwise, $\langle a^k \rangle$ is a proper, nontrivial subgroup of $G = \langle a \rangle$ for any positive integer k, a contradiction.

Let $|G| = n > 1$. By Theorem 2 (b), we have $G \cong \mathbf{Z}_n$. In particular, for each divisor d of n, there exists a (unique) subgroup H of order d since G is a finite cyclic group. By assumption, d has only two possibilities, that is, $d = 1$ or $d = n$. This implies that n has to be a prime number p. Therefore, $G \cong \mathbf{Z}_p$.