

ตอนที่ 1 : (20 คะแนน) จงกากบาทข้อที่ถูกต้องที่สุดเพียงข้อเดียว ข้อละ 2 คะแนน

1. กำหนดให้ $a, b \in \mathbb{Z}$ ข้อใดกล่าวถูกต้อง

ก. ถ้า $a \mid b^2$ แล้ว $a \mid b$

ข. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = b$

ค. ถ้า $a \mid b$ แล้ว $a^2 \mid b$

ง. ถ้ามี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$ แล้ว $d = \gcd(a, b)$

จ. ถ้า $a \mid (a + b)(a - b)$ แล้ว $a \mid b^2$

2. ให้ r เป็นความสัมพันธ์บน \mathbb{Z} ที่นิยามโดย

$$x r y \quad \text{ก็ต่อเมื่อ} \quad 3 \mid (x^2 - y^2)$$

ข้อใดกล่าวไม่ถูกต้อง

ก. r มีสมบัติสะท้อน (Reflexive)

ข. r มีสมบัติสมมาตร (Symmetric)

ค. r มีสมบัติถ่ายทอด (Transitive)

ง. สำหรับ $x, y \in \mathbb{Z}$ ถ้า $x r y$ และ $y r x$ แล้ว $x = y$

จ. มีชั้นสมมูล (Equivalent class) ทั้งหมด 2 ชั้นคือ $[0]_r, [1]_r$

3. ให้ G เป็นกรุป โดยที่ $a, b, c \in G$ ข้อใดกล่าวไม่ถูกต้อง

ก. ถ้า $a^2 = b^2$ แล้ว $a = b$

ข. ถ้า $ab = ac$ แล้ว $b = c$

ค. ถ้า $o(a) = 1$ และ $a = e$ (เป็นเอกลักษณ์)

ง. $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$

จ. ถ้า a ไม่ใช่เอกลักษณ์ และ $a^5 = e$ แล้ว $o(a) = 5$

4. สมาชิกของกรุปในข้อใดที่ อันดับ(order) ต่างจากข้ออื่น

ก. $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$ ใน $GL_2(\mathbb{R})$

ข. $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ ใน \mathbb{C}^*

ค. 5 ใน \mathbb{Z}_{12}^\times

ง. 6 ใน \mathbb{Z}_{12}

จ. $(2\ 4)$ ใน S_4

5. พิจารณาการบวก $\mathbb{Z}_4 \times \mathbb{Z}_9$ ข้อใดกล่าวไม่ถูกต้อง

ก. ตัวผกผัน (inverse) ของ $(\bar{2}, \bar{1})$ คือ $(\bar{2}, \bar{8})$

ข. $[\mathbb{Z}_4 \times \mathbb{Z}_9 : \langle(\bar{0}, \bar{3})\rangle] = 12$

ค. อันดับ (order) ของ $(\bar{0}, \bar{3})$ เท่ากับ 6

ง. $\mathbb{Z}_4 \times \mathbb{Z}_9$ เป็นกรุปวัฏจักร (cyclic group)

จ. กรุปย่อย (subgroup) ทั้งหมดของ $\mathbb{Z}_4 \times \mathbb{Z}_9$ มี 9 กรุป

ตอนที่ 2 : (20 คะแนน) จงเติมคำตอบในช่องว่าง (ด้านซ้ายบน) ให้ถูกต้อง ข้อละ 2 คะแนน

6. _____

จงหาค่าของ $\tau(2^4 \cdot 6^7)$

7. _____

ตัวต่อกำเนิด (generator) ของ $\mathbb{Z}_{24} \times \mathbb{Z}_{67}$ มีทั้งหมดกี่ตัว

8. _____

ถ้าทราบว่า $\bar{3}$ เป็นตัวต่อกำเนิด (generator) ของ \mathbb{Z}_{17}^\times จงหาตัวกำเนิดตัวอื่น ๆ (ตอบอย่างน้อย 1 ตัว)

9. _____

จากกรุปย่อยของ S_3 ต่อไปนี้

$$\langle (1\ 2) \rangle, \langle (1\ 3) \rangle, \langle (2\ 3) \rangle, \langle (1\ 2\ 3) \rangle$$

กรุปย่อยใดเป็น กรุปย่อยปกติ (Normal subgroup)

10. _____

จงหาตัวผกผัน (inverse) ของ $\langle \bar{4} \rangle + \bar{1}$ ในกรุปผลหาร $\mathbb{Z}_8 / \langle \bar{4} \rangle$

ตอนที่ 3 : (80 คะแนน) จงแสดงวิธีโดยละเอียด ข้อละ 10 คะแนน

11. (10 คะแนน) นิยามการดำเนินการทวิภาค * บนเซต $G = \{1, 2, 3, 4\}$ ถ้า * มีสมบัติสลับที่ (commutative law) และมีสมบัติการเปลี่ยนกลุ่ม (associative law) โดยมีผลการดำเนินการแสดงดังตารางต่อไปนี้

*	1	2	3	4
1	a	3	2	b
2	3	1	4	2
3	c	4	1	3
4	1	2	3	4

11.1 (3 คะแนน) จงหา a, b และ c

11.2 (2 คะแนน) จงหา เอกลักษณ์ (identity) ของ G (พร้อมให้เหตุผล)

11.3 (3 คะแนน) จงหา ตัวผกผัน (inverse) ของสมาชิกทุกตัว ใน G (เติมคำตอบในตารางให้สมบูรณ์)

สมาชิก (Elements)	ตัวผกผัน (Inverses)	เหตุผล (Reasons)
1		
2		
3		
4		

11.4 (2 คะแนน) จงหา อันดับ (order) ของ 2 ใน G

12. (10 คะแนน) จงตอบคำถามต่อไปนี้

12.1 (5 คะแนน) จงพิสูจน์ข้อความต่อไปนี้ด้วยอุปนัยเชิงคณิตศาสตร์

$$2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2 \quad \text{สำหรับทุก } n \in \mathbb{N}$$

12.2 (5 คะแนน) ให้ G เป็นกรุป โดยที่ $a \in G$ จงแสดงว่า

$$\text{ถ้า } o(a) = n \text{ แล้ว } o(a^{-1}) = n$$

13. (10 คะแนน) นิยามการดำเนินการทวิภาค $*$ บน \mathbb{R} ดังนี้

$$a * b = a + b + 2ab$$

จงตรวจสอบว่า $(\mathbb{R}, *)$ เป็น กึ่งกรุป (semi-group) / โมนอยด์ (monoid) / หรือกรุป (group)

14. (10 คะแนน) จงตอบคำถามต่อไปนี้

14.1 (5 คะแนน) ให้ α เป็นวัฏจักร ใน S_{67} ที่ไม่ใช่เอกลักษณ์ โดยที่

$$[(2\ 4)\alpha(2\ 4)]^{67} = (1)$$

จงหา อันดับ (order) ของ α

14.2 (5 คะแนน) จงหา ตัวผกผันการคูณ (multiplicative inverse) ของ $\overline{17}$ ใน \mathbb{Z}_{24}^\times

15. (10 คะแนน) จงตอบคำถามต่อไปนี้

15.1 (5 คะแนน) จงตรวจสอบว่า H เป็นกรุปย่อย(subgroup) ของ $GL_2(\mathbb{R})$ หรือไม่

$$H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2^x \end{bmatrix} : x \in \mathbb{R} \right\}$$

15.2 (5 คะแนน) กำหนดให้ $A = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$ เป็นสมาชิกใน $GL_2(\mathbb{R})$

จงเขียนกรุปย่อย $\langle A \rangle$ ในรูปแบบมีเงื่อนไขที่ไม่ติดเลขชี้กำลัง

16. (10 คะแนน) พิจารณาการคูณ \mathbb{Z}_{22}^\times

16.1 (3 คะแนน) จงหา ตัวก่อกำเนิด (generator) ของ \mathbb{Z}_{22}^\times

16.2 (4 คะแนน) จงหา กรุปย่อย (subgroup) ทั้งหมดของ \mathbb{Z}_{22}^\times (พร้อมแจกแจงสมาชิกของกรุปย่อย)

16.3 (3 คะแนน) จงนำกรุปย่อยจากข้อ 16.2 เขียน แลตทิซ (lattice)

17. (10 คะแนน) ให้ G เป็นกรุปจำกัดที่ $|G| = 6$

จงใช้ทฤษฎีบทลากรองจ์ (Lagrange's Theorem) แสดงว่ามีสมาชิกใน G ที่มีอันดับเท่ากับ 2 หรือ 3

18. (10 คะแนน) ให้ N เป็นกรุปย่อย (subgroup) ของกรุป G จงพิสูจน์ว่า

$$\text{ถ้า } gNg^{-1} \subseteq N \text{ ทุก } g \in G \text{ แล้ว } (Nh)(Nk) = N(hk) \text{ ทุก } h, k \in G$$



มหาวิทยาลัยราชภัฏสวนสุนันทา
คณะครุศาสตร์ สาขาวิชาคณิตศาสตร์
เฉลยข้อสอบกลางภาคเรียนที่ 1 ปีการศึกษา 2567

รหัสวิชา MAC3310	ชื่อวิชา พีชคณิตนามธรรม	วันเวลาสอบ เวลา 13:00 - 16:00 วันศุกร์ ที่ 30 สิงหาคม 2567	คะแนนเต็ม 100 คะแนน 25%
---------------------	----------------------------	--	-------------------------------

โดย ผู้ช่วยศาสตราจารย์ ดร.ธนัชศ จ่าปาหวาย

ตอนที่ 1 : (10 คะแนน) จงกากบาทข้อที่ถูกต้องที่สุดเพียงข้อเดียว ข้อละ 2 คะแนน

1. กำหนดให้ $a, b \in \mathbb{Z}$ ข้อใดกล่าวถูกต้อง

- ก. ถ้า $a \mid b^2$ แล้ว $a \mid b$
- ข. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = b$
- ค. ถ้า $a \mid b$ แล้ว $a^2 \mid b$
- ง. ถ้ามี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$ แล้ว $d = \gcd(a, b)$
- จ. ถ้า $a \mid (a + b)(a - b)$ แล้ว $a \mid b^2$ **Answer**

ตอบข้อ จ.

- ก. ถ้า $a \mid b^2$ แล้ว $a \mid b$ ไม่ถูกต้องเมื่อเลือก $a = 4$ และ $b = 2$
- ข. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = b$ ไม่ถูกต้องเมื่อเลือก $a = 2$ และ $b = -2$
- ค. ถ้า $a \mid b$ แล้ว $a^2 \mid b$ ไม่ถูกต้องเมื่อเลือก $a = 2$ และ $b = 2$
- ง. ถ้ามี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$ แล้ว $d = \gcd(a, b)$ ไม่ถูกต้องเมื่อเลือก $d = 2$ และ $a = 2, b = 3$ และ $x = -5, y = 4$
- จ. ถ้า $a \mid (a + b)(a - b)$ แล้ว $a \mid b^2$ ถูกต้อง
เนื่องจาก $(a - b)(a + b) = a^2 - b^2$ เนื่องจาก $a \mid a^2$ ดังนั้น $a \mid b^2$

2. ให้ r เป็นความสัมพันธ์บน \mathbb{Z} ที่นิยามโดย

$$x r y \quad \text{ก็ต่อเมื่อ} \quad 3 \mid (x^2 - y^2)$$

ข้อใดกล่าวไม่ถูกต้อง

- ก. r มีสมบัติสะท้อน (Reflexive)
- ข. r มีสมบัติสมมาตร (Symmetric)
- ค. r มีสมบัติถ่ายทอด (Transitive)
- ง. สำหรับ $x, y \in \mathbb{Z}$ ถ้า $x r y$ และ $y r x$ แล้ว $x = y$ **Answer**
- จ. มีชั้นสมมูล (Equivalent class) ทั้งหมด 2 ชั้นคือ $[0]_r, [1]_r$

ตอบข้อ ง. พิจารณา

- ก. สมบัติสะท้อน
สำหรับจำนวนเต็ม x ใด ๆ จะได้ว่า $x^2 - x^2 = 0$ ดังนั้น $2 \mid (x^2 - x^2)$ สรุปได้ว่า $x r x$
- ข. สมบัติสมมาตร
ให้ $x, y \in \mathbb{Z}$ สมมติว่า $x r y$ นั่นคือ $2 \mid (x^2 - y^2)$ แล้ว $2 \mid (-1)(x^2 - y^2)$ หรือ $2 \mid (y^2 - x^2)$ สรุปได้ว่า $y r x$
- ค. สมบัติถ่ายทอด
ให้ $x, y, z \in \mathbb{Z}$ สมมติว่า $x r y$ และ $y r z$ จะได้ว่า $2 \mid (x^2 - y^2)$ และ $2 \mid (y^2 - z^2)$
จะได้ว่า $2 \mid [(x^2 - y^2) + (y^2 - z^2)]$ หรือ $2 \mid (x^2 - z^2)$ สรุปได้ว่า $x r z$
- ง. ไม่ถูกต้องเมื่อเลือก $x = 1$ และ $y = 2$ จะเห็นว่า $x r y$ และ $y r x$ แต่ $x \neq y$
- จ. จาก ก-ค r เป็นความสัมพันธ์สมมูลบน \mathbb{Z} พิจารณาชั้นสมมูลต่อไปนี้

$$[0]_r = \{a : 3 \mid (a^2 - 0)\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1]_r = \{a : 3 \mid (a^2 - 1)\} = \{\pm 1, \pm 2, \pm 4, \pm 5, \dots\}$$

ดังนั้นมีชั้นสมมูลทั้งหมด 2 ชั้นคือ $[0]_r, [1]_r$

3. ให้ G เป็นกรุป โดยที่ $a, b, c \in G$ ข้อใดกล่าวไม่ถูกต้อง

ก. ถ้า $a^2 = b^2$ แล้ว $a = b$ **Answer**

ข. ถ้า $ab = ac$ แล้ว $b = c$

ค. ถ้า $\circ(a) = 1$ และ $a = e$ (เป็นเอกลักษณ์)

ง. $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$

จ. ถ้า a ไม่ใช่เอกลักษณ์ และ $a^5 = e$ แล้ว $\circ(a) = 5$

ตอบข้อ ก. ไม่ถูกต้อง เมื่อเลือก $G = \mathbb{R}^*$ (กรุปการคูณ) และ $a = -2, b = 2$

4. สมาชิกของกรุปในข้อใดที่ **อันดับ(order)** ต่างจากข้ออื่น

ก. $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$ ใน $GL_2(\mathbb{R})$

ข. $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ ใน \mathbb{C}^* **Answer**

ค. $\bar{5}$ ใน \mathbb{Z}_{12}^\times

ง. $\bar{6}$ ใน \mathbb{Z}_{12}

จ. $(2\ 4)$ ใน S_4

ตอบข้อ ข. พิจารณา

$$\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \quad \longrightarrow \quad \circ \left(\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} \right) = 2$$

$$\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right)^8 = (\text{cis } \frac{\pi}{4})^8 = \text{cis } 2\pi = 1 \quad \longrightarrow \quad \circ \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right) = 8$$

$$(\bar{5})^2 = \bar{25} = \bar{1} \quad \longrightarrow \quad \circ(\bar{5}) = 2$$

$$2(\bar{6}) = \bar{12} = \bar{0} \quad \longrightarrow \quad \circ(\bar{6}) = 2$$

$$(2\ 4)^2 = (1) \quad \longrightarrow \quad \circ((2\ 4)) = 2$$

5. พิจารณาการบวก $\mathbb{Z}_4 \times \mathbb{Z}_9$ ข้อใดกล่าวไม่ถูกต้อง

- ก. ตัวผกผัน (inverse) ของ $(\bar{2}, \bar{1})$ คือ $(\bar{2}, \bar{8})$
- ข. $[\mathbb{Z}_4 \times \mathbb{Z}_9 : \langle (\bar{0}, \bar{3}) \rangle] = 12$
- ค. อันดับ (order) ของ $(\bar{0}, \bar{3})$ เท่ากับ 6 **Answer**
- ง. $\mathbb{Z}_4 \times \mathbb{Z}_9$ เป็นกรุปวัฏจักร (cyclic group)
- จ. กรุปย่อย (subgroup) ทั้งหมดของ $\mathbb{Z}_4 \times \mathbb{Z}_9$ มี 9 กรุป

ตอบข้อ ค.

ก. เนื่องจาก $(\bar{2}, \bar{1}) + (\bar{2}, \bar{8}) = (\bar{0}, \bar{0})$ ดังนั้น ตัวผกผันของ $(\bar{2}, \bar{1})$ คือ $(\bar{2}, \bar{8})$

ข. $[\mathbb{Z}_4 \times \mathbb{Z}_9 : \langle (\bar{0}, \bar{3}) \rangle] = \frac{|\mathbb{Z}_4 \times \mathbb{Z}_9|}{o(\langle (\bar{0}, \bar{3}) \rangle)} = \frac{4 \times 9}{3} = 12$

ค. ไม่ถูกต้องเนื่องจาก

$$3(\bar{0}, \bar{3}) = (\bar{0}, \bar{0})$$

ดังนั้นอันดับของ $(\bar{0}, \bar{3})$ เท่ากับ 3 **Answer**

ง. $\mathbb{Z}_4 \times \mathbb{Z}_9$ เป็นกรุปวัฏจักร (cyclic group) เนื่องจาก $\gcd(4, 9) = 1$

จ. เนื่องจาก $\mathbb{Z}_4 \times \mathbb{Z}_9$ เป็นกรุปวัฏจักร ดังนั้นกรุปย่อยทั้งหมดเท่ากับ จำนวนตัวหารของ $n = 4 \times 9$

$$\tau(4 \times 9) = \tau(2^2 \times 3^2) = (2 + 1)(2 + 1) = 9$$

ตอนที่ 2 : (10 คะแนน) จงเติมคำตอบในช่องว่าง (ด้านซ้ายมือ) ให้ถูกต้อง ข้อละ 2 คะแนน

6. ตอบ **96**

จงหาค่าของ $\tau(2^4 \cdot 6^7)$

แนวคำตอบ จะได้ว่า

$$\begin{aligned} \tau(2^4 \cdot 6^7) &= \tau(2^4 \cdot 2^7 \cdot 3^7) = \tau(2^{11} \cdot 3^7) \\ &= (11 + 1)(7 + 1) \\ &= 12(8) \\ &= 96 \quad \# \end{aligned}$$

7. ตอบ **528**

ตัวต่อกำเนิด (generator) ของ $\mathbb{Z}_{24} \times \mathbb{Z}_{67}$ มีทั้งหมดกี่ตัว

แนวคำตอบ $\mathbb{Z}_{24} \times \mathbb{Z}_{67}$ เป็นกรุปวัฏจักร (cyclic group) เนื่องจาก $\gcd(24, 67) = 1$ จำนวนตัวต่อกำเนิดเท่ากับ

$$\begin{aligned} \phi(24 \cdot 67) &= \phi(2^3 \cdot 3 \cdot 67) \\ &= (2^3 - 2^2)(3 - 1)(67 - 1) \\ &= 4(2)(66) \\ &= 528 \end{aligned}$$

8. ตอบ **5, 6, 7, 10, 11, 12, 14**

ถ้าทราบว่า 3 เป็นตัวต่อกำเนิด (generator) ของ \mathbb{Z}_{17}^\times จงหาตัวกำเนิดตัวอื่น ๆ (ตอบอย่างน้อย 1 ตัว)

แนวคำตอบ จะเห็นว่า $n = \phi(17) = 16$ พิจารณา

$$1 \leq k < 16 \text{ และ } \gcd(k, 16) = 1 \text{ นั่นคือ } k = 1, 3, 5, 7, 9, 11, 13, 15$$

ดังนั้นตัวต่อกำเนิดของ \mathbb{Z}_{17}^\times คือ

$$a^k = \begin{cases} (\bar{3})^1 &= \bar{3} \\ (\bar{3})^3 &= \bar{10} \\ (\bar{3})^5 &= \bar{5} \\ (\bar{3})^7 &= \bar{11} \\ (\bar{3})^9 &= \bar{14} \\ (\bar{3})^{11} &= \bar{7} \\ (\bar{3})^{13} &= \bar{12} \\ (\bar{3})^{15} &= \bar{6} \end{cases}$$

9. ตอบ $\langle(1\ 2\ 3)\rangle$

จากกรุปย่อยของ S_3 ต่อไปนี้

$$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \langle(1\ 2\ 3)\rangle$$

กรุปย่อยใดเป็น กรุปย่อยปกติ (Normal subgroup)

แนวคำตอบ เนื่องจาก

$$[S_3 : \langle(1\ 2\ 3)\rangle] = \frac{|S_3|}{o(\langle(1\ 2\ 3)\rangle)} = \frac{3!}{3} = 2$$

โดยทฤษฎีบทสรุปได้ว่า $\langle(1\ 2\ 3)\rangle$ เป็นกรุปย่อยปกติ

10. ตอบ $\langle\bar{4}\rangle + \bar{3}$

จงหาตัวผกผัน (inverse) ของ $\langle\bar{4}\rangle + \bar{1}$ ในกรุปผลหาร $\mathbb{Z}_8 / \langle\bar{4}\rangle$

แนวคำตอบ พิจารณา

$$\begin{aligned}\langle\bar{4}\rangle &= \{\bar{0}, \bar{4}\} \\ \langle\bar{4}\rangle + \bar{1} &= \{\bar{1}, \bar{5}\} \\ \langle\bar{4}\rangle + \bar{2} &= \{\bar{2}, \bar{6}\} \\ \langle\bar{4}\rangle + \bar{3} &= \{\bar{3}, \bar{7}\}\end{aligned}$$

จะเห็นว่า $\langle\bar{4}\rangle$ เป็นเอกลักษณ์ของ

$$\mathbb{Z}_8 / \langle\bar{4}\rangle = \{\langle\bar{4}\rangle, \langle\bar{4}\rangle + \bar{1}, \langle\bar{4}\rangle + \bar{2}, \langle\bar{4}\rangle + \bar{3}\}$$

เนื่องจาก

$$(\langle\bar{4}\rangle + \bar{1}) + (\langle\bar{4}\rangle + \bar{3}) = \langle\bar{4}\rangle + \bar{4} = \langle\bar{4}\rangle$$

ดังนั้น $\langle\bar{4}\rangle + \bar{3}$ เป็นตัวผกผันของ $\langle\bar{4}\rangle + \bar{1}$

ตอนที่ 3 : (80 คะแนน) จงแสดงวิธีโดยละเอียด ข้อละ 10 คะแนน

11. (10 คะแนน) นิยามการดำเนินการทวิภาค * บนเซต $G = \{1, 2, 3, 4\}$ ถ้า * มีสมบัติสลับที่ (commutative law) และมีสมบัติการเปลี่ยนกลุ่ม (associative law) โดยมีผลการดำเนินการแสดงดังตารางต่อไปนี้

*	1	2	3	4
1	a	3	2	b
2	3	1	4	2
3	c	4	1	3
4	1	2	3	4

- 11.1 (3 คะแนน) จงหา a, b และ c โดยสมบัติการสลับที่จะได้ว่า

$$c = 3 * 1 = 1 * 3 = 2 \quad \#$$

$$b = 1 * 4 = 4 * 1 = 1 \quad \#$$

โดยสมบัติการเปลี่ยนกลุ่ม

$$a = 1 * 1 = 1 * (2 * 2) = (1 * 2) * 2 = 3 * 2 = 4 \quad \#$$

- 11.2 (2 คะแนน) จงหา เอกลักษณ์ (identity) ของ G (พร้อมให้เหตุผล)
แนวคำตอบ จากตารางและข้อ 11.1 จะเห็นว่า

$$a * 4 = a = 4 * a \quad \text{ทุก } a \in G$$

ดังนั้น 4 เป็นเอกลักษณ์ของ G

- 11.3 (3 คะแนน) จงหา ตัวผกผัน (inverse) ของสมาชิกทุกตัว ใน G (เติมคำตอบในตารางให้สมบูรณ์)

สมาชิก (Elements)	ตัวผกผัน (Inverses)	เหตุผล (Reasons)
1	1	$1 * 1 = 4$
2	3	$2 * 3 = 4 = 3 * 2$
3	2	$3 * 2 = 4 = 2 * 3$
4	4	$4 * 4 = 4$

- 11.4 (2 คะแนน) จงหา อันดับ (order) ของ 2 ใน G
แนวคำตอบ เนื่องจาก $e = 4$ พิจารณา

$$2^2 = 2 * 2 = 1$$

$$2^3 = 2^2 * 2 = 1 * 2 = 2$$

$$2^4 = 2^3 * 2 = 2 * 2 = 1$$

ดังนั้น $\text{ord}(2) = 2 \quad \#$

12. (10 คะแนน) จงตอบคำถามต่อไปนี้

12.1 (5 คะแนน) จงพิสูจน์ข้อความต่อไปนี้ด้วยอุปนัยเชิงคณิตศาสตร์

$$2 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 2 \quad \text{สำหรับทุก } n \in \mathbb{N}$$

แนวคำตอบ ให้ $n \in \mathbb{N}$ และ $P(n)$ แทนข้อความ

$$2 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 2$$

กรณี $n = 1$ จะได้ว่า $2 = 4 - 2 = 2^{1+1} - 2$ ดังนั้น $P(1)$ เป็นจริง

ให้ $k \in \mathbb{N}$ สมมติว่า $P(k)$ เป็นจริง จะได้ว่า

$$\begin{aligned} 2 + 2^2 + 2^3 + \dots + 2^k + 2^{k+1} &= 2^{k+1} - 2 + 2^{k+1} \\ &= 2 \cdot 2^{k+1} - 2 \\ &= 2^{k+2} - 2 \end{aligned}$$

ดังนั้น $P(k + 1)$ เป็นจริง โดยอุปนัยเชิงคณิตศาสตร์สรุปได้ว่า

$$2 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 2 \quad \text{สำหรับทุก } n \in \mathbb{N}$$

12.2 (5 คะแนน) ให้ G เป็นกรุป โดยที่ $a \in G$ จงแสดงว่า

$$\text{ถ้า } o(a) = n \text{ แล้ว } o(a^{-1}) = n$$

แนวคำตอบ สมมติว่า $o(a) = n$ จะได้ว่า $a^n = e$ พิจารณา

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$$

ให้ $k \in \mathbb{N}$ โดยที่ $(a^{-1})^k = e$ จะได้ว่า

$$\begin{aligned} (a^k)^{-1} &= (a^{-1})^k = e \\ [(a^k)^{-1}]^{-1} &= e^{-1} \\ a^k &= e \end{aligned}$$

ดังนั้น $n \mid k$ นั่นคือ $n \leq k$
สรุปได้ว่า $o(a^{-1}) = n$

13. (10 คะแนน) นิยามการดำเนินการทวิภาค $*$ บน \mathbb{R} ดังนี้

$$a * b = a + b + 2ab$$

จงตรวจสอบว่า $(\mathbb{R}, *)$ เป็น กึ่งกรุป (semi-group) / โมนอยด์ (monoid) / หรือกรุป (group)

แนวคำตอบ ให้ $a, b, c \in G$

$$\begin{aligned} a * (b * c) &= a * (b + c + 2bc) \\ &= a + (b + c + 2bc) + 2a(b + c + 2bc) \\ &= a + b + c + 2bc + 2ab + 2ac + 4abc \\ &= a + b + 2ab + c + 2ac + 2bc + 4abc \\ &= (a + b + 2ab) + c + 2(a + b + 2ab)c \\ &= (a + b + 2ab) * c \\ &= (a * b) * c \end{aligned}$$

ดังนั้น $*$ มีสมบัติการเปลี่ยนกลุ่มบนเซต G เนื่องจาก

$$\begin{aligned} a * 0 &= a + 0 + 2 \cdot a \cdot 0 = a \\ 0 * a &= 0 + a + 2 \cdot 0 \cdot a = a \end{aligned}$$

จะได้ว่า 0 เป็นเอกลักษณ์ใน G

สมมติว่า $a = -\frac{1}{2}$ มีตัวผกผันเป็น $b \in \mathbb{R}$ จะได้ว่า

$$0 = -\frac{1}{2} * b = -\frac{1}{2} + b + 2 \left(-\frac{1}{2} \right) b = -\frac{1}{2} + b - b = -\frac{1}{2}$$

ซึ่งเป็นไปไม่ได้

สรุปได้ว่า $(\mathbb{R}, *)$ เป็นโมนอยด์

14. (10 คะแนน) จงตอบคำถามต่อไปนี้

14.1 (5 คะแนน) ให้ α เป็นวัฏจักร ใน S_{67} ที่ไม่ใช่เอกลักษณ์ โดยที่

$$[(2\ 4)\alpha(2\ 4)]^{67} = (1)$$

จงหา อันดับ (order) ของ α

แนวคำตอบ

$$\begin{aligned} [(2\ 4)\alpha(2\ 4)]^2 &= [(2\ 4)\alpha(2\ 4)][(2\ 4)\alpha(2\ 4)] = (2\ 4)\alpha(2\ 4)^2\alpha(2\ 4) \\ &= (2\ 4)\alpha(1)\alpha(2\ 4) = (2\ 4)\alpha^2(2\ 4) \\ [(2\ 4)\alpha(2\ 4)]^3 &= [(2\ 4)\alpha^2(2\ 4)][(2\ 4)\alpha(2\ 4)] = (2\ 4)\alpha^2(2\ 4)^2\alpha(2\ 4) \\ &= (2\ 4)\alpha^2(1)\alpha(2\ 4) = (2\ 4)\alpha^3(2\ 4) \\ [(2\ 4)\alpha(2\ 4)]^4 &= [(2\ 4)\alpha^3(2\ 4)][(2\ 4)\alpha(2\ 4)] = (2\ 4)\alpha^3(2\ 4)^2\alpha(2\ 4) \\ &= (2\ 4)\alpha^3(1)\alpha(2\ 4) = (2\ 4)\alpha^4(2\ 4) \\ &\vdots \\ [(2\ 4)\alpha(2\ 4)]^{67} &= (2\ 4)\alpha^{67}(2\ 4) \\ (1) &= (2\ 4)\alpha^{67}(2\ 4) \\ (2\ 4)(1)(2\ 4) &= (2\ 4)(2\ 4)\alpha^{67}(2\ 4)(2\ 4) \\ (2\ 4)^2 &= (2\ 4)^2\alpha^{67}(2\ 4)^2 \\ (1) &= (1)\alpha^{67}(1) \\ (1) &= \alpha^{67} \end{aligned}$$

จะได้ว่า $o(\alpha) \mid 67$ ฉะนั้น $o(\alpha) = 1, 67$ (67 เป็นจำนวนเฉพาะ)

เนื่องจาก α ไม่ใช่เอกลักษณ์ นั่นคือ $o(\alpha) \neq 1$ สรุปได้ว่า $o(\alpha) = 67 \quad \#$

14.2 (5 คะแนน) จงหา ตัวผกผันการคูณ (multiplicative inverse) ของ $\overline{17}$ ใน \mathbb{Z}_{24}^\times

แนวคำตอบ พิจารณาเมทริกซ์ในการหา $\gcd(17, 24) = 1$

$$\begin{array}{llll} 24 & 1 & 0 & R_1 \\ 17 & 0 & 1 & R_2 \\ 7 & 1 & -1 & R_3 = R_1 - R_2 \\ 3 & -2 & 3 & R_4 = R_2 - 2R_3 \\ 1 & 5 & -7 & R_5 = R_3 - 2R_4 \end{array}$$

ดังนั้น $1 = 24(5) + 17(-7)$ จะได้ว่า

$$\overline{1} = \overline{24(5) + 17(-7)} = \overline{17} \cdot \overline{-7}$$

ดังนั้น $\overline{-7} = \overline{17}$ เป็นตัวผกผันการคูณของ $\overline{17}$ ใน \mathbb{Z}_{24}^\times

15. (10 คะแนน) จงตอบคำถามต่อไปนี้

15.1 (5 คะแนน) จงตรวจสอบว่า H เป็นกรุปย่อย(subgroup) ของ $GL_2(\mathbb{R})$ หรือไม่

$$H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2^x \end{bmatrix} : x \in \mathbb{R} \right\}$$

แนวคำตอบ เลือก $x = 0$ จะได้ว่า $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$ ดังนั้น $H \neq \emptyset$

ให้ $A = \begin{bmatrix} 1 & 0 \\ 0 & 2^x \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & 0 \\ 0 & 2^y \end{bmatrix}$ เป็นสมาชิกใน H นั่นคือ $x, y \in \mathbb{R}$ จะได้ว่า

$$AB^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 2^x \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2^y \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 2^x \end{bmatrix} \frac{1}{2^y} \begin{bmatrix} 2^y & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2^x \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2^{-y} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2^{x-y} \end{bmatrix} \in H$$

เนื่องจาก $x - y \in \mathbb{R}$ จะได้ว่า $AB^{-1} \in H$ ดังนั้น H เป็นกรุปย่อยของ $GL_2(\mathbb{R})$

15.2 (5 คะแนน) กำหนดให้ $A = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$ เป็นสมาชิกใน $GL_2(\mathbb{R})$

จงเขียนกรุปย่อย $\langle A \rangle$ ในรูปแบบมีเงื่อนไขที่ไม่ติดเลขชี้กำลัง

แนวคำตอบ พิจารณา

$$\begin{aligned} A &= \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} \\ A^2 &= \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \\ A^3 &= A^2A = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 3 \\ 0 & -1 \end{bmatrix} \\ A^4 &= A^3A = \begin{bmatrix} -1 & 3 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -4 \\ 0 & 1 \end{bmatrix} \\ &\vdots \\ A^n &= \begin{bmatrix} (-1)^n & (-1)^{n+1}n \\ 0 & (-1)^n \end{bmatrix} \end{aligned}$$

ดังนั้น $A^n = \begin{bmatrix} (-1)^n & (-1)^{n+1}n \\ 0 & (-1)^n \end{bmatrix}$ เมื่อ $n \in \mathbb{N}$ และ I เป็นเมตริกซ์เอกลักษณ์

จะเห็นว่า $A^{-1} = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$ แล้ว

$$A^{-n} = (A^n)^{-1} = \begin{bmatrix} (-1)^n & (-1)^{n+1}n \\ 0 & (-1)^n \end{bmatrix}^{-1} = \begin{bmatrix} (-1)^n & (-1)^{n+1}(-n) \\ 0 & (-1)^n \end{bmatrix} \text{ เมื่อ } n \in \mathbb{N}$$

และ $A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$ สรุปได้ว่า

$$\langle A \rangle = \left\{ \begin{bmatrix} (-1)^n & (-1)^{n+1}n \\ 0 & (-1)^n \end{bmatrix} : n \in \mathbb{Z} \right\}$$

16. (10 คะแนน) พิจารณาการคูณ \mathbb{Z}_{22}^\times

16.1 (3 คะแนน) จงหา ตัวก่อกำเนิด (generator) ของ \mathbb{Z}_{22}^\times

แนวคำตอบ จะเห็นว่า $n = \phi(22) = \phi(2 \cdot 11) = (2 - 1)(11 - 1) = 10$ พิจารณา

$$\begin{aligned} (\bar{7})^1 &= \bar{7} \\ (\bar{7})^2 &= \overline{49} = \bar{5} \\ (\bar{7})^3 &= (\bar{7})(\bar{2})^2 = (\bar{7})(\bar{5}) = \overline{35} = \bar{13} \\ (\bar{7})^4 &= (\bar{7})(\bar{7})^3 = (\bar{7})(\bar{13}) = \overline{91} = \bar{3} \\ (\bar{7})^5 &= (\bar{7})(\bar{7})^4 = (\bar{7})(\bar{3}) = \overline{21} = \bar{-1} \\ (\bar{7})^6 &= (\bar{7})(\bar{7})^5 = (\bar{7})(\bar{-1}) = \overline{-7} = \bar{15} \\ (\bar{7})^7 &= (\bar{7})(\bar{7})^6 = (\bar{7})(\bar{-7}) = \overline{-49} = \bar{17} = \bar{-5} \\ (\bar{7})^8 &= (\bar{7})(\bar{7})^7 = (\bar{7})(\bar{-5}) = \overline{-35} = \bar{9} \\ (\bar{7})^9 &= (\bar{7})(\bar{7})^8 = (\bar{7})(\bar{9}) = \overline{63} = \bar{19} = \bar{-3} \\ (\bar{7})^{10} &= (\bar{7})(\bar{7})^9 = (\bar{7})(\bar{-3}) = \overline{-21} = \bar{1} \end{aligned}$$

ดังนั้น $\circ(\bar{7}) = 10 = n$

สรุปได้ว่า $\bar{7}$ เป็นตัวก่อกำเนิดของ \mathbb{Z}_{22}^\times #

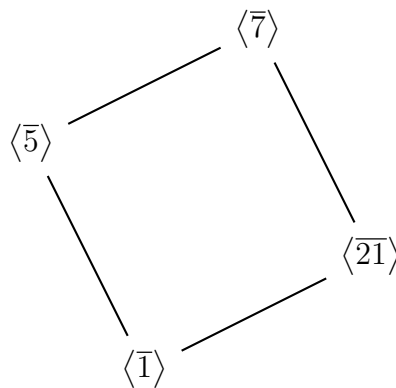
16.2 (4 คะแนน) จงหา กรุปย่อย (subgroup) ทั้งหมดของ \mathbb{Z}_{22}^\times (พร้อมแจกแจงสมาชิกของกรุปย่อย)

แนวคำตอบ จาก $\langle \bar{7} \rangle = \mathbb{Z}_{22}^\times$ ตัวหารของ 10 คือ 1, 2, 5, 10 ดังนั้นกรุปย่อยของ \mathbb{Z}_{22}^\times คือ

$$\begin{aligned} \langle (\bar{7})^{\frac{10}{1}} \rangle &= \langle (\bar{7})^{10} \rangle = \langle \bar{1} \rangle = \{ \bar{1} \} \\ \langle (\bar{7})^{\frac{10}{2}} \rangle &= \langle (\bar{7})^5 \rangle = \langle \bar{21} \rangle = \{ \bar{1}, \bar{21} \} \\ \langle (\bar{7})^{\frac{10}{5}} \rangle &= \langle (\bar{7})^2 \rangle = \langle \bar{5} \rangle = \{ \bar{1}, \bar{5}, \bar{3}, \bar{15}, \bar{9} \} \\ \langle (\bar{7})^{\frac{10}{10}} \rangle &= \langle (\bar{7})^1 \rangle = \langle \bar{7} \rangle = \mathbb{Z}_{22}^\times = \{ \bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{13}, \bar{15}, \bar{17}, \bar{19}, \bar{21} \} \end{aligned}$$

16.3 (3 คะแนน) จงนำกรุปย่อยจากข้อ 16.2 เขียน แลตทิซ (lattice)

แนวคำตอบ เขียนแลตทิซได้ดังนี้



17. (10 คะแนน) ให้ G เป็นกรุปจำกัดที่ $|G| = 6$

จงใช้ทฤษฎีบทลากรองจ์ (Lagrange's Theorem) แสดงว่ามีสมาชิกใน G ที่มีอันดับเท่ากับ 2 หรือ 3

แนวคำตอบ สมมติว่าไม่มีสมาชิกใน G ที่มีอันดับเท่ากับ 2 และ 3
ให้ $a \in G$ โดยที่ a ไม่ใช่เอกลักษณ์ จะได้ว่า

$\langle a \rangle$ เป็นกรุปย่อยของ G

โดยทฤษฎีบทลากรองจ์ (Lagrange's Theorem) $|\langle a \rangle|$ หาร $|G|$ ลงตัว หรือ $o(a) \mid 6$
ฉะนั้น $o(a) = 1, 2, 3, 6$ แต่ a ไม่ใช่เอกลักษณ์และไม่มีอันดับ 2 และ 3 ดังนั้น $o(a) = 6 = |G|$
ทำให้ได้ว่า ทุกสมาชิกใน G ที่ไม่ใช่เอกลักษณ์มีอันดับเท่ากับ 6 หรือกล่าวได้ว่า

ทุกสมาชิกที่ไม่ใช่เอกลักษณ์ เป็นตัวก่อกำเนิดของ G

นั่นคือจำนวนตัวก่อกำเนิดของ G เท่ากับ 5 เกิดข้อขัดแย้งกับทฤษฎีบทที่ว่าตัวก่อกำเนิดของ G เท่ากับ $\phi(6) = 2$

18. (10 คะแนน) ให้ N เป็นกรุปย่อย (subgroup) ของกรุป G จงพิสูจน์ว่า

$$\text{ถ้า } gNg^{-1} \subseteq N \text{ ทุก } g \in G \text{ แล้ว } (Nh)(Nk) = N(hk) \text{ ทุก } h, k \in G$$

แนวคำตอบ ให้ N เป็นกรุปย่อยของกรุป G สมมติว่า $gNg^{-1} \subseteq N$ ทุก $g \in G$
ให้ $h, k \in G$

ขั้นที่ 1 จะแสดงว่า $(Nh)(Nk) \subseteq N(hk)$

ให้ $x \in (Nh)(Nk)$ จะได้ว่ามี $n_1, n_2 \in N$ ซึ่ง $x = (n_1h)(n_2k) = n_1(hn_2)k$

$$\text{จะเห็นว่า } hn_2h^{-1} \in hNh^{-1} \subseteq N$$

นั่นคือมี $n_3 \in N$ ซึ่ง

$$\begin{aligned} hn_2h^{-1} &= n_3 \\ hn_2 &= n_3h \end{aligned}$$

เนื่องจาก $n_1n_3 \in N$ จะได้ว่า

$$x = n_1(hn_2)k = n_1(n_3h)k = (n_1n_3)hk \in N(hk)$$

ขั้นที่ 2 จะแสดงว่า $N(hk) \subseteq (Nh)(Nk)$

ให้ $x \in N(hk)$ จะได้ว่ามี $n \in N$ ซึ่ง $x = n(hk)$ เนื่องจาก $e \in N$ ฉะนั้น

$$x = n(hk) = (nh)(ek) \in (Nh)(Nk)$$

สรุปได้ว่า $(Nh)(Nk) = N(hk)$