

การพิสูจน์เชิงการสร้างเพื่อหาโฮโมมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัด

ปริญญานิพนธ์

ของ

อัจฉริยา ชมะนันท์

เสนอต่อบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ เพื่อเป็นส่วนหนึ่งของการศึกษา

ตามหลักสูตรปริญญาการศึกษามหาบัณฑิต วิชาเอกคณิตศาสตร์

กุมภาพันธ์ 2543

ลิขสิทธิ์เป็นของ มหาวิทยาลัยศรีนครินทรวิโรฒ

512

0513 n

3.3

การพิสูจน์เชิงการสร้างเพื่อหาไฮโมมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัด

บทคัดย่อ

ของ

อัจฉริยา ชมะนันท์

19 May 2543

เสนอต่อบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ เพื่อเป็นส่วนหนึ่งของการศึกษา

ตามหลักสูตรปริญญาการศึกษามหาบัณฑิต วิชาเอกคณิตศาสตร์

กุมภาพันธ์ 2543

อัจฉริยา ชมะนันท์. (2543) การพิสูจน์เชิงการสร้างเพื่อหาโฮโมมอร์ฟิซึมของโครงสร้างทาง.

พีชคณิตจำกัด. ปรินซ์ตันพรีส กศ.ม. (คณิตศาสตร์). กรุงเทพฯ : บัณฑิตวิทยาลัย
มหาวิทยาลัยศรีนครินทรวิโรฒ. คณะกรรมการควบคุม: รองศาสตราจารย์ ดร. ณรงค์
ปັນนิม, รองศาสตราจารย์ กมล เอกไทยเจริญ

ผู้วิจัยได้ศึกษาเอกสารที่เขียนโดย แกลเลี่ยน และ บัสเคอร์ค (1984) ซึ่งแสดงจำนวน
ของกรุปโฮโมมอร์ฟิซึม และริงโฮโมมอร์ฟิซึม และเอกสารที่เขียนโดย ซาเลซ โยเซฟ และอาบู-
ฮไล (1998) ซึ่งแสดงการหาจำนวนของโฮโมมอร์ฟิซึมจาก $Z_{m_1} \times Z_{m_2} \times Z_{m_3} \times \dots \times Z_{m_r}$
ไป $Z_{k_1} \times Z_{k_2} \times Z_{k_3} \times \dots \times Z_{k_s}$ แล้วติดต่อกับ แกลเลี่ยน และ ซาเลซ ทางไปรษณีย์
อิเล็กทรอนิกส์ทำให้ได้รับเอกสารฉบับล่าสุดเกี่ยวกับการพิสูจน์เรื่องดังกล่าวข้างต้น อย่างไรก็ตาม
ผู้วิจัยพบว่าการพิสูจน์นั้นได้แสดงเพียงวิธีการหาจำนวนของโฮโมมอร์ฟิซึมเท่านั้น แต่ไม่ได้
แสดงถึงลักษณะของโฮโมมอร์ฟิซึม ดังนั้นผู้วิจัยจึงเกิดแนวคิดที่จะศึกษาถึงลักษณะของ
โฮโมมอร์ฟิซึมจาก Z_m ไป Z_n $Z_m[i]$ ไป $Z_n[i]$ และ $Z_m[p]$ ไป $Z_n[p]$ โดยใช้
การพิสูจน์เชิงการสร้าง และความรู้พื้นฐานทางคณิตศาสตร์ ซึ่งได้แก่ ทฤษฎีจำนวนเบื้องต้น
พีชคณิตนามธรรม และเทคนิคการนับ ผลการศึกษานี้ นอกจากจะยืนยันผลลัพธ์ตามเอกสาร
ของแกลเลี่ยนดังกล่าวแล้ว ยังสามารถสร้างลักษณะทั้งหมดของโฮโมมอร์ฟิซึมได้อีกด้วย

ON CONSTRUCTED PROOF IN FINDING HOMOMORPHISMS OF
FINITE ALGEBRAIC STRUCTURES

AN ABSTRACT
BY
ACHARIYA CHAMANUNTANA

Presented in partial fulfillment of the requirements for the
Master of Education degree in Mathematics
at Srinakharinwirot University
February 2000

Achariya Chamanuntana (2000). *On Constructed Proof in Finding Homomorphisms of Finite Algebraic Structures*. Master thesis, M.A.(Mathematics). Bangkok : Graduate School, Srinakharinwirot University. Advisor committee: Assoc.Prof.Dr.Narong Punnim, Assoc.Prof.Kamon Eakthaichareon.

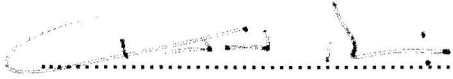
The researcher started this thesis by studying literatures concerning the number of group homomorphisms and ring homomorphisms those have been written by Gallian and Buskirk(1984). The researcher has studied a similar work in finding the number of homomorphisms from $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots \times \mathbb{Z}_{m_r}$ into $\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \mathbb{Z}_{k_3} \times \dots \times \mathbb{Z}_{k_s}$ which has been done by Saleh , Saleh & Abu-Hlail (1998).By contacting Gallian and Saleh via e-mail, the researcher has received more update literature from both of them. However, the researcher found that the original proof displayed only how to find the number of the corresponding homomorphisms of a given algebraic structure without showing how to characterize such homomorphisms. Therefore , the researcher had an idea to characterize all group homomorphisms and ring homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$, $\mathbb{Z}_m[i]$ into $\mathbb{Z}_n[i]$ and $\mathbb{Z}_m[\rho]$ into $\mathbb{Z}_n[\rho]$. By using constructed proof and elementary knowledge in mathematics such as : Elementary Number Theory, Abstract Algebra and Counting Technique, the researcher has show not only to confirm all those results in the literatures but she has constructed all of those results explicitly.

ปริญญานิพนธ์
เรื่อง

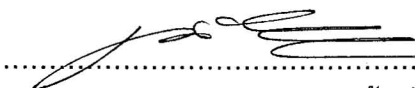
การพิสูจน์เชิงการสร้างเพื่อหาไฮโมเมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัด

ของ
นางสาวอัจฉริยา ชมะนันท์

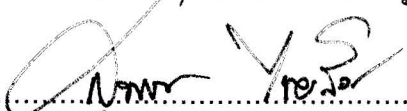
ได้รับอนุมัติจากบัณฑิตวิทยาลัยให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาการศึกษามหาบัณฑิต วิชาเอกคณิตศาสตร์
ของมหาวิทยาลัยศรีนครินทรวิโรฒ

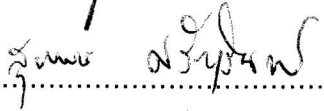
 คณบดีบัณฑิตวิทยาลัย
(ศาสตราจารย์ ดร.เสริมศักดิ์ วิศาลาภรณ์)
วันที่ เดือน พ.ศ. 2543

คณะกรรมการสอบปริญญานิพนธ์

 ประธาน
(รองศาสตราจารย์ ดร.ณรงค์ ป้านิยม)

 กรรมการ
(รองศาสตราจารย์ กมล เอกไทยเจริญ)

 กรรมการแต่งตั้งเพิ่มเติม
(ผู้ช่วยศาสตราจารย์ ดร.สุพจน์ ไชยสังข์)

 กรรมการแต่งตั้งเพิ่มเติม
(ผู้ช่วยศาสตราจารย์ สุภาพร ศรีบุรินทร์)

ประกาศคุณูปการ

งานวิจัยนี้ได้รับทุนสนับสนุนการวิจัย " ทุนภูมิพล "

ผู้วิจัยขอโน้มระลึกถึงพระคุณคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิทยาการแก่

ผู้วิจัย

ปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยความกรุณาจากรองศาสตราจารย์ ดร.ณรงค์ ปันนัม ประธานกรรมการควบคุมปริญญานิพนธ์ และ รองศาสตราจารย์ กมล เอกไทยเจริญ กรรมการควบคุมปริญญานิพนธ์ ในการสละเวลาเวลาอันมีค่าของท่านให้คำปรึกษา คำแนะนำแนวคิด และตรวจอ่านปริญญานิพนธ์ ทำให้งานวิจัยมีความชัดเจน สมบูรณ์ ก่อให้เกิดประโยชน์แก่ผู้วิจัยอย่างยิ่ง ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอกราบขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.สุพจน์ ไชยสังข์ และ ผู้ช่วยศาสตราจารย์ สุภาพร ศรีบรินทร์ ได้กรุณาเป็นกรรมการสอบปริญญานิพนธ์ และให้คำแนะนำที่เป็นประโยชน์ต่อการนำเสนอผลงานวิจัยเป็นอย่างยิ่ง

ขอขอบคุณ ดร. วรณวิภา สุทธเกียรติ อาจารย์ 2 ระดับ 7 โรงเรียนสามเสนวิทยาลัย ที่ให้คำแนะนำตลอดจนความช่วยเหลือในทุกๆ ด้าน

ท้ายนี้ผู้วิจัยขอกราบขอบพระคุณ คุณป้า และคุณน้าทั้งหลายได้แก่ คุณสุรี คุณวัฒนา คุณภรณ์ พ.อ.(พิเศษ)หญิง พรพรรณ คุณเพียงเพ็ญ สุคันธนาถ ผู้ให้การอุปการะอบรมเลี้ยงดูวางพื้นฐานทางการศึกษา และตลอดจนให้กำลังใจ รวมถึง คุณวิภาวดี ชมนันทน์ ที่ให้ความช่วยเหลือในทุกๆ ด้าน

อัจฉริยา ชมนันทน์

สารบัญ

บทที่		หน้า
1	บทนำ.....	1
	ภูมิหลัง.....	1
	จุดมุ่งหมายของการวิจัย.....	3
	ความสำคัญของการวิจัย.....	3
	ขอบเขตของการวิจัย.....	3
	นิยามศัพท์เฉพาะ.....	4
2	เอกสารและงานวิจัยที่เกี่ยวข้อง.....	7
3	แนวทางในการพิสูจน์เชิงการสร้างเพื่อหาไฮโมอร์ฟิซึมของโครงสร้าง ทางพีชคณิตจำกัด.....	11
4	วิธีดำเนินการพิสูจน์.....	14
	1. ทฤษฎีบทพื้นฐานในการพิสูจน์.....	14
	2. การพิสูจน์พิสูจน์เชิงการสร้างเพื่อหาไฮโมอร์ฟิซึม ของโครงสร้างทางพีชคณิตจำกัด.....	25
	2.1 การพิสูจน์หาจำนวนและลักษณะของกลุ่มไฮโมอร์ฟิซึม.....	25
	2.2 การพิสูจน์หาจำนวนและลักษณะของริงไฮโมอร์ฟิซึม.....	34
5	สรุปผล	84
	บรรณานุกรม.....	97
	ประวัติย่อผู้วิจัย.....	99

บทที่ 1

บทนำ

ภูมิหลัง

ปัจจุบัน เราถือว่าคณิตศาสตร์เป็นวิชาหนึ่งเดียวที่สามารถนำเนื้อหาและวิธีการในสาขาต่าง ๆ มาพัฒนาร่วมกัน ผสมผสานกันโดยไม่มีการแบ่งแยก และถือว่าระบบคณิตศาสตร์แต่ละระบบประกอบด้วย อนิยาม บทนิยาม และ สัจพจน์ แล้วสรุปเป็นทฤษฎีบท โดยอาศัยการให้เหตุผลตามหลักตรรกศาสตร์อย่างสมเหตุสมผล (สุเทพ จันทรสมศักดิ์. 2536 : 33) ถ้าเราศึกษาวิชาคณิตศาสตร์แยกตามสาขาต่าง ๆ โดยเด็ดขาด เช่น เลขคณิต พีชคณิต เรขาคณิต ทฤษฎีจำนวน เป็นต้น ในแต่ละสาขาจะแก้ปัญหามันเองได้ระดับหนึ่ง แต่บางปัญหาไม่สามารถที่จะแก้ได้อย่างสมบูรณ์ จะมีปัญหาที่คิดไม่ออกเนื่องจากการขาดมโนคติ หรือวิธีการที่จำเป็นในการแก้ปัญหานั้น ดังนั้น ควรจะศึกษาคณิตศาสตร์สาขาต่าง ๆ ร่วมกัน เพื่อนำจุดเด่นของสาขาหนึ่งไปใช้แก้ไขจุดอ่อนของอีกสาขาหนึ่ง ซึ่งเป็นแนวทางที่ทำให้การแก้ปัญหามีประสิทธิภาพมากขึ้น (พิชากร แปลงประสพโชค. 2534 : 22-30) ดังนั้น คณิตศาสตร์ทุกสาขาสามารถนำไปประยุกต์ใช้ในสาขาอื่นได้เพื่อทำให้เกิดความเข้าใจได้รวดเร็วและดียิ่งขึ้น และโครงสร้างของระบบคณิตศาสตร์ใดๆ ก็ตาม เราจะศึกษาได้ดีและรวดเร็วเมื่อเรามีความเข้าใจต่อโครงสร้างของระบบคณิตศาสตร์นั้น หรือเป็นโครงสร้างที่เราคุ้นเคยแล้วพยายามหาข้อคล้ายคลึงกันเพื่อทำให้การศึกษาโครงสร้างที่ยากขึ้นไปนั้นทำได้ง่ายขึ้น (ณรงค์ บัณฑิต. 2536 : คำนำ)

พีชคณิตนามธรรมเป็นสาขาหนึ่งในคณิตศาสตร์ที่ถูกนิยามขึ้นในปี ค.ศ.1882 พีชคณิตนามธรรมนั้น พิสูจน์ทฤษฎีบทเพียงครั้งเดียว แต่สามารถนำไปใช้ได้หลายกรณี ตัวอย่างเกี่ยวกับกรุปไม่ได้ใช้ประโยชน์ในวิชาคณิตศาสตร์เท่านั้น แต่ยังสามารถนำแบบจำลองของกรุปไปประยุกต์ใช้ในวิชาต่าง ๆ มากมาย อาทิ เคมี ฟิสิกส์ และ เศรษฐศาสตร์ ทฤษฎีบท

ต่าง ๆ ของกรุปสามารถใช้กับแบบจำลองเหล่านี้ได้ด้วย ถ้าเปลี่ยนแปลงสมบัติในระบบ เราก็จะสร้างระบบพีชคณิตมากมายที่มีโครงสร้างแตกต่างกัน ระบบพีชคณิตนามธรรมที่สำคัญได้แก่ กรุป ริง ฟิลด์ มอดูล ในที่นี้เราสนใจกรุปและริง เพราะกรุปและริงนั้นมีโครงสร้างคล้ายกัน ถ้าเราเข้าใจโครงสร้างของกรุปเป็นอย่างดีแล้ว จะทำให้เราศึกษาถึงโครงสร้างของริงได้ง่ายยิ่งขึ้น

โฮโมมอร์ฟิซึมเป็นเครื่องมือที่สำคัญในการตรวจสอบสมบัติทางโครงสร้างทางพีชคณิตของกรุปและริง โดยอ่านจากโครงสร้างทางพีชคณิตของกรุปหรือริงที่ง่ายกว่านำไปสู่กรุปและริงที่มีโครงสร้างซับซ้อนมากกว่าได้ ในปี ค.ศ.1984 แกลเลียน และ บัสเคอร์ค (Gallian and Buskirk, 1984 : 196-197) ได้เขียนผลงานวิจัยเรื่อง The Number of Homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ ตีพิมพ์ในวารสารชื่อ The American Mathematical Monthly และในปี ค.ศ. 1998 ซาเลซ, โยเซฟ และอาบู-ฮไล (Saleh, Yousef & Abu-Hlail, 1998 : 326-329) ได้เขียนผลงานวิจัยเรื่อง The Number of Homomorphisms from $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots \times \mathbb{Z}_{m_r}$ into $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3} \times \dots \times \mathbb{Z}_{n_s}$ ตีพิมพ์ในวารสารชื่อ Dirasat : ซึ่งศึกษาจำนวนของกรุปโฮโมมอร์ฟิซึมและจำนวนของริงโฮโมมอร์ฟิซึม เมื่อผู้วิจัยได้ติดต่อกับ แกลเลียน (Gallian, 1998) และ ซาเลซ (Saleh, 1999) จนได้รับเอกสารจากพวกเขาทั้งสองมาศึกษาพบว่า ในบทพิสูจน์ของพวกเขาเน้นเพียงแต่แสดงการหาจำนวนโฮโมมอร์ฟิซึมเท่านั้น แต่ไม่ได้แสดงวิธีหาลักษณะของโฮโมมอร์ฟิซึมดังกล่าว ทำให้ผู้วิจัยเกิดแนวความคิดที่จะแสดงการพิสูจน์ให้เห็นว่ากรุปโฮโมมอร์ฟิซึมและ ริงโฮโมมอร์ฟิซึม จาก $\mathbb{Z}_m$ ไป $\mathbb{Z}_n$, $\mathbb{Z}_m[i]$ ไป $\mathbb{Z}_n[i]$ และ $\mathbb{Z}_m[p]$ ไป $\mathbb{Z}_n[p]$ มีลักษณะอย่างไร และแจกแจงได้เมื่อกำหนดทุก ๆ จำนวนเต็มบวก m, n ทั้งนี้วิธีการพิสูจน์ที่ผู้วิจัยใช้คือ การพิสูจน์เชิงการสร้าง (constructed proof) ซึ่งเป็นการพิสูจน์ในแนวที่แตกต่างจากเดิม โดยที่การพิสูจน์เชิงการสร้างนี้สามารถบอกถึงลักษณะและรายละเอียดของสมาชิกภายใน เซตคำตอบได้ ซึ่งสอดคล้องกับความต้องการของผู้วิจัยที่ต้องการแสดงลักษณะของ กรุปโฮโมมอร์ฟิซึมและริงโฮโมมอร์ฟิซึมดังกล่าว

จุดมุ่งหมายของการวิจัย

เสนอการพิสูจน์เพื่อหาจำนวนของกลุ่มโฮโมมอร์ฟิซึมและริงโฮโมมอร์ฟิซึมแนวใหม่ ซึ่งการพิสูจน์นี้สามารถแสดงให้เห็นถึงลักษณะของกลุ่มโฮโมมอร์ฟิซึมและริงโฮโมมอร์ฟิซึม จาก Z_m ไป Z_n , $Z_m[i]$ ไป $Z_n[i]$, $Z_m[p]$ ไป $Z_n[p]$ และแจกแจงได้เมื่อกำหนดทุก ๆ จำนวนเต็มบวก m, n

ความสำคัญของการวิจัย

1. รูปแบบการพิสูจน์เชิงการสร้างที่แสดงในงานวิจัยนี้ สามารถนำไปใช้เป็นแนวทางของการพิสูจน์เนื้อหาอื่นๆ ทางคณิตศาสตร์ต่อไป
2. ผลสรุปที่ได้จากการวิจัย สามารถนำไปใช้เป็นเอกสารอ้างอิงสำหรับผู้สนใจต่อไป

ขอบเขตของการวิจัย

ในการหาลักษณะของกลุ่มโฮโมมอร์ฟิซึมและริงโฮโมมอร์ฟิซึม และแจกแจงได้เมื่อกำหนดทุก ๆ จำนวนเต็มบวก m, n นั้น จะศึกษาเฉพาะ 3 กรณี ดังนี้

1. จาก Z_m ไป Z_n
2. จาก $Z_m[i]$ ไป $Z_n[i]$
3. จาก $Z_m[p]$ ไป $Z_n[p]$

นิยามศัพท์เฉพาะ

1. ออยเลอร์ ฟาย-ฟังก์ชัน (Euler ϕ -function)

บทนิยาม กำหนด $n \in \mathbb{Z}^+$ ซึ่ง $n \geq 2$; $\mathbb{Z}_n^* = \{ \bar{a} \in \mathbb{Z}_n \mid \gcd(a,n) = 1 \}$

ให้ $\phi(n)$ แทนจำนวนสมาชิกของ $\mathbb{Z}_n^*$

ฟังก์ชัน ϕ มีชื่อเรียกโดยทั่วไปว่า ออยเลอร์ ฟาย-ฟังก์ชัน

2. ชิคคลิกสับกรุป (cyclic subgroup)

บทนิยาม ให้ G เป็นกรุป $a \in G$ เรียกสับกรุป $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$

ว่า ชิคคลิกสับกรุป G ที่มี a เป็นเจนเนอเรเตอร์ (generator)

3. แฟกเตอร์กรุป (factor group)

บทนิยาม ให้ N เป็นนอร์มัลสับกรุป (normal subgroup) ของ G เรียก

$$G/N = \{ aN \mid a \in G \} \text{ ว่า แฟกเตอร์กรุปของ } G$$

เมื่อเทียบกับ นอร์มัลสับกรุป N

4. แฟกเตอร์ริง (factor ring)

บทนิยาม ให้ A เป็นไอดีล (ideal) ของริง R เรียก

$$R/A = \{ r+A \mid r \in R \} \text{ ว่า แฟกเตอร์ริงของ } R$$

เมื่อเทียบกับไอดีล A

5. กรุปโฮโมมอร์ฟิซึม (group homomorphism)

บทนิยาม กำหนดกรุป $\langle G, * \rangle$ และ $\langle H, \circ \rangle$

เรียก $f: G \rightarrow H$ ว่าโฮโมมอร์ฟิซึม จากกรุป G ไป H ก็ต่อเมื่อ

สำหรับทุก ๆ สมาชิก a, b ใน G ซึ่ง $f(a*b) = f(a) \circ f(b)$

เขียน $\text{GroupHom}(G, H)$ แทนเซตของกรุปโฮโมมอร์ฟิซึมทั้งหมด
จาก G ไป H

6. ริงโฮโมมอร์ฟิซึม (ring homomorphism)

บทนิยาม กำหนดริง $\langle R, +, \cdot \rangle$ และ $\langle S, \oplus, \otimes \rangle$

เรียก $f: R \rightarrow S$ ว่าโฮโมมอร์ฟิซึม จากริง R ไป S ก็ต่อเมื่อ

สำหรับทุก ๆ สมาชิก a, b ใน R ซึ่ง $f(a + b) = f(a) \oplus f(b)$

และ $f(a \cdot b) = f(a) \otimes f(b)$

เขียน $\text{RingHom}(R, S)$ แทนเซตของริงโฮโมมอร์ฟิซึมทั้งหมด
จาก R ไป S

7. จำนวนเต็มแบบเกาส์ และจำนวนเต็มแบบเกาส์มอดุโล n (the Gaussian integer and the Gaussian integer modulo n)

บทนิยาม กำหนด $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}, i^2 + 1 = 0\}$

และ $\mathbb{Z}_n[i] = \mathbb{Z}[i] / \langle n \rangle$

เรียก $\mathbb{Z}[i]$ แทนเซตของจำนวนเต็มแบบเกาส์

และ $\mathbb{Z}_n[i]$ แทนเซตของจำนวนเต็มแบบเกาส์มอดุโล n

8. จำนวนเต็มแบบไอเซนสไตน์-จาคอบี และจำนวนเต็มแบบไอเซนสไตน์-จาคอบี

มอดูโล n (the Eisenstein – Jacobi integer and the Eisenstein – Jacobi integer modulo n)

บทนิยาม กำหนด $\mathbb{Z}[\rho] = \{ a+b\rho \mid a, b \in \mathbb{Z}, \rho^2 + \rho + 1 = 0 \}$

$$\text{และ } \mathbb{Z}_n[\rho] = \mathbb{Z}[\rho] / \langle n \rangle$$

เรียก $\mathbb{Z}[\rho]$ แทนเซตของจำนวนเต็มแบบไอเซนสไตน์-จาคอบีและ

$\mathbb{Z}_n[\rho]$ แทนเซตของจำนวนเต็มแบบไอเซนสไตน์-จาคอบี มอดูโล n

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

แกลเลี่ยน และ บัสเคอร์ค (Gallian and Buskirk. 1984 : 196-197) แห่งมหาวิทยาลัยมินนิโซตา สหรัฐอเมริกา ได้ศึกษาเกี่ยวกับการหาจำนวนของกลุ่มโฮโมมอร์ฟิซึม และริงโฮโมมอร์ฟิซึม จาก Z_m ไป Z_n ได้ผลดังต่อไปนี้

จำนวนของกลุ่มโฮโมมอร์ฟิซึม จาก Z_m ไป Z_n เท่ากับ $\gcd(m,n)$ และ

จำนวนของริงโฮโมมอร์ฟิซึม จาก Z_m ไป Z_n เท่ากับ 2^β

$$\text{โดยที่ } \beta = \omega(n) - \omega\left(\frac{n}{\gcd(m,n)}\right) \text{ เมื่อ}$$

$\omega(n)$ คือจำนวนของจำนวนเฉพาะที่แตกต่างกันและหาร n ลงตัว

ต่อมาในปี ค.ศ. 1988 แกลเลี่ยนและจังก์เรลส (Gallian and Jungrels. 1988 : 247-248) ได้ศึกษาต่อเกี่ยวกับการหาจำนวนของกลุ่มโฮโมมอร์ฟิซึม และริงโฮโมมอร์ฟิซึม จาก $Z_m[i]$ ไป $Z_n[i]$ และ $Z_m[p]$ ไป $Z_n[p]$ โดยที่ $i^2 + 1 = 0$ และ $p^2 + p + 1 = 0$ ได้ผลดังต่อไปนี้

จำนวนของกลุ่มโฮโมมอร์ฟิซึม จาก $Z_m[i]$ ไป $Z_n[i]$ และ $Z_m[p]$ ไป $Z_n[p]$

เท่ากับ $(\gcd(m,n))^4$

จำนวนของริงโฮโมมอร์ฟิซึมจาก $Z[i]$ ไป $Z_n[i]$ เท่ากับ $C_n \cdot 3^{\omega(n)}$

ซึ่ง $\omega(n)$ คือจำนวนของจำนวนเฉพาะที่แตกต่างกันและหาร n ลงตัว

โดยที่ $C_n = 1$ ถ้า $4 \nmid n$,

$$C_n = \frac{5}{3} \quad \text{ถ้า } 4 \mid n \text{ แต่ } 8 \nmid n$$

$$\text{และ } C_n = 3 \quad \text{ถ้า } 8 \mid n$$

จำนวนของริงโฮโมมอร์ฟิซึมจาก $\mathbb{Z}_m[i]$ ไป $\mathbb{Z}_n[i]$ เท่ากับ $C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 4 \nmid n \text{ หรือ } 2 \mid \left(\frac{n}{\gcd(m, n)} \right),$$

$$C_n = \frac{5}{3} \quad \text{ถ้า } 2 \nmid \left(\frac{n}{\gcd(m, n)} \right) \text{ และ } 4 \mid n \text{ แต่ } 8 \nmid n$$

$$\text{และ } C_n = 3 \quad \text{ถ้า } 2 \nmid \left(\frac{n}{\gcd(m, n)} \right) \text{ และ } 8 \mid n$$

จำนวนของริงโฮโมมอร์ฟิซึม จาก $\mathbb{Z}[p]$ ไป $\mathbb{Z}_n[p]$ เท่ากับ $C_n \cdot 3^{\omega(n)}$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 3 \nmid n,$$

$$C_n = \frac{4}{3} \quad \text{ถ้า } 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ } C_n = \frac{7}{3} \quad \text{ถ้า } 9 \mid n$$

จำนวนริงโฮโมมอร์ฟิซึมจาก $\mathbb{Z}_m[p]$ ไป $\mathbb{Z}_n[p]$ เท่ากับ $C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 3 \nmid n \text{ แต่ } 3 \mid \left(\frac{n}{\gcd(m, n)} \right),$$

$$C_n = \frac{4}{3} \quad \text{ถ้า } 3 \nmid \left(\frac{n}{\gcd(m, n)} \right) \text{ และ } 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ } C_n = \frac{7}{3} \quad \text{ถ้า } 3 \nmid \left(\frac{n}{\gcd(m, n)} \right) \text{ และ } 9 \mid n$$

และงานชิ้นที่ 3 ของ แกลเลียน (Gallian. n.d. : 1-3) ที่ได้ศึกษาเกี่ยวกับจำนวนของ
กรุปโฮโมมอร์ฟิซึม และริงโฮโมมอร์ฟิซึม คือการหาจำนวนกรุปและริงโฮโมมอร์ฟิซึม $Z_m[\Delta]$

ไป $Z_n[\Delta]$ โดยที่ Δ คือ The Golden Section $[\Delta = \frac{1}{2}(1+\sqrt{5})]$ ได้ผลดังต่อไปนี้

จำนวนของกรุปโฮโมมอร์ฟิซึมจาก $Z_m[\Delta]$ ไป $Z_n[\Delta]$ เท่ากับ $(\gcd(m,n))^4$

จำนวนของริงโฮโมมอร์ฟิซึมจาก $Z[\Delta]$ ไป $Z_n[\Delta]$ เท่ากับ $C_n \cdot 3^{(n)}$

โดยที่ $C_n = 1$ ถ้า $5 \nmid n$

$C_n = 2$ ถ้า $5 \mid n$ แต่ $25 \nmid n$

และ $C_n = \frac{11}{3}$ ถ้า $25 \mid n$

จำนวนของริงโฮโมมอร์ฟิซึมจาก $Z_m[\Delta]$ ไป $Z_n[\Delta]$ เท่ากับ $C_n \cdot 3^B$

โดยที่ $C_n = 1$ ถ้า $5 \nmid n$ หรือ $5 \mid \left(\frac{n}{\gcd(m,n)}\right)$,

$C_n = 2$ ถ้า $5 \nmid \left(\frac{n}{\gcd(m,n)}\right)$ และ $5 \mid n$ แต่ $25 \nmid n$

และ $C_n = \frac{11}{3}$ ถ้า $5 \nmid \left(\frac{n}{\gcd(m,n)}\right)$ และ $25 \mid n$

นอกจากนี้ ซาเลซ, โยเซฟ และอาบู ฮไล (Soleh ,Yousef and Abu-Hlail 1998 :
326-329) ได้ศึกษาเกี่ยวกับจำนวนของกรุปโฮโมมอร์ฟิซึม และริงโฮโมมอร์ฟิซึม จาก Finite
Abelian Group ไป Finite Abelian Group ได้ผลดังต่อไปนี้

จำนวนของกรุปโฮโมมอร์ฟิซึม จาก $Z_{m_1} \times Z_{m_2} \times Z_{m_3} \times \dots \times Z_{m_r}$ ไป

$Z_{k_1} \times Z_{k_2} \times Z_{k_3} \times \dots \times Z_{k_s}$ เท่ากับ $\prod_{i=1, j=1}^{i=r, j=s} \gcd(m_i, k_j)$

จำนวนของริงโฮโมมอร์ฟิซึม จาก $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots \times \mathbb{Z}_{m_r}$ ไป

$$\mathbb{Z}_{p^e} \text{ เท่ากับ } 1 + N_{pe}(m_1, m_2, m_3, \dots, m_r)$$

โดยที่ $N_{pe}(m_1, m_2, m_3, \dots, m_r)$ คือ จำนวนพจน์ที่แตกต่างกันของลำดับ

$m_1, m_2, m_3, \dots, m_r$ ที่ถูกหารลงตัวโดย p^e และ $e \in \mathbb{Z}^+$

จำนวนของริงโฮโมมอร์ฟิซึม จาก $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots \times \mathbb{Z}_{m_r}$ ไป

$$\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \mathbb{Z}_{p_3^{e_3}} \times \dots \times \mathbb{Z}_{p_s^{e_s}} \text{ เท่ากับ}$$

$$\prod_{i=1}^{i=s} \left(1 + N_{p^e}(m_1, m_2, m_3, \dots, m_i) \right)$$

โดยที่ p_i ($1 \leq i \leq s$) ไม่จำเป็นต้องเป็นจำนวนเฉพาะที่แตกต่างกัน

จำนวนของริงโฮโมมอร์ฟิซึม จาก $\mathbb{Z}_m \times \mathbb{Z}_n$ ไป $\mathbb{Z}_n$ เท่ากับ $3^\alpha \cdot 2^\lambda$

$$\text{โดยที่ } \alpha = \omega(k) - \omega\left(\frac{k}{\gcd(m, n, k)}\right)$$

$$\lambda = 2\omega\left(\frac{k}{\gcd(m, n, k)}\right) - \omega\left(\frac{k}{\gcd(m, k)}\right) - \omega\left(\frac{k}{\gcd(n, k)}\right)$$

และ $\omega(n)$ คือจำนวนของจำนวนเฉพาะที่แตกต่างกันและหาร n ลงตัว ใน $\mathbb{Z}$

จำนวนของริงโฮโมมอร์ฟิซึม จาก $\mathbb{Z}_n \times \mathbb{Z}_n$ ไป $\mathbb{Z}_k$ เท่ากับ 3^γ

$$\text{โดยที่ } \gamma = \omega(k) - \omega\left(\frac{k}{\gcd(n, k)}\right)$$

และจำนวนของริงโฮโมมอร์ฟิซึมจาก $\mathbb{Z}_n$ ไป $\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \mathbb{Z}_{k_3} \times \dots \times \mathbb{Z}_{k_s}$

$$\text{เท่ากับ } 2^\eta \text{ โดยที่ } \eta = \sum_{i=1}^s \omega(k_i) - \sum_{i=1}^s \omega\left(\frac{k_i}{\gcd(k_i, n)}\right)$$

บทที่ 3

แนวทางในการพิสูจน์เชิงการสรางเพื่อหาไฮโมมอร์ฟิซึมของ

โครงสร้างทางพีชคณิตจำกัด

จากการที่ผู้วิจัยได้ศึกษาถึงงานวิจัยของแกลเลียนและซาเลซ และงานวิจัยอื่น ๆ ตลอดจนบทความที่เกี่ยวข้องกับกรุปไฮโมมอร์ฟิซึมและริงไฮโมมอร์ฟิซึม รวมถึงศึกษาในเนื้อหา 3 เรื่องหลักต่อไปนี้

1. ทฤษฎีจำนวน (theory of number)
2. พีชคณิตนามธรรม (abstract algebra)
3. เทคนิคการนับเบื้องต้น (counting technique)

พบว่า แกลเลียนและคณะได้พิสูจน์เกี่ยวกับจำนวนของกรุปไฮโมมอร์ฟิซึมและริงไฮโมมอร์ฟิซึม ไว้ดังนี้

จำนวนของกรุปไฮโมมอร์ฟิซึม จาก $\mathbb{Z}_m$ ไป $\mathbb{Z}_n$ เท่ากับ $\gcd(m,n)$ และ

จำนวนของริงไฮโมมอร์ฟิซึม จาก $\mathbb{Z}_m$ ไป $\mathbb{Z}_n$ เท่ากับ 2^β

$$\text{โดยที่ } \beta = \omega(n) - \omega\left(\frac{n}{\gcd(m,n)}\right)$$

จำนวนของกรุปไฮโมมอร์ฟิซึม จาก $\mathbb{Z}_m[i]$ ไป $\mathbb{Z}_n[i]$ และ $\mathbb{Z}_m[p]$ ไป $\mathbb{Z}_n[p]$

เท่ากับ $(\gcd(m,n))^4$

จำนวนของริงไฮโมมอร์ฟิซึมจาก $\mathbb{Z}[i]$ ไป $\mathbb{Z}_n[i]$ เท่ากับ $C_n \cdot 3^{\omega(n)}$

โดยที่ $C_n = 1$ ถ้า $4 \nmid n$,

$$C_n = \frac{5}{3} \quad \text{ถ้า } 4 \mid n \text{ แต่ } 8 \nmid n$$

$$\text{และ } C_n = 3 \quad \text{ถ้า } 8 \mid n$$

จำนวนของริงโฮโมมอร์ฟิซึมจาก $Z_m[i]$ ไป $Z_n[i]$ เท่ากับ $C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 4 \mid n \text{ หรือ } 2 \mid \left(\frac{n}{\gcd(m,n)} \right),$$

$$C_n = \frac{5}{3} \quad \text{ถ้า } 2 \nmid \left(\frac{n}{\gcd(m,n)} \right) \text{ และ } 4 \mid n \text{ แต่ } 8 \nmid n$$

$$\text{และ } C_n = 3 \quad \text{ถ้า } 2 \nmid \left(\frac{n}{\gcd(m,n)} \right) \text{ และ } 8 \mid n$$

จำนวนของริงโฮโมมอร์ฟิซึม จาก $Z[p]$ ไป $Z_n[p]$ เท่ากับ $C_n \cdot 3^{\omega(n)}$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 3 \nmid n,$$

$$C_n = \frac{4}{3} \quad \text{ถ้า } 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ } C_n = \frac{7}{3} \quad \text{ถ้า } 9 \mid n$$

จำนวนริงโฮโมมอร์ฟิซึมจาก $Z_m[p]$ ไป $Z_n[p]$ เท่ากับ $C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 3 \nmid n \text{ แต่ } 3 \mid \left(\frac{n}{\gcd(m,n)} \right),$$

$$C_n = \frac{4}{3} \quad \text{ถ้า } 3 \nmid \left(\frac{n}{\gcd(m,n)} \right) \text{ และ } 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ } C_n = \frac{7}{3} \quad \text{ถ้า } 3 \nmid \left(\frac{n}{\gcd(m,n)} \right) \text{ และ } 9 \mid n$$

แต่เกลเลียนและคณะไม่ได้แสดงให้เห็นว่ากรุปโฮโมมอร์ฟิซึม และริงโฮโมมอร์ฟิซึม
จาก Z_m ไป Z_n มีลักษณะอย่างไร

ดังนั้นผู้วิจัย จะใช้การพิสูจน์เชิงการสร้างเพื่อหาฟังก์ชันทั้งหมดของปัญหา 2 ข้อ ดังนี้

1. เมื่อกำหนด $\langle G, + \rangle, \langle H, + \rangle$ เป็นกรุป $f: G \rightarrow H$ และ

$f(a+b) = f(a)+f(b)$; $\forall a,b \in G$ โดยพิจารณาเฉพาะ 6 กรณี ต่อไปนี้

1.1 G, H เป็น $\langle \mathbb{Z}, + \rangle$ และ $\langle \mathbb{Z}_n, + \rangle$ ตามลำดับ

1.2 G, H เป็น $\langle \mathbb{Z}_m, + \rangle$ และ $\langle \mathbb{Z}_n, + \rangle$ ตามลำดับ

1.3 G, H เป็น $\langle \mathbb{Z}[i], + \rangle$ และ $\langle \mathbb{Z}_n[i], + \rangle$ ตามลำดับ

1.4 G, H เป็น $\langle \mathbb{Z}_m[i], + \rangle$ และ $\langle \mathbb{Z}_n[i], + \rangle$ ตามลำดับ

1.5 G, H เป็น $\langle \mathbb{Z}[\rho], + \rangle$ และ $\langle \mathbb{Z}_n[\rho], + \rangle$ ตามลำดับ

1.6 G, H เป็น $\langle \mathbb{Z}_m[\rho], + \rangle$ และ $\langle \mathbb{Z}_n[\rho], + \rangle$ ตามลำดับ

2. เมื่อกำหนด $\langle R, +, \cdot \rangle, \langle S, +, \cdot \rangle$ เป็นริง $f: R \rightarrow S$

$f(a+b) = f(a) + f(b)$ และ $f(a \cdot b) = f(a) \cdot f(b)$; $\forall a,b \in R$ โดยพิจารณาเฉพาะ 6 กรณี ต่อไปนี้

2.1 R, S เป็น $\langle \mathbb{Z}, +, \cdot \rangle$ และ $\langle \mathbb{Z}_n, +, \cdot \rangle$ ตามลำดับ

2.2 R, S เป็น $\langle \mathbb{Z}_m, +, \cdot \rangle$ และ $\langle \mathbb{Z}_n, +, \cdot \rangle$ ตามลำดับ

2.3 R, S เป็น $\langle \mathbb{Z}[i], +, \cdot \rangle$ และ $\langle \mathbb{Z}_n[i], +, \cdot \rangle$ ตามลำดับ

2.4 R, S เป็น $\langle \mathbb{Z}_m[i], +, \cdot \rangle$ และ $\langle \mathbb{Z}_n[i], +, \cdot \rangle$ ตามลำดับ

2.5 R, S เป็น $\langle \mathbb{Z}[\rho], +, \cdot \rangle$ และ $\langle \mathbb{Z}_n[\rho], +, \cdot \rangle$ ตามลำดับ

2.6 R, S เป็น $\langle \mathbb{Z}_m[\rho], +, \cdot \rangle$ และ $\langle \mathbb{Z}_n[\rho], +, \cdot \rangle$ ตามลำดับ

บทที่ 4

วิธีดำเนินการพิสูจน์

ผู้วิจัยได้แบ่งการดำเนินการพิสูจน์เชิงการสร้างเพื่อหาไฮโมมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัด ออกเป็น 2 ส่วน คือ

1. ทฤษฎีบทพื้นฐานในการพิสูจน์
2. การพิสูจน์เชิงการสร้างเพื่อหาไฮโมมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัด

ซึ่งแบ่งเป็น 2 กรณีดังนี้

2.1 การพิสูจน์หาจำนวนและลักษณะของกลุ่มไฮโมมอร์ฟิซึม

สุญหาจำนวนและลักษณะของริงไฮโมมอร์ฟิซึม

1. ทฤษฎีบทพื้นฐานในการพิสูจน์

ทฤษฎีบทพื้นฐานที่ใช้ในการพิสูจน์ ได้แก่

- ทฤษฎีจำนวน เช่น สมการคอนกรูเอนซ์ การแก้ระบบสมการคอนกรูเอนซ์
- พีชคณิตนามธรรม เช่น สมบัติทาง direct product ของ โครงสร้างทางพีชคณิตจำกัด สมบัติของกลุ่ม สมบัติของริง สมบัติของไฮโมมอร์ฟิซึม สมบัติของไฮโมมอร์ฟิซึม
- เทคนิคการนับเบื้องต้น

ทั้งนี้ ผู้วิจัยได้รวบรวมทฤษฎีบทพื้นฐานที่ใช้ในการพิสูจน์ตามลำดับเนื้อหา ซึ่งประกอบด้วย นิยาม 9 นิยาม ทฤษฎีประกอบ 2 ทฤษฎี ทฤษฎีบท 34 ทฤษฎี และบทแทรก 3 บท ข้อสังเกต โดยมีรายละเอียดดังต่อไปนี้

บทนิยาม 1 กำหนด $n \in \mathbb{Z}^+$ ซึ่ง $n \geq 2$; $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

ให้ $\phi(n)$ แทนจำนวนสมาชิกของ $\mathbb{Z}_n^*$

ฟังก์ชัน ϕ มีชื่อเรียกโดยทั่วไปว่า ออยเลอร์ ฟาย-ฟังก์ชัน

ทฤษฎีบทประกอบ

1. สำหรับ $n \in \mathbb{Z}^+$; $x, y \in \mathbb{Z}$ และ $x \equiv y \pmod{n}$ จะได้ว่า

$$\gcd(x, n) = \gcd(y, n)$$

2. สำหรับ $a \in \mathbb{Z}$ และ $\gcd(a, n) = 1$ จะได้ว่ามี $i \in \mathbb{Z}_n^*$

เพียงตัวเดียวเท่านั้น ซึ่ง $a \equiv i \pmod{n}$

3. ถ้า $m, n \in \mathbb{Z}^+$ และ $\gcd(m, n) = 1$ และ $\bar{r} \in \mathbb{Z}_m^*$, $\bar{s} \in \mathbb{Z}_n^*$

จะได้ว่ามี $i \in \mathbb{Z}_n^*$ เพียงตัวเดียวเท่านั้นซึ่ง $i \equiv r \pmod{m}$

และ $i \equiv s \pmod{n}$

(ณรงค์ ป้านิม. 2536 : 28)

ทฤษฎีบท 1 ให้ $m, n \in \mathbb{Z}^+$ ซึ่ง $\gcd(m, n) = 1$ จะได้ $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

(ณรงค์ ป้านิม. 2536 : 29)

ทฤษฎีบท 2 กำหนด $m, n \in \mathbb{Z}$ และ $\gcd(m, n) = 1$ จะได้ว่า

$$\sum_{d \mid mn} \phi(d) = \sum_{d \mid m} \phi(d) \sum_{d \mid n} \phi(d)$$

(ณรงค์ ป้านิม. 2536 : 29-30)

ทฤษฎีบท 3 กำหนด $n \in \mathbb{Z}^+$ จะได้ว่า $\sum_{d|n} \phi(d) = n$

(ณรงค์ ปันนั่ม. 2536 : 30)

ทฤษฎีบท 4 ให้ $n \in \mathbb{Z}^+$ และ $a \in \mathbb{Z}$ ซึ่ง $\gcd(a, n) = 1$

$$\text{จะได้ว่า } a^{\phi(n)} \equiv 1 \pmod{n}$$

(ณรงค์ ปันนั่ม. 2536 : 30)

บทแทรก ให้ p เป็นจำนวนเฉพาะ $a \in \mathbb{Z}$ และ $\gcd(a, p) = 1$ จะได้ว่า

$$a^{p-1} \equiv 1 \pmod{p} \text{ นอกจากนั้น สำหรับ } a \in \mathbb{Z} \text{ จะได้ว่า } a^p \equiv a \pmod{p}$$

(ณรงค์ ปันนั่ม. 2536 : 31)

บทนิยาม 2 ให้ G เป็นกรุป เราเรียกสับกรุป $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z}_n \}$ ว่า

ซิคิลิกสับกรุป(cyclic subgroup) ของ G ที่มี a เป็นเจนเนอเรเตอร์(generator)

(ณรงค์ ปันนั่ม. 2536 : 61)

บทนิยาม 3 ให้ G เป็นกรุป ที่มี e เป็นสมาชิกเอกลักษณ์ และ $a \in G$ เราเรียก a ว่า

เป็นสมาชิกที่มีขนาดจำกัด (finite order) ใน G ก็ต่อเมื่อ

$$\text{มี } k \in \mathbb{Z}^+ \text{ ซึ่ง } a^k = e$$

(ณรงค์ ปันนั่ม. 2536 : 61)

ทฤษฎีบท 5 ให้ $G = \langle a \rangle$ และ $|G| = n$ จะได้ว่า

$$1. \text{ ถ้า } \gcd(m, n) = 1 \text{ แล้ว } G = \langle a^m \rangle$$

2. ถ้า $\gcd(m,n) = d$ แล้ว $|\langle a^m \rangle| = \frac{n}{d}$

(ณรงค์ ปั่นนิ่ม. 2536 : 68)

ทฤษฎีบท 6 ให้ $G = \langle a \rangle$ และ $|G| = n$ ถ้า d เป็นตัวหารที่เป็นบวกของ n

จะได้ว่า G มีสับกรุป S ที่มีขนาด d และ G จะมีสับกรุป ที่มีขนาด d
เพียงสับกรุปเดียวเท่านั้น

(ณรงค์ ปั่นนิ่ม. 2536 : 68)

ทฤษฎีบท 7 (Lagrange's theorem) ให้ G เป็นกรุปที่มีขนาดเท่ากับ n และ $H \leq G$

ซึ่ง $|H| = m$ จะได้ว่า $m | n$

(ณรงค์ ปั่นนิ่ม. 2536 : 76)

บทนิยาม 4 กำหนดกรุป $\langle G, * \rangle$ และ $\langle H, \circ \rangle$ โฮโมมอร์ฟิซึม จาก G ไป H คือ

ฟังก์ชัน $f: G \rightarrow H$ ซึ่ง $f(a*b) = f(a) \circ f(b)$ สำหรับ a, b ทุกคู่ใน G

เราเขียน $\text{GroupHom}(G, H)$ แทนเซตของกรุปของโฮโมมอร์ฟิซึมทั้งหมด จาก G ไป H

(ณรงค์ ปั่นนิ่ม. 2536 : 136)

ทฤษฎีบท 8 ให้ $f \in \text{GroupHom}(G, H)$ จะได้ว่า

1. $f(e) = e$

2. $f(a^{-1}) = (f(a))^{-1}$

3. $f(G) = \{ f(g) \mid g \in G \} \leq H$

4. ถ้า G เป็น ซิคติกกรุป และ $G = \langle a \rangle$ แล้ว

$$f(a^k) = (f(a))^k \text{ ทุกๆ } k \in \mathbb{Z}$$

(ณรงค์ ปั่นนิ่ม. 2536 : 137)

บทนิยาม 5 กำหนดริง $\langle R, +, \cdot \rangle$ และ $\langle S, \oplus, \otimes \rangle$

เราจะเรียกฟังก์ชัน $f: R \rightarrow S$ ว่า โฮโมมอร์ฟิซึมหนึ่งจากริง R ไป S

ก็ต่อเมื่อสำหรับสมาชิก a, b ทุกคู่ใน R

$$f(a+b) = f(a) \oplus f(b) \text{ และ } f(a \cdot b) = f(a) \otimes f(b)$$

เราจะเขียน $\text{RingHom}(R, S)$ แทนเซตของริงโฮโมมอร์ฟิซึมทั้งหมดจากริง R ไปริง S

(ณรงค์ ปั่นนิ่ม. 2536 : 245)

ทฤษฎีบท 9 กำหนดริง R และริง S จะได้ว่า

1. $\text{RingHom}(R, S) \neq \emptyset$
2. ถ้า $f \in \text{RingHom}(R, S)$ แล้ว $f(0)$ ทำหน้าที่เป็นสมาชิกเอกลักษณ์สำหรับการบวกในริง $f(R)$
3. ถ้า $f \in \text{RingHom}(R, S)$ แล้ว $f(-a) = -f(a)$, ทุกๆ $a \in R$
4. $f(R) = \{ f(r) \mid r \in R \}$ เป็นสับริงของ S
5. ถ้า R เป็นคอมมิวเททีฟริงแล้ว $f(R)$ เป็นคอมมิวเททีฟริงด้วย

(ณรงค์ ปั่นนิ่ม. 2536 : 246-247)

ทฤษฎีบท 10 กำหนด $f \in \text{RingHom}(R, S)$ และ R มี 1 เป็นสมาชิกเอกลักษณ์

จะได้ว่า $f(1) = 0$ หรือ $f(1)$ ทำหน้าที่เป็นสมาชิกเอกลักษณ์ในริง $f(R)$

(ณรงค์ ปั่นนิ่ม. 2536 : 247)

กำหนดให้ G เป็นอบีเลียนกรุปจำกัดมี ขนาด(order) n

โดยที่ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$, $\alpha_j \in \mathbb{Z}^+$, p_j เป็นจำนวนเฉพาะที่แตกต่างกัน แล้ว

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \mathbb{Z}_{p_3^{\alpha_3}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}$$

(Malik, Mordeson & Sen. 1997 : 253)

ทฤษฎีบท 11 ให้ p เป็นจำนวนเฉพาะ แล้วสมการ $x^2 \equiv -1 \pmod{p}$ มีคำตอบ

ในระบบจำนวนเต็มก็ต่อเมื่อ $p = 2$ หรือ $p \equiv 1 \pmod{4}$

(ณรงศ์ ปั่นนิ่ม. 2531 : 44)

บทนิยาม 8 สมการดีกรี 1 คือ สมการที่เขียนอยู่ในรูป $kx \equiv b \pmod{m}$ และ

$$k \not\equiv 0 \pmod{m}$$

(ณรงศ์ ปั่นนิ่ม. 2531 : 49)

ทฤษฎีบท 12 ถ้า $(k, m) = d$ และ $ka \equiv ka' \pmod{m}$ แล้ว $a \equiv a' \pmod{\frac{m}{d}}$

(Hardy & Wright. 1960 : 51)

ทฤษฎีบทแทรก ถ้า $(k, m) = 1$ และ $ka \equiv ka' \pmod{m}$

$$\text{แล้ว } a \equiv a' \pmod{m}$$

(Hardy & Wright. 1960 : 51)

ทฤษฎีบท 13 1. ถ้า $(k, m) = d$ แล้ว $kx \equiv b \pmod{m}$ จะมีคำตอบในระบบจำนวนเต็ม

ก็ต่อเมื่อ $d \mid b$ และจะมี d คำตอบ

2. ถ้า $(k,m) = 1$ แล้ว $kx \equiv b(\text{mod } m)$ จะมี 1 คำตอบ

(Hardy & Wright. 1960 : 51)

ทฤษฎีบท 14 ถ้า $\alpha \in \mathbb{Z}$ ซึ่ง $\alpha > 0$ และ p เป็นจำนวนเฉพาะ และ $m \equiv 1(\text{mod } p^\alpha)$

$$\text{แล้ว } m^p \equiv 1(\text{mod } p^{\alpha+1})$$

(Hardy & Wright. 1960 : 65)

ทฤษฎีบท 15 ถ้า $d|m$, $d > 0$ และ u เป็นคำตอบของสมการ $f(x) \equiv 0(\text{mod } m)$

$$\text{แล้ว } u \text{ จะเป็นคำตอบของสมการ } f(x) \equiv 0(\text{mod } d)$$

(ณรงค์ ปันนิม. 2531 : 49)

ทฤษฎีบท 16 ให้ $g = \gcd(k,m)$ จะได้ว่า ถ้า $g \nmid b$ แล้ว สมการ $kx \equiv b(\text{mod } m)$

ไม่มีคำตอบ และถ้า $g|b$ แล้ว สมการ $kx \equiv b(\text{mod } m)$ จะมี g คำตอบ

$$\text{และสามารถเขียนได้ในรูป } x \equiv \frac{b}{k}x_0 + t\left(\frac{m}{g}\right)(\text{mod } m),$$

$$t = 0, 1, 2, \dots, g-1 \text{ เมื่อ } x_0 \text{ คือคำตอบของสมการ } \frac{k}{g}x \equiv 1(\text{mod } \frac{m}{g})$$

(ณรงค์ ปันนิม. 2531 : 50)

ทฤษฎีบท 17(Chinese Remainder theorem) ให้ $m_1, m_2, \dots, m_r$ ซึ่ง $(m_i, m_j) = 1$

สำหรับ $1 \leq i < j \leq r$ และ $i \neq j$ ให้ $a_1, a_2, \dots, a_r$ เป็นจำนวนเต็มซึ่ง

$$x \equiv a_i(\text{mod } m_i) \quad i = 1, 2, \dots, r \text{ จะได้ว่ามีจำนวนเต็ม } a \text{ ซึ่ง}$$

$$x \equiv a(\text{mod } m_i), \quad i = 1, 2, \dots, r \quad \text{นอกจากนั้น}$$

ถ้าจำนวนเต็ม u, v เป็นคำตอบร่วม 2 คำตอบใดๆ จะได้ว่า

$$u \equiv v \pmod{m_1 m_2 \dots m_r}$$

(ณรงค์ ป้านิยม. 2531 : 51)

ทฤษฎีบท 18 ให้ $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n, a_i \in \mathbb{Z}$,

$$a_0 \equiv 0 \pmod{m} \text{ ถ้า } u \text{ เป็นคำตอบของ } f(x) \equiv 0 \pmod{m}$$

$$\text{และ } u \equiv v \pmod{m} \text{ จะได้ว่า } v \text{ เป็นคำตอบของ } f(x) \equiv 0 \pmod{m}$$

(ณรงค์ ป้านิยม. 2531 : 54)

ทฤษฎีบท 19 กำหนดให้ $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ และ p_j เป็นจำนวนเฉพาะที่แตกต่างกัน.

และไม่สามารถลดทอนได้ สมการ $f(x) \equiv 0 \pmod{m}$ จะมีคำตอบ

ก็ต่อเมื่อสมการ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ มีคำตอบทุก ๆ $i = 1, 2, \dots, s$

(ณรงค์ ป้านิยม. 2531 : 54)

บทนิยาม 7 ให้ $\alpha = a + bi \in \mathbb{Z}[i]$ เราจะเขียน $\bar{\alpha} = a - bi$ และเรียก $\bar{\alpha}$ ว่า

คอนจูเกต (conjugate) ของ α และกำหนด นอร์ม (norm) ของ α

$$\text{คือ } N(\alpha) = \alpha \bar{\alpha} = a^2 + b^2$$

(ณรงค์ ป้านิยม. 2531 : 76)

ทฤษฎีบท 20 กำหนด $\alpha, \beta \in \mathbb{Z}[i]$ จะได้ว่า

$$1. \quad \overline{\overline{\alpha}} = \alpha$$

$$2. \quad \overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$$

$$3. \quad \overline{\alpha \cdot \beta} = \bar{\alpha} \cdot \bar{\beta}$$

4. $\bar{\alpha} = \alpha$ ก็ต่อเมื่อ $\alpha \in \mathbb{Z}$
5. $N(\alpha) \in \mathbb{Z}$ และ $N(\alpha) \geq 0$
6. $N(\alpha) = 0$ ก็ต่อเมื่อ $\alpha = 0$
7. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$
8. $N(\alpha) = 1$ ก็ต่อเมื่อ $\alpha = 1, -1, i, -i$

(ณรงค์ ปั่นนึ่ง. 2531 : 76)

ทฤษฎีบท 21 เรียก $\lambda \in \mathbb{Z}[i]$ ว่า ยูนิต เมื่อ $\lambda \mid 1$

เราพบว่า ยูนิตทั้งหมดของ $\mathbb{Z}[i]$ คือ $1, -1, i, -i$

(ณรงค์ ปั่นนึ่ง. 2531 : 78)

บทนิยาม 8 เรียก $\lambda \in \mathbb{Z}[i]$ ว่า จำนวนเฉพาะแบบเกาส์ ก็ต่อเมื่อ λ ไม่ใช่ยูนิต

และถ้า $\lambda = \alpha\beta$ สำหรับ $\alpha, \beta \in \mathbb{Z}[i]$ แล้ว α เป็นยูนิต

หรือ β เป็นยูนิต

ทฤษฎีบท 22 ถ้า $\alpha \in \mathbb{Z}[i]$ และ $N(\alpha)$ เป็นจำนวนเฉพาะ

จะได้ว่า α เป็นจำนวนเฉพาะแบบเกาส์

(ณรงค์ ปั่นนึ่ง. 2531 : 82)

ทฤษฎีบท 23 ถ้า λ เป็นจำนวนเฉพาะแบบเกาส์ และ $\lambda \mid \alpha_1 \alpha_2 \dots \alpha_n$

จะได้ว่ามี i บางตัว ซึ่ง $\lambda \mid \alpha_i$

(ณรงค์ ปั่นนึ่ง. 2531 : 82)

ทฤษฎีบท 241. ถ้า α เป็นจำนวนเฉพาะแบบเกาส์ แล้ว $\bar{\alpha}$ เป็นจำนวนเฉพาะแบบเกาส์

2. ถ้า $\alpha = a+bi$ เป็นจำนวนเฉพาะแบบเกาส์ ซึ่ง $a \neq 0$ และ $b \neq 0$

จะได้ว่า $N(\alpha) = p$ เมื่อ p เป็นจำนวนเฉพาะซึ่ง $p = 2$ หรือ

$$p \equiv 1 \pmod{4}$$

3. ให้ p เป็นจำนวนเฉพาะ จะได้ว่า p เป็นจำนวนเฉพาะแบบเกาส์

ก็ต่อเมื่อ $p \equiv 3 \pmod{4}$

(ณรงค์ ปั่นนิ่ม. 2531 : 83)

ทฤษฎีบท 25 ให้ $p \in \mathbb{Z}[i]$ และ p เป็นจำนวนเฉพาะแบบเกาส์ ก็ต่อเมื่อ

$\lambda = up$ เมื่อ p เป็นจำนวนเฉพาะ , $p \equiv 3 \pmod{4}$ และ u เป็นยูนิต

หรือ $\lambda = u(a+bi)$, $u(a-bi)$, $u(b+ai)$, $u(b-ai)$

เมื่อ p เป็นจำนวนเฉพาะ ซึ่ง $p = 2$ หรือ $p \equiv 1 \pmod{4}$

และ $p = a^2 + b^2$; $a, b \in \mathbb{Z}$

(ณรงค์ ปั่นนิ่ม. 2531 : 84)

ทฤษฎีบท 261. ถ้า $b \neq 0$ แล้ว $a+bi$ เป็นจำนวนเฉพาะแบบเกาส์

ก็ต่อเมื่อ $N(a+bi)$ เป็นจำนวนเฉพาะ

2. ถ้า $b = 0$ แล้ว $a+bi = a$ เป็นจำนวนเฉพาะแบบเกาส์

ก็ต่อเมื่อ a เป็นจำนวนเฉพาะ และ $a \equiv 3 \pmod{4}$.

(ณรงค์ ปั่นนิ่ม. 2531 : 84)

ทฤษฎีบท 27 จำนวนเฉพาะแบบเกาส์ มีจำนวนไม่จำกัด

(ณรงค์ ปั่นนิ่ม. 2531 : 84)

บทนิยาม 9 ให้ $\gamma = a + bp \in \mathbb{Z}[p]$ นอร์มของ γ คือ $N(\gamma) = a^2 - ab + b^2$

เราเรียก $\mathbb{Z}[p]$ ว่าจำนวนเต็มแบบไอเซนสไตน์-จาโคบี โดยที่ $p^2 + p + 1 = 0$

(Hardy & Wright. 1960 : 220)

ทฤษฎีบท 28 ให้ $\gamma \in \mathbb{Z}[p]$ และ p เป็นจำนวนเฉพาะแบบไอเซนสไตน์-จาโคบี

ก็ต่อเมื่อ $\gamma = up$ เมื่อ u เป็นยูนิต ($u = \pm 1, \pm p, \pm p^2$)

(Hardy & Wright. 1960 : 221)

2. การพิสูจน์เชิงการสร้างเพื่อหาโฮโมมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัด

การพิสูจน์เชิงการสร้างเพื่อหาโฮโมมอร์ฟิซึมของโครงสร้างทางพีชคณิตจำกัดนี้ ผู้วิจัยได้ใช้ความรู้เกี่ยวกับ ทฤษฎีจำนวน เช่น สมการคอนกรูเอนซ์ ระบบสมการคอนกรูเอนซ์ พีชคณิตนามธรรม เทคนิคการนับเบื้องต้น และสมบัติเบื้องต้นของโครงสร้างทางพีชคณิตจำกัด ได้แก่ สมบัติของกรุปโฮโมมอร์ฟิซึม และสมบัติของริงโฮโมมอร์ฟิซึม มาช่วยในการพิสูจน์ โดยพิจารณาแยกเป็น 2 กรณี ดังนี้

2.1 การพิสูจน์หาจำนวนและลักษณะของกรุปโฮโมมอร์ฟิซึม

2.2 การพิสูจน์หาจำนวนและลักษณะของริงโฮโมมอร์ฟิซึม

2.1 การพิสูจน์หาจำนวนและลักษณะของกรุปโฮโมมอร์ฟิซึม ซึ่งประกอบด้วย ทฤษฎีบทหน้า 13 ทฤษฎีบท ทฤษฎีบท 6 ทฤษฎีบท โดยเรียงตามลำดับเนื้อหา ดังต่อไปนี้

ให้ $n \in \mathbb{Z}^+$ และ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ p_j เป็นจำนวนเฉพาะที่แตกต่างกัน และ $\alpha_j \geq 1$ โดย ทฤษฎีบทพื้นฐานทางเลขคณิต จะได้ว่า n สามารถเขียนได้ในรูปแบบดังกล่าวได้เพียงแบบเดียวเท่านั้น และจากสมบัติเบื้องต้นของ direct sum ของโครงสร้างทางพีชคณิตจำกัด จะได้

$$1. \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \mathbb{Z}_{p_3^{\alpha_3}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}$$

เมื่อ $\mathbb{Z}_n$ และ $\mathbb{Z}_{p_j^{\alpha_j}}$, ($i = 1, 2, 3, \dots, s$) แทน กรุป และ ริงของ

จำนวนเต็มในมอดูโลต่างๆ

$$2. \mathbb{Z}_n[i] \cong \mathbb{Z}_{p_1^{\alpha_1}}[i] \oplus \mathbb{Z}_{p_2^{\alpha_2}}[i] \oplus \mathbb{Z}_{p_3^{\alpha_3}}[i] \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}[i]$$

เมื่อ $Z_n[i]$ และ $Z_{p_j^{\alpha_j}}[i]$, ($i = 1, 2, 3, \dots, s$) แทน กรุป และ รังของ

จำนวนเต็มในมอดูโลต่างๆ

$$3. Z_n[p] \cong Z_{p_1^{\alpha_1}}[p] \oplus Z_{p_2^{\alpha_2}}[p] \oplus Z_{p_3^{\alpha_3}}[p] \oplus \dots \oplus Z_{p_s^{\alpha_s}}[p]$$

เมื่อ $Z_n[p]$ และ $Z_{p_j^{\alpha_j}}[p]$, ($i = 1, 2, 3, \dots, s$) แทน กรุป และ รัง

ของจำนวนเต็มในมอดูโลต่างๆ

ทฤษฎีบทนำ 1 กำหนดให้ G และ H เป็นกรุปจำกัด แล้ว $G \oplus H$ เป็นกรุปจำกัด และ

$$|G \oplus H| = |G| |H|$$

(Steinberger. 1994 : 44)

ทฤษฎีบทนำ 2 ให้ G, H และ K เป็นกรุปจำกัด จะได้ว่า

$$|\text{GroupHom}(G, H \times K)| = |\text{GroupHom}(G, H)| |\text{GroupHom}(G, K)|$$

พิสูจน์ เพราะว่า $H \times K = \{ (h, k) \mid h \in H, k \in K \}$

ให้ $f \in \text{GroupHom}(G, H \times K)$ กำหนด

$$f_H: G \rightarrow H \text{ และ } f_K: G \rightarrow K$$

โดย $f_H(g) = h \Leftrightarrow f(g) = (h, k)$ สำหรับ k บางตัวใน K และ

$f_K(g) = k \Leftrightarrow f(g) = (h, k)$ สำหรับ h บางตัวใน H จะเห็นได้ชัดว่า

การกำหนด f_H, f_K ข้างต้น ส่งผลให้ $f_H \in \text{GroupHom}(G, H)$

และ $f_K \in \text{GroupHom}(G, K)$

ในทางกลับกัน ถ้า $f_1 \in \text{GroupHom}(G, H)$ และ $f_2 \in \text{GroupHom}(G, K)$

เราสามารถสร้าง $f: G \rightarrow H \times K$ โดย $f(g) = (f_1(g), f_2(g))$ จะได้ว่า

$f \in \text{GroupHom}(G, H \times K)$ ดังนั้นโดยหลักการนับเบื้องต้น และสมบัติของ direct product จะได้ว่า

$$|\text{GroupHom}(G, H \times K)| = |\text{GroupHom}(G, H)| + |\text{GroupHom}(G, K)|$$

ทฤษฎีบทหน้า 3 กำหนดให้ R, S และ T เป็นริงที่มีขนาดจำกัด แล้ว

$$|\text{RingHom}(R, S \oplus T)| = |\text{RingHom}(R, S)| + |\text{RingHom}(R, T)|$$

พิสูจน์ ทำนองเดียวกับการพิสูจน์ทฤษฎีบทหน้า 2 ข้างต้น

จากทฤษฎีบทหน้า 1 ถึง 3 สามารถสรุปเป็นทฤษฎีบทหน้า 4 ถึง 8 ที่จะนำไปใช้ต่อไปได้ดังนี้

ทฤษฎีบทหน้า 4 $|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})|$

เมื่อ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ $\alpha_j \in \mathbb{Z}^+$

และ p_j เป็นจำนวนเฉพาะที่แตกต่างกันและไม่สามารถลดทอนได้

ทฤษฎีบทหน้า 5 $|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])|$

เมื่อ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ $\alpha_j \in \mathbb{Z}^+$

และ p_j เป็นจำนวนเฉพาะแบบเกาส์ที่แตกต่างกันและ

ไม่สามารถลดทอนได้

ทฤษฎีบทหน้า 6 $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])|$

เมื่อ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ $\alpha_j \in \mathbb{Z}^+$

และ p_j เป็นจำนวนเฉพาะแบบเกาส์ที่แตกต่างกันและ

ไม่สามารถลดทอนได้

ทฤษฎีบทหน้า 7 $|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_n[\rho])| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])|$

เมื่อ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ $\alpha_j \in \mathbb{Z}^+$

และ p_j เป็นจำนวนเฉพาะแบบไอเซนสไตน์-จาโคบี ที่แตกต่างกัน

และไม่สามารถลดทอนได้

ทฤษฎีบทหน้า 8 $|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_n[\rho])| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])|$

เมื่อ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ $\alpha_j \in \mathbb{Z}^+$

และ p_j เป็นจำนวนเฉพาะแบบไอเซนสไตน์-จาโคบี ที่แตกต่างกัน

และไม่สามารถลดทอนได้

ทฤษฎีบท 1.1 $|\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)| = n$

พิสูจน์ กำหนดให้ $d \in \mathbb{Z}_n$

จะแสดงว่ามี $f \in \text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)$ เพียงฟังก์ชันเดียวเท่านั้น

ซึ่ง $f(1) = \bar{d}$

ให้ $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$

ที่กำหนดโดย $f(k) = k\bar{d}$

ดังนั้น $f(x+y) = (x+y) \cdot \bar{d}$

$$= x\bar{d} + y\bar{d}$$

$$= f(x) + f(y)$$

ดังนั้น $f \in \text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)$

เนื่องจาก $\mathbb{Z}$ เป็นซิกลิกกรุป ที่มี 1 เป็นเจนเนอเรเตอร์

ดังนั้น จะมี f เพียงฟังก์ชันเดียว

ซึ่งเป็นโฮโมมอร์ฟิซึม และ $f(1) = \bar{d}$

เพราะฉะนั้น $|\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)| = n$

□

จากทฤษฎีบท 1.1 เห็นจริงว่า $|\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)| = n$

และ เราสามารถสรุปลักษณะของ $\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)$ ได้ว่า

$$\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n) = \{ f_i \mid i = 0, 1, 2, \dots, n-1 \}$$

$$\text{โดยที่ } f_i(k) = k\bar{i}, k \in \mathbb{Z}$$

ทฤษฎีบทหน้า 9 ให้ G เป็นกรุปขนาดเท่ากับ n และ $H \leq G$ ซึ่ง $|H| = m$ แล้ว $m \mid n$

(ฉรณรงค์ ปันนัม. 2536 : 61)

ทฤษฎีบทหน้า 10 ถ้า $f \in \text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ และ $f(\bar{1}) = \bar{d}$ แล้ว $|\bar{d}| \mid m$

พิสูจน์ จาก $f(\bar{1}) = \bar{d}$

$$\text{จะได้ว่า } f(m \cdot \bar{1}) = m \cdot \bar{d} \dots\dots\dots (1)$$

$$\text{เพราะว่า } \bar{0} = f(\bar{0}) = f(m \cdot \bar{1}) \dots\dots\dots (2)$$

$$\text{จาก (1) และ (2) } m \cdot \bar{d} = \bar{0}$$

$$\text{ดังนั้นแสดงว่า } |\bar{d}| \mid m$$

□

ทฤษฎีบทหน้า 11 ถ้า $f \in \text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ และ $f(\bar{1}) = \bar{d}$ แล้ว $|\bar{d}| \mid \gcd(m, n)$

$$\text{พิสูจน์ } f(\bar{1}) = \bar{d} \quad \text{ดังนั้น } \bar{1} \in \mathbb{Z}_m \text{ และ } \bar{d} \in \mathbb{Z}_n$$

$$\text{จาก Lagrange's theorem จะได้ว่า } |\langle \bar{d} \rangle| \mid |\mathbb{Z}_n|$$

$$\Rightarrow |\bar{d}| \mid n$$

$$\text{และ จาก ทฤษฎีบทหน้า 10 จะได้ว่า } |\bar{d}| \mid m$$

$$\text{ดังนั้น } |\bar{d}| \mid \gcd(m, n)$$

□

ทฤษฎีบทหน้า 12 ถ้า $\bar{d} \in \mathbb{Z}_n$ และ $|\bar{d}| \mid \gcd(m, n)$ แล้วจะมี $f \in \text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)$

$$\text{เพียงฟังก์ชันเดียวเท่านั้นที่ } f(\bar{1}) = \bar{d}$$

$$\text{พิสูจน์ } \text{จาก } f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n \text{ และ } f(\bar{1}) = \bar{d}$$

$$\text{ดังนั้น } f(\bar{k}) = k\bar{d}$$

$$\text{กำหนดให้ } \bar{k}_1 = \bar{k}_2$$

$$\Rightarrow k_1 \equiv k_2 \pmod{m}$$

$$\Rightarrow m \mid (k_1 - k_2)$$

$$\Rightarrow (k_1 - k_2) \cdot \bar{d} = \bar{0}$$

$$\Rightarrow k_1 \cdot \bar{d} = k_2 \cdot \bar{d}$$

$$\Rightarrow f(\bar{k}_1) = f(\bar{k}_2)$$

$$\begin{aligned} \text{และ } f(\bar{k}_1 + \bar{k}_2) &= f(\overline{k_1 + k_2}) \\ &= (k_1 + k_2) \cdot \bar{d} \\ &= k_1 \cdot \bar{d} + k_2 \cdot \bar{d} \\ &= f(\bar{k}_1) + f(\bar{k}_2) \end{aligned}$$

จากการที่ $\mathbb{Z}_m, \mathbb{Z}_n$ เป็นซิคติกกรุป

ดังนั้น เป็นการเพียงพอที่จะสรุปได้ว่า f มีเพียงฟังก์ชันเดียว

$$\text{นั่นคือ } f(\bar{1}) = \bar{d}$$

□

จาก ทฤษฎีบทหน้า 9, 10, 11 และ 12 เป็นการเพียงพอที่จะสามารถสรุปได้ว่า

$$|\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = |\{\bar{d} \mid |\bar{d}| \mid \gcd(m, n)\}|$$

ทฤษฎีบทหน้า 13 $\sum_{d \mid n} \phi(d) = n$

(ณรงค์ ป้านิม. 2536 : 29)

ดังนั้น จาก $\phi(d)$ คือ จำนวนเจนเนอเรเตอร์ ของ ซิคติกกรุป ที่มีขนาดเท่ากับ d

และ $d \mid \gcd(m, n)$ จะมี 1 โฮโมมอร์ฟิซึม

เพราะฉะนั้น $\sum_{d \mid \gcd(m, n)} \phi(d) = \gcd(m, n)$

นั่นคือ $|\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \gcd(m, n)$

ทฤษฎีบท 1.2 $|\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \gcd(m, n)$

พิสูจน์ จากทฤษฎีบทหน้า 9 ถึง 13 สามารถสรุปได้ว่า

$$|\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \gcd(m, n)$$

และจะมีลักษณะดังต่อไปนี้คือ

ให้ $g = \gcd(m, n)$, $a > 0$ และ $a \mid g$

$$X_a = \left\{ i \left(\frac{n}{a} \right) \mid 1 \leq i \leq a \text{ และ } \gcd(i, a) = 1 \right\}$$

$$\text{จะได้ว่า } \left| i \left(\frac{n}{a} \right) \right| = a \text{ และ } |X_a| = \phi(a)$$

นอกจากนี้ ทุกๆ $\bar{d} \in X_a$ จะมีฟังก์ชัน f เพียงฟังก์ชันเดียวเท่านั้นที่

$$f \in \text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n) \text{ ซึ่ง } f(\bar{i}) = \bar{d}$$

□

ทฤษฎีบท 1.3 $|\text{GroupHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])| = n^4$

พิสูจน์ กำหนดให้ $\bar{\alpha} \in \{ \bar{a} + \bar{b}i \mid \bar{a}, \bar{b} \in \mathbb{Z}_n \}$

$$\bar{\beta} \in \{ \bar{a} + \bar{b}i \mid \bar{a}, \bar{b} \in \mathbb{Z}_n \}$$

ทุกครั้งเมื่อเลือก $\bar{\alpha}$ และ $\bar{\beta}$ สามารถสร้างโฮโมมอร์ฟิซึมจาก $\mathbb{Z}[i]$ ไป $\mathbb{Z}_n[i]$

$$\text{ซึ่ง } f(1) = \bar{\alpha} \text{ และ } f(i) = \bar{\beta}$$

จาก $f(1)$ สามารถเลือกได้ n^2 วิธี

และ $f(i)$ สามารถเลือกได้ n^2 วิธี

ดังนั้นเราสามารถสร้างโฮโมมอร์ฟิซึมจาก $\mathbb{Z}[i]$ ไป $\mathbb{Z}_n[i]$ ได้ทั้งหมด n^4 วิธี

$$\text{ดังนั้น } |\text{GroupHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])| = n^4$$

□

ทฤษฎีบท 1.4 $|\text{GroupHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| = (\gcd(m, n))^4$

พิสูจน์ จาก $\mathbb{Z}_m[i] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$

และ $\mathbb{Z}_n[i] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$

$$\begin{aligned} \text{ดังนั้น } |\text{GroupHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| &= |\text{GroupHom}(\mathbb{Z}_m \oplus \mathbb{Z}_m, \mathbb{Z}_n \oplus \mathbb{Z}_n)| \\ &= |\text{GroupHom}(\mathbb{Z}_m \oplus \mathbb{Z}_m, \mathbb{Z}_n)|^2 \\ &= |\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)|^4 \\ &= (\gcd(m, n))^4 \end{aligned}$$

□

ทฤษฎีบท 1.5 $|\text{GroupHom}(\mathbb{Z}[\rho], \mathbb{Z}_n[\rho])| = n^4$

พิสูจน์ ทำนองเดียวกับทฤษฎีบท 1.3 และ 1.4

□

ทฤษฎีบท 1.6 $|\text{GroupHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_n[\rho])| = (\gcd(m, n))^4$

พิสูจน์ ทำนองเดียวกับทฤษฎีบท 1.3 ถึง 1.5

□

เราจะใช้ความรู้จากทฤษฎีบท 1.1 ถึง 1.6 เป็นพื้นฐานในการพิสูจน์เพื่อหาจำนวนและ

ลักษณะของริงโฮโมมอร์ฟิซึมต่อไป

2.2 การพิสูจน์หาจำนวนและลักษณะของริงโฮโมมอร์ฟิซึม ซึ่งประกอบด้วย ทฤษฎี

บทนำ 27 ทฤษฎีบท และ ทฤษฎีบท 6 ทฤษฎีบท โดยเรียงตามลำดับเนื้อหา ดังต่อไปนี้

ทฤษฎีบทนำ 14 ถ้า $f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)$ และ $f(1) = \bar{d}$ แล้ว

$$f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_n) \text{ ก็ต่อเมื่อ } \bar{d} = (\bar{d})^2$$

พิสูจน์ $(\Rightarrow)$ ถ้า $f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)$

$$\begin{aligned} \text{ดังนั้น } \bar{d} &= f(1) \\ &= f(1 \cdot 1) \\ &= f(1) \cdot f(1) \\ &= \bar{d} \cdot \bar{d} \\ &= (\bar{d})^2 \end{aligned}$$

$$(\Leftarrow) \text{ ถ้า } \bar{d} = (\bar{d})^2 \text{ และ } \bar{x}, \bar{y} \in \mathbb{Z}_n$$

$$\begin{aligned} \text{ดังนั้น } f(x \cdot y) &= f(x \cdot y) \\ &= (xy) \cdot \bar{d} \\ &= (xy) \cdot (\bar{d})^2 \\ &= (x\bar{d}) \cdot (y\bar{d}) \\ &= f(x) \cdot f(y) \end{aligned}$$

นั่นคือ $f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)$ ก็ต่อเมื่อ $\bar{d} = (\bar{d})^2$, $\bar{d} \in X_a$ เมื่อ

$$X_a = \left\{ i \left(\frac{n}{a} \right) \mid 1 \leq i \leq a \text{ และ } \gcd(i, a) = 1 \right\}$$

ทฤษฎีบทหน้า 15 $|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_j^{\alpha_j}})| = |\{\bar{d} \mid \bar{d} \in \mathbb{Z}_{p_j^{\alpha_j}}, \bar{d} = (\bar{d})^2\}|$

พิสูจน์ จาก ทฤษฎีบทหน้า 1 และ 14 สามารถสรุปได้ว่า

$$|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_j^{\alpha_j}})| = |\{\bar{d} \mid \bar{d} \in \mathbb{Z}_{p_j^{\alpha_j}}, \bar{d} = (\bar{d})^2\}|$$

□

ดังนั้นจากทฤษฎีบทหน้า 15 จึงเพียงพอที่จะคำนวณหา $f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)$ จากแต่ละ $f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_j^{\alpha_j}})$ โดยคำนวณจากค่าของ $\bar{d}$

ทฤษฎีบทหน้า 16 $\bar{d} \in \mathbb{Z}_{p_j^{\alpha_j}}$ และ $\bar{d} = (\bar{d})^2$ ก็ต่อเมื่อ $\bar{d} = \bar{0}$ หรือ $\bar{d} = \bar{1}$

พิสูจน์ จาก $f(1) = \bar{d}$ และ $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$

$$(\bar{d})^2 = \bar{d} \Leftrightarrow (\bar{d})^2 - \bar{d} = 0$$

$$\Leftrightarrow p_j^{\alpha_j} \mid (d^2 - d)$$

$$\Leftrightarrow p_j^{\alpha_j} \mid d(d - 1)$$

$$\text{เพราะว่าถ้า } p_j^{\alpha_j} \mid d \text{ และ } p_j^{\alpha_j} \mid d - 1$$

$$\Leftrightarrow p_j^{\alpha_j} \mid d - (d - 1)$$

$$\Leftrightarrow p_j^{\alpha_j} \mid 1 \text{ (เกิดข้อขัดแย้ง)}$$

$$\text{ดังนั้น } p_j^{\alpha_j} \mid d \text{ หรือ } p_j^{\alpha_j} \mid d - 1 \text{ อย่างใดอย่างหนึ่ง}$$

$$\Leftrightarrow \bar{d} = \bar{0} \text{ หรือ } \bar{d} = \bar{1}$$

□

จาก ทฤษฎีบทหน้า 14, 15 และ 16 สามารถสรุปจำนวนและแจกแจงลักษณะ

ริงโฮโมมอร์ฟิซึมจาก $\mathbb{Z}$ ไป $\mathbb{Z}_n$ ได้ตาม ทฤษฎีบท 2.1 ดังนี้

ทฤษฎีบท 2.1 $|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)| = 2^{\omega(n)}$

พิสูจน์
$$|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_j^{\alpha_j}})|$$

เมื่อ $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$ โดยที่ $\alpha_j \in \mathbb{Z}^+$

ซึ่ง แต่ละ $|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_j^{\alpha_j}})| = 2$ ($f(1) = \bar{0}$ หรือ $f(1) = \bar{1}$)

ดังนั้นจากหลักการนับเบื้องต้นสามารถสรุปได้ว่า

$$|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)| = 2^s = 2^{\omega(n)}$$

และมีลักษณะดังนี้

ให้ $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \mathbb{Z}_{p_3^{\alpha_3}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}$ จะได้

$$f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \mathbb{Z}_{p_3^{\alpha_3}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}})$$

$$\Leftrightarrow f(1) = (\bar{a}_1, \bar{a}_2, \bar{a}_3, \dots, \bar{a}_s), \bar{a}_j = \bar{0} \text{ หรือ } \bar{1} \text{ ใน } \mathbb{Z}_{p_j^{\alpha_j}}$$

□

ทฤษฎีบทหน้า 17 $f \in \text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ และ $f(\bar{1}) = \bar{d}$

$$\Leftrightarrow f \in \text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n) \quad \text{และ} \quad \bar{d} = (\bar{d})^2$$

พิสูจน์ จากการที่ $f \in \text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ นั้น f จะต้องเป็นสมาชิกของ

$$\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n) \quad \text{ดังนั้น} \quad |\bar{d}| \mid \gcd(m, n)$$

$(\Rightarrow)$ ถ้า $f \in \text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$

$$\begin{aligned} \text{ดังนั้น } \bar{d} &= f(\bar{1}) \\ &= f(\bar{1} \cdot \bar{1}) \\ &= f(\bar{1}) \cdot f(\bar{1}) \\ &= \bar{d} \cdot \bar{d} \\ &= (\bar{d})^2 \end{aligned}$$

$(\Leftarrow)$ ถ้า $\bar{d} = (\bar{d})^2$ และ $\bar{x}, \bar{y} \in \mathbb{Z}_n$

$$\begin{aligned} \text{ดังนั้น } f(\bar{x} \cdot \bar{y}) &= f(\overline{xy}) \\ &= (\overline{xy})\bar{d} \\ &= (\overline{xy})(\bar{d})^2 \\ &= (\overline{xd})(\overline{yd}) \\ &= f(\bar{x})f(\bar{y}) \end{aligned}$$

นั่นคือ $f \in \text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ ก็ต่อเมื่อ $\bar{d} = (\bar{d})^2, \bar{d} \in X_a$

และ $\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$

$$= \{ \bar{d} \mid \bar{d} = (\bar{d})^2, \bar{d} \in X_a \}$$

□

ทฤษฎีบทหน้า 18 $|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})| = |\{ \bar{d} \mid \bar{d} \mid \gcd(m, p_j^{\alpha_j}) \text{ และ } \bar{d} = (\bar{d})^2 \}|$

พิสูจน์

จาก ทฤษฎีบทหน้า 4 และ 17 สามารถสรุปได้ว่า

$$|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})| = |\{ \bar{d} \mid \bar{d} \mid \gcd(m, p_j^{\alpha_j}) \text{ และ } \bar{d} = (\bar{d})^2 \}|$$

□

ดังนั้นในการหา $|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})|$ จะพบว่า

$$|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})| = 2 \quad \text{หรือ} \quad 1 \quad \text{นอกจากนี้}$$

$$|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})| = 1 \quad \text{ถ้า} \quad p_j^{\alpha_j} \nmid m \quad \text{และ}$$

$$|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_j^{\alpha_j}})| = 2 \quad \text{ถ้า} \quad p_j^{\alpha_j} \mid m$$

และจากทฤษฎีบทหน้า 4 $|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \prod_{i=1}^s |\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_{p_i^{\alpha_i}})|$

เราจึงสรุปว่า

ทฤษฎีบท 2.2 $|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = 2^\beta$ โดยที่ $\beta = \omega(n) - \omega\left(\frac{n}{\gcd(m, n)}\right)$

และ $\omega(k)$ คือจำนวนของจำนวนเฉพาะที่ต่างกันและหาร k ลงตัว

ลักษณะของ $\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ สามารถกำหนดได้ดังต่อไปนี้

$$f \in \text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$$

$$f(1) = (\overline{a_1}, \overline{a_2}, \overline{a_3}, \dots, \overline{a_s})$$

และขึ้นอยู่กับเงื่อนไขดังต่อไปนี้คือ

$$\text{ให้ } m = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_s^{\beta_s}$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$$

$$g = \gcd(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} p_3^{\gamma_3} \dots p_s^{\gamma_s}, \quad \gamma_j = \min(\beta_j, \alpha_j)$$

ถ้า $\beta_j \geq \alpha_j$ แล้ว $\overline{a} = \overline{0}$ หรือ $\overline{1}$

ถ้า $\beta_j < \alpha_j$ แล้ว $\overline{a} = \overline{0}$

ทฤษฎีบทหน้า 19 $f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ โดยที่

$$f(1) = \bar{\alpha} \text{ และ } f(i) = \bar{\beta} \Leftrightarrow \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta}, (\bar{\beta})^2 = -\bar{\alpha}$$

พิสูจน์

$$(\Rightarrow) \text{ จาก } f(1) = \bar{\alpha} \dots\dots\dots (1)$$

$$f(i) = \bar{\beta} \dots\dots\dots (2)$$

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$$

$$\bar{\alpha} = (\bar{\alpha})^2 \dots\dots\dots (3)$$

$$f(i) = f(1 \cdot i) = f(1) \cdot f(i)$$

$$\bar{\beta} = \bar{\alpha} \cdot \bar{\beta} \dots\dots\dots (4)$$

$$f(i \cdot i) = f(i) \cdot f(i)$$

$$f(-1) = \bar{\beta} \cdot \bar{\beta}$$

$$-f(1) = (\bar{\beta})^2 \dots\dots\dots (5)$$

$$\text{จาก (1) และ (5); } -\bar{\alpha} = (\bar{\beta})^2 \dots\dots\dots (6)$$

($\Leftarrow$) เห็นได้จริงว่า

$$\text{จาก } \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta}, (\bar{\beta})^2 = -\bar{\alpha}$$

นั่นมาจากสมบัติที่ว่า $1 \cdot 1 = 1, 1 \cdot i = i, i^2 = -1$

ดังนั้นจึงสามารถสรุปได้ว่า

$f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ โดยที่

$$f(1) = \bar{\alpha} \text{ และ } f(i) = \bar{\beta}$$

ทฤษฎีบทหน้า 20 $|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])|$

$$= |\{ (\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p_j^{\alpha_j}}, \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } (\bar{\beta})^2 = -\bar{\alpha} \}|$$

พิสูจน์ จากทฤษฎีบทหน้า 5 และ 19 สามารถสรุปได้ว่า

$$\begin{aligned} & |\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| \\ &= |\{ (\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p_j^{\alpha_j}}, \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } (\bar{\beta})^2 = -\bar{\alpha} \}| \end{aligned}$$

□

ดังนั้นจึงเพียงพอที่เราจะคำนวณหา $f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])$ จาก

แต่ละ $f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ โดยคำนวณจากค่าของ $\bar{\alpha}$ และ $\bar{\beta}$

ทฤษฎีบทหน้า 21 ถ้า $\bar{\alpha} \in \mathbb{Z}_{p_j^{\alpha_j}}[i]$ และ $\bar{\alpha} = (\bar{\alpha})^2$ แล้ว $\bar{\alpha} = \bar{0}$ หรือ $\bar{\alpha} = \bar{1}$

พิสูจน์ จาก $f(1) = \bar{\alpha}$

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$$

$$\bar{\alpha} = (\bar{\alpha})^2$$

$$(\bar{\alpha})^2 = \bar{\alpha} \Rightarrow (\bar{\alpha})^2 - \bar{\alpha} = \bar{0}$$

$$\Rightarrow p_j^{\alpha_j} \mid (\alpha^2 - \alpha)$$

$$\Rightarrow p_j^{\alpha_j} \mid \alpha(\alpha - 1) \text{ (ทำนองเดียวกับ ท.บ.หน้า 16)}$$

$$\Rightarrow p_j^{\alpha_j} \mid \alpha \vee p_j^{\alpha_j} \mid \alpha - 1$$

$$\Rightarrow \bar{\alpha} = \bar{0} \text{ หรือ } \bar{\alpha} = \bar{1}$$

□

ทฤษฎีบทหน้า 22 ให้ $f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ และ $f(1) = \bar{0}$ แล้ว $f(\alpha) = \bar{0}$

$$\text{ทุกๆ } \alpha \in \mathbb{Z}[i]$$

พิสูจน์ จาก $f(1) = \bar{0}$

$$\begin{aligned}
 f(\alpha) &= f(1\alpha) \\
 &= f(1) \cdot f(\alpha) \\
 &= \bar{0}
 \end{aligned}$$

$\therefore f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ และ $f(1) = \bar{0}$ แล้ว $f(\alpha) = \bar{0}$ ทุกๆ $\alpha \in \mathbb{Z}[i]$

□

ทฤษฎีบทหน้า 23 ให้ $f \in \text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$, $f(1) = \bar{i}$ และ $f(i) = \bar{\beta}$

$$\text{แล้ว } (\bar{\beta})^2 = -\bar{i}$$

ซึ่ง p_j เป็นจำนวนเฉพาะแบบเกาส์ที่ไม่สามารถลดทอนได้

นอกจากนั้น เราสามารถสร้าง $f(i)$ เมื่อกำหนดค่า p_j จาก

23.1 ถ้า $p_j \neq 1+i$ (หรือ its associate)

$$\text{แล้ว } f(i) = \bar{i} \text{ หรือ } f(i) = -\bar{i}$$

23.2 ถ้า $p_j = 1+i$ (หรือ its associate)

$$\text{แล้ว แยกได้เป็นกรณี } p_j^\beta = (1+i)^{2t}; \beta = 2t$$

1. $t = 1$ ค่าของ $f(i)$ มี 2 กรณีดังนี้คือ

$$1.1 \quad f(i) = \bar{i}$$

$$1.2 \quad f(i) = -\bar{i}$$

2. $t = 2$ ค่าของ $f(i)$ มี 4 กรณีดังนี้คือ

$$2.1 \quad f(i) = \bar{i}$$

$$2.2 \quad f(i) = \overline{3i}$$

$$2.3 \quad f(i) = \bar{2} + \bar{i}$$

$$2.4 \quad f(i) = \bar{2} + \overline{3i}$$

3 $t = 3$ ค่าของ $f(i)$ มี 8 กรณีดังนี้คือ

$$3.1 \quad f(i) = \bar{i}$$

$$3.2 \quad f(i) = \overline{3i}$$

$$3.3 \quad f(i) = \overline{5i}$$

$$3.4 \quad f(i) = \overline{7i}$$

$$3.5 \quad f(i) = \overline{4 + i}$$

$$3.6 \quad f(i) = \overline{4 + 3i}$$

$$3.7 \quad f(i) = \overline{4 + 5i}$$

$$3.8 \quad f(i) = \overline{4 + 7i}$$

4 $t \geq 3$ ค่าของ $f(i)$ มี 8 กรณีดังนี้คือ

$$4.1 \quad f(i) = \overline{0 + 1i}$$

$$4.2 \quad f(i) = \overline{0 + (\overline{2^{t-1}-1})i}$$

$$4.3 \quad f(i) = \overline{0 + (\overline{2^{t-1}+1})i}$$

$$4.4 \quad f(i) = \overline{0 + (\overline{2^t-1})i}$$

$$4.5 \quad f(i) = (\overline{2^{t-1}}) + \overline{1i}$$

$$4.6 \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$4.7 \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$4.8 \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^t-1})i$$

พิสูจน์ พิสูจน์ทฤษฎีบทหน้า 23.1

$$\text{ถ้า } \bar{\alpha} = \bar{i} \text{ แล้ว } (\bar{\beta})^2 = -\bar{i}$$

$$\text{จาก } (\bar{\beta})^2 = -\bar{i}$$

$$\Leftrightarrow \beta^2 \equiv -1 \pmod{p_j^{\alpha_j}} \text{ ใน } \mathbb{Z}_{p_j^{\alpha_j}}[i]$$

$$\text{ให้ } \bar{\beta} = \bar{h} + \bar{k}i ; \bar{h}, \bar{k} \in \mathbb{Z}_{p_j^{\alpha_j}}$$

$$p_j \neq 1+i$$

$$\Rightarrow p_j^{\alpha_j} \mid (\beta^2 + 1)$$

$$\Rightarrow p_j^{\alpha_j} \mid (\beta + i)(\beta - i)$$

$$\Rightarrow p_j \mid (\beta + i) \text{ หรือ } p_j \mid (\beta - i) \quad \text{อย่างใดอย่างหนึ่งเท่านั้น}$$

$$\text{เพราะว่าถ้า } p_j \mid (\beta + i) \text{ และ } p_j \mid (\beta - i)$$

$$\Rightarrow p_j \mid (\beta + i) - (\beta - i)$$

$$\Rightarrow p_j \mid 2i$$

$$\Rightarrow p_j \mid 2$$

$$\Rightarrow p_j = 1+i, 1-i, -1+i, -1-i \text{ (เกิดข้อขัดแย้ง)}$$

$$\text{ดังนั้น } \bar{\beta} = \bar{i} \text{ หรือ } \bar{\beta} = -\bar{i}$$

ดังนั้นสรุปได้ว่ากรณี $p_j \neq 1+i$ จะมีค่าของ $f(i)$ 2ค่าจาก

$$1. f(i) = \bar{i}$$

$$2. f(i) = -\bar{i}$$

พิสูจน์ทฤษฎีบทนำ 23.2

$$\text{ให้ } \bar{b} = \bar{h} + \bar{k}i ; \bar{h}, \bar{k} \in \mathbb{Z}_{p_j^{\alpha_j}}$$

$$\text{พิจารณา } b^2 \equiv -1 \pmod{2^t}$$

$$h^2 - k^2 + 1 + 2hki \equiv 0 \pmod{2^t}$$

$$\text{ดังนั้น } h^2 - k^2 + 1 \equiv 0 \pmod{2^t} \quad \text{และ} \quad 2hk \equiv 0 \pmod{2^t}$$

$$\text{และ } h \not\equiv k \pmod{2}$$

$$\Rightarrow 2^t \mid (h^2 - k^2 + 1) \quad \wedge \quad 2^t \mid (2hk) \quad \wedge \quad h \not\equiv k \pmod{2}$$

$$\text{กรณี 1 } t = 1 ;$$

$$1. \quad h \text{ เป็นจำนวนคี่ ; } k \text{ เป็นจำนวนคู่} \Rightarrow h = 1, k = 0$$

$$2. \quad h \text{ เป็นจำนวนคู่ ; } k \text{ เป็นจำนวนคี่} \Rightarrow h = 0, k = 1$$

$$\text{กรณี 2 } t > 1 ;$$

h เป็นจำนวนคี่ เป็นไปไม่ได้ ดังนั้น h ต้องเป็นจำนวนคู่

และ k เป็นจำนวนคี่

$$\Rightarrow 2^t \mid (2hk) \Rightarrow h = 0 \text{ หรือ } 2^{t-1}$$

$$\text{และ } k^2 \equiv 1 \pmod{2^t} \text{ ใน } \mathbb{Z}$$

$$t = 2 \Rightarrow k^2 \equiv 1 \pmod{2^2}$$

$$\Rightarrow k^2 \equiv 1 \pmod{4}$$

$$\Rightarrow k = 1, 3$$

ถ้า $t = 2$ แล้วค่าของ $f(i)$ ดังนี้คือ

$$2.1 \quad f(i) = \bar{i}$$

$$2.2 \quad f(i) = \overline{3i}$$

$$2.3 \quad f(i) = \overline{2 + i}$$

$$2.4 \quad f(i) = \overline{2} + \overline{3i}$$

กรณี 3 $t = 3$

$$t = 3 \Rightarrow k^2 \equiv 1 \pmod{2^3}$$

$$\Rightarrow k^2 \equiv 1 \pmod{8}$$

$$\Rightarrow k = 1, 3, 5, 7$$

ถ้า $t = 3$ แล้วค่าของ $f(i)$ ดังนี้คือ

$$3.1 \quad f(i) = \overline{i}$$

$$3.2 \quad f(i) = \overline{3i}$$

$$3.3 \quad f(i) = \overline{5i}$$

$$3.4 \quad f(i) = \overline{7i}$$

$$3.5 \quad f(i) = \overline{4} + \overline{i}$$

$$3.6 \quad f(i) = \overline{4} + \overline{3i}$$

$$3.7 \quad f(i) = \overline{4} + \overline{5i}$$

$$3.8 \quad f(i) = \overline{4} + \overline{7i}$$

กรณี 4 $t > 3$

$$t > 3 \Rightarrow k^2 \equiv 1 \pmod{2^t}$$

$$\Rightarrow k = 1, 2^{t-1} - 1, 2^{t-1} + 1, 2^t - 1$$

จากการที่ สมการ h มี 2 คำตอบ คือ $0, 2^{t-1}$

k จะมีคำตอบ 4 คำตอบเท่านั้น

1. สมการ $k^2 \equiv 1 \pmod{2^t}$ จะมีคำตอบใน $\mathbb{Z}$ อย่างน้อย 4 คำตอบ

เพราะ $(\pm 1)^2 \equiv 1 \pmod{2^t}$ และ

$$(2^{t-1} \pm 1)^2 \equiv 2^{2t-2} \pm 2 \cdot 2^{t-1} + 1 \equiv 1 \pmod{2^t}$$

$\therefore k$ มีคำตอบใน $\mathbb{Z}$ อย่างน้อย 4 คำตอบ

2. พิจารณา $k^2 \equiv 1 \pmod{2^t}$

$$k^2 - 1 \equiv 0 \pmod{2^t}$$

$$\text{เพราะ } 2^t \mid (k^2 - 1) \Rightarrow 2^t \mid (k-1)(k+1)$$

$$\Rightarrow 2^r \mid (k-1) \wedge 2^s \mid (k+1)$$

$$\text{โดยที่ } t = r + s$$

$$t \geq 4 \Rightarrow 2^r \mid (k-1) \wedge 2^s \mid (k+1)$$

$$\text{ถ้า } r \geq 2 \text{ และ } s \geq 2 \Rightarrow 4 \mid (k-1) \wedge 4 \mid (k+1)$$

$$\Rightarrow 4 \mid [(k-1) - (k+1)]$$

$$\Rightarrow 4 \mid -2 \text{ เกิดข้อขัดแย้ง}$$

ดังนั้น $2^t \mid (k-1)(k+1)$ เป็นไปได้เพียง

$$[2^t \mid (k-1)] \text{ หรือ } [2^t \mid (k+1)]$$

$$\text{หรือ } [2 \mid (k-1) \wedge 2^{t-1} \mid (k+1)]$$

$$\text{หรือ } [2^{t-1} \mid (k-1) \wedge 2 \mid (k+1)]$$

$\therefore k$ มีคำตอบใน $\mathbb{Z}$ อย่างมาก 4 คำตอบ

จาก 1 และ 2 สามารถสรุปได้ว่า k มีคำตอบใน $\mathbb{Z}$ 4 คำตอบ

$$\text{ดังนั้น } h = 0, 2^{t-1} \text{ และ } k = 1, 2^{t-1} - 1, 2^{t-1} + 1, 2^t - 1$$

ดังนั้น ถ้า $t \geq 3$ แล้วค่าของ $f(i)$ มีดังนี้คือ

$$4.1 \quad f(i) = \bar{0} + \bar{1}i$$

$$4.2 \quad f(i) = \bar{0} + (\overline{2^{t-1}-1})i$$

$$4.3 \quad f(i) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$4.4 \quad f(i) = \bar{0} + (\overline{2^t-1})i$$

$$4.5 \quad f(i) = (\overline{2^{t-1}}) + \bar{1}i$$

$$4.6 \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$4.7 \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$4.8 \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^t-1})i$$

ทฤษฎีบทหน้า 24 ถ้า $f(1) = \bar{1}$ และ $f(i) = \bar{\beta}$ เราสามารถสร้าง $\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$

ซึ่ง p_j เป็นจำนวนเฉพาะแบบเกาส์ที่ไม่สามารถลดทอนได้ โดยแยกเป็นกรณี

24.1 $p_j \neq 1+i$ (หรือ its associate)

$$\text{คือ } 1.f(1) = \bar{1} \text{ และ } f(i) = \bar{i}$$

$$2.f(1) = \bar{1} \text{ และ } f(i) = -\bar{i}$$

24.2 $p_j = 1+i$ (หรือ its associate)

แยกได้เป็น กรณี $p_j^\beta = (1+i)^{2t}$; $\beta = 2t$

1. $t = 1$ ค่าของ $f(i)$ มี 2 กรณีดังนี้คือ

$$1.1 \quad f(1) = \bar{1} \text{ และ } f(i) = \bar{1}$$

$$1.2 \quad f(1) = \bar{1} \text{ และ } f(i) = \bar{i}$$

2. $t = 2$ ค่าของ $f(i)$ มี 4 กรณีดังนี้คือ

$$2.1 \quad f(1) = \bar{1} \text{ และ } f(i) = \bar{i}$$

$$2.2 \quad f(1) = \bar{1} \text{ และ } f(i) = \overline{3i}$$

$$2.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{2} + \bar{i}$$

$$2.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{2} + \bar{3i}$$

3 $t = 3$ ค่าของ $f(i)$ มี 8 กรณีดังนี้คือ

$$3.1 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$3.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{3i}$$

$$3.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{5i}$$

$$3.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{7i}$$

$$3.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4} + \bar{i}$$

$$3.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4} + \bar{3i}$$

$$3.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4} + \bar{5i}$$

$$3.8 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4} + \bar{7i}$$

4 $t \geq 3$ ค่าของ $f(i)$ มี 8 กรณีดังนี้คือ

$$4.1 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + \bar{1i}$$

$$4.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + (\overline{2^{t-1}-1})i$$

$$4.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$4.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + (\overline{2^t-1})i$$

$$4.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + \bar{1i}$$

$$4.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$4.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$4.8 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^t - 1})i$$

พิสูจน์

ทฤษฎีบทหน้า 24 ได้จาก ทฤษฎีบทหน้า 23

จากทฤษฎีบทหน้า 22 ถึง 24 และ ทฤษฎีบท 2.1 สามารถสรุปจำนวนและแจกแจงลักษณะ

ของริงโฮโมมอร์ฟิซึมจาก $\mathbb{Z}[i]$ ไป $\mathbb{Z}_n[i]$ ได้ตามทฤษฎีบท 2.3 ดังนี้

$$\text{ทฤษฎีบท 2.3} \quad |\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])| = C_n \cdot 3^{\omega(n)}$$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 4 \nmid n$$

$$C_n = \frac{5}{3} \quad \text{ถ้า } 4 \mid n \text{ แต่ } 8 \nmid n$$

$$\text{และ } C_n = 3 \quad \text{ถ้า } 8 \mid n$$

พิสูจน์

ในการหา $|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])|$ จะพบว่า

$$\text{กรณี 1} \quad p_j \neq 1+i$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$1. \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2. \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$3. \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = -\bar{i}$$

$$\text{กรณี 2} \quad p_j = 1+i$$

$$\text{จะแบ่งเป็นกรณี } p_j^\beta = (1+i)^{2t}, \beta = 2t$$

$$2.1 \quad t = 1$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$2.1.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.1.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{1}$$

$$2.1.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$2.2 \quad t = 2$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 5$$

และริงโฮโมมอร์ฟิซึมที่ห้าสามารถกำหนดได้ดังนี้คือ

$$2.2.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.2.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$2.2.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{3i}$$

$$2.2.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{2 + i}$$

$$2.2.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{2 + 3i}$$

$$2.3 \quad t = 3$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้คือ

$$2.3.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.3.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$2.3.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{3i}$$

$$2.3.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{5i}$$

$$2.3.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{7i}$$

$$2.3.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4 + i}$$

$$2.3.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4 + 3i}$$

$$2.3.8 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4 + 5i}$$

$$2.3.9 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{4 + 7i}$$

$$2.4 \quad t \geq 3$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{p_j}^{\alpha_j}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้คือ

$$2.4.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.4.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0 + \bar{1}i}$$

$$2.4.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0 + (\overline{2^{t-1}-1})i}$$

$$2.4.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0 + (\overline{2^{t-1}+1})i}$$

$$2.4.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0 + (\overline{2^t-1})i}$$

$$2.4.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + \bar{1}i$$

$$2.4.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$2.4.8 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$2.4.9 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^t-1})i$$

ทฤษฎีบทหน้า 25 $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ ที่กำหนดโดย

$$f(\bar{1}) = \bar{\alpha} \text{ และ } f(\bar{i}) = \bar{\beta} \Leftrightarrow f \in \text{GrougHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$$

$$\bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta}, (\bar{\beta})^2 = -\bar{\alpha}$$

พิสูจน์ ทำนองเดียวกับทฤษฎีบทหน้า 17 และ 19

□

ทฤษฎีบทหน้า 26 $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])|$

$$= |\{(\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p_j^{\alpha_j}}[i], \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } (\bar{\beta})^2 = -\bar{\alpha}\}|$$

พิสูจน์ จากทฤษฎีบทหน้า 6 , 24 และทฤษฎีบท 2.3 สามารถสรุปได้ว่า

$$\begin{aligned} & |\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| \\ &= |\{(\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p_j^{\alpha_j}}[i], \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } (\bar{\beta})^2 = -\bar{\alpha}\}| \end{aligned}$$

ดังนั้นจึงเพียงพอที่เราจะคำนวณหา $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])$ จากแต่ละ

$f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ โดยคำนวณจากค่าของ $\bar{\alpha}$ และ $\bar{\beta}$

□

ทฤษฎีบทหน้า 27 ให้ $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ และ $f(\bar{1}) = \bar{\alpha}$ แล้ว $\bar{\alpha} = \bar{0}$ หรือ

$$\bar{\alpha} = \bar{1} \quad \text{นอกจากนั้นจะมี } f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i]) \text{ ซึ่ง}$$

$$f(\bar{1}) = \bar{1} \text{ ก็ต่อเมื่อ } p_j^{\alpha_j} \mid m$$

พิสูจน์ จาก $f(\bar{1}) = \bar{\alpha}$

$$f(\bar{1}) = f(\bar{1} \cdot \bar{1}) = f(\bar{1}) \cdot f(\bar{1})$$

$$\bar{\alpha} = (\bar{\alpha})^2$$

$$\begin{aligned}
(\bar{\alpha})^2 &= \bar{\alpha} \Rightarrow (\bar{\alpha})^2 - \bar{\alpha} = \bar{0} \\
&\Rightarrow p_j^{\alpha_j} \mid (\alpha^2 - \alpha) \\
&\Rightarrow p_j^{\alpha_j} \mid \alpha(\alpha - 1) \\
&\Rightarrow p_j^{\alpha_j} \mid \alpha \vee p_j^{\alpha_j} \mid \alpha - 1 \\
&\Rightarrow \bar{\alpha} = \bar{0} \quad \text{หรือ} \quad \bar{\alpha} =
\end{aligned}$$

($\Rightarrow$) ถ้า $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ และ $f(\bar{1}) = \bar{1}$

เพราะว่า $|f(\bar{1})| = |\bar{1}| = p_j^{\alpha_j}$

ดังนั้น $|f(\bar{1})| \mid |\bar{1}|$

$\therefore p_j^{\alpha_j} \mid m$

($\Leftarrow$) $p_j^{\alpha_j} \mid m$

ดังนั้นเราสามารถสร้าง f ที่ $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ ได้

และสร้างได้เพียงฟังก์เดียวเท่านั้นคือ $f(\bar{1}) = \bar{1}$

$\therefore p_j^{\alpha_j} \mid m$

□

ทฤษฎีบทหน้า 28 ให้ $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$ และ $f(\bar{1}) = \bar{0}$ ก็ต่อเมื่อ

$f(\bar{\alpha}) = \bar{0}$ ทุกๆ $\bar{\alpha} \in \mathbb{Z}_m[i]$

พิสูจน์

ทำนองเดียวกับทฤษฎีบทหน้า 22

□

ทฤษฎีบทหน้า 29 ให้ $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{\alpha_j p_j}[i])$ และ $f(\bar{i}) = \bar{i}$ ถ้า $f(\bar{i}) = \bar{\beta}$.

$$\text{แล้ว } (\bar{\beta})^2 = -\bar{i}$$

นอกจากนั้น เราสามารถสร้าง $f(\bar{i})$ ได้โดยแยกเป็น

29.1 ถ้า $p_j \neq 1+i$ (หรือ its associate)

$$\text{แล้ว } f(\bar{i}) = \bar{i} \text{ หรือ } f(\bar{i}) = -\bar{i}$$

29.2 ถ้า $p_j = 1+i$ (หรือ its associate) สามารถแยกเป็น

$$\text{แล้วกรณี } p_j^\beta = (1+i)^{2t}, \beta = 2t$$

1 $t = 1$ แล้วค่าของ $f(\bar{i})$ มีดังนี้คือ

$$1.1 \quad f(\bar{i}) = 1$$

$$1.2 \quad f(\bar{i}) = \bar{i}$$

2 $t = 2$ แล้วค่าของ $f(\bar{i})$ มีดังนี้คือ

$$2.1 \quad f(\bar{i}) = \bar{i}$$

$$2.2 \quad f(\bar{i}) = \overline{3i}$$

$$2.3 \quad f(\bar{i}) = \overline{2 + i}$$

$$2.4 \quad f(\bar{i}) = \overline{2 + 3i}$$

3 $t = 3$ แล้วค่าของ $f(\bar{i})$ มีดังนี้คือ

$$3.1 \quad f(\bar{i}) = \bar{i}$$

$$3.2 \quad f(\bar{i}) = \overline{3i}$$

$$3.3 \quad f(\bar{i}) = \overline{5i}$$

$$3.4 \quad f(\bar{i}) = \overline{7i}$$

$$3.5 \quad f(\bar{i}) = \bar{4} + \bar{i}$$

$$3.6 \quad f(\bar{i}) = \bar{4} + \bar{3i}$$

$$3.7 \quad f(\bar{i}) = \bar{4} + \bar{5i}$$

$$3.8 \quad f(\bar{i}) = \bar{4} + \bar{7i}$$

4 $t \geq 3$ แล้วค่าของ $f(\bar{i})$ มีดังนี้คือ

$$4.1 \quad f(\bar{i}) = \bar{0} + (\bar{1})i$$

$$4.2 \quad f(\bar{i}) = \bar{0} + (\overline{2^{t-1}-1})i$$

$$4.3 \quad f(\bar{i}) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$4.4 \quad f(\bar{i}) = \bar{0} + (\overline{2^t-1})i$$

$$4.5 \quad f(\bar{i}) = (\overline{2^{t-1}}) + \bar{1}i$$

$$4.6 \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$4.7 \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$4.8 \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^t-1})i$$

พิสูจน์

ทฤษฎีบทหน้า 29 พิสูจน์ทำนองเดียวกับทฤษฎีบทหน้า 23

ทฤษฎีบทหน้า 30 ถ้า $f(\bar{1}) = \bar{1}$ และ $f(\bar{i}) = \bar{\beta}$

เราสามารถสร้าง $\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$

ซึ่ง p_j เป็นจำนวนเฉพาะแบบเกาส์ที่ไม่สามารถลดทอนได้ โดยแยกเป็น

30.1 $p_j \neq 1+i$ (หรือ its associate)

คือ 1. $f(\bar{1}) = \bar{1}$ และ $f(i) = i$

2. $f(\bar{1}) = \bar{1}$ และ $f(i) = -i$

30.2 $p_j = 1+i$ (หรือ its associate)

แยกได้เป็น กรณี $p_j^\beta = (1+i)^{2t}$; $\beta = 2t$

1. $t = 1$ ค่าของ $f(i)$ มี 2 กรณีดังนี้คือ

1.1 $f(\bar{1}) = \bar{1}$ และ $f(i) = 1$

1.2 $f(\bar{1}) = \bar{1}$ และ $f(i) = \bar{i}$

2. $t = 2$ ค่าของ $f(i)$ มี 4 กรณีดังนี้คือ

2.1 $f(\bar{1}) = \bar{1}$ และ $f(i) = \bar{i}$

2.2 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{3i}$

2.3 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{2+i}$

2.4 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{2+3i}$

3. $t = 3$ ค่าของ $f(i)$ มี 8 กรณีดังนี้คือ

3.1 $f(\bar{1}) = \bar{1}$ และ $f(i) = \bar{i}$

3.2 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{3i}$

3.3 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{5i}$

3.4 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{7i}$

3.5 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{4+i}$

3.6 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{4+3i}$

3.7 $f(\bar{1}) = \bar{1}$ และ $f(i) = \overline{4+5i}$

$$3.8 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{4} + \bar{7}i$$

4. $t \geq 3$ ค่าของ $f(\bar{i})$ มี 8 กรณีดังนี้คือ

$$4.1 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{0} + \bar{1}i$$

$$4.2 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{0} + (\overline{2^{t-1}-1})i$$

$$4.3 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$4.4 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{0} + (\overline{2^t-1})i$$

$$4.5 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = (\overline{2^{t-1}}) + \bar{1}i$$

$$4.6 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$4.7 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$4.8 \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^t-1})i$$

พิสูจน์

ทฤษฎีบทหน้า 30.1 ได้จาก ทฤษฎีบทหน้า 29.1

ทฤษฎีบทหน้า 30.2 ได้จาก ทฤษฎีบทหน้า 29.2

จากทฤษฎีบทหน้า 25 ถึง 30 และ ทฤษฎีบท 2.2 และ 2.3 สามารถสรุปจำนวนและ

แจกแจงลักษณะของริงโฮโมมอร์ฟิซึมจาก $Z_m[i]$ ไป $Z_n[i]$ ได้ตามทฤษฎีบท 2.4 ดังนี้

ทฤษฎีบท 2.4 $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| = C_n \cdot 3^\beta$

โดยที่ $C_n = 1$ ถ้า $4 \nmid n$ หรือ $2 \mid \left(\frac{n}{\gcd(m, n)}\right)$

$C_n = \frac{5}{3}$ ถ้า $2 \nmid \left(\frac{n}{\gcd(m, n)}\right)$ และ $4 \mid n$ แต่ $8 \nmid n$

และ $C_n = 3$ ถ้า $2 \nmid \left(\frac{n}{\gcd(m, n)}\right)$ และ $8 \mid n$

โดยที่ $\beta = \omega(n) - \omega\left(\frac{n}{\gcd(m, n)}\right)$

พิสูจน์

ในการหา $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])|$ จะพบว่า

ถ้า $p_j^{\alpha_j} \nmid m$ จะได้ว่า $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 1$

นั่นคือ ถ้า $p_j^{\alpha_j} \nmid m$ จะมี $f \in \text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])$

เพียงฟังก์ชันเดียวคือ $f(\bar{\alpha}) = \bar{0}$ ทุกๆ $\bar{\alpha} \in \mathbb{Z}_m[i]$

ดังนั้น $\beta = \omega(p_j^{\alpha_j}) - \omega\left(\frac{p_j^{\alpha_j}}{\gcd(m, p_j^{\alpha_j})}\right) = 1 - 1 = 0$

ดังนั้น $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 1 \cdot 3^0 = 1$ ในกรณีที่

$p_j^{\alpha_j} \mid m$

ดังนั้นจึงเป็นการเพียงพอที่จะสนใจเฉพาะกรณีที่ $p_j^{\alpha_j} \mid m$

กรณี 1 $p_j \neq 1+i$

จากทฤษฎีบท 2.2 และ 2.3 จะได้

$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 3$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้ ดังนี้คือ

$$1. f(\bar{1}) = \bar{0} \text{ และ } f(\bar{i}) = \bar{0}$$

$$2. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{i}$$

$$3. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = -\bar{i}$$

กรณี 2 $p_j = 1+i$

ในกรณี $p_j^\beta = (1+i)^{2t}$

$$2.1 \quad t = 1$$

จากทฤษฎีบท 2.2 และ 2.3 จะได้

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้ คือ

$$2.1.1. f(\bar{1}) = \bar{0} \text{ และ } f(\bar{i}) = \bar{0}$$

$$2.1.2. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{1}$$

$$2.1.3. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{i}$$

$$2.2 \quad t = 2$$

จากทฤษฎีบท 2.2 และ 2.3 จะได้

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 5$$

และริงโฮโมมอร์ฟิซึมทั้งห้าสามารถกำหนดได้ดังนี้ คือ

$$2.2.1. f(\bar{1}) = \bar{0} \text{ และ } f(\bar{i}) = \bar{0}$$

$$2.2.2. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \bar{i}$$

$$2.2.3. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \overline{3i}$$

$$2.2.4. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{i}) = \overline{2+i}$$

$$2.2.5. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{2} + \bar{3i}$$

2.3 $t=3$

จากทฤษฎีบท 2.2 และ 2.3 จะได้

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้ คือ

$$2.3.1. \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2.3.2. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{i}$$

$$2.3.3. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{3i}$$

$$2.3.4. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{5i}$$

$$2.3.5. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{7i}$$

$$2.3.6. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{4} + \bar{i}$$

$$2.3.7. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{4} + \bar{3i}$$

$$2.3.8. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{4} + \bar{5i}$$

$$2.3.9. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{4} + \bar{7i}$$

2.4 $t \geq 3$

จากทฤษฎีบท 2.2 และ 2.3 จะได้

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้ คือ

$$2.4.1 \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2.4.2 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + \bar{1i}$$

$$2.4.3. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + (\overline{2^{t-1}-1})i$$

$$2.4.4. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$2.4.5. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + (\overline{2^t-1})i$$

$$2.4.6. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + \bar{1}i$$

$$2.4.7. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$2.4.8. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$2.4.9. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^t-1})I$$

ทฤษฎีบทหน้า 31 $f \in \text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p^j}[\rho])$ ที่กำหนดโดย

$$f(1) = \bar{\alpha} \quad \text{และ} \quad f(\rho) = \bar{\beta} \Leftrightarrow \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta},$$

$$\bar{\beta}^2 + \bar{\beta} + \bar{1} = \bar{0}$$

พิสูจน์

$$(\Rightarrow) \quad \text{จาก} \quad f(1) = \bar{\alpha} \dots\dots\dots (1)$$

$$f(\rho) = \bar{\beta} \dots\dots\dots (2)$$

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$$

$$\bar{\alpha} = (\bar{\alpha})^2 \dots\dots\dots (3)$$

$$f(\rho) = f(1 \cdot \rho) = f(1) \cdot f(\rho)$$

$$\bar{\beta} = \bar{\alpha} \cdot \bar{\beta} \dots\dots\dots (4)$$

$$f(0) = f(\rho^2 + \rho + 1) = (f(\rho))^2 + f(\rho) + f(1)$$

$$\bar{0} = \bar{\beta}^2 + \bar{\beta} + \bar{1} \dots\dots\dots (5)$$

$$(\Leftarrow) \quad \text{เห็นได้ชัดว่า} \quad \bar{\alpha} = (\bar{\alpha})^2; \bar{\alpha} \cdot \bar{\beta} = \bar{\beta}; \bar{\beta}^2 + \bar{\beta} + \bar{1} = \bar{0}$$

มาจากสมบัติที่ว่า $1 \cdot 1 = 1, 1 \cdot \rho = \rho, \rho^2 + \rho + 1 = 0$

ดังนั้นจึงสามารถสรุปได้ว่า $f \in \text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p^{\alpha_j}}[p])$

$$\text{โดยที่ } f(1) = \bar{\alpha} \text{ และ } f(p) = \bar{\beta} \quad \square$$

ทฤษฎีบทหน้า 32 $|\text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p^{\alpha_j}}[p])|$

$$= |\{(\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p^{\alpha_j}}[p], \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } \bar{\beta}^2 + \bar{\beta} + 1 = \bar{0}\}|$$

พิสูจน์

จากทฤษฎีบทหน้า 7 และ 30

สามารถสรุปได้ดังทฤษฎีบทว่า $|\text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p^{\alpha_j}}[p])|$

$$= |\{(\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p^{\alpha_j}}[p], \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } \bar{\beta}^2 + \bar{\beta} + 1 = \bar{0}\}|$$

ดังนั้นจึงเพียงพอที่เราจะคำนวณหา $f \in \text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_n[p])$ จาก

แต่ละ $f \in \text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p^{\alpha_j}}[p])$ โดยคำนวณจากค่าของ $\bar{\alpha}$ และ $\bar{\beta}$

$\square$

ทฤษฎีบทหน้า 33 ถ้า $\bar{\alpha} \in \mathbb{Z}_{p^{\alpha_j}}[p]$ และ $\bar{\alpha} = (\bar{\alpha})^2$ แล้ว $\bar{\alpha} = \bar{0}$ หรือ $\bar{\alpha} = \bar{1}$

พิสูจน์

$$\text{จาก } f(1) = \bar{\alpha}$$

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$$

$$\bar{\alpha} = (\bar{\alpha})^2$$

$$(\bar{\alpha})^2 = \bar{\alpha} \Rightarrow (\bar{\alpha})^2 - (\bar{\alpha}) = \bar{0}$$

$$\Rightarrow p^{\alpha_j} \mid \alpha^2 - \alpha$$

$$\Rightarrow p^{\alpha_j} \mid \alpha(\alpha - 1)$$

$$\Rightarrow p^{\alpha_j} \mid \alpha \text{ หรือ } p^{\alpha_j} \mid \alpha - 1$$

(ทำนองเดียวกับทฤษฎีบทหน้า 21)

$$\Rightarrow \bar{\alpha} = \bar{0} \text{ หรือ } \bar{\alpha} = \bar{1}$$

□

ทฤษฎีบทหน้า 34 ให้ $f \in \text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$ และ $f(1) = \bar{0}$ แล้ว $f(\alpha) = \bar{0}$

$$\text{ทุกๆ } \alpha \in \mathbb{Z}[\rho]$$

พิสูจน์ จาก $f(1) = \bar{0}$

$$\begin{aligned} f(\alpha) &= f(1 \cdot \alpha) \\ &= \bar{0} \end{aligned}$$

□

$\therefore f \in \text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$ และ $f(1) = \bar{0}$

$$f(\alpha) = \bar{0} \quad \text{ทุกๆ } \alpha \in \mathbb{Z}[\rho]$$

ทฤษฎีบทหน้า 35 ให้ $f \in \text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$, $f(1) = \bar{1}$ และ $f(\rho) = \bar{\beta}$

$$\text{แล้ว } (\bar{\beta})^2 + \bar{\beta} + \bar{1} = \bar{0}$$

ซึ่ง p_j เป็นจำนวนเฉพาะแบบแบบไอเซนสไตน์-จาคอบีที่ไม่สามารถลดทอนได้

นอกจากนั้นเราสามารถสร้าง $f(\rho)$ เมื่อกำหนดค่า p_j จาก

35.1 ถ้า $p_j \neq 1 - \rho$ (หรือ its associate)

จะมีค่า $f(\rho)$ 2 ค่าคือ

$$f(\rho) = \bar{1}\rho \text{ หรือ } f(\rho) = \bar{1}\rho^2$$

35.2 ถ้า $p_j = 1 - \rho$ (หรือ its associate) แล้วแบ่งเป็น

$$p_j^\beta = (1 - \rho)^{2\alpha}, \quad \beta = 2\alpha \quad \text{แล้ว}$$

$1 \leq \alpha = 1$ จะมีค่า $f(\rho)$ ที่เป็นไปได้แก่

$$1.1 \quad f(\rho) = \bar{1} + \bar{0}\rho$$

$$1.2 \quad f(\rho) = \bar{0} + \bar{1}\rho$$

$$1.3 \quad f(\rho) = \bar{2} + \bar{2}\rho$$

2 $\alpha = 2$ จะมีค่า $f(\rho)$ ที่เป็นไปได้แก่

$$2.1 \quad f(\rho) = \bar{1}\rho$$

$$2.2 \quad f(\rho) = \bar{5} + \bar{2}\rho$$

$$2.3 \quad f(\rho) = \bar{6} + \bar{4}\rho$$

$$2.4 \quad f(\rho) = \bar{2} + \bar{5}\rho$$

$$2.5 \quad f(\rho) = \bar{3} + \bar{7}\rho$$

$$2.6 \quad f(\rho) = \bar{8} + \bar{8}\rho$$

3 $\alpha \geq 3$ จะมีค่า $f(\rho)$ ที่เป็นไปได้แก่

$$3.1 \quad f(\rho) = \bar{0} + \bar{1}\rho$$

$$3.2 \quad f(\rho) = \overline{(-1+2\cdot 3^{\alpha-1})} + \overline{(-1+3^{\alpha-1})}\rho$$

$$3.3 \quad f(\rho) = \overline{(2\cdot 3^{\alpha-1})} + \overline{(1+3^{\alpha-1})}\rho$$

$$3.4 \quad f(\rho) = \overline{(-1+3^{\alpha-1})} + \overline{(-1+2\cdot 3^{\alpha-1})}\rho$$

$$3.5 \quad f(\rho) = \overline{(3^{\alpha-1})} + \overline{(1+2\cdot 3^{\alpha-1})}\rho$$

$$3.6 \quad f(\rho) = \overline{(-1+3^{\alpha})} + \overline{(-1+3^{\alpha})}\rho$$

พิสูจน์

พิสูจน์ทฤษฎีบทหน้า 35.1

$$\text{เห็นได้ชัดว่า} \quad \rho^2 + \rho + 1 = 0$$

$$(\rho^2)^2 + (\rho^2) + 1 = 0$$

$$\text{ถ้า } \bar{\alpha} = \bar{1} \text{ แล้ว } (\bar{\beta})^2 + \bar{\beta} + \bar{1} = \bar{0}$$

$$\Rightarrow \beta^2 + \beta + 1 \equiv 0 \pmod{p_j^{\alpha_j}}$$

$$\Rightarrow (\beta - \rho)(\beta - \rho^2) \equiv 0 \pmod{p_j^{\alpha_j}}$$

$$\Leftrightarrow p_j^{\alpha_j} \mid (\beta - \rho)(\beta - \rho^2)$$

ถ้า $p_j \neq 1 - \rho$ (หรือ its associate)

แล้ว $p_j \mid (\beta - \rho)$ หรือ $p_j \mid (\beta - \rho^2)$ เพียงอย่างใดอย่างหนึ่งเท่านั้น

เพราะว่าถ้า $p_j \mid (\beta - \rho) \wedge p_j \mid (\beta - \rho^2)$

แล้ว $p_j \mid (\rho^2 - \rho)$ ซึ่ง $\rho^2 - \rho = -\rho(1 - \rho)$

ดังนั้น $p_j \mid (1 - \rho)$ เกิดข้อขัดแย้ง

$\therefore p_j \mid (\beta - \rho)$ หรือ $p_j \mid (\beta - \rho^2)$

$$\Leftrightarrow \beta = \rho \text{ หรือ } \beta = \rho^2$$

ดังนั้น กรณี $p_j \neq 1 - \rho$ (หรือ its associate) จะได้ว่า

$$1. f(\rho) = \bar{1}\rho$$

$$2. f(\rho) = \bar{1}\rho^2$$

พิสูจน์ทฤษฎีบทหน้า 35.2

ถ้า $p_j = 1 - \rho$ (หรือ its associate)

จะได้ว่า $p_j^\beta = (1 - \rho)^\beta$; $\beta = 2\alpha$, $\alpha = 1$

จาก $\bar{x} + \bar{y}\rho \in \mathbb{Z}_3[\rho] \Rightarrow \bar{x}, \bar{y} \in \mathbb{Z}_3$;

กรณี 1 ถ้า $\alpha = 1$; $p_j^\beta = (1 - \rho)^2 = 3^1$

จาก $(\bar{\beta})^2 + \bar{\beta} + \bar{1} = \bar{0}$ (ต้องการหาคำนวณค่า $\bar{x}, \bar{y}$ ซึ่ง $\bar{\beta} = \bar{x} + \bar{y}\rho$)

$$\text{จะได้ว่า } (\bar{x} + \bar{y}\rho)^2 + (\bar{x} + \bar{y}\rho) + \bar{1} = \bar{0}$$

$$\bar{x}^2 + 2\bar{x}\bar{y}\rho + \bar{y}^2\rho^2 + \bar{x} + \bar{y}\rho + \bar{1} = \bar{0}$$

$$(\bar{x}^2 + \bar{x} + \bar{1} - \bar{y}^2) + (2\bar{x}\bar{y} - \bar{y}^2 + \bar{y})\rho = \bar{0}$$

$$\Rightarrow x^2 + x + 1 - y^2 \equiv 0 \pmod{3^\alpha}$$

$$\text{และ } 2xy - y^2 + y \equiv 0 \pmod{3^\alpha}$$

$$\therefore x^2 + x + 1 - y^2 \equiv 0 \pmod{3}$$

$$\text{และ } y(2x - y + 1) \equiv 0 \pmod{3}$$

ดังนั้น จะต้องคำนวณค่าของ x, y จากระบบสมการ

$$x^2 + x + 1 - y^2 \equiv 0 \pmod{3} \dots\dots\dots (*)$$

$$y(2x - y + 1) \equiv 0 \pmod{3} \dots\dots\dots (*)$$

$$\text{ถ้า } y = 0 \Rightarrow x^2 + x \equiv -1 \pmod{3}$$

$$0 \equiv 0 \pmod{3}$$

$$\Rightarrow x = 1$$

$$\therefore y = 0 \text{ และ } x = 1 \dots\dots\dots (1)$$

$$\text{ถ้า } y = 1 \Rightarrow x^2 + x \equiv 0 \pmod{3}$$

$$2x \equiv 0 \pmod{3}$$

$$\Rightarrow x = 0$$

$$\therefore y = 1 \text{ และ } x = 0 \dots\dots\dots (2)$$

$$\text{ถ้า } y = 2 \Rightarrow x^2 + x \equiv 0 \pmod{3}$$

$$2x \equiv 1 \pmod{3}$$

$$\Rightarrow x = 2$$

$$\therefore y = 2 \text{ และ } x = 2 \dots\dots\dots (3)$$

จาก (1) ,(2) และ (3) สรุปได้ว่า

$$\text{สำหรับ } p^\beta = (1-p)^\beta ; \beta = 2\alpha ; \alpha = 1$$

จะมี 3 คำตอบคือ

$$1. y = 0 \text{ และ } x = 1$$

$$2. y = 1 \text{ และ } x = 0$$

$$3. y = 2 \text{ และ } x = 2$$

ดังนั้น ในกรณีนี้ ค่าของ $f(p)$ มี 3 กรณีได้แก่

$$1. f(p) = \bar{1} + \bar{0}p$$

$$2. f(p) = \bar{0} + \bar{1}p$$

$$3. f(p) = \bar{2} + \bar{2}p$$

กรณี 2 $\alpha = 2$

ดังนั้น จะต้องคำนวณค่าของ x, y จากระบบสมการ

$$x^2 + x + 1 - y^2 \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$$y(2x - y + 1) \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

2.1 ในกรณี $y = 3k$

$$\Rightarrow x^2 + x + 1 \equiv 3^2 k^2 \pmod{3^2} \dots\dots\dots (*)$$

$$3k(2x - 3k + 1) \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$$\Rightarrow x^2 + x + 1 \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$$k(2x - 3k + 1) \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$\Rightarrow$ ไม่มีคำตอบในระบบสมการ

2.2 ในกรณี $\gcd(y,a) = 1$

$$\Rightarrow x^2 + x \equiv y^2 - 1 \pmod{3^2} \dots\dots\dots (*)$$

$$2x - y + 1 \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$$\text{ถ้า } y = 1 \Rightarrow x^2 + x \equiv 0 \pmod{3^2}$$

$$2x \equiv 0 \pmod{3^2}$$

$$\Rightarrow x = 0$$

$$\therefore y = 1 \text{ และ } x = 0 \dots\dots\dots (1)$$

$$\text{ถ้า } y = 2 \Rightarrow x^2 + x \equiv 3 \pmod{3^2}$$

$$2x \equiv 1 \pmod{3^2}$$

$$\Rightarrow x = 5$$

$$\therefore y = 2 \text{ และ } x = 5 \dots\dots\dots (2)$$

$$\text{ถ้า } y = 4 \Rightarrow x^2 + x \equiv 6 \pmod{3^2}$$

$$2x \equiv 3 \pmod{3^2}$$

$$\Rightarrow x = 6$$

$$\therefore y = 4 \text{ และ } x = 6 \dots\dots\dots (3)$$

$$\text{ถ้า } y = 5 \Rightarrow x^2 + x \equiv 6 \pmod{3^2}$$

$$2x \equiv 4 \pmod{3^2}$$

$$\Rightarrow x = 2$$

$$\therefore y = 5 \text{ และ } x = 2 \dots\dots\dots (4)$$

$$\text{ถ้า } y = 7 \Rightarrow x^2 + x \equiv 3 \pmod{3^2}$$

$$2x \equiv 6 \pmod{3^2}$$

$$\Rightarrow x = 3$$

$$\therefore y = 7 \text{ และ } x = 3 \dots\dots\dots (5)$$

$$\text{ถ้า } y = 8 \Rightarrow x^2 + x \equiv 0 \pmod{3^2}$$

$$2x \equiv 7 \pmod{3^2}$$

$$\Rightarrow x = 8$$

$$\therefore y = 8 \text{ และ } x = 8 \dots\dots\dots (6)$$

จาก (1) ถึง (6) สรุปได้ว่า

$$\text{สำหรับ } p_j^\beta = (1-p)^\beta ; \beta = 2\alpha ;$$

$\alpha = 2$ จะมี 6 คำตอบคือ

$$1. y = 1 \text{ และ } x = 0$$

$$2. y = 2 \text{ และ } x = 5$$

$$3. y = 4 \text{ และ } x = 6$$

$$4. y = 5 \text{ และ } x = 2$$

$$5. y = 7 \text{ และ } x = 3$$

$$6. y = 8 \text{ และ } x = 8$$

$$\text{ดังนั้นในกรณี } p_j^\beta = (1-p)^\beta ; \beta = 2\alpha ;$$

$\alpha = 2$ จะมีค่า $f(p)$ ที่เป็นไปได้ 6 กรณี ได้แก่

$$1. f(p) = 1p$$

$$2. f(p) = 5 + 2p$$

$$3. f(p) = 6 + 4p$$

$$4. f(p) = 2 + 5p$$

$$5. f(p) = 3 + 7p$$

$$6. f(p) = 8 + 8p$$

กรณี $3 \leq \alpha$ จะมีค่าของ $f(p)$ 6 กรณี เท่านั้นจาก

3.1 กรณี $y = 3k$ ในระบบสมการ

$$\Rightarrow x^2 + x + 1 \equiv 3^2 k^2 \pmod{3^\alpha} \dots\dots\dots (*)$$

$$3k(2x - 3k + 1) \equiv 0 \pmod{3^\alpha} \dots\dots\dots (*)$$

$$\Rightarrow x^2 + x + 1 \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$$k(2x - 3k + 1) \equiv 0 \pmod{3^2} \dots\dots\dots (*)$$

$\Rightarrow$ ไม่มีคำตอบในระบบสมการ

3.2 ในกรณี $\gcd(y, a) = 1$

$$\Rightarrow x^2 + x \equiv y^2 - 1 \pmod{3^\alpha} \dots\dots\dots (*)$$

$$2x - y + 1 \equiv 0 \pmod{3^\alpha} \dots\dots\dots (*)$$

$$\Rightarrow x = \frac{1}{2}(y - 1)$$

$$\Rightarrow (y - 1)^2 + (y - 1) + 1 \equiv 4y^2 \pmod{3^\alpha}$$

$$\Rightarrow y^2 - 2y + 1 + 2y - 2 + 4 \equiv 4y^2 \pmod{3^\alpha}$$

$$\Rightarrow 3y^2 - 3 \equiv 0 \pmod{3^\alpha}$$

$$\Rightarrow y^2 - 1 \equiv 0 \pmod{3^{\alpha-1}}$$

$$\Rightarrow (y + 1)(y - 1) \equiv 0 \pmod{3^{\alpha-1}}$$

$$\Leftrightarrow y \equiv -1 \pmod{3^{\alpha-1}} \text{ หรือ } y \equiv 1 \pmod{3^{\alpha-1}}$$

$$\Rightarrow y = -1 + k \cdot 3^{\alpha-1} \text{ หรือ } y = 1 + k \cdot 3^{\alpha-1}$$

$$\Rightarrow k = 0, 1, 2$$

$$\Rightarrow k = 0, y = -1, y = 1$$

$$\Rightarrow k = 1, y = -1 + 3^{\alpha-1}, y = 1 + 3^{\alpha-1}$$

$$\Rightarrow k = 2, y = -1 + 2 \cdot 3^{\alpha-1}, y = 1 + 2 \cdot 3^{\alpha-1}$$

$$\text{ถ้า } y = 1 \Rightarrow x^2 + x \equiv 0 \pmod{3^\alpha}$$

$$2x \equiv 0 \pmod{3^\alpha}$$

$$\Rightarrow x = 0$$

$$\therefore y = 1 \text{ และ } x = 0 \dots\dots\dots(1)$$

$$\text{ถ้า } y = -1 + 3^{\alpha-1} \Rightarrow x^2 + x \equiv 3^{\alpha-1} - 2 \pmod{3^\alpha}$$

$$2x \equiv 3^{\alpha-1} \pmod{3^\alpha}$$

$$\Rightarrow x = 2 \cdot 3^{\alpha-1} - 1$$

$$\therefore y = -1 + 3^{\alpha-1} \text{ และ } x = 2 \cdot 3^{\alpha-1} - 1 \dots\dots\dots(2)$$

$$\text{ถ้า } y = 1 + 3^{\alpha-1} \Rightarrow x^2 + x \equiv 3^{\alpha-1} \pmod{3^\alpha}$$

$$2x + 2 \equiv 3^{\alpha-1} \pmod{3^\alpha}$$

$$\Rightarrow x = 2 \cdot 3^{\alpha-1}$$

$$\therefore y = 1 + 3^{\alpha-1} \text{ และ } x = 2 \cdot 3^{\alpha-1} \dots\dots\dots(3)$$

$$\text{ถ้า } y = -1 + 2 \cdot 3^{\alpha-1} \Rightarrow x^2 + x \equiv 2 \cdot 3^{\alpha-1} \pmod{3^\alpha}$$

$$2x \equiv 2 \cdot 3^{\alpha-1} - 2 \pmod{3^\alpha}$$

$$\Rightarrow x = 3^{\alpha-1} - 1$$

$$\therefore y = -1 + 2 \cdot 3^{\alpha-1} \text{ และ } x = 3^{\alpha-1} - 1 \dots\dots\dots(4)$$

$$\text{ถ้า } y = 1 + 2 \cdot 3^{\alpha-1} \Rightarrow x^2 + x \equiv 2 \cdot 3^{\alpha-1} \pmod{3^\alpha}$$

$$2x \equiv 2 \cdot 3^{\alpha-1} \pmod{3^\alpha}$$

$$\Rightarrow x = 3^{\alpha-1}$$

$$\therefore y = 1 + 2 \cdot 3^{\alpha-1} \text{ และ } x = 3^{\alpha-1} \dots\dots\dots(5)$$

$$\text{ถ้า } y = 3^\alpha - 1 \Rightarrow x^2 + x \equiv 3^{\alpha-1} \pmod{3^\alpha}$$

$$2x \equiv 2 \cdot 3^{\alpha-1} \pmod{3^\alpha}$$

$$\Rightarrow x = 3^{\alpha-1}$$

$$\therefore y = 3^\alpha - 1 \text{ และ } x = 3^{\alpha-1} \dots\dots\dots(6)$$

จากกรณี 3 สรุปได้ว่า

$$p_j^\beta = (1-p)^\beta \quad ; \beta = 2\alpha, \alpha \geq 3 \text{ จะมี 6 คำตอบคือ}$$

1. $y = 1$ และ $x = 0$
2. $y = -1+3^{\alpha-1}$ และ $x = -1+2\cdot 3^{\alpha-1}$
3. $y = 1+3^{\alpha-1}$ และ $x = 2\cdot 3^{\alpha-1}$
4. $y = -1+2\cdot 3^{\alpha-1}$ และ $x = -1+3^{\alpha-1}$
5. $y = 1+2\cdot 3^{\alpha-1}$ และ $x = 3^{\alpha-1}$
6. $y = -1+3^\alpha$ และ $x = -1+3^\alpha$

ดังนั้นจะมีค่า $f(p)$ ที่เป็นไปได้ 6 กรณีเท่านั้นจาก

1. $f(p) = \overline{0+1p}$
2. $f(p) = \overline{(-1+2\cdot 3^{\alpha-1})} + \overline{(-1+3^{\alpha-1})p}$
3. $f(p) = \overline{(2\cdot 3^{\alpha-1})} + \overline{(1+3^{\alpha-1})p}$
4. $f(p) = \overline{(-1+3^{\alpha-1})} + \overline{(-1+2\cdot 3^{\alpha-1})p}$
5. $f(p) = \overline{(3^{\alpha-1})} + \overline{(1+2\cdot 3^{\alpha-1})p}$
6. $f(p) = \overline{(-1+3^\alpha)} + \overline{(-1+3^\alpha)p}$

□

ทฤษฎีบทหน้า 36 ถ้า $f(1) = \bar{1}$ และ $f(p) = \bar{\beta}$ ($\bar{\beta} = \bar{h} + \bar{k}p$) และ

$$\bar{h}, \bar{k} \in \mathbb{Z}_{p_j^{\alpha_j}} \text{ เราสามารถสร้าง } \text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p_j^{\alpha_j}}[p])$$

ซึ่ง p_j เป็นจำนวนเฉพาะแบบเกาส์ที่ไม่สามารถลดทอนได้ โดยแยกเป็น

36.1 กรณี $p_j \neq 1-p$ (หรือ its associate) แล้ว

$$1. f(1) = \bar{1} \text{ และ } f(p) = \bar{1}p$$

$$2. f(1) = \bar{1} \text{ และ } f(p) = \bar{1}p^2$$

36.2 กรณี $p_j = 1 - p$ (หรือ its associate) แบ่งเป็น

$$\text{ถ้า } p_j^\beta = (1 - p)^{2\alpha}, \quad \beta = 2\alpha \quad \text{แล้ว}$$

1 $\alpha = 1$ จะมีค่าดังนี้คือ

$$1.1 f(1) = \bar{1} \text{ และ } f(p) = \bar{1} + \bar{0}p$$

$$1.2 f(1) = \bar{1} \text{ และ } f(p) = \bar{0} + \bar{1}p$$

$$1.3 f(1) = \bar{1} \text{ และ } f(p) = \bar{2} + \bar{2}p$$

2 $\alpha = 2$ จะมีค่าดังนี้คือ

$$2.1 f(1) = \bar{1} \text{ และ } f(p) = \bar{1}p$$

$$2.2 f(1) = \bar{1} \text{ และ } f(p) = \bar{5} + \bar{2}p$$

$$2.3 f(1) = \bar{1} \text{ และ } f(p) = \bar{6} + \bar{4}p$$

$$2.4 f(1) = \bar{1} \text{ และ } f(p) = \bar{2} + \bar{5}p$$

$$2.5 f(1) = \bar{1} \text{ และ } f(p) = \bar{3} + \bar{7}p$$

$$2.6 f(1) = \bar{1} \text{ และ } f(p) = \bar{8} + \bar{8}p$$

3 $\alpha \geq 3$ จะมีค่า $f(p)$ ที่เป็นไปได้แก่

$$3.1 f(1) = \bar{1} \text{ และ } f(p) = \bar{0} + \bar{1}p$$

$$3.2 f(1) = \bar{1} \text{ และ } f(p) = (\overline{-1+2 \cdot 3^{\alpha-1}}) + (\overline{-1+3^{\alpha-1}})p$$

$$3.3 f(1) = \bar{1} \text{ และ } f(p) = (\overline{2 \cdot 3^{\alpha-1}}) + (\overline{1+3^{\alpha-1}})p$$

$$3.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = (\overline{-1+3^{\alpha-1}}) + (\overline{-1+2 \cdot 3^{\alpha-1}})\rho$$

$$3.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = (\overline{3^{\alpha-1}}) + (\overline{1+2 \cdot 3^{\alpha-1}})\rho$$

$$3.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = (\overline{-1+3^\alpha}) + (\overline{-1+3^\alpha})\rho$$

พิสูจน์ ทฤษฎีบทหน้า 36 ผลจากทฤษฎีบทหน้า 35

จากทฤษฎีบทหน้า 34,36 สามารถสรุปจำนวนได้ตามทฤษฎีบท 2.5

และแจกแจงลักษณะของริงโฮโมมอร์ฟิซึมจาก $\mathbb{Z}[\rho]$ ไป $\mathbb{Z}_n[\rho]$ ดังนี้

ทฤษฎีบท 2.5 $|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_n[\rho])| = C_n \cdot 3^{\omega(n)}$

โดยที่ $C_n = 1$ ถ้า $3 \nmid n$

$$C_n = \frac{4}{3} \quad \text{ถ้า} \quad 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ} \quad C_n = \frac{7}{3} \quad \text{ถ้า} \quad 9 \mid n$$

พิสูจน์ ในการหา $|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{\alpha_j}[\rho])|$ จะพบว่า

กรณี 1 $p_j \neq 1 - \rho$ (หรือ its associate)

$$|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{\alpha_j}[\rho])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$1. \quad f(1) = \bar{0} \quad \text{และ} \quad f(\rho) = \bar{0}$$

$$2. \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = \bar{1}\rho$$

$$3. \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = \bar{1}\rho^2$$

2. กรณี $p_j = 1-p$ โดยที่ $p_j^\beta = (1-p)^{2\alpha}$, $\beta = 2\alpha$

สามารถแยกเป็นกรณีดังนี้

$$2.1 \alpha = 1$$

$$|\text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p_j^{\alpha_j}}[p])| = 4$$

และริงโฮโมมอร์ฟิซึมทั้งสี่สามารถกำหนดได้ดังนี้คือ

$$2.1.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(p) = \bar{0}$$

$$2.1.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = 1 + \bar{0}p$$

$$2.1.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{0} + \bar{1}p$$

$$2.1.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{2} + \bar{2}p$$

$$2.2 \alpha = 2$$

$$|\text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{p_j^{\alpha_j}}[p])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.2.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(p) = \bar{0}$$

$$2.2.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{0} + \bar{1}p$$

$$2.2.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{5} + \bar{2}p$$

$$2.2.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{6} + \bar{4}p$$

$$2.2.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{2} + \bar{5}p$$

$$2.2.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{3} + \bar{7}p$$

$$2.2.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(p) = \bar{8} + \bar{8}p$$

2.3. $\alpha \geq 3$

$$|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.3.1 \quad f(1) = \bar{0} \text{ และ } f(\rho) = \bar{0}$$

$$2.3.2 \quad f(1) = \bar{1} \text{ และ } f(\rho) = \bar{0} + \bar{1}\rho$$

$$2.3.3 \quad f(1) = \bar{1} \text{ และ } f(\rho) = \overline{(-1+2 \cdot 3^{\alpha-1})} + \overline{(-1+3^{\alpha-1})}\rho$$

$$2.3.4 \quad f(1) = \bar{1} \text{ และ } f(\rho) = \overline{(2 \cdot 3^{\alpha-1})} + \overline{(1+3^{\alpha-1})}\rho$$

$$2.3.5 \quad f(1) = \bar{1} \text{ และ } f(\rho) = \overline{(-1+3^{\alpha-1})} + \overline{(-1+2 \cdot 3^{\alpha-1})}\rho$$

$$2.3.6 \quad f(1) = \bar{1} \text{ และ } f(\rho) = \overline{(3^{\alpha-1})} + \overline{(1+2 \cdot 3^{\alpha-1})}\rho$$

$$2.3.7 \quad f(1) = \bar{1} \text{ และ } f(\rho) = \overline{(-1+3^\alpha)} + \overline{(-1+3^\alpha)}\rho$$

□

ทฤษฎีบทหน้า 37 $f \in \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$ ที่กำหนดโดย

$$f(\bar{1}) = \bar{\alpha} \text{ และ } f(\bar{\rho}) = \bar{\beta} \Leftrightarrow f \in \text{GroupHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$$

$$\bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta}, \bar{\beta}^2 + \bar{\beta} + \bar{1} = \bar{0}$$

พิสูจน์

ทำนองเดียวกันกับทฤษฎีบทหน้า 17

ทฤษฎีบทหน้า 38 $|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])|$

$$= |\{(\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p_j^{\alpha_j}}[\rho], \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } \bar{\beta}^2 + \bar{\beta} + \bar{1} = \bar{0}\}|$$

พิสูจน์

จากทฤษฎีบทหน้า 8, 36

สามารถสรุปได้ดังทฤษฎีบทว่า

$$\begin{aligned} & \left| \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho]) \right| \\ &= \left| \{(\bar{\alpha}, \bar{\beta}) \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Z}_{p_j^{\alpha_j}}[\rho], \bar{\alpha} = (\bar{\alpha})^2, \bar{\alpha} \cdot \bar{\beta} = \bar{\beta} \text{ และ } \bar{\beta}^2 + \bar{\beta} + \bar{1} = \bar{0}\} \right| \end{aligned}$$

□

ดังนั้นจึงเพียงพอที่เราจะคำนวณหา $f \in \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_n[\rho])$

จากแต่ละ $f \in \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$ โดยคำนวณจากค่าของ $\bar{\alpha}$ และ $\bar{\beta}$

ทฤษฎีบทหน้า 38 ให้ $f \in \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$ และ $f(\bar{1}) = \bar{\alpha}$ แล้ว

$$\bar{\alpha} = \bar{0} \text{ หรือ } \bar{\alpha} = \bar{1} \text{ นอกจากนี้จะมี}$$

$$f \in \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho]) \text{ นี้จะซึ่ง } f(\bar{1}) = \bar{1}$$

$$\text{ก็ต่อเมื่อ } p_j^{\alpha_j} \mid m$$

พิสูจน์

ทำนองเดียวกันกับ ทฤษฎีบทหน้า 26

ทฤษฎีบทหน้า 40 ให้ $f \in \text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])$ และ $f(\bar{1}) = \bar{0}$ ก็ต่อเมื่อ

$$f(\bar{\alpha}) = \bar{0} \text{ ทุกๆ } \bar{\alpha} \in \mathbb{Z}_m[\rho]$$

พิสูจน์

ทำนองเดียวกันกับ ทฤษฎีบทหน้า 27

ทฤษฎีบทหน้า 41 ให้ $f \in \text{RingHom}(\mathbb{Z}_m[p], \mathbb{Z}_{\alpha_j} [p])$ และ $f(\bar{1}) = \bar{1}$

$$\text{ถ้า } f(\bar{p}) = \bar{\beta} \text{ แล้ว } \bar{\beta}^2 + \bar{\beta} + \bar{1} = \bar{0}$$

นอกจากนั้นเราสามารถสร้าง $f(\bar{p})$ โดยแยกได้ดังนี้

41.1 ถ้า $p_j \neq 1-p$ (หรือ its associate) แล้ว

$$f(\bar{p}) = \bar{1}p \text{ หรือ } f(\bar{p}) = \bar{1}p^2$$

41.2 ถ้า $p_j = 1-p$ (หรือ its associate) แล้ว

จะมีหลายกรณีที่แตกต่างกัน

$$\text{ถ้า } p_j^\beta = (1-p)^{2\alpha} \quad \beta = 2\alpha$$

1 $\alpha = 1$ จะมีค่า $f(\bar{p})$ ที่เป็นไปได้แก่

$$1.1 \quad f(\bar{p}) = \bar{1} + \bar{0}p$$

$$1.2 \quad f(\bar{p}) = \bar{0} + \bar{1}p$$

$$1.3 \quad f(\bar{p}) = \bar{2} + \bar{2}p$$

2 $\alpha = 2$ จะมีค่า $f(\bar{p})$ ที่เป็นไปได้แก่

$$2.1 \quad f(\bar{p}) = \bar{1}p$$

$$2.2 \quad f(\bar{p}) = \bar{5} + \bar{2}p$$

$$2.3 \quad f(\bar{p}) = \bar{6} + \bar{4}p$$

$$2.4 \quad f(\bar{p}) = \bar{2} + \bar{5}p$$

$$2.5 \quad f(\bar{p}) = \bar{3} + \bar{7}p$$

$$2.6 \quad f(\bar{p}) = \bar{8} + \bar{8}p$$

3. $\alpha \geq 3$ จะมีค่า $f(\bar{\rho})$ ที่เป็นไปได้แก่

$$3.1 \ f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$3.2 \ f(\bar{\rho}) = (\overline{-1+2 \cdot 3^{\alpha-1}}) + (\overline{-1+3^{\alpha-1}})\rho$$

$$3.3 \ f(\bar{\rho}) = (\overline{2 \cdot 3^{\alpha-1}}) + (\overline{1+3^{\alpha-1}})\rho$$

$$3.4 \ f(\bar{\rho}) = (\overline{-1+3^{\alpha-1}}) + (\overline{-1+2 \cdot 3^{\alpha-1}})\rho$$

$$3.5 \ f(\bar{\rho}) = (\overline{3^{\alpha-1}}) + (\overline{1+2 \cdot 3^{\alpha-1}})\rho$$

$$3.6 \ f(\bar{\rho}) = (\overline{-1+3^{\alpha}}) + (\overline{-1+3^{\alpha}})\rho$$

พิสูจน์

ทฤษฎีบทหน้า 41.1 พิสูจน์ทำนองเดียวกันกับทฤษฎีบทหน้า 35.1

ทฤษฎีบทหน้า 41.1 พิสูจน์ทำนองเดียวกันกับทฤษฎีบทหน้า 35.2

□

ทฤษฎีบทหน้า 42 ถ้า $f(1) = \bar{1}$ และ $f(\bar{\rho}) = \bar{\beta}$

ทุกๆ จำนวนเฉพาะ p_j ที่ไม่สามารถลดทอนได้

เราสามารถสร้าง $\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{\alpha_j}[\rho])$
 p_j

42.1 ถ้า $p_j \neq 1 - \rho$ (หรือ its associate) ดังนี้คือ

$$1. \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{1}\rho$$

$$2. \ f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{1}\rho^2$$

42.2 กรณี $p_j = 1 - \rho$ (หรือ its associate) แล้ว

จะมีหลายกรณีที่แตกต่างกัน

$$\text{ถ้า } p_j^\beta = (1 - \rho)^{2\alpha}, \quad \beta = 2\alpha$$

1. $\alpha = 1$ ดังนี้คือ

$$1.1 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{1} + \bar{0}\rho$$

$$1.2 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$1.3 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{2} + \bar{2}\rho$$

2 $\alpha = 2$ ดังนี้คือ

$$2.1 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \rho$$

$$2.2 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{5} + \bar{2}\rho$$

$$2.3 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{6} + \bar{4}\rho$$

$$2.4 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{2} + \bar{5}\rho$$

$$2.5 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{3} + \bar{7}\rho$$

$$2.6 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{8} + \bar{8}\rho$$

3. $\alpha \geq 3$ จะมีค่า $f(\bar{\rho})$ ที่เป็นไปได้แก่

$$3.1 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$3.2 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+2\cdot 3^{\alpha-1})} + \overline{(-1+3^{\alpha-1})}\rho$$

$$3.3 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(2\cdot 3^{\alpha-1})} + \overline{(1+3^{\alpha-1})}\rho$$

$$3.4 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+3^{\alpha-1})} + \overline{(-1+2\cdot 3^{\alpha-1})}\rho$$

$$3.5 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(3^{\alpha-1})} + \overline{(1+2\cdot 3^{\alpha-1})}\rho$$

$$3.6 f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+3^{\alpha})} + \overline{(-1+3^{\alpha})}\rho$$

พิสูจน์

ทฤษฎีบทหน้า 42 ได้มาจาก ทฤษฎีบทหน้า 40,41

□

จากทฤษฎีบทหน้า 42 และ ทฤษฎีบท 2.2 และ 2.5 สรุปจำนวนได้ตามทฤษฎีบท 2.6

และแจกแจงลักษณะของริงโฮโมมอร์ฟิซึมจาก $Z_m[p]$ ไป $Z_n[p]$ ดังนี้

ทฤษฎีบท 2.6 $|\text{RingHom}(Z_m[p], Z_n[p])| = C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \text{ ถ้า } 3 \nmid n \text{ แต่ } 3 \mid \left(\frac{n}{\gcd(m, n)}\right),$$

$$C_n = \frac{4}{3} \text{ ถ้า } 3 \nmid \left(\frac{n}{\gcd(m, n)}\right) \text{ และ } 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ } C_n = \frac{7}{3} \text{ ถ้า } 3 \nmid \left(\frac{n}{\gcd(m, n)}\right) \text{ และ } 9 \mid n$$

$$\text{โดยที่ } \beta = \omega(n) - \omega\left(\frac{n}{\gcd(m, n)}\right)$$

พิสูจน์

ในการหา $|\text{RingHom}(Z_m[p], Z_{p_j^{\alpha_j}}[p])|$ จะพบว่า

$$\text{ถ้า } p_j^{\alpha_j} \nmid m \text{ จะได้ว่า } |\text{RingHom}(Z_m[p], Z_{p_j^{\alpha_j}}[p])| = 1$$

$$\text{นั่นคือ ถ้า } p_j^{\alpha_j} \nmid m \text{ จะมี } f \in \text{RingHom}(Z_m[p], Z_{p_j^{\alpha_j}}[p])$$

$$\text{เพียงฟังก์ชันเดียวคือ } f(\bar{\alpha}) = \bar{0} \text{ ทุกๆ } \bar{\alpha} \in Z_m[p]$$

$$\text{ดังนั้น } \beta = \omega(p_j^{\alpha_j}) - \omega\left(\frac{p_j^{\alpha_j}}{\gcd(m, p_j^{\alpha_j})}\right) = 1 - 1 = 0$$

$$\text{ดังนั้น } |\text{RingHom}(Z_m[p], Z_{p_j^{\alpha_j}}[p])| = 1 \cdot 3^0 = 1 \text{ ในกรณีที่}$$

$$p_j^{\alpha_j} \nmid m$$

ดังนั้นจึงเป็นการเพียงพอที่จะสนใจเฉพาะกรณีที่ $p_j^{\alpha_j} \mid m$

สามารถสรุปได้ตามทฤษฎีบทและแจกแจงได้ดังนี้คือ

ริงโฮโมมอร์ฟิซึมจาก $f: \mathbb{Z}_m[p] \rightarrow \mathbb{Z}_{p_j^{\alpha_j}}[p]$ จะมีลักษณะดังนี้

1. กรณี $p_j \neq 1 - p$ (หรือ its associate) จะได้ว่า

$$|\text{RingHom}(\mathbb{Z}_m[p], \mathbb{Z}_{p_j^{\alpha_j}}[p])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$1.1 \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{p}) = \bar{0}$$

$$1.2 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{p}) = \bar{1}p$$

$$1.3 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{p}) = \bar{1}p^2$$

2. กรณี $p_j = 1 - p$ (หรือ its associate)

โดยที่ $p_j^\beta = (1-p)^{2\alpha}$, $\beta = 2\alpha$ สามารถแยกเป็นกรณีดังนี้

$$2.1 \quad \alpha = 1$$

$$|\text{RingHom}(\mathbb{Z}_m[p], \mathbb{Z}_{p_j^{\alpha_j}}[p])| = 4$$

และริงโฮโมมอร์ฟิซึมทั้งสี่สามารถกำหนดได้ดังนี้คือ

$$2.1.1 \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{p}) = \bar{0}$$

$$2.1.2 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{p}) = 1 + \bar{0}p$$

$$2.1.3 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{p}) = \bar{0} + \bar{1}p$$

$$2.1.4 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{p}) = \bar{2} + \bar{2}p$$

$$2.2 \quad \alpha = 2$$

$$|\text{RingHom}(\mathbb{Z}_m[p], \mathbb{Z}_{p_j^{\alpha_j}}[p])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.2.1. f(\bar{1}) = \bar{0} \text{ และ } f(\bar{\rho}) = \bar{0}$$

$$2.2.2. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$2.2.3. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{5} + \bar{2}\rho$$

$$2.2.4. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{6} + \bar{4}\rho$$

$$2.2.5. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{2} + \bar{5}\rho$$

$$2.2.6. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{3} + \bar{7}\rho$$

$$2.2.7. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{8} + \bar{8}\rho$$

2.3. $\alpha \geq 3$

$$|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p^{\alpha_j}}[\rho])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.3.1. f(\bar{1}) = \bar{0} \text{ และ } f(\bar{\rho}) = \bar{0}$$

$$2.3.2. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$2.3.3. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+2 \cdot 3^{\alpha-1})} + \overline{(-1+3^{\alpha-1})}\rho$$

$$2.3.4. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(2 \cdot 3^{\alpha-1})} + \overline{(1+3^{\alpha-1})}\rho$$

$$2.3.5. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+3^{\alpha-1})} + \overline{(-1+2 \cdot 3^{\alpha-1})}\rho$$

$$2.3.6. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(3^{\alpha-1})} + \overline{(1+2 \cdot 3^{\alpha-1})}\rho$$

$$2.3.7. f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+3^{\alpha})} + \overline{(-1+3^{\alpha})}\rho$$

□

บทที่ 5

สรุปผล

จากการพิสูจน์เชิงการสร้างในการหาจำนวนของกรุปโฮโมมอร์ฟิซึมและจำนวนของริงโฮโมมอร์ฟิซึม ผลของการพิสูจน์ยืนยันตามทฤษฎีของแกลเลียน(Gallian) และสามารถแจกแจงลักษณะได้ตามทฤษฎีต่อไปนี้คือ

ทฤษฎีบท 1.1 $|\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)| = n$

จะมี $f \in \text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n)$

และจะมีลักษณะดังต่อไปนี้คือ

$$\text{GroupHom}(\mathbb{Z}, \mathbb{Z}_n) = \{ f_i \mid i = 0, 1, 2, \dots, n-1 \}$$

$$\text{โดยที่ } f_i(k) = ki \pmod{n}, k \in \mathbb{Z}$$

ทฤษฎีบท 1.2 $|\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = \gcd(m, n)$

จะมี $f \in \text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)$

และจะมีลักษณะดังต่อไปนี้คือ

$$f(1) = \bar{d} \text{ และ } \bar{d} \in X_a$$

$$\text{โดยที่ให้ } g = \gcd(m, n), a > 0 \text{ และ } a \mid g$$

$$X_a = \left\{ i \left(\frac{n}{a} \right) \mid 1 \leq i \leq a \text{ และ } \gcd(i, a) = 1 \right\}$$

ทฤษฎีบท 1.3 $|\text{GroupHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])| = n^4$

$$\text{กำหนดให้ } \bar{\alpha} \in \{ \bar{a} + \bar{b}i \mid \bar{a}, \bar{b} \in \mathbb{Z}_n \}$$

$$\bar{\beta} \in \{ \bar{a} + \bar{b}i \mid \bar{a}, \bar{b} \in \mathbb{Z}_n \}$$

ทุกครั้งเมื่อเลือก $\bar{\alpha}$ และ $\bar{\beta}$ สามารถสร้างโฮโมมอร์ฟิซึมจาก $\mathbb{Z}[i]$ ไป $\mathbb{Z}_n[i]$

$$\text{ซึ่ง } f(1) = \bar{\alpha} \text{ และ } f(i) = \bar{\beta}$$

ทฤษฎีบท 1.4 $|\text{GroupHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| = (\gcd(m, n))^4$

$$\text{จาก } \mathbb{Z}_m[i] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$$

$$\text{และ } \mathbb{Z}_n[i] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$$

$$\begin{aligned} \text{ดังนั้น } |\text{GroupHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| &= |\text{GroupHom}(\mathbb{Z}_m \oplus \mathbb{Z}_m, \mathbb{Z}_n \oplus \mathbb{Z}_n)| \\ &= |\text{GroupHom}(\mathbb{Z}_m \oplus \mathbb{Z}_m, \mathbb{Z}_n)|^2 \\ &= |\text{GroupHom}(\mathbb{Z}_m, \mathbb{Z}_n)|^4 \\ &= (\gcd(m, n))^4 \end{aligned}$$

ทฤษฎีบท 1.5 $|\text{GroupHom}(\mathbb{Z}[\rho], \mathbb{Z}_n[\rho])| = n^4$

ทำนองเดียวกับทฤษฎีบท 1.3 และ 1.4

ทฤษฎีบท 1.6 $|\text{GroupHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_n[\rho])| = (\gcd(m, n))^4$

ทำนองเดียวกับทฤษฎีบท 1.3 ถึง 1.5

ทฤษฎีบท 2.1 $|\text{RingHom}(\mathbb{Z}, \mathbb{Z}_n)| = 2^{\omega(n)}$

และมีลักษณะดังนี้

$$\text{ให้ } \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \mathbb{Z}_{p_3^{\alpha_3}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}} \text{ จะได้}$$

$$f \in \text{RingHom}(\mathbb{Z}, \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \mathbb{Z}_{p_3^{\alpha_3}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}})$$

$$\Leftrightarrow f(1) = (\overline{a_1}, \overline{a_2}, \overline{a_3}, \dots, \overline{a_s}), \overline{a_j} = \overline{0} \text{ หรือ } \overline{1} \text{ ใน } \mathbb{Z}_{p_j^{\alpha_j}}$$

ทฤษฎีบท 2.2 $|\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)| = 2^\beta$ โดยที่ $\beta = \omega(n) - \omega\left(\frac{n}{\gcd(m, n)}\right)$

และ $\omega(k)$ คือจำนวนของจำนวนเฉพาะที่แตกต่างกันและหาร k ลงตัว

ลักษณะของ $\text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$ สามารถกำหนดได้ดังต่อไปนี้

$$f \in \text{RingHom}(\mathbb{Z}_m, \mathbb{Z}_n)$$

$$f(1) = (\overline{a_1}, \overline{a_2}, \overline{a_3}, \dots, \overline{a_s})$$

และขึ้นอยู่กับเงื่อนไขดังต่อไปนี้คือ

$$\text{ให้ } m = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_s^{\beta_s}$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$$

$$g = \gcd(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} p_3^{\gamma_3} \dots p_s^{\gamma_s}, \gamma_j = \min(\beta_j, \alpha_j)$$

ถ้า $\beta_j \geq \alpha_j$ แล้ว $\overline{a} = \overline{0}$ หรือ $\overline{1}$

ถ้า $\beta_j < \alpha_j$ แล้ว $\overline{a} = \overline{0}$

ทฤษฎีบท 2.3 $|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_n[i])| = C_n \cdot 3^{\omega(n)}$

โดยที่ $C_n = 1$ ถ้า $4 \nmid n$

$$C_n = \frac{5}{3} \text{ ถ้า } 4 \mid n \text{ แต่ } 8 \nmid n$$

และ $C_n = 3$ ถ้า $8 \mid n$

ในการหา $|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{\frac{n}{p_j^{\alpha_j}}}[i])|$ จะพบว่า

กรณี 1 $p_j \neq 1+i$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{\frac{n}{p_j^{\alpha_j}}}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$1. f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2. f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$3. f(1) = \bar{1} \quad \text{และ} \quad f(i) = -\bar{i}$$

กรณี 2 $p_j = 1 + i$

$$\text{จะแบ่งเป็นกรณี } p_j^\beta = (1 + i)^{2t}, \beta = 2t$$

$$2.1 \quad t = 1$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{\alpha_j}^{p_j}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$2.1.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.1.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{1}$$

$$2.1.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$2.2 \quad t = 2$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{\alpha_j}^{p_j}[i])| = 5$$

และริงโฮโมมอร์ฟิซึมทั้งห้าสามารถกำหนดได้ดังนี้คือ

$$2.2.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.2.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$2.2.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{3i}$$

$$2.2.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{2 + i}$$

$$2.2.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{2+3i}$$

$$2.3 \quad t=3$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{\alpha_j, p_j}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้คือ

$$2.3.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.3.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{i}$$

$$2.3.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{3i}$$

$$2.3.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{5i}$$

$$2.3.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{7i}$$

$$2.3.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{4+i}$$

$$2.3.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{4+3i}$$

$$2.3.8 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{4+5i}$$

$$2.3.9 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{4+7i}$$

$$2.4 \quad t \geq 3$$

$$|\text{RingHom}(\mathbb{Z}[i], \mathbb{Z}_{\alpha_j, p_j}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้คือ

$$2.4.1 \quad f(1) = \bar{0} \quad \text{และ} \quad f(i) = \bar{0}$$

$$2.4.2 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{0+1i}$$

$$2.4.3 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \overline{0 + (2^{t-1}-1)i}$$

$$2.4.4 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$2.4.5 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = \bar{0} + (\overline{2^t-1})i$$

$$2.4.6 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + \bar{1}i$$

$$2.4.7 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$2.4.8 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$2.4.9 \quad f(1) = \bar{1} \quad \text{และ} \quad f(i) = (\overline{2^{t-1}}) + (\overline{2^t-1})i$$

ทฤษฎีบท 2.4 $|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])| = C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \quad \text{ถ้า } 4 \nmid n \text{ หรือ } 2 \mid \left(\frac{n}{\gcd(m,n)}\right)$$

$$C_n = \frac{5}{3} \quad \text{ถ้า } 2 \nmid \left(\frac{n}{\gcd(m,n)}\right) \text{ และ } 4 \mid n \text{ แต่ } 8 \nmid n$$

$$\text{และ } C_n = 3 \quad \text{ถ้า } 2 \nmid \left(\frac{n}{\gcd(m,n)}\right) \text{ และ } 8 \mid n$$

$$\text{โดยที่ } \beta = \omega(n) - \omega\left(\frac{n}{\gcd(m,n)}\right)$$

$\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_n[i])$ สามารถแยกได้เป็น

$$\text{กรณี } 1 \quad p_j \neq 1+i$$

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้ ดังนี้คือ

$$1. \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{i}$$

$$3. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = -\bar{i}$$

$$\text{กรณี 2 } p_j = 1+i$$

$$\text{ในกรณี } p_j^{\beta} = (1+i)^{2t}$$

$$2.1 \quad t = 1$$

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้ คือ

$$2.1.1. f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2.1.2. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{1}$$

$$2.1.3. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{i}$$

$$2.2 \quad t = 2$$

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 5$$

และริงโฮโมมอร์ฟิซึมทั้งห้าสามารถกำหนดได้ดังนี้ คือ

$$2.2.1. f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2.2.2. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{i}$$

$$2.2.3. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{3i}$$

$$2.2.4. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{2} + \bar{i}$$

$$2.2.5. f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{2} + \bar{3i}$$

$$2.3 \quad t = 3$$

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้ คือ

$$2.3.1. f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2.3.2. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{i}$$

$$2.3.3. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{3i}$$

$$2.3.4. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{5i}$$

$$2.3.5. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{7i}$$

$$2.3.6. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{4 + i}$$

$$2.3.7. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{4 + 3i}$$

$$2.3.8. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{4 + 5i}$$

$$2.3.9. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \overline{4 + 7i}$$

2.4 $t \geq 3$

$$|\text{RingHom}(\mathbb{Z}_m[i], \mathbb{Z}_{p_j^{\alpha_j}}[i])| = 9$$

และริงโฮโมมอร์ฟิซึมทั้งเก้าสามารถกำหนดได้ดังนี้ คือ

$$2.4.1 \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{i}) = \bar{0}$$

$$2.4.2 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + \bar{1}i$$

$$2.4.3. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + (\overline{2^{t-1}-1})i$$

$$2.4.4. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + (\overline{2^{t-1}+1})i$$

$$2.4.5. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = \bar{0} + (\overline{2^t-1})i$$

$$2.4.6. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + \bar{1}i$$

$$2.4.7. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}-1})i$$

$$2.4.8. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^{t-1}+1})i$$

$$2.4.9. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{i}) = (\overline{2^{t-1}}) + (\overline{2^t - 1})i$$

ทฤษฎีบท 2.5 $|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_n[\rho])| = C_n \cdot 3^{\omega(n)}$

โดยที่ $C_n = 1$ ถ้า $3 \nmid n$

$$C_n = \frac{4}{3} \quad \text{ถ้า} \quad 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ} \quad C_n = \frac{7}{3} \quad \text{ถ้า} \quad 9 \mid n$$

พิสูจน์

ในการหา $|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])|$ จะพบว่า

กรณี 1 $p_j \neq 1 - \rho$ (หรือ its associate)

$$|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$1. \quad f(1) = \bar{0} \quad \text{และ} \quad f(\rho) = \bar{0}$$

$$2. \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = \bar{1}\rho$$

$$3. \quad f(1) = \bar{1} \quad \text{และ} \quad f(\rho) = \bar{1}\rho^2$$

2. กรณี $p_j = 1 - \rho$ โดยที่ $p_j^\beta = (1 - \rho)^{2\alpha}$, $\beta = 2\alpha$

สามารถแยกเป็นกรณีดังนี้

$$2.1 \quad \alpha = 1$$

$$|\text{RingHom}(\mathbb{Z}[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])| = 4$$

และริงโฮโมมอร์ฟิซึมทั้งสี่สามารถกำหนดได้ดังนี้คือ

$$2.1.1 \quad f(1) = \bar{0} \text{ และ } f(p) = \bar{0}$$

$$2.1.2 \quad f(1) = \bar{1} \text{ และ } f(p) = 1 + \bar{0}p$$

$$2.1.3 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{0} + \bar{1}p$$

$$2.1.4 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{2} + \bar{2}p$$

$$2.2 \quad \alpha = 2$$

$$|\text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{\alpha_j}^{p_j}[p])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.2.1 \quad f(1) = \bar{0} \text{ และ } f(p) = \bar{0}$$

$$2.2.2 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{0} + \bar{1}p$$

$$2.2.3 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{5} + \bar{2}p$$

$$2.2.4 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{6} + \bar{4}p$$

$$2.2.5 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{2} + \bar{5}p$$

$$2.2.6 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{3} + \bar{7}p$$

$$2.2.7 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{8} + \bar{8}p$$

$$2.3. \quad \alpha \geq 3$$

$$|\text{RingHom}(\mathbb{Z}[p], \mathbb{Z}_{\alpha_j}^{p_j}[p])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.3.1 \quad f(1) = \bar{0} \text{ และ } f(p) = \bar{0}$$

$$2.3.2 \quad f(1) = \bar{1} \text{ และ } f(p) = \bar{0} + \bar{1}p$$

$$2.3.3 \quad f(1) = \bar{1} \text{ และ } f(\rho) = (\overline{-1+2\cdot 3^{\alpha-1}}) + (\overline{-1+3^{\alpha-1}})\rho$$

$$2.3.4 \quad f(1) = \bar{1} \text{ และ } f(\rho) = (\overline{2\cdot 3^{\alpha-1}}) + (\overline{1+3^{\alpha-1}})\rho$$

$$2.3.5 \quad f(1) = \bar{1} \text{ และ } f(\rho) = (\overline{-1+3^{\alpha-1}}) + (\overline{-1+2\cdot 3^{\alpha-1}})\rho$$

$$2.3.6 \quad f(1) = \bar{1} \text{ และ } f(\rho) = (\overline{3^{\alpha-1}}) + (\overline{1+2\cdot 3^{\alpha-1}})\rho$$

$$2.3.7 \quad f(1) = \bar{1} \text{ และ } f(\rho) = (\overline{-1+3^\alpha}) + (\overline{-1+3^\alpha})\rho$$

ทฤษฎีบท 2.6 $|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_n[\rho])| = C_n \cdot 3^\beta$

$$\text{โดยที่ } C_n = 1 \text{ ถ้า } 3 \nmid n \text{ แต่ } 3 \mid \left(\frac{n}{\gcd(m, n)}\right),$$

$$C_n = \frac{4}{3} \text{ ถ้า } 3 \nmid \left(\frac{n}{\gcd(m, n)}\right) \text{ และ } 3 \mid n \text{ แต่ } 9 \nmid n$$

$$\text{และ } C_n = \frac{7}{3} \text{ ถ้า } 3 \nmid \left(\frac{n}{\gcd(m, n)}\right) \text{ และ } 9 \mid n$$

$$\text{โดยที่ } \beta = \omega(n) - \omega\left(\frac{n}{\gcd(m, n)}\right)$$

ริงโฮโมมอร์ฟิซึมจาก $f: \mathbb{Z}_m[\rho] \rightarrow \mathbb{Z}_{p_j^{\alpha_j}}[\rho]$ จะมีลักษณะดังนี้

1. กรณี $p_j \neq 1 - \rho$ (หรือ its associate) จะได้ว่า

$$|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha_j}}[\rho])| = 3$$

และริงโฮโมมอร์ฟิซึมทั้งสามสามารถกำหนดได้ดังนี้คือ

$$1.1 \quad f(1) = \bar{0} \text{ และ } f(\bar{\rho}) = \bar{0}$$

$$1.2 \quad f(1) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{1}\rho$$

$$1.3 \quad f(1) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{1}\rho^2$$

2. กรณี $p_j = 1 - \rho$ (หรือ its associate)

โดยที่ $p_j^\beta = (1 - \rho)^{2\alpha}$, $\beta = 2\alpha$ สามารถแยกเป็นกรณีดังนี้

2.1 $\alpha = 1$

$$|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha j}}[\rho])| = 4$$

และริงโฮโมมอร์ฟิซึมทั้งสี่ที่สามารถกำหนดได้ดังนี้คือ

$$2.1.1 \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{\rho}) = \bar{0}$$

$$2.1.2 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = 1 + \bar{0}\rho$$

$$2.1.3 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$2.1.4 \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{2} + \bar{2}\rho$$

2.2 $\alpha = 2$

$$|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p_j^{\alpha j}}[\rho])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดที่สามารถกำหนดได้ดังนี้คือ

$$2.2.1. \quad f(\bar{1}) = \bar{0} \quad \text{และ} \quad f(\bar{\rho}) = \bar{0}$$

$$2.2.2. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$2.2.3. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{5} + \bar{2}\rho$$

$$2.2.4. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{6} + \bar{4}\rho$$

$$2.2.5. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{2} + \bar{5}\rho$$

$$2.2.6. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{3} + \bar{7}\rho$$

$$2.2.7. \quad f(\bar{1}) = \bar{1} \quad \text{และ} \quad f(\bar{\rho}) = \bar{8} + \bar{8}\rho$$

2.3. $\alpha \geq 3$

$$|\text{RingHom}(\mathbb{Z}_m[\rho], \mathbb{Z}_{p^{\alpha_j}}[\rho])| = 7$$

และริงโฮโมมอร์ฟิซึมทั้งเจ็ดสามารถกำหนดได้ดังนี้คือ

$$2.3.1 \quad f(\bar{1}) = \bar{0} \text{ และ } f(\bar{\rho}) = \bar{0}$$

$$2.3.2 \quad f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \bar{0} + \bar{1}\rho$$

$$2.3.3 \quad f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+2\cdot 3^{\alpha-1})} + \overline{(-1+3^{\alpha-1})}\rho$$

$$2.3.4 \quad f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(2\cdot 3^{\alpha-1})} + \overline{(1+3^{\alpha-1})}\rho$$

$$2.3.5 \quad f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+3^{\alpha-1})} + \overline{(-1+2\cdot 3^{\alpha-1})}\rho$$

$$2.3.6 \quad f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(3^{\alpha-1})} + \overline{(1+2\cdot 3^{\alpha-1})}\rho$$

$$2.3.7 \quad f(\bar{1}) = \bar{1} \text{ และ } f(\bar{\rho}) = \overline{(-1+3^{\alpha})} + \overline{(-1+3^{\alpha})}\rho$$

□

บรรณานุกรม

บรรณานุกรม

ณรงค์ ปันนัม. (2531). *ทฤษฎีจำนวน*. กรุงเทพฯ : มหาวิทยาลัยศรีนครินทรวิโรฒ
อัสสัมชัญ.

----- . (2536). *พีชคณิตมหาวิทยาลัย*. กรุงเทพฯ : ชมรมเพื่อนเด็ก.

พิชากร แปลงประสพโชค. (2534, พฤษภาคม). "ศึกษาคณิตศาสตร์แนวทางใดจึงมีประสิทธิภาพในการแก้ปัญหา," *วารสารคณิตศาสตร์*. ปริมา 35 ฉบับ 392-393 ; 22-30.

สุเทพ จันทน์สมศักดิ์. (2536). "ธรรมชาติและโครงสร้างของคณิตศาสตร์," ใน *สารัตถะและ
วิทยวิธีทางวิชาคณิตศาสตร์*. 1-36. นนทบุรี : มหาวิทยาลัยสุโขทัยธรรมาธิราช.

Gallian, J.A. & Buskirk, J. (1984, March). "The Number of Homomorphisms from $\mathbb{Z}_m$
into $\mathbb{Z}_n$." *The American Math. Monthly*. 91 ; 196-197.

Gallian, J.A. & Jungreis, D. S. (1988, March). "Homomorphisms from $\mathbb{Z}_m[i]$ into
 $\mathbb{Z}_n[i]$ and $\mathbb{Z}_m[\rho]$ into $\mathbb{Z}_n[\rho]$ where $i^2+1=0$ and $\rho^2+\rho+1=0$," *The American
Math. Monthly*. 95 : 247-249.

Gallian, J.A. (n.d.). "Counting Homomorphisms from $\mathbb{Z}_m[\Delta]$ into $\mathbb{Z}_n[\Delta]$ where Δ is
the Golden Section," 1-3.

----- . (1994). *Contemporary Abstract Algebra*. 3rd. Lexington : D.C. Heath.

----- . (1998, September). Re-homomorphisms. (Online). Available E-mail:
jgallian@d.umn.edu.

Hardy, G.H. & Wright, E.M. (1959). *An Introduction to the Theory of Number*. 4th ed.
London : Oxford University Press.

Malik, D.S. ,Mordeson, J.M. and Sen, M.K. (1997). *Fundamentals of Abstract Algebra*.
Singapore : Mc Graw-Hill.

Saleh, M. , Yousef, H. & Abu-Hlail, J. (1998, March). "The Number of
Homomorphisms from $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \dots \times \mathbb{Z}_{m_r}$ into $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times$
 $\mathbb{Z}_{n_3} \times \dots \times \mathbb{Z}_{n_s}$," : *Dirasat J.* , 326-329.

Saleh, M. (1999, June). # Homomorphisms. (Online). Available E-mail:
mohammad@math.birzeit.edu.

ประวัติย่อผู้วิจัย

ประวัติย่อผู้วิจัย

ชื่อ	นางสาวอัจฉริยา ชมะนันท์
วันเดือนปีเกิด	29 มกราคม พุทธศักราช 2506
สถานที่เกิด	เขตพญาไท กรุงเทพมหานคร
สถานที่อยู่ปัจจุบัน	11/27 ซอยพงษ์เพชร 7 วัดบัวขวัญ ถนนงามวงศ์วาน บางเขน อำเภอเมือง นนทบุรี 11000
ตำแหน่งหน้าที่การงาน	อาจารย์ 1 ระดับ 4
สถานที่ทำงานปัจจุบัน	โรงเรียนสามเสนวิทยาลัย เขตพญาไท กรุงเทพมหานคร รหัสไปรษณีย์ 10400
ประวัติการศึกษา	
พ.ศ.2522	มัธยมศึกษาปีที่ 3 โรงเรียนเขมะสิริอนุสสรณ์
พ.ศ.2524	มัธยมศึกษาปีที่ 5 โรงเรียนสันติราษฎร์วิทยาลัย
พ.ศ.2528	การศึกษาระดับบัณฑิต กศ.บ.(คณิตศาสตร์) มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร
พ.ศ.2543	การศึกษามหาบัณฑิต กศ.ม.(คณิตศาสตร์) มหาวิทยาลัยศรีนครินทรวิโรฒ