คณิตศาสตร์

เฉลย Assignment 5
MAC3310 พีชคณิตนามธรรม

หัวข้อ กรุปวัฏจักร และกรุปวัฏจักร **สัปดาห์ที่** 5 **คะแนนเต็ม** 10 คะแนน
ผู้สอน ผศ.ดร.ธนัชยศ จำปาหวาย สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

---

1. จงพิสูจน์ว่ากรุปวัฏจักรเป็นกรุปอาบีเลียน

   บทพิสูจน์. ให้ G เป็นกรุปวัฏจักร จะได้ว่ามี $a \in G$ ซึ่ง $\langle a \rangle = G$ ให้ $x, y \in G$ แล้ว $x = a^n$ และ $y = a^m$ โดยที่ $n, m \in \mathbb{Z}$ จะได้ว่า

   $$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$$

   ดังนั้น G เป็นกรุปอาบีเลียน □

2. จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_4 \times \mathbb{Z}_9$
   วิธีทำ จะเห็นได้ว่า $(\bar{1}, \bar{1})$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_4 \times \mathbb{Z}_9$ และ $|\mathbb{Z}_4 \times \mathbb{Z}_9| = 4 \times 9 = 36$
   ตัวหารของ 36 คือ 1, 2, 3, 4, 6, 9, 12, 18, 36 ดังนั้นกรุปย่อยของ คือ $\mathbb{Z}_4 \times \mathbb{Z}_9$

   $$\left\langle \tfrac{36}{1}(\bar{1}, \bar{1}) \right\rangle \quad \left\langle \tfrac{36}{2}(\bar{1}, \bar{1}) \right\rangle \quad \left\langle \tfrac{36}{3}(\bar{1}, \bar{1}) \right\rangle$$
   $$\left\langle \tfrac{36}{4}(\bar{1}, \bar{1}) \right\rangle \quad \left\langle \tfrac{36}{6}(\bar{1}, \bar{1}) \right\rangle \quad \left\langle \tfrac{36}{9}(\bar{1}, \bar{1}) \right\rangle$$
   $$\left\langle \tfrac{36}{12}(\bar{1}, \bar{1}) \right\rangle \quad \left\langle \tfrac{36}{18}(\bar{1}, \bar{1}) \right\rangle \quad \left\langle \tfrac{36}{36}(\bar{1}, \bar{1}) \right\rangle$$

   นั่นคือ

   $$\langle (\bar{0}, \bar{0}) \rangle \quad \langle (\bar{2}, \bar{0}) \rangle \quad \langle (\bar{0}, \bar{3}) \rangle$$
   $$\langle (\bar{5}, \bar{0}) \rangle \quad \langle (\bar{2}, \bar{6}) \rangle \quad \langle (\bar{0}, \bar{4}) \rangle$$
   $$\langle (\bar{3}, \bar{3}) \rangle \quad \langle (\bar{2}, \bar{2}) \rangle \quad \langle (\bar{1}, \bar{1}) \rangle$$

3. จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_{27}^{\times}$
   วิธีทำ $|\mathbb{Z}_{27}^{\times}| = \phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$ จะเห็นว่า

$(\bar{2})^1 = \bar{2}$	$(\bar{2})^7 = \overline{20}$	$(\bar{2})^{13} = \overline{-16} = \overline{11}$
$(\bar{2})^2 = \bar{4}$	$(\bar{2})^8 = \overline{40} = \overline{13}$	$(\bar{2})^{14} = \overline{22}$
$(\bar{2})^3 = \bar{8}$	$(\bar{2})^9 = \overline{26} = \overline{-1}$	$(\bar{2})^{15} = \overline{44} = \overline{17}$
$(\bar{2})^4 = \overline{16}$	$(\bar{2})^{10} = \overline{-2} = \overline{25}$	$(\bar{2})^{16} = \overline{34} = \bar{7}$
$(\bar{2})^5 = \overline{32} = \bar{5}$	$(\bar{2})^{11} = \overline{-4} = \overline{23}$	$(\bar{2})^{17} = \overline{14}$
$(\bar{2})^6 = \overline{10}$	$(\bar{2})^{12} = \overline{-8} = \overline{17}$	$(\bar{2})^{18} = \overline{28} = \bar{1}$

   ดังนั้น $\langle \bar{2} \rangle = \mathbb{Z}_{27}^{\times}$ ตัวหารของ 18 คือ 1, 2, 3, 6, 9, 18 ดังนั้นกรุปย่อยของ $\mathbb{Z}_{27}^{\times}$ คือ

   $$\left\langle (\bar{2})^{\frac{18}{1}} \right\rangle, \left\langle (\bar{2})^{\frac{18}{2}} \right\rangle, \left\langle (\bar{2})^{\frac{18}{3}} \right\rangle, \left\langle (\bar{2})^{\frac{18}{6}} \right\rangle, \left\langle (\bar{2})^{\frac{18}{9}} \right\rangle \text{ และ } \left\langle (\bar{2})^{\frac{18}{18}} \right\rangle$$

นั่นคือ

$$\langle\bar{1}\rangle,\ \langle\overline{26}\rangle,\ \langle\overline{10}\rangle,\ \langle\overline{8}\rangle,\ \langle\bar{4}\rangle \text{ และ } \langle\bar{2}\rangle$$

4. จงหาตัวก่อกำเนิดของ $\mathbb{Z}_3 \times \mathbb{Z}_5$
วิธีทำ จะเห็นได้ว่า $(\bar{1},\bar{1})$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_3 \times \mathbb{Z}_5$ และ $|\mathbb{Z}_3 \times \mathbb{Z}_5| = 3 \times 5 = 15$ และ $1 \leq k < 15$ ซึ่ง $\gcd(k, 15) = 1$
ประกอบไปด้วย $k = 1, 2, 4, 7, 8, 11, 13, 14,$ ตัวก่อกำเนิดทั้งหมดคือ

$$1(\bar{1},\bar{1}),\ 2(\bar{1},\bar{1}),\ 4(\bar{1},\bar{1}),\ 7(\bar{1},\bar{1}),\ 8(\bar{1},\bar{1}),\ 9(\bar{1},\bar{1}),\ 11(\bar{1},\bar{1}),\ 13(\bar{1},\bar{1}) \text{ และ } 14(\bar{1},\bar{1})$$

นั่นคือ

$$(\bar{1},\bar{1}),\ (\bar{2},\bar{2}),\ (\bar{1},\bar{4}),\ (\bar{4},\bar{2}),\ (\bar{2},\bar{3}),\ (\bar{0},\bar{4}),\ (\bar{2},\bar{1}),\ (\bar{1},\bar{3}) \text{ และ } (\bar{2},\bar{4})$$

5. จงหาตัวก่อกำเนิดของ $\mathbb{Z}_{26}^{\times}$
วิธีทำ $|\mathbb{Z}_{26}^{\times}| = \phi(26) = \phi(2 \cdot 13) = 12$ จะเห็นว่า

$(\bar{7})^1 = \bar{7}$	$(\bar{7})^5 = \overline{63} = \overline{11}$	$(\bar{7})^9 = \overline{21} = \overline{-5}$
$(\bar{7})^2 = \overline{49} = \overline{-3}$	$(\bar{7})^6 = \overline{77} = \overline{-1}$	$(\bar{7})^{10} = \overline{-35} = \overline{-9} = \overline{17}$
$(\bar{7})^3 = \overline{-21} = \bar{5}$	$(\bar{7})^7 = \overline{-7} = \overline{19}$	$(\bar{7})^{11} = \overline{-63} = \overline{-11} = \overline{15}$
$(\bar{7})^4 = \overline{35} = \bar{9}$	$(\bar{7})^8 = \overline{-49} = \bar{3}$	$(\bar{7})^{12} = \overline{-77} = \bar{1}$

ดังนั้น $\langle\bar{7}\rangle = \mathbb{Z}_{26}^{\times}$ และ $1 \leq k < 12$ ซึ่ง $\gcd(k, 12) = 1$ ประกอบไปด้วย $k = 1, 5, 7, 11$
ตัวก่อกำเนิดทั้งหมดคือ $(\bar{7})^1,\ (\bar{7})^5,\ (\bar{7})^7$ และ $(\bar{7})^{11}$ นั่นคือ

$$\bar{7},\ \overline{11},\ \overline{19} \text{ และ } \overline{15} \text{ ตัวก่อกำเนิดทั้งหมดของ } \mathbb{Z}_{26}^{\times}$$

6. ให้ x เป็นสมาชิกในกรุป G โดยที่ $\circ(x) = n$ เมื่อ $n \in \mathbb{N}$ จงพิสูจน์ว่า สำหรับจำนวนเต็ม k

$$\text{ถ้า} \quad \gcd(k, n) = 1 \quad \text{แล้ว} \quad \circ(x^k) = n$$

บทพิสูจน์. ให้ $x \in G$ โดยที่ $\circ(x) = n$ เมื่อ $n \in \mathbb{N}$ และ $k \in \mathbb{Z}$
สมมติว่า $\gcd(k, n) = 1$ จะได้ว่า

$$(x^k)^n = (x^n)^k = e^k = e$$

ให้ $m \in \mathbb{N}$ ซึ่ง $(x^k)^m = e$ จะแสดงว่า $n \leq m$ (แสดงว่า n เป็นตัวเล็กสุด)
โดยขั้นตอนวิธีการหารจะได้ว่ามี $q, r \in \mathbb{Z}$ ซึ่ง

$$m = nq + r \qquad \text{เมื่อ } 0 \leq r < n$$

ดังนั้น

$$e = (x^k)^m = x^{km} = x^{knq+kr} = (x^n)^{kq}x^{kr} = e^{kq}x^{kr} = ex^{kr} = x^{kr}$$

เนื่องจาก $\circ(x) = n$ โดยทฤษฎีบทจะได้ว่า $n \mid (kr)$ แต่ $\gcd(k, n) = 1$ ดังนั้น $n \mid r$
นั่นคือ $r = nd$ สำหรับบางจำนวนเต็ม d แล้ว

$$m = nq + nd = n(q + d)$$

ฉะนั้น $n \mid m$ เนื่องจาก $m > 0$ และ $n > 0$ ดังนั้น $n \leq m$ สรุปได้ว่า $\circ(x^k) = n$ □

7. จงหาจำนวนกรุปย่อยทั้งหมดของ $\mathbb{Z}_{2564} \times \mathbb{Z}_{2021}$

วิธีทำ เนื่องจาก $\gcd(2564, 2021) = 1$ จะได้ว่า $\mathbb{Z}_{2564} \times \mathbb{Z}_{2021}$ เป็นกรุปวัฏจักร ฉะนั้นจำนวนกรุปย่อยทั้งหมดจะเท่ากับจำนวนตัวหารของ $|\mathbb{Z}_{2564} \times \mathbb{Z}_{2021}| = 2562 \cdot 2021$ หรือเท่ากับ

$$\begin{aligned} \tau(2564 \cdot 2021) &= \tau(2^2 \cdot 641 \cdot 43 \cdot 47) \\ &= (2+1)(1+1)(1+1)(1+1) \\ &= 24 \quad \# \end{aligned}$$

8. ถ้า $\langle a \rangle$ เป็นกรุปอนันต์ จงพิสูจน์ว่า

$$a^m = a^n \quad \text{ก็ต่อเมื่อ} \quad m = n$$

บทพิสูจน์. ให้ $\langle a \rangle$ เป็นกรุปอนันต์ ถ้า $m = n$ เห็นได้ชัดว่า $a^m = a^n$ ในทางกลับกันให้ $a^m = a^n$ สมมติว่า $m \neq n$ โดยไม่เสียนัยทั่วไป $m > n$ นั่นคือ $m - n \in \mathbb{N}$ แล้ว

$$a^{m-n} = a^m a^{-n} = a^n a^{-n} = e$$

กำหนดให้

$$S = \{k \in \mathbb{N} : a^k = e\}$$

แล้ว $S \subseteq \mathbb{N}$ เนื่องจาก $m - n \in S$ ดังนั้น $S \neq \varnothing$ โดยหลักการจัดอันดับดีจะได้ว่า S มีสมาชิกตัวเล็กสุดซึ่งเท่ากับ $\circ(a)$ จะได้ว่า

$$|\langle a \rangle| = \circ(a) \quad \text{มีค่าจำกัด}$$

เกิดข้อขัดแย้งกับ $\langle a \rangle$ เป็นกรุปอนันต์ สรุปได้ว่า $m = n$ □