พีชคณิตนามธรรม

Abstract Algebra

โดย ศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

พิมพ์ครั้งที่ 2 (ฉบับแก้ไขครั้งที่1) : 2556 จำนวน 225 หน้า
พิมพ์ที่ โรงพิมพ์มหาวิทยาลัยศิลปากร

โครงการตำรา คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

คำนำ

วิชาพีชคณิตนามธรรมเป็นการศึกษาในลักษณะวางนัยโครงสร้างที่รู้จัก โดยเฉพาะการขยายแนวคิดจากสมบัติของระบบจำนวน ดังนั้นกระบวนวิธีคิดในวิชาคณิตศาสตร์แขนง "พีชคณิต" จึงเป็นนามธรรมล้วนๆ ซึ่งนักศึกษาส่วนใหญ่มักไม่คุ้นเคยและไม่เข้าใจเจตคติของวิชา ทำให้เกิดปัญหาในระหว่างเรียนอยู่เสมอ ผู้เขียนได้สอนรายวิชาเหล่านี้มาหลายปี ทั้งในระดับปริญญาตรีและปริญญาโท จึงค่อนข้างเข้าใจปัญหาของนักศึกษา ทำให้เกิดแรงบันดาลใจที่จะเขียนหนังสืออ่านประกอบวิชาพีชคณิตนามธรรมในทุกระดับ แต่ไม่สามารถบรรจุทุกเรื่องราวไว้ในหนังสือเพียงเล่มเดียว ผู้เขียนจึงเริ่มต้นด้วยหนังสือเรื่อง "ทฤษฎีกรุปเบื้องต้น" ในปี 2553 โดยเน้นเฉพาะเรื่อง "กรุป" เพียงเรื่องเดียวและเขียนในรายละเอียดของความเป็นมา โดยมุ่งหวังให้นักศึกษาเข้าใจการศึกษาเชิงนามธรรม เพื่อจะทำให้การศึกษาคณิตศาสตร์แขนงอื่นๆ เข้าใจได้ง่ายขึ้น สำหรับหนังสือเรื่อง "พีชคณิตนามธรรม" เล่มนี้ผู้เขียนตั้งใจให้เป็นตำราประกอบรายวิชาพีชคณิตนามธรรมในระดับปริญญาโท ชั้นปีที่ 1 จึงเขียนเน้นแนวคิดในเชิงวิจัยของนักคณิตศาสตร์เจ้าขององค์ความรู้ที่อยู่เบื้องหลัง เพื่อให้นักศึกษาได้เห็นวิธีคิดและวิธีศึกษาวิจัยในทางคณิตศาสตร์เพื่อเป็นพื้นฐานของการทำวิจัยต่อไป เนื้อหาจึงเป็นเรื่องราวของพีชคณิตนามธรรมเบื้องต้นและการประยุกต์ระดับกลาง

ในหนังสือเล่มนี้ประกอบด้วยหกบท โดยไม่มีบทใดบรรจุเรื่องราวของความรู้มูลฐานที่จำเป็นต่อการศึกษาวิชาคณิตศาสตร์โดยทั่วไปดังเช่นตำราเล่มอื่นๆ ทั้งนี้เพราะได้ใช้การอ้างอิงจากหนังสือ "ทฤษฎีกรุปเบื้องต้น" ซึ่งผู้เขียนได้เขียนไว้แล้ว อย่างไรก็ตามผู้เขียนได้ทบทวนเรื่องราวของกรุปไว้ในบทที่ 1 รวมทั้งได้กล่าวในเชิงลึกของเนื้อหาที่ทบทวน สำหรับบทที่ 2 เป็นการศึกษาเพื่อหาวิธีการตอบปัญหาการจำแนกกรุปจำกัดทั้งหมดซึ่งยังคงเป็นคำถามเปิดจนถึงปัจจุบันนี้ และได้แสดงโครงสร้างของกรุปอาบีเลียนด้วยการจำแนกกรุปอาบีเลียนก่อกำเนิดแบบจำกัด แม้คำถามเปิดจะยังไม่ได้รับคำตอบทั้งหมด แต่ในบทที่ 3 ผู้เขียนแสดงแนวคิดของนักคณิตศาสตร์ที่พยายามตอบปัญหานี้สำหรับกรุปนอนอาบีเลียนบางหมู่ และผลของการศึกษาเป็นรากฐานของแขนงวิชาใหม่นั่นคือ "วิชาคอมบินาทอริกส์" ซึ่งเป็นวิชาที่ว่าด้วยการนับล้วน ๆ

ในบทที่ 4 – 5 – 6 จะเป็นการศึกษาการวางนัยโครงสร้างของระบบจำนวนอย่างเต็มรูปแบบ นั่นคือ "ทฤษฎีริง" ทำให้ได้เห็นริงที่มีประโยชน์มากมาย ตัวอย่างเช่นริงของไอดีลหลัก ริงแบบยุคลิด ริงของการแยกตัวประกอบได้แบบเดียวและริงพหุนาม โดยเฉพาะผลของการศึกษาริงพหุนามทำให้กาลัวส์พิสูจน์ได้ว่าฟิลด์ใดที่จะมีรากทั้งหมดของพหุนาม ซึ่งเป็นเนื้อหาที่ผู้เขียนตั้งใจจะเขียนเป็นหนังสือเล่มต่อไป

สำหรับคำศัพท์เทคนิค ผู้เขียนได้แปลเป็นภาษาไทยทั้งหมดโดยยึดพจนานุกรมศัพท์คณิตศาสตร์ ฉบับราชบัณฑิตยสถานเป็นหลัก และวงเล็บศัพท์ภาษาอังกฤษดั้งเดิมไว้ด้วย นอกจากนี้ยังรวบรวมศัพท์เทคนิคทั้งหมดไว้ในบัญชีศัพท์ท้ายเล่ม

ผู้เขียนหวังเป็นอย่างยิ่งว่า หนังสือเล่มนี้จะเป็นประโยชน์สำหรับผู้ศึกษาวิชาพีชคณิตนามธรรม และประโยชน์ใดๆ ที่เกิดขึ้นจากความรู้ของหนังสือเล่มนี้ผู้เขียนขอน้อมรำลึกในพระคุณของอาจารย์ที่ได้ประสิทธิ์ประสาทความรู้ให้เสมอมา ส่วนข้อบกพร่องที่ท่านพบ ผู้เขียนขอน้อมรับในความผิดพลาดนั้นไว้

ผู้เขียนขอขอบคุณ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร ที่ให้ทุนสนับสนุนการเขียนตำราจากกองทุนส่งเสริมและพัฒนาคณะวิทยาศาสตร์ เพื่อส่งเสริมให้คณาจารย์เขียนตำราที่มีคุณภาพ ขอขอบพระคุณท่านผู้ทรงคุณวุฒิที่ให้คำเสนอแนะเพื่อการปรับปรุงวิธีเขียนและเนื้อหา ขอขอบคุณ คุณฐกร ธรรมประทีป ที่ได้ช่วยวาดรูปสวยๆ ในหนังสือเล่มนี้ ขอบคุณฝาแฝดพี่-น้อง นางสาวนริศราและนางสาวชาลินี เค้าฉิม นักศึกษาชั้นปีที่ 4 วิชาเอกคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร ที่ได้ลงทะเบียนเรียนรายวิชา 511 441 เป็นวิชาเลือกในปีการศึกษา 2556 และได้หมั่นเพียร ทั้งอ่านทำความเข้าใจและทำแบบฝึกหัด ทำให้ผู้เขียนพบความบกพร่องและผิดพลาดมากมายในการพิมพ์ครั้งแรก ผู้เขียนได้ปรับปรุงและเพิ่มเติมเนื้อหาให้ถูกต้องและมีความสมบูรณ์ สุดท้ายผู้เขียนขอขอบคุณสามีและลูกๆ ที่เป็นกำลังใจให้เสมอมา

ศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ

มิถุนายน 2556

สารบัญ

บทที่ 1
สาระของทฤษฎีกรุป

ในบทนี้ เราจะศึกษาและทบทวนเรื่องราวของทฤษฎีกรุปเบื้องต้นที่ได้เคยศึกษามาแล้วในวิชาพีชคณิตนามธรรม ระดับปริญญาตรี (สำหรับผู้สนใจรายละเอียดในระดับพื้นฐานสามารถศึกษาได้จาก [2]) โดยจะกล่าวในเชิงลึกของเนื้อหาเหล่านั้นซึ่งจะเป็นพื้นฐานของการศึกษาเรื่องกรุปขั้นกลางและขั้นสูงที่จะศึกษากันในบทต่อๆ ไป

1.1 กำเนิดกรุป

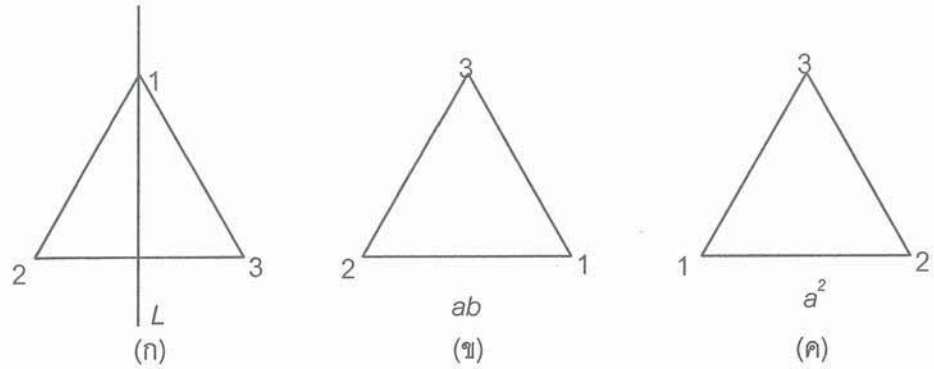
ในวิชาคณิตศาสตร์มีการใช้นัยแห่งการสมมาตรอย่างไม่ชัดแจ้งมาโดยตลอด ดังจะเห็นว่าเมื่อย้อนคิดกลับไปประมาณ 2500 ปี ต้นกำเนิดวิชาเรขาคณิตเป็นของชนชาติกรีกโบราณ กล่าวถึงเรื่องราวซึ่งมีพื้นฐานเป็นเรื่องการสมมาตรเกือบทั้งสิ้น แต่ชาวกรีกก็ไม่เคยศึกษาแก่นสารของการสมมาตรอย่างชัดแจ้งเลย หรือแม้แต่เรื่องราวของจำนวนที่เราศึกษากันอย่างต่อเนื่องมาแต่โบราณก็มีการสมมาตรเป็นพื้นฐานเช่นกัน กรุปเป็นเรื่องแรกและอาจกล่าวได้ว่าเป็นเรื่องเดียวที่ศึกษาเรื่องการสมมาตรอย่างชัดแจ้ง การศึกษาทฤษฎีกรุปเริ่มขึ้นเมื่อราวคริสต์ศักราช 1830 ซึ่งเป็นช่วงเวลาที่นักคณิตศาสตร์กำลังมุ่งศึกษาหาสูตรคำตอบของสมการพหุนาม โดยเป็นที่ทราบกันแล้วว่า สูตรคำตอบของพหุนามกำลังสอง ax^2+bx+c เมื่อ a,b และ c เป็นจำนวนจริง คือ

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

และแม้คำตอบของพหุนามกำลังสามและกำลังสี่จะยังไม่มีสูตรการหาที่แน่นอน แต่ขั้นตอนวิธีสำหรับการหาคำตอบก็ยังมีรูปแบบเดียวกัน จึงเกิดคำถามว่าจะมีกระบวนการหาคำตอบของพหุนามกำลังที่สูงกว่านี้หรือสำหรับทุกๆ พหุนามหรือไม่ ในกาลเวลาต่อมา กาลัวส์ (Galois) นักคณิตศาสตร์ชาวฝรั่งเศสก็ได้ตอบคำถามนี้อย่างสมบูรณ์ในที่สุด โดยอธิบายในเชิงของการสมมาตร ทำให้นักคณิตศาสตร์หันมาศึกษาทฤษฎีกรุปอย่างจริงจัง จนเป็นที่ประจักษ์ในปัจจุบันว่าทฤษฎีกรุปเป็นประโยชน์ต่อการประยุกต์ทางวิทยาศาสตร์มากมาย

วิธีดีที่สุดเพื่ออธิบายว่า นิยามเชิงนามธรรมของกรุปสัมพันธ์กับการสมมาตรอย่างไร ต้องอาศัยการอธิบายเชิงเรขาคณิต เริ่มต้นด้วยการพิจารณาสามเหลี่ยมด้านเท่ารูปหนึ่งในปริภูมิและจะหาวิธีเคลื่อนย้าย (นั่นคือการแปลง) สามเหลี่ยมด้านเท่ารูปนี้ทั้งหมด โดยหลังจากการเคลื่อนย้ายแล้วให้ได้รูปสามเหลี่ยมด้านเท่าในลักษณะที่เสมือนไม่ได้เคลื่อนย้าย และเพื่ออธิบายวิธีการเคลื่อนย้าย เรากำหนดหมายเลข 1, 2 และ 3 ให้กับแต่ละจุดยอดของสามเหลี่ยม และให้ L เป็น

เส้นตรงที่ลากผ่านจุดยอดที่มีหมายเลข 1 และตั้งฉากกับด้านที่ลากเชื่อมโยงจุดยอดที่มีหมายเลข 2 และ 3 ดังรูป 1.1.1 (ก) ให้ L ไม่เคลื่อนที่ แล้วพิจารณาการเคลื่อนย้าย 2 แบบต่อไปนี้



รูป 1.1.1

1. หมุนสามเหลี่ยมรอบเส้นตรงที่ตั้งฉากกับระนาบที่ประกอบโดยสามเหลี่ยมด้านเท่ารูปนี้ในทิศทางทวนเข็มนาฬิกาไป $\frac{2\pi}{3}$ เรเดียน และเราจะแทนการหมุนเช่นนี้ด้วยสัญลักษณ์ a

2. หมุนสามเหลี่ยมรอบเส้นตรง L ไป π เรเดียน และเราจะแทนการหมุนเช่นนี้ด้วยสัญลักษณ์ b

เราใช้สัญลักษณ์ xy แทนการเคลื่อนย้ายที่เกิดจากการหมุนแบบ y ตามด้วยการหมุนแบบ x เมื่อ $x, y \in \{a, b\}$ และ x^2 แทนการเคลื่อนย้ายที่เกิดจากการหมุนแบบ x ตามด้วยการหมุนแบบ x ดังเช่นในรูป 1.1.1 (ข) เป็นการเคลื่อนย้ายที่เกิดจากการหมุนแบบ b ตามด้วยการหมุนแบบ a และรูป 1.1.1 (ค) เป็นการเคลื่อนย้ายแบบ a^2 เป็นต้น โดยวิธีนี้เราจะได้การเคลื่อนย้ายทั้งหมด คือ $a, a^2, a^3, b, b^2, ab, a^2b = ba, a^3b$ ส่วนการการเคลื่อนย้ายใดเป็นรูปเดียวกับรูปตั้งต้น จะแทนด้วยสัญลักษณ์ e เช่นการเคลื่อนย้าย a^3 และ b^2 เป็นต้น ทำให้ได้การเคลื่อนย้ายที่ต่างกันทั้งหมด 6 แบบซึ่งคือวิธีเรียงสับเปลี่ยนทั้งหมดบนเซต $\{1, 2, 3\}$ นั่นเอง

เมื่อต้องการแปลความหมายของการสมมาตรในรูปสัจพจน์เชิงนามธรรม นั่นคือในรูปที่ไม่ขึ้นกับการอธิบายด้วยตัวอย่าง เราหันกลับมาพิจารณาการสมมาตรของสามเหลี่ยมด้านเท่าดังข้างต้น เรามีการเคลื่อนย้าย 6 แบบคือ e, a, a^2, b, ab, a^2b และเราสามารถกระทำการประกอบกันระหว่างการเคลื่อนย้ายทั้ง 6 แบบซึ่งจะเรียกว่า "การคูณ" ตัวอย่างเช่นการเคลื่อนย้าย a^2b ประกอบกันกับการเคลื่อนย้าย ab (พิจารณาหมุนรูป 1.1.1) จะได้การเคลื่อนย้าย a^2 ในลักษณะเช่นนี้เรากล่าวว่า "ผลคูณของ a^2b และ ab คือ a^2" และแทนด้วยสัญลักษณ์ $(a^2b)(ab) = a^2$ เป็นต้น ดังนั้นในเชิงนามธรรมเราต้องมีเซต G กับ "การคูณ" บน G ซึ่งกำหนดสมาชิกตัวหนึ่งและเพียงตัวเดียวเท่านั้นสำหรับแต่ละคู่ x และ y ใน G นั่นคือการดำเนินการทวิภาคบน G และแทน

สมาชิกที่เป็นผลคูณของแต่ละคู่ x และ y ใน G ด้วยสัญลักษณ์ xy แต่เท่านี้ยังไม่เพียงพอ เรายังต้องการสัจพจน์ที่จะกำหนดการสมมาตรให้กับผลคูณนี้ด้วย จึงต้องพิจารณาพฤติกรรมของ "การคูณ" (นั่นคือการหมุนสามเหลี่ยมด้านเท่า) ข้างต้นต่อไป และพบว่า

1. $x(yz)$ หมายถึงการหมุน z ตามด้วยการหมุน y ผลที่ได้เป็นการหมุนที่ตามด้วยการหมุน x ซึ่งเราพบว่าเป็นการหมุนเดียวกับการหมุน $(xy)z$ นั่นคือกฎการเปลี่ยนหมู่ของการหมุนเป็นจริง

2. แม้ว่าเราสามารถเปรียบเทียบ การหมุนสามเหลี่ยมด้านเท่า กับ "การคูณ" ของจำนวนเต็มซึ่งกฎการเปลี่ยนหมู่เป็นจริงเช่นเดียวกันก็ตาม แต่ "การคูณ" ของจำนวนเต็มสอดคล้องกับกฎการสลับที่ นั่นคือ $xy = yx$ ทุกๆ จำนวนเต็ม x และ y ในขณะที่การหมุนสามเหลี่ยมด้านเท่าไม่เป็นไปตามกฎข้อนี้ เพราะ $ab \neq ba$

3. การสมมาตรของสามเหลี่ยมด้านเท่า มีการหมุน e ซึ่ง $ex = e = xe$ สำหรับทุกๆ การหมุน x

4. แต่ละการหมุน x มีการหมุน y ซึ่งกระทำต่อเนื่องกันไม่ว่าจะเริ่มด้วยการหมุนใดก่อนจะไม่เปลี่ยนแปลงสามเหลี่ยมด้านเท่าเริ่มต้นนั่นคือ $xy = yx = e$ และสังเกตว่าการหมุน y ดังกล่าวมีเพียงหนึ่งเดียวสำหรับแต่ละการหมุน x จึงแทนการหมุน y ของการหมุน x เช่นนี้ด้วยสัญลักษณ์ x^{-1} เพราะฉะนั้น $xx^{-1} = e = x^{-1}x$ สำหรับแต่ละการหมุน x

เมื่อรวบรวมพฤติกรรมเหล่านี้เข้าด้วยกันทั้งหมด เราสามารถเขียนสัจพจน์ที่กำหนดแนวความคิดของการสมมาตรได้ดังต่อไปนี้

1.1.1 **บทนิยาม** *กรุป (group)* ประกอบด้วยเซต G ที่ไม่ใช่เซตว่างและการดำเนินการทวิภาค (binary operation) บน G ซึ่งเรียกว่า "การคูณ" และเขียนแทนผลคูณของแต่ละ x และ y ใน G ด้วย "xy" สอดคล้องกับสัจพจน์ต่อไปนี้

1. กฎการเปลี่ยนหมู่ (associative law) นั่นคือ $x(yz) = (xy)z$ สำหรับทุกๆ $x, y, z \in G$
2. มีสมาชิก e ใน G ซึ่ง $ex = x = xe$ สำหรับทุกๆ $x \in G$

   [**หมายเหตุ** ขอให้พิสูจน์เป็นแบบฝึกหัดว่าสมาชิก e ของสัจพจน์นี้มีเพียงตัวเดียว ซึ่งเรียกว่า *เอกลักษณ์ (identity)* ของ G]
3. แต่ละ $x \in G$ มี $y \in G$ ซึ่ง $xy = yx = e$

   [**หมายเหตุ** ขอให้พิสูจน์เป็นแบบฝึกหัดว่าสมาชิก y ของสัจพจน์นี้มีเพียงตัวเดียว เราจึงใช้สัญลักษณ์แทนได้ ในที่นี้จะแทนด้วย x^{-1} และเรียกว่า *ตัวผกผัน (inverse)* ของ x ดังนั้น $xx^{-1} = e = x^{-1}x$]

เพื่อให้เห็นว่านิยามของกรุปเป็นมโนมติของการสมมาตร ผู้อ่านควรพิสูจน์ว่าสัจพจน์ของกรุปที่เขียนไว้ข้างต้นได้กำหนดไว้เกินความจำเป็น นั่นคือพิสูจน์แบบฝึกหัด 1.1 ข้อ 2 และข้อ 3

เราเรียกกรุป G ว่า *กรุปสลับที่ (commutative group)* หรือ *กรุปอาบีเลียน (abelian group)* ถ้า G สอดคล้องสัจพจน์ข้อที่ 4 ต่อไปนี้ด้วยคือ

4. กฎการสลับที่ (commutative law) นั่นคือ $xy = yx$ สำหรับทุกๆ $x, y \in G$

แต่ถ้า G ไม่เป็นกรุปอาบีเลียน เราเรียก G ว่า *กรุปนอนอาบีเลียน (non-abelian group)* หรือ *กรุปไม่สลับที่ (non-commutative group)*

ถ้าเซต G ประกอบด้วยสมาชิกจำนวนจำกัด เราเรียก G ว่า *กรุปจำกัด (finite group)* แต่ถ้า G ไม่ใช่กรุปจำกัด จะเรียก G ว่า *กรุปอนันต์ (infinite group)* และเรียกขนาด (cardinality) ของเซต G ว่า *อันดับ (order)* ของกรุป G และแทนด้วยสัญลักษณ์ $|G|$

1.1.2 **บทนิยาม** เรียกเซต G ที่ไม่ใช่เซตว่าง กับการดำเนินการทวิภาคที่สอดคล้องกับกฎการเปลี่ยนหมู่ว่า *กึ่งกรุป (semigroup)*

เราเรียกกึ่งกรุป G ว่า *โมนอยด์ (monoid)* ถ้ามีสมาชิกใน G ที่เป็นเอกลักษณ์ [ขอให้สังเกตว่ากรุปก็คือโมนอยด์ซึ่งแต่ละสมาชิกมีตัวผกผันนั่นเอง]

1.1.3 **ทฤษฎีบท** ให้ G เป็นกรุป

1. ถ้า $c \in G$ และ $cc = c$ แล้ว $c = e$
2. *กฎการตัดออกทางซ้ายและทางขวา (left- and right- cancellation law)* เป็นจริง นั่นคือถ้า $ab = ac$ หรือ $ab = ac$ (ตามลำดับ) แล้ว $b = c$ สำหรับทุกๆ $a, b, c \in G$
3. $(a^{-1})^{-1} = a$ สำหรับทุกๆ $a \in G$
4. $(ab)^{-1} = b^{-1}a^{-1}$ สำหรับทุกๆ $a, b \in G$
5. ถ้า $a, b \in G$ แล้วสมการ $ax = b$ และ $ya = b$ ต่างมีเพียงคำตอบเดียวใน G คือ $x = a^{-1}b$ และ $y = ba^{-1}$ ตามลำดับ

บทพิสูจน์ การพิสูจน์ข้อ 1 ให้ $c \in G$ ซึ่ง $cc = c$ แล้ว $c = ec = (c^{-1}c)c = c^{-1}(cc) = c^{-1}c = e$ การพิสูจน์ข้อ 2 และข้อ 5 ทำได้ในทำนองเดียวกับข้อ 1 และการพิสูจน์ข้อ 3 และข้อ 4 ทำได้ในทำนองเดียวกัน จึงจะพิสูจน์เฉพาะข้อ 4 โดยให้ $a, b \in G$ แล้ว $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = (ae)a^{-1} = aa^{-1} = e$ ซึ่งแสดงว่า $b^{-1}a^{-1}$ เป็นตัวผกผันของ ab แต่ตัวผกผันของแต่ละสมาชิกของกรุปมีเพียงหนึ่งเดียว ทำให้ได้ $(ab)^{-1} = b^{-1}a^{-1}$ ❑

ความสำคัญประการหนึ่งของกฎการเปลี่ยนหมู่ในกึ่งกรุป G คือทำให้สามารถ "ละ" หรือ "ใส่" วงเล็บในอันดับใดก็ได้สำหรับการคูณสมาชิก n ตัวใดๆ ของ G ดังจะแสดงการพิสูจน์ให้เห็นจริงในทฤษฎีบทต่อไป

1.1.4 ทฤษฎีบทวางนัยทั่วไปของกฎการเปลี่ยนหมู่ (Generalization of the associative law)

ให้ G เป็นเซตที่ไม่ใช่เซตว่างและการดำเนินการทวิภาคที่กำหนดบน G สอดคล้องกฎการเปลี่ยนหมู่ ถ้า $x_1, x_2, ..., x_n \in G$ เมื่อ n เป็นจำนวนเต็มบวก แล้วการเปลี่ยนหมู่ในอันดับ $x_1, x_2, ..., x_n$ จะเป็นเช่นใดก็ตาม ผลคูณของสมาชิก n ตัวนี้ในอันดับ $x_1, x_2, ..., x_n$ เป็นสมาชิกตัวเดียวกันใน G

บทพิสูจน์ จากกฎการเปลี่ยนหมู่ จะได้ว่าทฤษฎีบทเป็นจริงเมื่อ $n = 3$ จึงสมมติให้ทฤษฎีบทเป็นจริงสำหรับผลคูณของสมาชิกที่มีจำนวนน้อยกว่า n และให้ผลคูณของสมาชิก n ตัวในอันดับ $x_1, x_2, ..., x_n$ สามารถคำนวณได้จากผลคูณของสองวงเล็บในสองแบบใดๆ คือ

$$(x_1x_2...x_r)\,(x_{r+1}x_{r+2}...x_n) \quad \text{และ} \quad (x_1x_2...x_s)\,(x_{s+1}x_{s+2}...x_n)$$

โดยที่ $r \le s$ แล้วสังเกตว่าผลคูณในแต่ละวงเล็บเป็นผลคูณของสมาชิกที่มีจำนวนน้อยกว่า n ตัว ดังนั้นตามสมมติฐาน เราสามารถเขียนวงเล็บลงระหว่างหมู่สมาชิกในแต่ละวงเล็บในตำแหน่งใดก็ได้ และถ้า $r = s$ แล้วผลคูณของสองวงเล็บในทั้งสองแบบข้างต้นจะเป็นแบบเดียวกัน เราจึงพิจารณาเมื่อ $r < s$ และเพราะว่า $s < n$ เราจะได้เอกลักษณ์ต่อไปนี้

$$\begin{aligned}(x_1x_2...x_s)(x_{s+1}x_{s+2}...x_n) &= ((x_1x_2...x_r)(x_{r+1}x_{r+2}...x_s))(x_{s+1}x_{s+2}...x_n)\\ &= (x_1x_2...x_r)((x_{r+1}x_{r+2}...x_s)(x_{s+1}x_{s+2}...x_n)) \quad \text{(กฎการเปลี่ยนหมู่ของสมาชิก 3 ตัว)}\\ &= (x_1x_2...x_r)(x_{r+1}x_{r+2}...x_n)\end{aligned}$$

เพราะฉะนั้นการวางนัยทั่วไปของกฎการเปลี่ยนหมู่เป็นจริงสำหรับผลคูณของสมาชิก n ตัวเมื่อการวางนัยทั่วไปของกฎการเปลี่ยนหมู่เป็นจริงสำหรับผลคูณของสมาชิกที่มีน้อยกว่า n ตัว ดังนั้นโดยอุปนัยเชิงคณิตศาสตร์ จะได้ว่าทฤษฎีบทวางนัยทั่วไปของกฎการเปลี่ยนหมู่เป็นจริงสำหรับผลคูณของสมาชิก n ตัวใดๆ ซึ่งเป็นอันจบการพิสูจน์ ❑

1.1.5 หมายเหตุ ให้ G เป็นกรุปและ $x \in G$

1. จะแทนผลคูณ $xx\cdots x$ (n ครั้ง) ด้วยสัญลักษณ์ x^n และอ่านว่า "กำลัง n ของ x" หรือ "x ยกกำลัง n" ดังนั้น

$$x^1 = x,\ x^2 = xx,\ x^3 = (xx)x = xxx, ...,\ x^n = x^{n-1}x$$

และขอให้สังเกตว่า อาจมี $x^m = x^n$ แม้ว่า $m \neq n$ ตัวอย่างเช่น $i^2 = i^6 = -1$ ในเซตของจำนวนเชิงซ้อน เป็นต้น

2. ถ้า $n = 0$ นิยามให้ $x^0 = e$ และสำหรับ $n > 0$ กำหนดตัวผกผันของ x^n ด้วยสัญลักษณ์ x^{-n} และนิยาม $(x^n)^{-1} = (x^{-1})^n$ ดังนั้น $x^{-n} = (x^n)^{-1} = (x^{-1})^n$

3. ถ้าการดำเนินการบน G เขียนในรูป "การบวก +" จะกำหนดสัญลักษณ์ต่างๆ ให้สอดคล้องกับการบวกดังต่อไปนี้

"กำหนด 0 แทนเอกลักษณ์ e และ $-x$ แทนตัวผกผัน x^{-1}

ส่วน nx แทน x^n ซึ่งจะทำให้ได้ $0x = 0,\ 1x = x$ และ $nx = (n-1)x + x$"

1.1.6 **ทฤษฎีบท** ให้ G เป็นกรุป $a \in G$ และ m, n เป็นจำนวนเต็ม แล้ว

1. $a^m a^n = a^{m+n}$ [หรือในรูป "การบวก" $ma + na = (m+n)a$]
2. $(a^m)^n = a^{mn}$ [หรือในรูป "การบวก" $n(ma) = (nm)a$] ❑

เราเริ่มสืบสมุฏฐานกรุปด้วยการพิจารณาความสมมาตรของสามเหลี่ยมด้านเท่า ขณะนี้จึงมีเซตของจุดยอด 3 จุดกับการหมุนของสามเหลี่ยมด้านเท่าดังกล่าว เป็นตัวอย่างของกรุปเพียงตัวอย่างเดียวซึ่งเราเรียกกรุปนี้ว่า กรุปการสมมาตรของสามเหลี่ยมด้านเท่าและเขียนแทนด้วยสัญลักษณ์ D_3 ต่อไปนี้จะให้ตัวอย่างกรุปอื่นๆ ที่คุ้นเคยและสำคัญซึ่งจะเกี่ยวข้องกับการศึกษาเรื่องกรุปต่อไป

1.1.7 **ตัวอย่าง** เซตของจำนวนเต็มทั้งหมด $\mathbb{Z}$ เซตของจำนวนตรรกยะทั้งหมด $\mathbb{Q}$ และเซตของจำนวนจริงทั้งหมด $\mathbb{R}$ กับ "การบวก" ในความหมายปกติ ต่างเป็นกรุปอาบีเลียน ซึ่งเรียกว่า "กรุปการบวกของจำนวน" แต่ $\mathbb{Z}, \mathbb{Q}$ และ $\mathbb{R}$ ไม่เป็นกรุปภายใต้ "การคูณ" ในความหมายปกติ ทั้งนี้เพราะจำนวน 0 ไม่มีตัวผกผันภายใต้การคูณ ❍

1.1.8 **ตัวอย่าง** ให้ S เป็นเซตที่ไม่ใช่เซตว่างและ $A(S)$ แทนเซตของฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงทั้งหมดจาก S ไปทั่วถึง S แล้ว $A(S)$ กับ *ฟังก์ชันประกอบ (composition)* เป็นกรุป ทั้งนี้เพราะฟังก์ชันประกอบสอดคล้องกฎการเปลี่ยนหมู่ การประกอบกันของฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ฟังก์ชันเอกลักษณ์ (identity function) 1_S หรือ id_S เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง สุดท้ายแต่ละฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงมีฟังก์ชันผกผันเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ❍

เราเรียกแต่ละสมาชิกของ $A(S)$ ว่า *วิธีเรียงสับเปลี่ยน (pertmutations)* บน S และเรียก $A(S)$ ว่า *กรุปสมมาตร (symmetric group)* บน S และกรณีที่ S เป็นเซตจำกัดซึ่งประกอบด้วย

สมาชิก n ตัว เราเรียก $A(S)$ ว่า *กรุปสมมาตรบน n ตัวอักษร (symmetric group on n letters)* และแทนด้วยสัญลักษณ์ S_n ดังนั้น S_n เป็นกรุปจำกัดที่มีอันดับ $|S_n| = n!$ และมีความสำคัญในการศึกษาเรื่องกรุปจำกัดนอนอาบีเลียนซึ่งจะกล่าวรายละเอียดของกรุปเหล่านี้อีกครั้งในหัวข้อต่อไป

1.1.9 **ตัวอย่าง** เราจะแสดงการสร้างกรุปจากกรุปที่กำหนดและได้กรุปที่มีอันดับอย่างน้อยเท่ากับอันดับของกรุปที่กำหนด

ให้ G และ H เป็นกรุปที่มี e_G และ e_H เป็นเอกลักษณ์ตามลำดับและนิยามการดำเนินการทวิภาคบนผลคูณคาร์ทีเซียน $G \times H$ ดังนี้

$$(a,b)(x,y) = (ax,by) \quad \text{เมื่อ } a,x \in G \text{ และ } b,y \in H$$

[ขอให้สังเกตว่า มีการดำเนินการ 3 การดำเนินการของ G, H และ $G \times H$ อยู่ในประโยคเดียวกัน] แล้วเราพิสูจน์ได้ไม่ยากว่า $G \times H$ กับการดำเนินการที่นิยามดังข้างต้นเป็นกรุปที่มี (e_G, e_H) เป็นเอกลักษณ์และ (a^{-1}, b^{-1}) เป็นตัวผกผันของแต่ละ (a,b) ใน $G \times H$ นอกจากนี้ $G \times H$ เป็นกรุปที่มีอันดับเท่ากับผลคูณของอันดับของ G และของ H และถ้า G และ H เป็นกรุปอาบีเลียนแล้ว $G \times H$ เป็นกรุปอาบีเลียน ❍

เรียกการดำเนินการบน $G \times H$ ที่นิยามดังในตัวอย่าง 1.1.9 ว่า *การดำเนินการตามองค์ประกอบ (component wise)* และเรียกกรุป $G \times H$ ในตัวอย่าง 1.1.9 ภายใต้การดำเนินการตามองค์ประกอบว่า *ผลคูณตรง (direct product)* ของ G และ H สำหรับกรณีที่ใช้การดำเนินการเป็น "การบวก" จะแทน $G \times H$ ด้วย $G \oplus H$ และเรียกว่า *ผลบวกตรง (direct sum)*

1.1.10 **ทฤษฎีบท** ให้ $\sim$ เป็นความสัมพันธ์สมมูลบนกรุป G ซึ่งสอดคล้องข้อความ "สำหรับทุกๆ $a_i, b_i \in G$ เมื่อ $i \in \{1,2\}$ ถ้า $a_1 \sim a_2$ และ $b_1 \sim b_2$ แล้ว $a_1b_1 \sim a_2b_2$" และให้ $G/\sim$ แทนเซตของเซตสมมูล $\bar{x}$ (เมื่อ $x \in G$) ทั้งหมดของ G ภายใต้ $\sim$ แล้ว $G/\sim$ เป็นกรุปภายใต้การดำเนินการที่นิยามโดย $\bar{a}\bar{b} = \overline{ab}$ ทุกๆ $a,b \in G$

ยิ่งไปกว่านั้นถ้า G เป็นกรุปอาบีเลียนแล้ว $G/\sim$ เป็นกรุปอาบีเลียน

บทพิสูจน์ จะแสดงก่อนว่าการคูณระหว่างเซตสมมูลที่กำหนดตามสมมติฐานของทฤษฎีบทเป็นการกำหนดแจ่มชัด ด้วยการแสดงว่าการคูณเป็นอิสระจากการเลือกตัวแทนของเซตสมมูล โดยให้ $a_i, b_i \in G$ เมื่อ $i \in \{1,2\}$ ซึ่ง $\bar{a}_1 = \bar{a}_2$ และ $\bar{b}_1 = \bar{b}_2$ แล้ว $a_1 \sim a_2$ และ $b_1 \sim b_2$ และโดยสมมติฐานจะได้ $a_1b_1 \sim a_2b_2$ นั่นคือ $\overline{a_1b_1} = \overline{a_2b_2}$ ตามต้องการ

การคูณเป็นไปตามกฎการเปลี่ยนหมู่ เพราะ $\bar{a}(\bar{b}\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = (\overline{ab})\bar{c}$ $= (\bar{a}\bar{b})\bar{c}$ ทุกๆ $a,b,c \in G$ ส่วนเอกลักษณ์ของ $G/\sim$ คือเซตสมมูล $\bar{e}$ ที่มีเอกลักษณ์ e ของ G

เป็นสมาชิก เพราะ $\overline{ae} = \overline{a}\,\overline{e} = \overline{a}$ ทุกๆ $a \in G$ และสุดท้ายถ้า $\overline{a} \in G/_{\sim}$ แล้วเห็นได้ชัดว่า $\overline{a^{-1}}$ เป็นตัวผกผันของ $\overline{a}$

การพิสูจน์ทำนองเดียวกันจะได้ว่าถ้า G เป็นกรุปอาบีเลียนแล้ว $G/_{\sim}$ เป็นกรุปอาบีเลียน ❑

1.1.11 **ตัวอย่าง** ให้ m เป็นจำนวนเต็มบวกและนิยามความสัมพันธ์บนกรุปการบวก $\mathbb{Z}$ โดย

$$a \equiv b (\bmod m) \iff m \text{ เป็นตัวหารของ } a-b \iff m|(a-b)$$

สำหรับทุกๆ จำนวนเต็ม a และ b นั่นคือ *คอนกรูเอนซ์มอดูโล* m *(congruence modulo* m*)* ซึ่งเป็นที่รู้จักกันดีในทฤษฎีจำนวนและเห็นได้ชัดว่าคอนกรูเอนซ์มอดูโล m สอดคล้องสมมติฐานของทฤษฎีบท 1.1.10 ดังนั้นถ้า $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ แทนเซตของเซตสมมูลทั้งหมดแล้ว $\mathbb{Z}_m$ เป็นกรุปอาบีเลียนที่มี "การบวก" กำหนดดังนี้

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{เมื่อ } a \text{ และ } b \text{ เป็นจำนวนเต็ม}$$

ดังนั้นกรุปการบวก $\mathbb{Z}_m$ เป็นกรุปจำกัดอันดับ m และเพื่อความสะดวกในการศึกษาต่อไป จะเขียนแทนสมาชิกของกรุปนี้โดยไม่มีขีดกำกับข้างบน ในกรณีไม่ทำให้เกิดการสับสน ❍

1.1.12 **ตัวอย่าง** นิยามความสัมพันธ์ $\sim$ บนกรุปการบวก $\mathbb{Q}$ ดังนี้

$$a \sim b \iff a-b \text{ เป็นจำนวนเต็ม}$$

ทุกๆ $a, b \in \mathbb{Q}$ แล้วการพิสูจน์อย่างง่ายๆ แสดงว่า $\sim$ เป็นความสัมพันธ์สมมูลบน $\mathbb{Q}$ ที่สอดคล้องสมมติฐานของทฤษฎีบท 1.1.10 เราใช้สัญลักษณ์ $\mathbb{Q}/\mathbb{Z}$ แทนเซตของเซตสมมูลทั้งหมดของ $\mathbb{Q}$ ภายใต้ความสัมพันธ์ $\sim$ และขอให้สังเกตว่า $\mathbb{Q}/\mathbb{Z}$ เป็นเซตอนันต์ ดังนั้น $\mathbb{Q}/\mathbb{Z}$ เป็นกรุปอาบีเลียนอันดับอนันต์ซึ่งเรียกว่า *กรุปตรรกยะมอดูโลหนึ่ง (group of rationals modulo one)* ❍

ในการศึกษาโครงสร้างของกรุปต่อๆ ไป มักเกี่ยวข้องกับการคูณของสมาชิกในกรุปอยู่เสมอ ดังนั้นเพื่อความสะดวกและง่ายต่อการเข้าใจ โดยเฉพาะในการศึกษากรณีของกรุปจำกัด เรานิยมแสดงผลคูณในตารางที่เรียกว่า *ตารางการคูณ (multiplication table)* ซึ่งจะเขียนสมาชิกของกรุปเรียงลำดับโดยใช้สัญลักษณ์ $x_1, x_2, ..., x_n$ ให้เป็นแถวอยู่บนสุดและเป็นหลักอยู่ซ้ายสุดของตารางสี่เหลี่ยมจัตุรัสที่มีขนาดเท่ากับจำนวนสมาชิกของกรุป และให้ $x_i x_j$ แทนผลคูณของ x_i และ x_j ซึ่งเป็นสมาชิกตัวใดตัวหนึ่งใน $x_1, x_2, ..., x_n$ โดยจะเขียน $x_i x_j$ ลงในตาราง ณ ตำแหน่งที่ตัดกันของแถวที่มี x_i อยู่ซ้ายสุดและหลักที่มี x_j อยู่บนสุด นอกจากนี้เป็นที่สังเกตว่า เรานิยมให้เอกลักษณ์ของกรุปอยู่ซ้ายสุดของแถวบนสุดและอยู่บนสุดของหลักซ้ายสุด ดังนั้นในที่นี้ x_1 เป็นเอกลักษณ์

หลัก

			x_2	x_3	x_4	. . .
	x_1	x_1^2	x_1x_2	x_1x_3	x_1x_4	. . .
	x_2	x_2x_1	x_2^2	x_2x_3	x_2x_4	
แถว	x_3	x_3x_1	x_3x_2	x_3^2	x_3x_4	. . .
	x_4	x_4x_1	x_4x_2	x_4x_3	x_4^2	
	.		. . .			. . .
	.					
	.					

แบบฝึกหัด 1.1

1. จงให้ตัวอย่างกึ่งกรุปและโมนอยด์ ที่ไม่ใช่กรุป
2. ให้ G เป็นกรุป (ดังที่นิยามไว้ในบทนิยาม 1.1.1) จงแสดงว่าเอกลักษณ์และตัวผกผันของแต่ละสมาชิกใน G มีเพียงตัวเดียว
3. ให้ G เป็นเซตที่ไม่ใช่เซตว่างและกำหนดการดำเนินการทวิภาคบน G ซึ่งจะเรียกว่า "การคูณ" โดยผลคูณของแต่ละคู่ $x, y \in G$ แทนด้วย xy และสอดคล้องกับสัจพจน์ต่อไปนี้

   (ก) กฎการเปลี่ยนหมู่ [นั่นคือ $x(yz) = (xy)z$ สำหรับทุกๆ $x, y, z \in G$]

   (ข) มีเอกลักษณ์ทางซ้าย [นั่นคือมี $e \in G$ ซึ่ง $ex = x$ สำหรับทุกๆ $x \in G$

   (ค) แต่ละ $x \in G$ มีสมาชิก $y \in G$ เป็นตัวผกผันทางซ้ายของ x [นั่นคือ $yx = e$]

   จงแสดงว่าเซต G กับการดำเนินการทวิภาคนี้เป็นกรุป
4. ให้เซต G ไม่ใช่เซตว่างและมีการดำเนินการทวิภาคบน G ซึ่งสอดคล้องสมบัติต่อไปนี้

   (ก) กฎการเปลี่ยนหมู่ [นั่นคือ $x(yz) = (xy)z$ สำหรับทุกๆ $x, y, z \in G$]

   (ข) สำหรับแต่ละ $a, b \in G$ มี $x, y \in G$ ซึ่งทำให้ $ax = b$ และ $ya = b$

   จงแสดงว่าเซต G กับการดำเนินการทวิภาคนี้เป็นกรุป

   [**ข้อสังเกต** กรุป G ตามบทนิยาม 1.1.1 สอดคล้องสัจพจน์ในแบบฝึกหัด 1.1 ข้อ 3 และ 4]
5. จงพิสูจน์ทฤษฎีบทวางนัยทั่วไปของกฎการสลับที่ซึ่งกล่าวว่า "ถ้า G เป็นกึ่งกรุปสลับที่และ $a_1, a_2, ..., a_n \in G$ และ $i_1, i_2, ..., i_n$ เป็นวิธีเรียงสับเปลี่ยน (permutation) ใดๆ ของ $1, 2, ..., n$ แล้ว $a_1a_2 \cdots a_n = a_{i_1}a_{i_2} \cdots a_{i_n}$

6. จงแสดงว่าแต่ละสมาชิกของกรุปจำกัดจะปรากฏครั้งหนึ่งและเพียงครั้งเดียว ในแต่ละแถวและแต่ละหลักของตารางการคูณ

7. จงเขียนตาราง "การบวก" ของกรุปผลบวกตรง $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ [กรุปนี้รู้จักกันดีในชื่อ *"กรุปไคลน์-4 (Klien-4 group)* เพราะเป็นกรุปที่แนะนำโดย Felix Klein (1849 – 1925)]

8. ให้ p เป็นจำนวนเฉพาะและ $\mathbb{Z}(p^\infty) := \left\{ \overline{\left(\frac{a}{b}\right)} \in \mathbb{Q}/\mathbb{Z} \middle| a,b \in \mathbb{Z}, b = p^i \right.$ สำหรับบาง $\left. i \geq 0 \right\}$ จงแสดงว่า $\mathbb{Z}(p^\infty)$ กับ "การบวก" ของกรุป $\mathbb{Q}/\mathbb{Z}$ ในตัวอย่าง 1.1.12 เป็นกรุป

9. ให้ G เป็นกรุปที่มีการดำเนินการ + และ S เป็นเซตที่ไม่ใช่เซตว่าง ให้ G^S แทนเซตของฟังก์ชันทั้งหมดจาก S ไปยัง G และนิยามการดำเนินการ + บน G^S สำหรับ $f,g \in G^S$ โดย $(f+g)(x) = f(x)+g(x)$ ทุกๆ $x \in S$ จงพิสูจน์ว่า G^S เป็นกรุป และเป็นกรุปอาบีเลียนถ้า G เป็นกรุปอาบีเลียน

10. ให้ G เป็นกรุป จงแสดงว่าข้อความต่อไปนี้สมมูลกัน

    (ก) G เป็นกรุปอาบีเลียน (ข) $(ab)^n = a^n b^n$ ทุกๆ $n \in \mathbb{Z}$ และ $a,b \in G$

    (ค) $(ab)^2 = a^2b^2$ ทุกๆ $a,b \in G$ (ง) $(ab)^{-1} = a^{-1}b^{-1}$ ทุกๆ $a,b \in G$

11. จงพิสูจน์ว่าถ้า G เป็นกรุปซึ่ง $a^2 = e$ ทุกๆ $a \in G$ แล้ว G เป็นกรุปอาบีเลียน

12. จงพิสูจน์ว่าถ้า G เป็นกรุปที่มีอันดับเป็นจำนวนคู่ แล้วจะมี $a \in G$ ซึ่ง $a \neq e$ และ $a^2 = e$

13. ให้ G เป็นกรุปและ $a,b \in G$ จงพิสูจน์ว่าถ้ามีจำนวนเต็มบวก r ซึ่ง $bab^{-1} = a^r$ แล้ว $b^j ab^{-j} = a^{r^j}$ ทุกๆ จำนวนเต็มบวก j

14. ให้ G เป็นเซตจำกัดที่ไม่ใช่เซตว่างและมีการดำเนินการบน G ซึ่งสอดคล้องกฎการเปลี่ยนหมู่และสำหรับ $a,b,c \in G$ ถ้า $ab = ac$ แล้ว $b = c$ และถ้า $ba = ca$ แล้ว $b = c$ จงพิสูจน์ว่า G เป็นกรุป และพิสูจน์ด้วยว่าบทสรุปอาจไม่เป็นจริงสำหรับ G ที่เป็นเซตอนันต์

15. จงพิสูจน์ว่าถ้า $a_1, a_2, \ldots$ เป็นลำดับของสมาชิกในกึ่งกรุป G แล้วมี $\psi : \mathbb{N} \to G$ เพียงหนึ่งเดียวซึ่ง $\psi(1) = a_1$, $\psi(2) = a_1a_2$, $\psi(3) = (a_1a_2)a_3$ และ $\psi(n+1) = (\psi(n))a_{n+1}$ สำหรับ $n \geq 1$

1.2 กรุปสมมาตรและกรุปการสมมาตร

ในหัวข้อนี้ เราแนะนำตัวอย่างหมู่ของกรุปที่มีความสำคัญต่อการศึกษาเรื่องการสมสัณฐานของกรุปจำกัด นอกจากนี้ยังเป็นตัวอย่างที่เป็นรูปธรรมของกรุปไม่สลับที่

ถ้า S เป็นเซตที่ไม่ใช่เซตว่าง ขอทบทวนว่า *วิธีเรียงสับเปลี่ยน (permutations)* บน S คือ ฟังก์ชันชนิดหนึ่งต่อหนึ่งจาก S ไปทั่วถึง S และถ้า S เป็นเซตจำกัดที่ประกอบด้วยสมาชิก n ตัว ซึ่งอาจแทนสมาชิก n ตัวของ S ด้วย $1,2,...,n$ แล้ววิธีเรียงสับเปลี่ยน $f:S\to S$ อาจกำหนด โดย $f(1)=x_1,\ f(2)=x_2,...,\ f(n)=x_n$ เมื่อ $\{x_1,...,x_n\}=\{1,...,n\}$ ที่เรียงสับเปลี่ยนอันดับแบบใดแบบหนึ่ง เราจึงอาจแทน f ด้วยสัญลักษณ์ดังนี้

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix}$$

โดยมีความหมายว่า $f(i)=x_i$ อยู่ในตำแหน่งใต้ i อย่างไรก็ตามในความเป็นจริงจำนวนที่เขียนเรียงในแถวบนก็อาจอยู่ในอันดับใดก็ได้เช่นกัน เราจึงอาจแทน f ด้วยสัญลักษณ์อีกแบบหนึ่งดังนี้

$$\begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ f(b_1) & f(b_2) & f(b_3) & \cdots & f(b_n) \end{pmatrix}$$

ตัวอย่างเช่น $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ และ $\begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ เมื่อ $n=3$ เป็นวิธีเรียงสับเปลี่ยนเดียวกันกับการส่ง $f:\begin{matrix} 2\to 3 \\ 3\to 1 \end{matrix}$ ซึ่งก็คือการส่ง $f(1)=2,\ f(2)=3$ และ $f(3)=1$ เป็นต้น

ตัวอย่างข้างต้นยังเป็นกรณีเฉพาะของวิธีเรียงสับเปลี่ยนที่เรียกว่าวัฏจักร เพราะโดยทั่วไป *วัฏจักร (cycles)* คือวิธีเรียงสับเปลี่ยนที่เขียนได้ในรูป

$$\begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_r \\ b_2 & b_3 & b_4 & \cdots & b_1 \end{pmatrix} \text{ หรือเขียนอย่างสั้นๆ เป็น } \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_r \end{pmatrix}$$

โดยที่ r เป็น *ความยาว (length)* ของวัฏจักร และจะเรียกวัฏจักรว่า *ทรานโพสิชัน (transposition)* ถ้า $r=2$ และสองวัฏจักรใดๆ จะกล่าวว่าเป็น *วัฏจักรต่างสมาชิก (disjoint cycle)* ถ้าเซตของสมาชิกในวัฏจักรทั้งสองเป็นเซตต่างสมาชิก

ตัวอย่างเช่น $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ คือวัฏจักร $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ ที่มีความยาว 3 หรือ $\begin{pmatrix} 1 & 5 & 9 & 6 \\ 5 & 9 & 6 & 1 \end{pmatrix}$ คือวัฏจักร $\begin{pmatrix} 1 & 5 & 9 & 6 \end{pmatrix}$ บนเซต $S=\{1,2,3,4,5,6,7,8,9\}$ ที่มีความยาว 4 และ $(1\ 2)$ คือทรานโพสิชันบนเซตที่มีขนาดมากกว่าหรือเท่ากับ 2 ส่วนวัฏจักร $\begin{pmatrix} 1 & 5 & 9 & 6 \end{pmatrix}$ กับ $(2\ 3)$ เป็นวัฏจักรต่างสมาชิก เป็นต้น

ขอให้สังเกตว่าวัฏจักรความยาวหนึ่งซึ่งเขียนในรูป (m) จะหมายถึงวัฏจักรที่มีค่าของวัฏจักรที่ m คือ m นั่นคือไม่สับเปลี่ยนอันดับของ m เราจึงนิยมละทิ้งวัฏจักรเหล่านี้ในการเขียนผลคูณ

ของวัฏจักรและกล่าวว่า m *ถูกตรึง (left fixed)* โดยวัฏจักร หรือวัฏจักร*ตรึง(fixed)* m ตัวอย่างเช่น วัฏจักร $(1\ \ 5\ \ 9\ \ 6)$ ตรึง $2,3,4,7,8$ เป็นต้น

ถ้า S เป็นเซตที่ประกอบด้วยสมาชิก n ตัว แล้วจะมีวิธีเรียงสับเปลี่ยนบน S ทั้งหมด $n!$ ตัว และขอทบทวนว่าเราแทนเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบน S ด้วยสัญลักษณ์ S_n ส่วน "การคูณ" บน S_n คือ "ฟังก์ชันประกอบ" ซึ่งกำหนดผลคูณ $fg : S \to S$ สำหรับแต่ละคู่วิธีเรียงสับเปลี่ยน $f, g : S \to S$ โดย $(fg)(i) = f(g(i))$ ทุกๆ $i \in \{1,2,...,n\}$ ตัวอย่างเช่นถ้า $S = \{1,2,3\}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)(3) = (1\ 2)$ และ $g = (1\ 3)$ แล้ว

$$fg(1) = f(g(1)) = f(3) = 3,\ fg(2) = f(g(2)) = f(2) = 1,\ fg(3) = f(g(3)) = f(1) = 2$$

ดังนั้น $fg = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ เป็นต้น

เราจะพิสูจน์ว่า S_n เป็นกรุป (ที่มีอันดับ $n!$) *อย่างแรก* : "การคูณ" เป็นการดำเนินการทวิภาคบน S_n เพราะ "การคูณ" คือฟังก์ชัน $S_n \times S_n \to S_n$ ที่กำหนด $(f,g) \to fg$ สำหรับแต่ละคู่วิธีเรียงสับเปลี่ยน f และ g ได้เป็นวิธีเรียงสับเปลี่ยน fg เพียงหนึ่งเดียว *อย่างที่สอง* : เห็นได้ชัดว่าวิธีเรียงสับเปลี่ยนเอกลักษณ์ $1_S = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$ เป็นเอกลักษณ์ e ตามสัจพจน์ของกรุป เพราะสำหรับวิธีเรียงสับเปลี่ยน $\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix}$ ใดๆ ใน S_n จะได้ว่า

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix}$$

และ

$$\begin{aligned} &\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix} \end{aligned}$$

สุดท้าย*อย่างที่สาม* : สำหรับ $f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix}$ ใน S_n จะสร้างวิธีเรียงสับเปลี่ยน g ใน S_n ที่ทำให้ $fg = 1_S = gf$ โดยให้ $g = \begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$ ซึ่งทำให้ได้

$$fg=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ x_1 & x_2 & x_3 & \dots & x_n\end{pmatrix}\begin{pmatrix}x_1 & x_2 & x_3 & \dots & x_n\\ 1 & 2 & 3 & \dots & n\end{pmatrix}=\begin{pmatrix}x_1 & x_2 & x_3 & \dots & x_n\\ x_1 & x_2 & x_3 & \dots & x_n\end{pmatrix}=1_S$$

และ

$$gf=\begin{pmatrix}x_1 & x_2 & x_3 & \dots & x_n\\ 1 & 2 & 3 & \dots & n\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & \dots & n\\ x_1 & x_2 & x_3 & \dots & x_n\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ 1 & 2 & 3 & \dots & n\end{pmatrix}=1_S$$

ดังนั้น g เป็นตัวผกผันของ f ทำให้เขียนได้ว่า $g=f^{-1}=\begin{pmatrix}x_1 & x_2 & x_3 & \dots & x_n\\ 1 & 2 & 3 & \dots & n\end{pmatrix}$

เนื่องจาก S_n กับการคูณสอดคล้องกับสัจพจน์ของกรุปตามบทนิยาม 1.1.1 จึงได้ S_n เป็นกรุปอันดับ $n!$ แต่ S_n ไม่เป็นกรุปอาบีเลียนเมื่อ $n\geq 3$ เพราะว่า (1 3) และ (1 2 3) เป็นสมาชิกของ S_n ทุกๆ $n\geq 3$ ซึ่งมีผลคูณ $(1\ 3)(1\ 2\ 3)=(1\ 2)\neq(2\ 3)=(1\ 2\ 3)(1\ 3)$

เราเรียกกรุป S_n ว่า *กรุปสมมาตร (symmetric group)* บนเซตที่มีสมาชิก n ตัวและในกรณีเฉพาะเมื่อ $n=3$ กรุปสมมาตร S_3 ซึ่งมีอันดับ $3!=6$ เป็นกรุปนอนอาบีเลียนที่เล็กสุด จึงมักเป็นตัวอย่างสำหรับมโนมติเกี่ยวกับกรุปนอนอาบีเลียนที่จะศึกษากันต่อไป จึงขอเขียนตารางการคูณสำหรับ S_3 ไว้ดังนี้

	(1)	(1 2 3)	(1 3 2)	(1 2)	(1 3)	(2 3)
(1)	(1)	(1 2 3)	(1 3 2)	(1 2)	(1 3)	(2 3)
(1 2 3)	(1 2 3)	(1 3 2)	(1)	(1 3)	(2 3)	(1 2)
(1 3 2)	(1 3 2)	(1)	(1 2 3)	(2 3)	(1 2)	(1 3)
(1 2)	(1 2)	(2 3)	(1 3)	(1)	(1 3 2)	(1 2 3)
(1 3)	(1 3)	(1 2)	(2 3)	(1 2 3)	(1)	(1 3 2)
(2 3)	(2 3)	(1 3)	(1 2)	(1 3 2)	(1 2 3)	(1)

ผู้อ่านควรได้ทบทวนเรื่องราวของกรุปสมมาตร S_n บนเซตที่มีสมาชิก n ตัวซึ่งได้ศึกษามาแล้วในระดับปริญญาตรีอย่างละเอียด (อาจศึกษาใน [2]) ทฤษฎีบทต่อไปและบทแทรกของทฤษฎีบท ได้เขียนรวบรวมสาระดังกล่าวเพื่อสะดวกต่อการอ้างถึงต่อไป สำหรับการพิสูจน์ขอละไว้เป็นแบบฝึกหัดหรือหาอ่านได้ใน [2]

1.2.1 **ทฤษฎีบท** แต่ละวิธีเรียงสับเปลี่ยนใน S_n จะเป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์ หรือวัฏจักร หรือเป็นผลคูณของวัฏจักรต่างสมาชิกที่มีความยาวไม่น้อยกว่า 2 ❑

1.2.2 **บทแทรก** อันดับของวิธีเรียงสับเปลี่ยนเท่ากับตัวคูณร่วมน้อยของอันดับของวัฏจักรต่างสมาชิกในผลคูณที่เท่ากับวิธีเรียงสับเปลี่ยนนั้น ❑

1.2.3 **บทแทรก** แต่ละวิธีเรียงสับเปลี่ยนใน S_n เขียนได้ในรูปผลคูณของทรานโพสิชัน และไม่ว่าจะเขียนวิธีเรียงสับเปลี่ยนในรูปผลคูณของทรานโพสิชันด้วยวิธีใด จำนวนของทรานโพสิชันในผลคูณมีภาวะ (parity) เดียวกันเสมอ ❑

เรากล่าวว่า $\alpha \in S_n$ เป็น *วิธีเรียงสับเปลี่ยนคู่ (even permutation)* ถ้าจำนวนของทรานโพสิชันในผลคูณของ α มีภาวะคู่ นั่นคือเป็นจำนวนคู่เสมอ และ α เป็น *วิธีเรียงสับเปลี่ยนคี่ (odd permutation)* ถ้าจำนวนของทรานโพสิชันในผลคูณของ α มีภาวะคี่

1.2.4 **ทฤษฎีบท** ถ้า n เป็นจำนวนเต็มบวกและ $\alpha \in S_n$ แล้ว α จะเป็นวิธีเรียงสับเปลี่ยนคู่หรือวิธีเรียงสับเปลี่ยนคี่ อย่างใดอย่างหนึ่งเท่านั้น ❑

1.2.5 **ทฤษฎีบท** สำหรับแต่ละจำนวนเต็มบวก n ให้ A_n แทนเซตของวิธีเรียงสับเปลี่ยนคู่ทั้งหมดใน S_n แล้ว A_n เป็นกรุปที่มีอันดับเท่ากับ $\frac{|S_n|}{2} = \frac{n!}{2}$ ซึ่งเรียกว่า *กรุปสลับ(alternating group)*] ❑

ให้ S เป็นเซตที่ไม่ใช่เซตว่างและให้ $M(S)$ แทนเซตของฟังก์ชันทั้งหมดจาก S ไปยัง S แล้ว $A(S)$ ในตัวอย่าง 1.1.7 คือเซตของสมาชิกใน $M(S)$ ที่มีตัวผกผันนั่นเอง ดังนั้นด้วยการพิจารณาเช่นเดียวกับกรณีเมื่อ S เป็นเซตจำกัดดังข้างต้น เราจะได้ผลสำหรับกรณีทั่วไปเช่นกันว่า $A(S)$ เป็นกรุปภายใต้การคูณ "ฟังก์ชันประกอบ" เราจึงเรียก $A(S)$ ว่ากรุปสมมาตรเช่นกัน

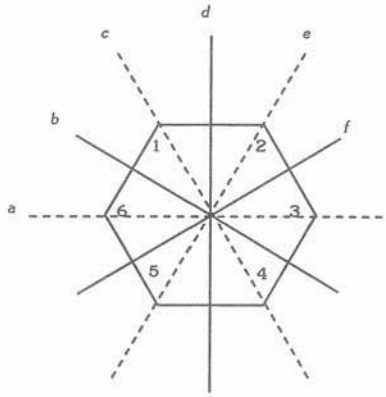
สังเกตว่าสำหรับแต่ละคู่จำนวนจริง a และ b โดยที่ $a \neq 0$ ฟังก์ชัน $\alpha_{a,b} : \mathbb{R} \to \mathbb{R}$ ซึ่งนิยามโดย $\alpha_{a,b}(x) = ax + b$ ทุกๆ $x \in \mathbb{R}$ แล้ว $\{\alpha_{a,b} | a,b \in \mathbb{R}\}$ เป็นเซตย่อยแท้ของ $A(\mathbb{R})$ เพราะทราบกันดีว่าฟังก์ชันเชิงกำลังเป็นสมาชิกของ $A(\mathbb{R})$ แต่ไม่เป็นสมาชิกของ $\{\alpha_{a,b} | a,b \in \mathbb{R}\}$ นอกจากนี้การเกริ่นเรื่องกำเนิดกรุปในตอนต้นหัวข้อ 1.1 ได้กล่าวถึงกรุปซึ่งยืนยงการเคลื่อนย้ายในระนาบของรูปสามเหลี่ยมด้านเท่า ทำให้เห็นว่ากรุปดังกล่าวคือกรุปสมมาตร S_3 แต่สำหรับกรุปการยืนยงรูปเหลี่ยมด้านเท่าและมุมเท่าอื่นๆ จะไม่ใช่ S_n แต่เป็นกรุปที่มีเอกภพเป็นเพียงเซตย่อยของ S_n เท่านั้น เราเรียกกรุปที่มีเอกภพเป็นเซตย่อยของกรุปสมมาตร (ภายใต้ "ฟังก์ชันประกอบ" ว่า *กรุปของวิธีเรียงสับเปลี่ยน (group of permutations)* หรือ *กรุปการสมมาตร (group of symmetries)*

สำหรับแต่ละจำนวนเต็ม $n \geq 3$ จะใช้สัญลักษณ์ D_n แทนกรุปการสมมาตรของรูป n เหลี่ยมปรกติ (regular polygon) นั่นคือรูป n เหลี่ยมด้านเท่าและมุมเท่าและเรียกกรุปการสมมาตรของรูป n เหลี่ยมปรกติว่า *กรุปไดฮิดรัล (dihedral group)* ตัวอย่างเช่น $D_3 = S_3$ คือกรุปไดฮิดรัล

ของสามเหลี่ยมด้านเท่า ส่วน D_4 คือกรุปไดฮิดรัลของสี่เหลี่ยมจัตุรัสและ D_5 คือกรุปไดฮิดรัลของห้าเหลี่ยมด้านเท่าและมุมเท่า และอื่นๆ นอกจากนี้สังเกตว่าอันดับของกรุปไดฮิดรัล D_n เท่ากับ $2n$ ทุกๆ จำนวนเต็ม $n \geq 3$

แบบฝึกหัด 1.2

1. แต่ละจำนวนเต็ม n ให้ $f_n : \mathbb{R} \to \mathbb{R}$ นิยามโดย $f_n(x) = x + n$ ทุกๆ $x \in \mathbb{R}$ จงแสดงว่า f_n เป็นวิธีเรียงสับเปลี่ยนบน $\mathbb{R}$ ทุกๆ จำนวนเต็ม n
2. ให้ n และ r เป็นจำนวนเต็มบวกซึ่ง $r \leq n$ จงพิสูจน์ว่า
   2.1 $|(a_1\ a_2 \cdots a_r)| = r$ สำหรับวัฏจักร $(a_1\ a_2 \cdots a_r)$ ความยาว r ในกรุปสมมาตร S_n
   2.2 ถ้า $\alpha \in S_n$ เขียนได้ในรูปผลคูณของวัฏจักรต่างสมาชิกเป็น $\alpha = \alpha_1\alpha_2 \cdots \alpha_r$ แล้ว $|\alpha|$ เท่ากับตัวคูณร่วมน้อยของ $|\alpha_1|, |\alpha_2|, \ldots, |\alpha_r|$
3. จงพิสูจน์ว่า "ไม่ว่าจะเขียนวิธีเรียงสับเปลี่ยนเอกลักษณ์ในรูปผลคูณของทรานโพสิชันด้วยวิธีใด จำนวนของทรานโพสิชันในผลคูณเป็นจำนวนคู่เสมอ"
4. จงหากรุปการสมมาตรของสามเหลี่ยมด้านเท่า พร้อมทั้งแสดงว่ากรุปการสมมาตรของสามเหลี่ยมด้านเท่าคือกรุปสมมาตร S_3
5. จงเปรียบเทียบกรุปการสมมาตรของสามเหลี่ยมหน้าจั่วและสามเหลี่ยมด้านเท่า
6. จงหากรุปการสมมาตรของรูปหกเหลี่ยมด้านเท่า มุมเท่า ดังรูป พร้อมทั้งเขียนตารางการคูณ



7. แต่ละจำนวนเต็ม $n \geq 3$ จงแสดงการหาสมาชิกทั้งหมดของกรุปไดฮิดรัล D_n พร้อมพิสูจน์ว่าอันดับของกรุปไดฮิดรัล D_n เท่ากับ $2n$
8. จงพิสูจน์ว่าข้อความในแต่ละข้อต่อไปนี้เป็นจริงใน A_n
   8.1 A_n มีสมบัติปิดภายใต้การคูณและ $1_S \in A_n$
   8.2 ถ้า $\alpha \in A_n$ และ $\beta \in S_n$ แล้ว $\alpha^{-1} \in A_n$ และ $\beta\alpha\beta^{-1} \in A_n$
   8.3 ถ้า $\alpha, \beta \in S_n$ แล้ว α และ $\beta\alpha\beta^{-1}$ เป็นวิธีเรียงสับเปลี่ยนคู่หรือคี่เหมือนๆ กัน

1.3 กรุปย่อย ตัวก่อกำเนิด อันดับของสมาชิกและอันดับของกรุปย่อย

เรากล่าวไว้ในหัวข้อ 1.2 ว่ากรุปสลับ A_n เป็นกรุปทุกๆ $n \geq 2$ สังเกตว่านอกจาก $A_n \subseteq S_n$ แล้ว "การคูณ" ของ A_n ก็คือ "การคูณ" ของ S_n ยิ่งไปกว่านั้นกรุปของจำนวนเต็ม กรุปของจำนวนตรรกยะ และกรุปของจำนวนจริง เหล่านี้ก็มีความสัมพันธ์เช่นดังกล่าวซึ่งเราจะเรียกความสัมพันธ์ในลักษณะเช่นนี้ว่า "กรุปย่อย" และในหัวข้อนี้เราจะให้บทนิยามของ "กรุปย่อย" สำหรับกรุปทั่วไปและศึกษาการก่อกำเนิดของกรุปย่อย ตลอดจนพิสูจน์ทฤษฎีบทของลากรองจ์ซึ่งกล่าวถึงความสัมพันธ์ของอันดับของกรุปกับอันดับของกรุปย่อยและอันดับของสมาชิกในกรุป

1.3.1 **บทนิยาม** ให้ G เป็นกรุปและ $H \subseteq G$ เรากล่าวว่า H เป็น *กรุปย่อย (subgroup)* ของ G ถ้า H เป็นกรุปภายใต้การดำเนินการของกรุป G ซึ่งกำกัด (restrict) ลงบน H

ทฤษฎีบท 1.3.2 ต่อไปนี้ ได้รวบรวมเกณฑ์การตรวจสอบกรุปย่อยซึ่งได้ศึกษามาแล้วในวิชาพีชคณิตนามธรรมในระดับปริญญาตรี จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

1.3.2 **ทฤษฎีบท** ให้ G เป็นกรุป

1. เซตย่อย S ของ G เป็นกรุปย่อยของ G ก็ต่อเมื่อ เงื่อนไขทั้งสามข้อต่อไปนี้เป็นจริง
   (ก) ถ้า $a,b \in S$ แล้ว $ab \in S$
   (ข) $e \in S$ เมื่อ e แทนเอกลักษณ์ของ G (และเป็นเอกลักษณ์ของ S)
   และ (ค) ถ้า $a \in S$ แล้ว $a^{-1} \in S$ เมื่อ a^{-1} แทนตัวผกผันของ a ใน G
2. เซตย่อย S ที่ไม่ใช่เซตว่างของ G เป็นกรุปย่อยของ G ก็ต่อเมื่อ $ab^{-1} \in S$ สำหรับทุกๆ คู่ $a,b \in S$
3. ถ้า G เป็นกรุปจำกัด แล้วเซตย่อยที่ไม่ใช่เซตว่าง S ของ G เป็นกรุปย่อยของ G ก็ต่อเมื่อ $ab \in S$ เมื่อใดก็ตามที่ $a,b \in S$ ❐

1.3.3 **ทฤษฎีบท** ให้ $\Delta \neq \phi$ เป็นเซตดรรชนี (index set) ถ้า $\{H_i \mid i \in \Delta\}$ เป็นเซตของกรุปย่อยของกรุป G แล้ว $\bigcap_{i \in \Delta} H_i$ เป็นกรุปย่อยของ G ❐

ให้ S เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G และ $\{H_i \mid i \in \Delta\}$ เป็นหมู่ของกรุปย่อยของ G ซึ่ง $S \subseteq H_i$ ทุกๆ $i \in \Delta$ โดยทฤษฎีบท 1.3.3 ได้ว่า $\bigcap_{i \in \Delta} H_i$ เป็นกรุปย่อยของ G โดยเฉพาะเราพิสูจน์ได้ไม่ยากว่า $\bigcap_{i \in \Delta} H_i$ เป็นกรุปย่อยเล็กสุดของ G ซึ่งมี S เป็นเซตย่อย จึงเรียกกรุปย่อย $\bigcap_{i \in \Delta} H_i$ ของ G ว่า *กรุปย่อยก่อกำเนิดโดย S (subgroup of G generated by S)* และเขียนแทนด้วยสัญลักษณ์ $< S >$

ถ้า S เป็นเซตจำกัด จะกล่าวว่า $<S>$ เป็นกรุปย่อย *ก่อกำเนิดแบบจำกัด (finitely generated)* และถ้า S ประกอบด้วยสมาชิกเพียงตัวเดียวนั่นคือมี $a \in G$ ซึ่ง $S = \{a\}$ จะเขียนแทน $<S>$ ด้วย $<a>$ และเรียกว่า *กรุปย่อยวัฏจักร (cyclic subgroup)* ก่อกำเนิดโดย a ยิ่งไปกว่านั้น ถ้า $G = <a>$ จะเรียก G ว่า *กรุปวัฏจักร (cyclic group)*

มีความสัมพันธ์ของสมาชิกในกรุปย่อยเหล่านี้กับสมาชิกใน S ดังกล่าวในทฤษฎีบทต่อไป

1.3.4 **ทฤษฎีบท** แต่ละสมาชิกในกรุปย่อย $<S>$ ของกรุป G เขียนได้ในรูปผลคูณ $a_1a_2\cdots a_n$ ของสมาชิก $a_i \in S$ หรือ $a_i^{-1} \in S$ ทุกๆ $i = 1,2,\ldots,n$ นั่นคือ

$$<S> = \{a_1a_2\cdots a_n \mid a_i \in S \text{ หรือ } a_i^{-1} \in S,\ i = 1,\ldots,n\}$$

บทพิสูจน์ ให้ $H = \{a_1a_2\cdots a_n \mid a_i \in S \text{ หรือ } a_i^{-1} \in S,\ i = 1,\ldots,n\}$ และให้ $x, y \in H$ แล้ว $x = a_1 a_2\cdots a_n$ และ $y = b_1b_2\cdots b_m$ โดยที่ $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in S$ หรือ $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}, b_1^{-1}, b_2^{-1}, \ldots, b_m^{-1} \in S$ แล้ว $xy^{-1} = a_1a_2\cdots a_nb_m^{-1}\cdots b_2^{-1}b_1^{-1} \in H$ ดังนั้น H เป็นกรุปย่อยของ G

ยิ่งไปกว่านั้น $S \subseteq H$ และเพราะ $<S>$ เป็นส่วนร่วมของทุกๆ กรุปย่อยที่มี S เป็นเซตย่อย จึงได้ $<S> \subseteq H$ แต่ $<S>$ เป็นกรุปย่อยที่มี S เป็นเซตย่อย (นั่นคือทุกๆ สมาชิกของ S เป็นสมาชิกของ $<S>$) ดังนั้น $<S>$ จะรวมสมาชิกในรูปผลคูณ $a_1a_2\cdots a_n$ โดยที่ $a_i \in S$ หรือ $a_i^{-1} \in S$ ทุกๆ $i = 1,2,\ldots,n$ นั่นคือ $H \subseteq <S>$ ดังนั้น $<S> = \{a_1a_2\cdots a_n \mid a_i \in S \text{ หรือ } a_i^{-1} \in S,\ i = 1,\ldots,n\}$ ❐

เราสังเกตว่า $<S>$ ในทฤษฎีบท 1.3.4 เขียนได้ในอีกรูปแบบหนึ่งดังนี้

$$<S> = \{a_1^{r_1}a_2^{r_2}\cdots a_n^{r_n} \mid a_i \in S, r_i \in \mathbb{Z}, i = 1,\ldots,n\}$$

และถ้า $S = \{a\}$ แล้ว $<a> = \{a^n \mid n \in \mathbb{Z}\}$ ซึ่งแสดงว่ากรุปวัฏจักรเป็นกรุปที่ประกอบด้วยสมาชิกที่เขียนได้ในรูปกำลังต่างๆ ของตัวก่อกำเนิด ในทฤษฎีบทต่อไปเราจะกล่าวสรุปธรรมชาติของกรุปย่อยของกรุปวัฏจักร (โดยละการพิสูจน์ไว้เป็นแบบฝึกหัด) ซึ่งผลดังกล่าวยังไม่สามารถกล่าวสรุปได้สำหรับกรุปทั่วไป

1.3.5 **ทฤษฎีบท**

1. ทุกๆ กรุปย่อยของกรุปวัฏจักรเป็นกรุปวัฏจักร
2. ถ้ากรุปวัฏจักร $<a>$ เป็นกรุปอันดับอนันต์ แล้ว $a^n = e$ ก็ต่อเมื่อ $n = 0$ ยิ่งไปกว่านั้น $a^m \neq a^n$ ทุกๆ จำนวนเต็ม $m \neq n$
3. ถ้ากรุปวัฏจักร $<a>$ เป็นกรุปอันดับจำกัด n แล้ว $<a>$ ประกอบด้วยสมาชิกที่ต่างกัน n ตัวได้แก่ $a, a^2, \ldots, a^n = e$

4. ถ้ากรุปวัฏจักร $<a>$ เป็นกรุปอันดับจำกัด n และ m เป็นตัวหารของ n แล้วจะมีกรุปย่อยอันดับ m ของ $<a>$ เพียงกรุปเดียวคือ $<a^{\frac{n}{m}}>$
5. ถ้า $<a>$ เป็นกรุปวัฏจักรอันดับจำกัด n แล้ว H เป็นกรุปย่อยของ $<a>$ ก็ต่อเมื่อมีจำนวนเต็มบวก m ซึ่งเป็นตัวหารของ n และ $H = <a^{\frac{n}{m}}>$ ❐

ตัวอย่างเช่นถ้า G เป็นกรุปวัฏจักรอันดับ 24 และให้ C_n แทนกรุปวัฏจักรอันดับ n แล้วเพราะตัวหาร (ที่เป็นจำนวนบวก) ทั้งหมดของ 24 คือ $1,2,3,4,6,8,12,24$ ดังนั้นโดยทฤษฎีบท 1.3.5 จะมีกรุปย่อยวัฏจักร C_m ของ G สำหรับแต่ละตัวหาร m ของ 24 และโดยกลับกัน ทำให้ได้ว่ากรุปย่อยทั้งหมดของ G ได้แก่ $C_1 = \{e\}, C_2, C_3, C_4, C_6, C_8, C_{12}$ และ $C_{24} = G$

สังเกตว่าในกรุปวัฏจักร G อันดับจำกัด n เราพิสูจน์ได้ไม่ยากว่าจะมีสมาชิก a ของ G ที่ทำให้ $e, a, a^2, \ldots, a^{n-1}$ เป็นสมาชิกที่ต่างกันทั้งหมดและนั่นคือสมาชิกทั้งหมดของ G ยิ่งไปกว่านั้น $a^n = e$ ทุกๆ $a \in G$ หรือในกรุป $D_3 = \{(1),(12),(13),(23),(123),(132)\}$ จะได้ $(123)(123) = (132)$ และ $(123)^3 = (123)(132) = (1)$ และโดยความเป็นจริงถ้า $x \in D_3$ แล้วมีจำนวนเต็มบวก r ซึ่ง $x^r = (1)$ และความจริงเช่นนี้ไม่ได้เกิดขึ้นเฉพาะกรุปวัฏจักรอันดับจำกัดหรือกรุปจำกัด D_3 เท่านั้น แต่เกิดขึ้นกับทุกๆ กรุปจำกัด โดยขอละการพิสูจน์ความจริงนี้ไว้เป็นแบบฝึกหัด

1.3.6 **บทนิยาม** ให้ G เป็นกรุปและ $x \in G$ เราเรียกจำนวนเต็มบวก r ตัวน้อยสุดซึ่ง $x^r = e$ ว่า *อันดับ (order)* ของ x แต่ถ้าไม่มีจำนวนเต็มบวกดังกล่าวสำหรับ x จะกล่าวว่า x มี *อันดับอนันต์ (infinite order)* และจะแทนอันดับของ x ด้วยสัญลักษณ์ $|x|$

สังเกตว่าอันดับของสมาชิกในกรุป ต่างจากอันดับของกรุป เพราะอันดับของกรุปคือขนาดของเอกภพของกรุป ตัวอย่างเช่นอันดับของกรุป D_3 คือ 6 แต่อันดับของ $(123) \in D_3$ คือ 3 เป็นต้น ยิ่งไปกว่านั้นถ้าพิจารณาอันดับของสมาชิกของกรุป D_3 ทุกๆ ตัว จะได้ข้อสังเกตว่าแต่ละสมาชิกของกรุปและตัวผกผันของสมาชิกนั้นมีอันดับเดียวกัน ทฤษฎีบทต่อไปได้รวบรวมสมบัติสำคัญเกี่ยวกับอันดับของสมาชิกของกรุป

1.3.7 **ทฤษฎีบท** ให้ G เป็นกรุป

1. $|a| = |a^{-1}|$ สำหรับทุกๆ $a \in G$
2. ให้ $a \in G$ และ m เป็นจำนวนเต็มบวกแล้ว $a^m = e$ ก็ต่อเมื่อ $|a|$ เป็นตัวหารของ m
3. $|a| = |xax^{-1}|$ สำหรับทุกๆ $a, x \in G$

4. ให้ m,n และ r เป็นจำนวนเต็มบวกและสัญลักษณ์ (m,n) แทนตัวหารร่วมมากของ m และ n และให้ $a \in G$ ซึ่ง $|a| = n$ และ $|a^r| = m$ ถ้า $(n,r) = d$ แล้ว $md = n$
5. ถ้า $a,b \in G$ ซึ่ง $(|a|,|b|) = 1$ และ $ab = ba$ แล้ว $|ab| = |a||b|$
6. ให้ $a \in G$ และ m และ n เป็นจำนวนเต็มบวกซึ่ง $|a| = mn$ ถ้า $(m,n) = 1$ แล้วมี c,d $c,d \in G$ เพียงคู่เดียวซึ่ง $|c| = m,\ |d| = n$ และ $a = cd$
7. ถ้า n เป็นจำนวนเต็มบวกซึ่ง $|a| = n$ แล้ว $a^r = a^s$ ก็ต่อเมื่อ $r \equiv s (\bmod n)$ ทุกๆจำนวนเต็ม r และ s

บทพิสูจน์ ขอละการพิสูจน์ 1 ไว้เป็นแบบฝึกหัด

2. ให้ $|a| = n$ แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม q และ r ซึ่ง $m = nq + r$ โดยที่ $0 \le r < n$ และเพราะ $a^m = e$ จะได้ $e = a^m = a^{nq+r} = (a^n)^q a^r = ea^r = a^r$ แต่ n เป็นจำนวนเต็มบวกน้อยสุดซึ่ง $a^n = e$ และ $0 \le r < n$ ดังนั้น $r = 0$ จึงได้ $m = nq$ นั่นคือ n เป็นตัวหารของ m ในทางกลับกันให้ $m = nq$ สำหรับบางจำนวนเต็ม q แล้ว $a^m = a^{nq} = (a^n)^q = e^q = e$

3. ให้ $a,x \in G$ และ $|a| = m$ และ $|xax^{-1}| = n$ แล้ว

$$(xax^{-1})^m = \underbrace{(xax^{-1})(xax^{-1})\cdots(xax^{-1})}_{(m\ times)} = xa^m x^{-1} = xex^{-1} = e$$

ทำให้ได้ $n \le m$ ในทำนองเดียวกัน ถ้าให้ $b = xax^{-1}$ แล้ว $a = x^{-1}bx$ ซึ่งทำให้ได้

$$a^n = (x^{-1}bx)^m = \underbrace{(x^{-1}bx)(x^{-1}bx)\cdots(x^{-1}bx)}_{(n\ times)} = x^{-1}a^m x = x^{-1}ex = e$$

และได้ $m \le n$ เพราะฉะนั้น $m = n$

4. ให้ $(n,r) = d$ แล้วมีจำนวนเต็ม s และ t ซึ่ง $n = sd,\ r = td$ โดยที่ $(s,t) = 1$ จะได้ $(a^r)^s = a^{std} = (a^n)^t = e^t = e$ และ $a^{tdm} = (a^r)^m = e$ แต่ $|a^r| = m$ และ $|a| = n$ ดังนั้น m เป็นตัวหารของ s และ n เป็นตัวหารของ tdm โดยที่ $n = sd$ จึงสรุปได้ว่า s เป็นตัวหารของ tm โดยที่ $(s,t) = 1$ เพราะฉะนั้น s เป็นตัวหารของ m ดังนั้น s และ m เป็นจำนวนเต็มบวกซึ่งเป็นตัวหารของกันและกัน ทำให้ได้ว่า $s = m$ ดังนั้น $n = sd = md$

5. ให้ $|a| = n$ และ $|b| = m$ แล้วจาก $ab = ba$ จะได้ $(ab)^{mn} = a^{mn}b^{mn} = e$ ดังนั้น $|ab|$ เป็นตัวหารของ mn ให้ $|ab| = m_1 n_1$ โดยที่ m_1 เป็นตัวหารของ m และ n_1 เป็นตัวหารของ n แล้ว $(m_1, n_1) = 1$ ดังนั้นมีจำนวนเต็มบวก s และ t ซึ่ง $m = tm_1$ และ $n = sn_1$ เพราะฉะนั้น $e = (ab)^{tm_1 n_1} = (ab)^{mn_1} = a^{mn_1}b^{mn_1} = a^{mn_1}$ ทำให้ได้ n เป็นตัวหารของ mn_1 โดยที่ $(m,n) = 1$ ดังนั้น n

เป็นตัวหารของ n_1 ทำให้ได้ $n = n_1$ และในทำนองเดียวกันจะได้ $m = m_1$ เพราะฉะนั้น $|ab| = mn$ $= |a||b|$

6. ให้ $(m,n) = 1$ แล้วมีจำนวนเต็ม M และ N ซึ่ง $Mm + Nn = 1$ ทำให้ได้ $a = a^{Mm+Nn}$ $= a^{Mm}a^{Nn}$ ถ้าให้ $c = a^{Mm}$ และ $d = a^{Nn}$ แล้ว $a = cd = dc$ แต่ $|a| = mn$ ดังนั้น $|a^m| = n$ ทำให้ได้โดยข้อ 4 ว่า $|c| = |a^{mM}| = n$ และจาก $Mm + Nn = 1$ จึงได้ $(M,N) = 1$ และโดยการพิสูจน์ในทำนองเดียวกัน จะได้ $|d| = |a^{nN}| = m$ ตามต้องการ

ในการพิสูจน์ว่า c และ d ดังกล่าวมีเพียงคู่เดียว สมมติให้ c_1 และ d_1 เป็นคู่ของจำนวนเต็มซึ่ง $a = c_1d_1 = d_1c_1, |c_1| = n$ และ $|d_1| = m$ แล้ว $c_1d_1 = a = cd$ ทำให้ได้ $(c_1d_1)^{Mm} = (cd)^{Mm}$ แต่ $c_1d_1 = d_1c_1, cd = dc$ และ $|d| = |d_1| = m$ ทำให้ $c_1^{Mm} = c_1^{Mm}d_1^{Mm} = (c_1d_1)^{Mm} = (cd)^{Mm} = c^{Mm}d^{Mm} = c^{Mm}$ และโดยการแทน $Mm + Nn = 1$ จะได้ $c_1^{1-Nn} = c^{1-Nn}$ ซึ่งสมมูลกับ $c_1c_1^{-Nn} = cc^{-Nn}$ ทำให้ได้ $c_1 = cc^{-Nn}c_1^{Nn} = cc^{-Nn}$ (เพราะ $|c_1| = n$) ดังนั้น $c = c_1c^{Nn} = c_1$ (เพราะ $|c| = n$) และโดยการพิสูจน์ในทำนองเดียวกันก็จะได้ว่า $d_1 = d$

7. ให้ $|a| = n$ และ r และ s เป็นจำนวนเต็มแล้ว $a^r = a^s$ ก็ต่อเมื่อ $a^{r-s} = e$ ซึ่งก็ต่อเมื่อ n เป็นตัวหารของ $r - s$ (โดยข้อ 2) นั่นคือก็ต่อเมื่อ $r \equiv s (\bmod n)$ ❐

ดังกล่าวแล้วว่าอันดับของสมาชิกในกรุปต่างจากอันดับของกรุป จึงอาจมีคำถามว่าจะมีความสัมพันธ์ของอันดับของกรุปกับอันดับของสมาชิกในกรุปหรือไม่ และความสัมพันธ์นั้นจะเป็นเช่นใด และโดยทฤษฎีบท 1.3.5 ซึ่งกล่าวว่าอันดับของกรุปย่อยของกรุปวัฏจักรเป็นตัวหารของกรุปวัฏจักรนั้น ก็อาจมีคำถามว่าความจริงเช่นนี้จะเกิดขึ้นสำหรับกรุปทั่วๆ ไปหรือไม่ คำถามเหล่านี้ยังคงเป็นคำถามเปิดจนกระทั่ง นักคณิตศาสตร์ชาวฝรั่งเศสชื่อ โชแซฟ ลากรองจ์ (Joseph Louis Lagrange; 1736 - 1813) ได้เกิดแนวความคิดในการพิสูจน์ทฤษฎีบทหนึ่งซึ่งรู้จักกันต่อมาในชื่อว่าทฤษฎีบทของลากรองจ์ (Lagrange's Theorem) เป็นทฤษฎีบทที่มีชื่อเสียงมาก เพราะนอกจากจะตอบคำถามเปิดข้างต้นแล้ว ยังมีประโยชน์เกี่ยวกับการนับจำนวนสมาชิกของกรุปจำกัดซึ่งเป็นรากฐานของวิชาการนับในสมัยต่อมาด้วย

ลากรองจ์ เริ่มต้นแนวคิดของการพิสูจน์ว่า "*อันดับของกรุปย่อยของกรุปจำกัดเป็นตัวหารของกรุปนั้น*" ด้วยการพยายามแบ่งกั้นเอกภพของกรุป G ออกเป็นเซตย่อยหลายๆ เซตโดยให้แต่ละคู่ของเซตย่อยเหล่านี้ไม่มีส่วนร่วมกัน นั่นคือเป็นเซตต่างสมาชิกและแต่ละเซตย่อยประกอบด้วยสมาชิกจำนวนเท่ากับจำนวนสมาชิกของกรุปย่อย H ของ G และเพราะ H ก็เป็นเซตย่อยของ G ที่มีจำนวนสมาชิกตามต้องการ จึงหาวิธีที่จะสร้างเซตย่อยอื่นๆ ที่เป็นเซตต่างสมาชิกกันและเป็นเซต

ต่างสมาชิกของ H และวิธีการหนึ่งก็คือกระทำการดำเนินการของกรุปกับทุกๆ สมาชิกของ H ด้วยสมาชิกต่างๆ ของ G

ให้ $a \in G$ และนิยามเซต $Ha := \{ha | h \in H\}$ ทำให้ได้ $h_1 a = h_2 a \Leftrightarrow h_1 = h_2$ ทุกๆ $h_1, h_2 \in H$ แสดงว่าฟังก์ชันจาก H ไปยัง Ha ซึ่งนิยามโดย $h \to ha$ ทุกๆ $h \in H$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ดังนั้นจำนวนสมาชิกของเซต Ha เท่ากับจำนวนสมาชิกของเซต H

เนื่องจาก $a = ea \in Ha$ จะได้ $\bigcup_{a \in G} Ha = G$ จึงเหลือเพียงการพิสูจน์ว่าเซตย่อยในรูป Ha เหล่านี้เป็นเซตต่างสมาชิกกัน ให้ $a, a' \in G$ โดยที่ $Ha \cap Ha' \neq \phi$ และให้ $x \in Ha \cap Ha'$ แล้วมี $h_1, h_2 \in H$ ซึ่ง $h_1 a = x = h_2 a'$ ทำให้ได้ $a = h_1^{-1} h_2 a' \in Ha'$ และ $a' = h_2^{-1} h_1 a \in Ha$ ถ้า $ha \in Ha$ แล้ว $ha = h(h_1^{-1} h_2 a') = (hh_1^{-1} h_2) a' \in Ha'$ และในทำนองเดียวกันถ้า $ha' \in Ha'$ แล้ว $ha' = h(h_2^{-1} h_1 a') = (hh_2^{-1} h_1) a \in Ha$ เพราะฉะนั้น $Ha = Ha'$

การพิสูจน์ข้างต้นแสดงว่าเซตสองเซตใดๆ ในรูป Ha เมื่อ $a \in G$ เป็นเซตเดียวกันหรือเป็นเซตต่างสมาชิกกันอย่างใดอย่างหนึ่งเสมอ

เพราะว่า $\bigcup_{a \in G} Ha = G$ เป็นเซตจำกัดและการพิสูจน์ในย่อหน้าก่อน แสดงว่ามี $a_1 = e, a_2, \ldots, a_r$ เป็นสมาชิกที่ต่างกัน r ตัวของ G ที่ทำให้ $G = \bigcup_{a \in G} Ha = \bigcup_{i=1}^{r} Ha_i$ โดยที่ $Ha_i \cap Ha_j$ เป็นเซตว่างเมื่อ $i \neq j$ ดังนั้น $|G| = |H_1| + |H_2| + \cdots + |H_r| = r|H|$ ซึ่งแสดงว่าอันดับของ H เป็นตัวหารของอันดับของ G

ถ้า G เป็นกรุปจำกัดและ $a \in G$ แล้ว $a, a^2, \ldots, a^n, \ldots \in G$ ทำให้ได้ว่ามีจำนวนเต็มบวก $r < s$ ซึ่ง $a^r = a^s$ ดังนั้น $a^{s-r} = e$ โดยที่ $s - r$ เป็นจำนวนเต็มบวก จึงได้โดยหลักการเป็นอันดับอย่างดีว่ามีจำนวนเต็มบวก n น้อยสุดที่ทำให้ $a^n = e$ ซึ่งแสดงว่า $|a| = n$ นอกจากนี้ $< a > = \{e, a, a^2, \ldots, a^{n-1}\}$ เป็นกรุปย่อยวัฏจักรของ G ซึ่ง $|< a >| = n$ แล้วผลการพิสูจน์อันดับแรกของลากรองจ์ในย่อหน้าก่อน ทำให้ได้ว่า $|a|$ เป็นตัวหารของอันดับของ G

ให้ G เป็นกรุปที่มีอันดับเป็นจำนวนเฉพาะ p นั่นคือ G ประกอบด้วยสมาชิกจำนวน p (>1) ตัว ดังนั้นมี $a \in G$ ซึ่ง $a \neq e$ แล้วผลการพิสูจน์ในย่อหน้าก่อนแสดงว่า $|a|$ เป็นจำนวนจำกัด นั่นคือมีจำนวนเต็มบวกน้อยสุด $r > 1$ ซึ่ง $a^r = e$ และ r เป็นตัวหารของ $|G| = p$ ซึ่งเป็นจำนวนเฉพาะ ทำให้ได้ว่า $r = p$ เพราะฉะนั้น $< a > = \{e, a, a^2, \ldots, a^{p-1}\}$ เป็นกรุปย่อยวัฏจักรของ G ที่มีอันดับเท่ากับอันดับของ G จึงได้ว่า $G = < a > = \{e, a, a^2, \ldots, a^{p-1}\}$ นั่นคือ G เป็นกรุปวัฏจักร การวิเคราะห์เหล่านี้ ทำให้สรุปได้เป็นทฤษฎีบทและผลพลอยได้ต่อไปนี้

1.3.8 **ทฤษฎีบทของลากรองจ์** (Lagrange's Theorem) ถ้า H เป็นกรุปย่อยของกรุปจำกัด G แล้ว $|H|$ เป็นตัวหารของ $|G|$ ❐

1.3.9 ผลพลอยได้ของทฤษฎีบทของลากรองจ์

1. ถ้า a เป็นสมาชิกของกรุปจำกัด G แล้ว $|a|$ เป็นตัวหารของ $|G|$
2. ถ้า G เป็นกรุปที่มีอันดับเป็นจำนวนเฉพาะแล้ว G เป็นกรุปวัฏจักร ❐

ขอจบหัวข้อนี้ด้วยการประยุกต์ทฤษฎีบทของลากรองจ์ เพื่อหากรุปย่อยทั้งหมดของ S_3 ดังนี้ จาก $|S_3| = 6 = (2)(3)$ โดยทฤษฎีบทของลากรองจ์ แต่ละกรุปย่อยของ S_3 เป็นกรุปอันดับ 1,2,3 หรือ 6 โดยที่กรุปย่อยอันดับ 1 และอันดับ 6 คือ $\{(1)\}$ และ S_3 แต่โดยทฤษฎีบทของลากรองจ์ ทุกๆ กรุปย่อยอันดับ 2 และอันดับ 3 ทั้งหมดเป็นกรุปย่อยวัฏจักรซึ่งก่อกำเนิดโดยสมาชิกที่มีอันดับ 2 และอันดับ 3 ตามลำดับ และกรุปย่อยเหล่านั้นได้แก่ $<(12)>, <(13)>, <(23)>, <(123)>$ และ $<(132)>$ โดยสังเกตว่า (123) และ (132) ต่างก่อกำเนิดกรุปย่อยเดียวกัน เนื่องจาก

$$<(123)> \;=\; \{(1),(123),(132)\} = \;<(132)>$$

ดังนั้นกรุปย่อยทั้งหมดของ S_3 ได้แก่ $\{(1)\}$, $<(12)>$, $<(13)>$, $<(23)>$, $<(123)>$ และ S_3

แบบฝึกหัด 1.3

1. จงแสดงว่ากรุป Q_8 ของเมทริกซ์จำนวนเชิงซ้อนซึ่งก่อกำเนิดโดย $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ และ $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ เมื่อ $i^2 = -1$ เป็นกรุปนอนอาบีเลียนอันดับ 8 [ซึ่งรู้จักกันดีในชื่อ *กรุปควอเทอร์เนียน (quaternion group)* พร้อมทั้งพิสูจน์ว่า กรุปของเมทริกซ์จำนวนจริงซึ่งก่อกำเนิดโดย $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ และ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ก็เป็นกรุปนอนอาบีเลียนอันดับ 8 ที่ต่างจาก Q_8
2. ให้ G เป็นกรุปของเมทริกซ์จำนวนตรรกยะขนาด 2×2 ทั้งหมดภายใต้การคูณของเมทริกซ์ จงแสดงว่าอันดับของ $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ และ $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ เท่ากับ 4 และ 3 ตามลำดับ แต่ ab มีอันดับอนันต์
3. จงแสดงว่า $A_n = <(123),(124),\ldots,(12n)>$ และ $S_n = <(12),(13),\ldots,(1n)>$ ทุกๆ $n \geq 3$
4. ให้ G เป็นกรุปและ $\{H_i | i \in I\}$ เป็นหมู่ของกรุปย่อยของ G
   4.1 จงหาเงื่อนไขที่ทำให้ $\bigcup_{i\in I} H_i$ เป็นกรุปย่อยของ G นั่นคือเงื่อนไขซึ่ง $\bigcup_{i\in I} H_i = <\bigcup_{i\in I} H_i>$
   4.2 จงแสดงว่า $\bigcap_{i\in I} H_i = \bigcap_{i\in I}(H_i a)$ สำหรับทุกๆ $a \in G$
5. จงพิสูจน์ว่ากรุปที่มีจำนวนกรุปย่อยเป็นจำนวนจำกัดเป็นกรุปจำกัด
6. ให้ G เป็นกรุป จงแสดงว่า $H = \{a \in G | (ax)^2 = (xa)^2$ ทุกๆ $x \in G\}$ เป็นกรุปย่อยของ G

7. จงพิสูจน์ว่าเซตย่อยจำกัด S ที่ไม่ใช่เซตว่างของกรุป G เป็นกรุปย่อย ก็ต่อเมื่อ S มีสมบัติปิดภายใต้การดำเนินการของ G
8. ให้ G เป็นกรุปอาบีเลียน จงพิสูจน์ว่าเซตซึ่งประกอบด้วยสมาชิกอันดับจำกัดทั้งหมดของ G เป็นกรุปย่อยของ G
9. ให้ p และ q เป็นจำนวนเฉพาะซึ่ง $p > q$ จงพิสูจน์ว่าทุกๆ กรุปอันดับ pq มีกรุปย่อยอันดับ p อย่างมากเพียงกรุปย่อยเดียว
10. ให้ S เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G และนิยามความสัมพันธ์ $\sim$ ใน G โดย

    $a \sim b$ ก็ต่อเมื่อ $ab^{-1} \in S$ ทุกๆ $a,b \in G$

    จงพิสูจน์ว่า $\sim$ เป็นความสัมพันธ์สมมูลใน G (ดูนิยามความสัมพันธ์สมมูลจาก [2]) ก็ต่อเมื่อ S เป็นกรุปย่อยของ G

1.4 กรุปย่อยปรกติและกรุปผลหาร

การพิสูจน์ทฤษฎีบทของลากรองจ์ได้จากแนวคิดของการสร้างเซตในรูปแบบ $Ha := \{ha | h \in H\}$ แล้วได้ $\{Ha | a \in G\}$ เป็นผลแบ่งกั้นของ G ซึ่งทุกๆ เซตในผลแบ่งกั้นมีขนาดเท่ากันและเท่ากับขนาดของกรุปย่อย H ความจริงดังกล่าวนี้แม้จะพิสูจน์ในกรณีของกรุปจำกัด แต่การพิสูจน์ยังครอบคลุมกรณีกรุปใดๆ และในทำนองคู่กัน การสร้างเซตในรูปแบบ $aH := \{ah | h \in H\}$ ก็ส่งผลเช่นเดียวกัน จึงได้มีการกำหนดชื่อเซตเหล่านี้ขึ้น ในหัวข้อนี้เราจะศึกษาสมบัติและแสดงประโยชน์ของเซตเหล่านี้

1.4.1 **บทนิยาม** สำหรับกรุปย่อย H ของกรุป G และ $a \in G$ เรียกเซตในรูปแบบ $Ha := \{ha | h \in H\}$ ว่า *โคเซตขวา (right coset)* ของ H ใน G และเรียกเซตในรูปแบบ $aH := \{ah | h \in H\}$ ว่า *โคเซตซ้าย (left coset)* ของ H ใน G

สังเกตว่าโคเซตซ้ายหรือโคเซตขวาของกรุปย่อย H ใน G ซึ่งไม่ใช่ H เป็นเพียงเซตย่อยของ G เท่านั้น (เพราะเซตเหล่านั้นไม่รวมเอกลักษณ์ของ G) จึงไม่ใช่กรุปย่อยของ G และสำหรับแต่ละ $a \in G$ จะได้ว่า

$$|aH| = |H| = |Ha|$$

จึงอาจมีคำถามว่าจำนวนโคเซตขวาทั้งหมดเท่ากับจำนวนโคเซตซ้ายทั้งหมดหรือไม่ สำหรับแต่ละกรุปย่อย H ของแต่ละกรุป G เราอาจตอบคำถามนี้โดยทฤษฎีบทของลากรองจ์ในกรณีของเซตจำกัดว่า จำนวนโคเซตขวาทั้งหมดเท่ากับ $\frac{|G|}{|H|}$ และเพราะจำนวนนี้ขึ้นกับอันดับของ G และอันดับ

ของ H เท่านั้น เราจึงพิสูจน์ความจริงเกี่ยวกับจำนวนโคเซตซ้ายทั้งหมดโดยการแทนโคเซตขวาด้วยโคเซตซ้ายในบทพิสูจน์ทฤษฎีบทของลากรองจ์ จำนวนโคเซตซ้ายทั้งหมดจึงเท่ากับ $\frac{|G|}{|H|}$ ด้วย (ขอให้สังเกตว่าวิธีการที่กล่าวนี้ไม่สามารถนำมาประยุกต์เพื่อพิสูจน์ในกรณีของกรุปอนันต์ได้) จึงขอสรุปเป็นทฤษฎีบทโดยละการพิสูจน์ไว้เป็นแบบฝึกหัด

1.4.2 **ทฤษฎีบท** ให้ H เป็นกรุปย่อยของกรุป G แล้วมีฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงระหว่างเซตของโคเซตซ้ายทั้งหมดของ H ใน G และเซตของโคเซตขวาทั้งหมดของ H ใน G ❐

เรียกจำนวนสมาชิกของเซตของโคเซตขวาทั้งหมดของ H ใน G ซึ่งก็คือจำนวนสมาชิกของเซตของโคเซตซ้ายทั้งหมดของ H ใน G ว่า *ดรรชนี (index)* ของ H ใน G และแทนด้วย $[G:H]$ และสังเกตว่าถ้า $H=\{e\}$ แล้ว $|G|=[G:\{e\}]$

โดยบทพิสูจน์ทฤษฎีบทของลากรองจ์ ถ้า G เป็นกรุปจำกัดแล้ว $|G|=|H|[G:H]$ นั่นคือ $[G:H]=\frac{|G|}{|H|}$ ทำให้ได้ว่าทั้ง $|H|$ และ $[G:H]$ เป็นตัวหารของ $|G|$

เพราะว่าเซตของโคเซตขวาทั้งหมดของกรุปย่อย H ของกรุป G เป็นผลแบ่งกั้น G ดังนั้นจะมีความสัมพันธ์สมมูล $\sim$ ซึ่งกำหนดโดยผลแบ่งกั้นนี้ และในการหานิยามของความสัมพันธ์ $\sim$ ดังกล่าวเราพิจารณาว่า ถ้า $a,b\in G$ ซึ่ง $a\sim b$ แล้ว a และ b เป็นสมาชิกในโคเซตขวาเดียวกัน แต่โคเซตขวาที่มี a และ b เป็นสมาชิกคือ Ha และ Hb ตามลำดับ ดังนั้น

$$a\sim b \;\Leftrightarrow\; Ha=Hb$$

และเพราะ $b\in Hb=Ha$ ดังนั้นมี $h\in H$ ซึ่ง $b=ha$ จึงได้ว่า $ba^{-1}=h\in H$ เพราะฉะนั้น

$$a\sim b \;\Leftrightarrow\; Ha=Hb \;\Leftrightarrow\; ba^{-1}\in H$$

ในทำนองคู่กัน ความสัมพันธ์สมมูล $\sim$ ซึ่งกำหนดโดยผลแบ่งกั้นซึ่งคือเซตของโคเซตซ้ายทั้งหมดของกรุปย่อย H ของกรุป G จะนิยามโดย

$$a\sim b \;\Leftrightarrow\; aH=bH \;\Leftrightarrow\; a^{-1}b\in H$$

เราจึงได้ทฤษฎีบทต่อไปนี้

1.4.3 **ทฤษฎีบท** ให้ H เป็นกรุปย่อยของกรุป G และ $a,b\in G$ แล้ว

1. $Ha=Hb$ ก็ต่อเมื่อ $ba^{-1}\in H$
2. $aH=bH$ ก็ต่อเมื่อ $a^{-1}b\in H$
3. $aH=H=Ha$ ก็ต่อเมื่อ $a\in H$ ❐

อาจมีคำถามว่าผลแบ่งกั้น G ที่เป็นเซตของโคเซตขวาทั้งหมดของ H ใน G และที่เป็นเซตของโคเซตซ้ายทั้งหมดของ H ใน G เป็นผลแบ่งกั้นเดียวกันหรือไม่ ถ้าคำตอบคือ "ไม่ใช่" แล้วภายใต้เงื่อนไขใดจึงจะทำให้ผลแบ่งกั้นทั้งสองเป็นเซตเดียวกัน เพื่อให้ได้คำตอบ เราพิจารณากรุปสมมาตร S_3 ซึ่งเราทราบจากหัวข้อ 1.3 แล้วว่ากรุปย่อยทั้งหมดของ S_3 ได้แก่ $\{(1)\}, <(12)>, <(13)>, <(23)>, <(123)>, S_3$

ถ้าพิจารณากรุปย่อย $H = <(12)> = \{(1),(12)\}$ จะได้โคเซตซ้ายที่ต่างกันทั้งหมดของ H ใน S_3 อยู่ 3 โคเซตคือ

$$(1)H = \{(1),(12)\} = (12)H,$$
$$(13)H = \{(13),(123)\} = (123)H,$$
$$(23)H = \{(23),(132)\} = (132)H$$

ในทำนองเดียวกัน จะได้โคเซตขวาที่ต่างกันทั้งหมดของ H ใน S_3 อยู่ 3 โคเซตคือ

$$H(1) = \{(1),(12)\} = H(12),$$
$$H(13) = \{(13),(132)\} = H(132),$$
$$H(23) = \{(23),(123)\} = H(123)$$

จะเห็นว่าเซตของโคเซตซ้ายทั้งหมดของ H ใน G **ไม่ใช่**เซตเดียวกันกับเซตของโคเซตขวาทั้งหมดของ H ใน G

แต่ถ้าพิจารณากรุปย่อย $H = <(123)> = \{(1),(123),(132)\}$ จะได้ว่าแต่ละโคเซตขวาของ H ใน S_3 ก็คือโคเซตซ้ายของ H ใน S_3 ซึ่งมีที่แตกต่างกันทั้งหมดได้แก่

$$(123)H = H(123) = \{(1),(123),(132)\} = (132)H = H(132)$$

และ $$(12)H = H(12) = (13)H = H(13) = (23)H = H(23) = \{(12),(13),(33)\}$$

ในกรณีทั่วไปถ้า H เป็นกรุปย่อยของกรุป G และ $a \in G$ แล้ว $a = ae \in aH$ และ $a = ea \in Ha$ เมื่อ e เป็นเอกลักษณ์ของ G ดังนั้นโคเซตซ้ายและโคเซตขวาที่มี a เป็นสมาชิกคือ aH และ Ha ตามลำดับ ทำให้ได้ว่าแต่ละโคเซตซ้ายของ H ใน G เป็นโคเซตขวาของ H ใน G ก็ต่อเมื่อ $aH = Ha$ ทุกๆ $a \in G$ เราเรียกกรุปย่อย H ของกรุป G ที่มีลักษณะเช่นนี้ว่ากรุปย่อยปรกติ

1.4.4 **บทนิยาม** เรียกกรุปย่อย N ของกรุป G ว่า *กรุปย่อยปรกติ (normal subgroup)* ถ้าทุกๆ โคเซตซ้ายของ N ใน G เป็นโคเซตขวาของ N ใน G นั่นคือ $aN = Na$ ทุกๆ $a \in G$

ทฤษฎีบทต่อไปแสดงเกณฑ์การเป็นกรุปย่อยปรกติ

1.4.5 **ทฤษฎีบท** ให้ H เป็นกรุปย่อยของกรุป G แล้วข้อความต่อไปนี้สมมูลกัน

1. $aH = Ha$ สำหรับทุกๆ $a \in G$

2. $aHa^{-1} = H$ สำหรับทุกๆ $a \in G$

3. $aHa^{-1} \subseteq H$ สำหรับทุกๆ $a \in G$

4. $aha^{-1} \in H$ สำหรับทุกๆ $a \in G$ และทุกๆ $h \in H$

บทพิสูจน์ เห็นได้ชัดว่า $(2) \Rightarrow (3) \Rightarrow (4)$

$(1) \Rightarrow (2)$ ให้ $a \in G$ ซึ่ง $aH = Ha$ ถ้า $x \in aHa^{-1}$ แล้ว $x = aha^{-1}$ สำหรับบาง $h \in H$ ทำให้ได้ $xa = (aha^{-1})a = ah \in aH = Ha$ จึงมี $h_1 \in H$ ซึ่ง $xa = ah = h_1 a$ ดังนั้น $x = h_1 aa^{-1} = h_1 \in H$ และถ้า $x \in H$ แล้ว $xa \in Ha = aH$ จึงมี $h_2 \in H$ ซึ่ง $xa = ah_2$ ดังนั้น $x = ah_2 a^{-1} \in aHa^{-1}$ เพราะฉะนั้น $aHa^{-1} = H$

$(4) \Rightarrow (1)$ ให้ $a \in G$ ถ้า $ah \in aH$ แล้วเพราะ $aha^{-1} \in H$ จึงให้ $aha^{-1} = h_1 \in H$ แล้วได้ $ah = h_1 a \in Ha$ ในทางกลับกัน ถ้า $ha \in Ha$ แล้วเพราะ $a^{-1} \in G$ และ $a^{-1}ha = a^{-1}h(a^{-1})^{-1} \in H$ ดังนั้นให้ $a^{-1}ha = h_2 \in H$ ทำให้ได้ $ha = ah_2 \in aH$ เพราะฉะนั้น $aH = Ha$ ❐

ทฤษฎีบทต่อไปกล่าวถึงสมบัติเกี่ยวกับกรุปย่อยปรกติซึ่งขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

1.4.6 ทฤษฎีบท

1. ถ้า H เป็นกรุปย่อยของกรุป G ซึ่ง $[G:H] = 2$ แล้ว H เป็นกรุปย่อยปรกติ

2. ถ้า H เป็นกรุปย่อยของกรุปอาบีเลียน G แล้ว H เป็นกรุปย่อยปรกติ ❐

จากอันดับของกรุปสลับ A_n เป็นครึ่งหนึ่งของ S_n ทุกๆ $n \geq 2$ ดังนั้น $[S_n : A_n] = 2$ เราจะได้บทแทรกต่อไปนี้

1.4.7 บทแทรก กรุปสลับ A_n เป็นกรุปย่อยปรกติของ S_n ทุกๆ จำนวนเต็มบวก n ❐

ถ้า N เป็นกรุปย่อยปรกติของกรุป G เราทราบแล้วว่า "โคเซตซ้าย" ของ N ใน G ก็คือ "โคเซตขวา" ของ N ใน G ยิ่งไปกว่านั้น $aN = Na$ ทุกๆ $a \in G$ เราจึงจะกล่าวโดยละคำว่า "ซ้าย" หรือ "ขวา" และเรียกรวมกันอย่างสั้นๆ ว่า "โคเซต" และจะแทนเซตของโคเซตทั้งหมดของ N ใน G ด้วยสัญลักษณ์ G/N นั่นคือ

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

จึงอาจมีคำถามว่า จะสามารถนิยามการดำเนินการบน G/N เพื่อให้เกิดกรุปใหม่ได้หรือไม่ และแน่นอนว่าเราควรนิยามการดำเนินการอย่างเป็นธรรมชาติ ดังนี้

$$(aN)(bN) = abN \qquad \text{สำหรับทุกๆ } a, b \in G$$

แต่เพราะ aN และ bN เป็นเซต จึงควรให้ความหมาย "การคูณ" ของเซตซึ่งจะนิยามดังนี้

$$(aN)(bN) = \{(an_1)(bn_2) \mid n_1, n_2 \in N\}$$

1.4.8 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยของกรุป G แล้ว N เป็นกรุปย่อยปรกติของ G ก็ต่อเมื่อ $(aN)(bN) = abN$ ทุกๆ $a, b \in G$

บทพิสูจน์ ให้ N เป็นกรุปย่อยปรกติของกรุป G และ $a, b \in G$ แล้วสำหรับ $n_1, n_2 \in N$ จะได้ $n_1 b \in Nb = bN$ ดังนั้นมี $n_3 \in N$ ซึ่ง $n_1 b = bn_3$ ทำให้ได้ $(an_1)(bn_2) = a(n_1 b)n_2 = abn_3 n_2 \in abN$ นอกจากนี้ $abn = (ae)(bn) \in (aN)(bN)$ ทุกๆ $n \in N$ ซึ่งแสดงว่า $(aN)(bN) = abN$

ในการพิสูจน์บทกลับให้ $a \in G$ และ $n \in N$ แล้ว $ana^{-1} = (an)(a^{-1}e) \in (aN)(a^{-1}N)$ แต่โดยสมมติฐาน $(aN)(a^{-1}N) = aa^{-1}N = eN = N$ ดังนั้น $ana^{-1} \in N$ และโดยทฤษฎีบท 1.4.5 จะได้ว่า N เป็นกรุปย่อยปรกติของ G ❐

แม้ทฤษฎีบท 1.4.8 จะแสดงว่าผลคูณของโคเซตของกรุปย่อยปรกติของกรุปเป็นโคเซตของกรุปย่อยปรกติของกรุปก็ตาม แต่ก็เป็นการแสดงการคูณในรูปของตัวแทนของแต่ละโคเซต ดังนั้นการแสดงว่า "การคูณ" ระหว่างโคเซตดังกล่าวเป็นการดำเนินการบนเซตของโคเซตทั้งหมด เราต้องพิสูจน์ว่า ไม่ว่าตัวแทนของโคเซต aN และ bN จะเป็นตัวใดก็ตาม ผลคูณของโคเซตทั้งสองยังคงได้เป็นโคเซต abN โคเซตเดียวกัน

1.4.9 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยปรกติของกรุป G และนิยาม "การคูณ" บน G/N โดย $(aN)(bN) = abN$ ทุกๆ $a, b \in G$ แล้ว G/N เป็นกรุป

บทพิสูจน์ ให้ $a, a', b, b' \in G$ ซึ่ง $aN = a'N$ และ $bN = b'N$ แล้ว $a^{-1}a' \in N$ และ $b^{-1}b' \in N$ เพราะว่า N เป็นกรุปย่อยปรกติ ดังนั้น $b^{-1}(a^{-1}a')b \in N$ ทำให้ได้ $(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = (b^{-1}a^{-1}a'b)\,(b^{-1}b') \in N$ เพราะฉะนั้น $abN = a'b'N$

สำหรับการพิสูจน์ว่า G/N เป็นกรุป ทำได้โดยตรง จึงขอละไว้เป็นแบบฝึกหัด ❐

เราเรียกกรุป G/N ในทฤษฎีบท 1.4.9 ว่า *กรุปผลหาร (quotient group)* ของ N ใน G

1.4.10 **ข้อสังเกต** 1. G/N คือกรุปของโคเซตทั้งหมดของกรุปย่อยปรกติ N ในกรุป G และในกรณี G เป็นกรุปจำกัด อันดับของกรุปผลหารจะเท่ากับดรรชนีของ N ใน G นั่นคือ

$$|G/N| = [G : N]$$

2. เนื่องจากการดำเนินการบนกรุป เราเรียกว่า "การคูณ" จึงเรียกการดำเนินการบนกรุปผลหารว่า "การคูณระหว่างโคเซต" หรือเรียกสั้นๆ ว่า "การคูณ" แต่ถ้า G เป็น "กรุปการบวก" นั่นคือการดำเนินการของ G คือ + แล้วเพื่อให้สอดคล้องกับการดำเนินการของ G สัญลักษณ์แทนโคเซต

ของ N ใน G จึงเขียนเป็น $a+N$ หรือ $N+a$ และการดำเนินการบนกรุปผลหารก็จะเป็นการบวกเช่นเดียวกัน กล่าวคือสำหรับแต่ละ $a,b \in G$ จะเขียนการบวกของโคเซตดังนี้

$$(a+N)+(b+N)=(a+b)+N$$

3. ถ้า G เป็นกรุปอาบีเลียน แล้ว G/N เป็นกรุปอาบีเลียน ทุกๆ กรุปย่อย N ของ G

1.4.11 ตัวอย่าง พิจารณากรุปย่อยปรกติ $N=<r_2>$ ของกรุป D_4 แล้วโคเซตของ N ใน D_4 ที่ต่างกันทั้งหมดจะเป็นสมาชิกของกรุปผลหาร $D_4/<r_2>$ ทำให้ได้

$$D_4/<r_2>=\{\{e,r_2\},\{r_1,r_3\},\{h,v\},\{d_1,d_2\}\}$$

และตารางข้างล่างเป็นตารางการคูณของกรุปผลหารนี้ โดยตัวอย่างการคูณระหว่าง $\{d_1,d_2\}$ กับ $\{r_1,r_3\}$ เป็นดังนี้ $(d_1N)(r_1N)=d_1r_1N=hN=\{h,v\}$

	$\{e,r_2\}$	$\{r_1,r_3\}$	$\{h,v\}$	$\{d_1,d_2\}$
$\{e,r_2\}$	$\{e,r_2\}$	$\{r_1,r_3\}$	$\{h,v\}$	$\{d_1,d_2\}$
$\{r_1,r_3\}$	$\{r_1,r_3\}$	$\{e,r_2\}$	$\{d_1,d_2\}$	$\{h,v\}$
$\{h,v\}$	$\{h,v\}$	$\{d_1,d_2\}$	$\{e,r_2\}$	$\{r_1,r_3\}$
$\{d_1,d_2\}$	$\{d_1,d_2\}$	$\{h,v\}$	$\{r_1,r_3\}$	$\{e,r_2\}$

❍

1.4.12 ตัวอย่าง พิจารณากรุปวัฏจักรของจำนวนเต็ม $\mathbb{Z}$ ซึ่งเป็นกรุปการบวก ดังนั้นทุกๆ กรุปย่อยของ $\mathbb{Z}$ เป็นกรุปวัฏจักรในรูปแบบ $<n>$ เมื่อ n เป็นจำนวนเต็มและเพราะกรุปวัฏจักรเป็นกรุปอาบีเลียน ดังนั้นทุกๆ กรุปย่อย $<n>$ ของ $\mathbb{Z}$ เป็นกรุปย่อยปรกติ และสำหรับโคเซตของ $<n>$ ใน $\mathbb{Z}$ เขียนได้ในรูปแบบดังต่อไปนี้

$$a+<n>=\{a+kn \mid k\in\mathbb{Z}\}$$

ทุกๆ จำนวนเต็ม a แต่สมาชิกของ $a+<n>$ ซึ่งอยู่ในรูปแบบ $a+kn$ เป็นจำนวนเต็มซึ่งสัมพันธ์คอนกรูเอนซ์กับ a มอดูโล n ดังนั้น $a+<n>=\bar{a}$ ทุกๆ จำนวนเต็ม a ซึ่งแสดงว่ากรุปผลหาร $\mathbb{Z}/<n>$ ก็คือกรุปวัฏจักร $\mathbb{Z}_n$ นั่นเอง ❍

1.4.13 ตัวอย่าง พิจารณกรุปย่อย $N=<\bar{3}>\times<\bar{2}>$ ของกรุป $G=\mathbb{Z}_{12}\times\mathbb{Z}_4$ เพราะ G เป็นกรุปอาบีเลียน ดังนั้น N เป็นกรุปย่อยปรกติและโดยวิธีการหาโคเซตทั้งหมดของ N ใน G ดังที่เคยกล่าวมา จะได้สมาชิกทั้งหมดของกรุปผลหาร G/N ดังต่อไปนี้

$$N_{0,0}=N,$$

$$N_{0,1}=(\bar{0},\bar{1})+N=\{(\bar{0},\bar{1}),(\bar{0},\bar{3}),(\bar{3},\bar{1}),(\bar{3},\bar{3}),(\bar{6},\bar{1}),(\bar{6},\bar{3}),(\bar{9},\bar{1}),(\bar{9},\bar{3})\},$$

$$N_{1,0}=(\bar{1},\bar{0})+N=\{(\bar{1},\bar{0}),(\bar{1},\bar{2}),(\bar{4},\bar{0}),(\bar{4},\bar{2}),(\bar{7},\bar{0}),(\bar{7},\bar{2}),(\overline{10},\bar{0}),(\overline{10},\bar{2})\},$$

$$N_{1,1} = (\bar{1},\bar{1}) + N = \{(\bar{1},\bar{1}),(\bar{1},\bar{3}),(\bar{4},\bar{1}),(\bar{4},\bar{3}),(\bar{7},\bar{1}),(\bar{7},\bar{3}),(\overline{10},\bar{1}),(\overline{10},\bar{3})\},$$
$$N_{2,0} = (\bar{2},\bar{0}) + N = \{(\bar{2},\bar{0}),(\bar{2},\bar{2}),(\bar{5},\bar{0}),(\bar{5},\bar{2}),(\bar{8},\bar{0}),(\bar{8},\bar{2}),(\overline{11},\bar{0}),(\overline{11},\bar{2})\},$$
$$N_{2,1} = (\bar{2},\bar{1}) + N = \{(\bar{2},\bar{1}),(\bar{2},\bar{3}),(\bar{5},\bar{1}),(\bar{5},\bar{3}),(\bar{8},\bar{1}),(\bar{8},\bar{3}),(\overline{11},\bar{1}),(\overline{11},\bar{3})\}$$

ซึ่งมีตารางการคูณของกรุปผลหาร แสดงในตารางข้างล่างนี้

$+$	$N_{0,0}$	$N_{0,1}$	$N_{1,0}$	$N_{1,1}$	$N_{2,0}$	$N_{2,1}$
$N_{0,0}$	$N_{0,0}$	$N_{0,1}$	$N_{1,0}$	$N_{1,1}$	$N_{2,0}$	$N_{2,1}$
$N_{0,1}$	$N_{0,1}$	$N_{0,0}$	$N_{1,1}$	$N_{1,0}$	$N_{2,1}$	$N_{2,0}$
$N_{1,0}$	$N_{1,0}$	$N_{1,1}$	$N_{2,0}$	$N_{2,1}$	$N_{0,0}$	$N_{0,1}$
$N_{1,1}$	$N_{1,1}$	$N_{1,0}$	$N_{2,1}$	$N_{2,0}$	$N_{0,1}$	$N_{0,0}$
$N_{2,0}$	$N_{2,0}$	$N_{2,1}$	$N_{0,0}$	$N_{0,1}$	$N_{1,0}$	$N_{1,1}$
$N_{2,1}$	$N_{2,1}$	$N_{2,0}$	$N_{0,1}$	$N_{0,0}$	$N_{1,1}$	$N_{1,0}$

แบบฝึกหัด 1.4

1. ให้ G เป็นกรุปและ H, K และ N เป็นกรุปย่อยของ G จงพิสูจน์ว่า

   1.1 ถ้า K เป็นกรุปย่อยของ H แล้ว $[G:K] = [G:H][H:K]$ และสองจำนวนใดๆ ในสามจำนวนนี้เป็นจำนวนจำกัด จำนวนที่สามจะเป็นจำนวนจำกัด

   1.2 ถ้า H และ K เป็นกรุปย่อยจำกัด และ $HK = \{hk \mid h \in H, k \in K\}$ แล้ว $|HK| = \dfrac{|H||K|}{|H \cap K|}$

   1.3 ถ้า $[G:H]$ และ $[H:K]$ เป็นจำนวนจำกัดซึ่งเป็นจำนวนเฉพาะสัมพัทธ์ แล้ว $G = HK$

   1.4 ถ้า H เป็นกรุปย่อยของ N แล้ว $(HK) \cap N = H(K \cap N)$

   1.5 ถ้า K เป็นกรุปย่อยของ H, $H \cap N = K \cap N$ และ $HN = KN$ แล้ว $H = K$

2. ให้ K และ N เป็นกรุปย่อยของกรุป G โดยที่ N เป็นกรุปย่อยปรกติ จงพิสูจน์ว่า

   2.1 $N \cap K$ เป็นกรุปย่อยปรกติของ K

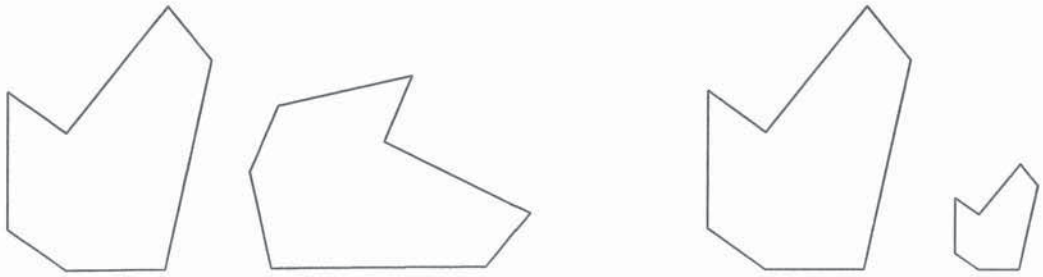
   2.2 N เป็นกรุปย่อยปรกติของ $< N \cup K >$ และ $NK = < N \cup K > = KN$

   2.3 ถ้า K เป็นกรุปย่อยปรกติของ G และ $N \cap K = \{e\}$ แล้ว $nk = kn$ ทุกๆ $k \in K$ และ $n \in N$

3. ทุกๆ กรุปย่อยของรุปควอเทอร์เนียน Q_8 เป็นกรุปย่อยปรกติ
4. ให้ G เป็นกรุป จงพิสูจน์ว่าเซต $\{a \in G | xa = ax$ ทุกๆ $x \in G\}$ ซึ่งเรียกว่า *ศูนย์กลาง (center)* ของ G เป็นกรุปย่อยปรกติของ G
5. กรุปย่อยของกรุปอาบีเลียนเป็นกรุปย่อยปรกติ
6. จงพิสูจน์ว่าถ้า H เป็นกรุปย่อยปรกติของกรุป G ซึ่ง H และ G/H ต่างเป็นกรุปก่อกำเนิดแบบจำกัดแล้ว G เป็นกรุปก่อกำเนิดแบบจำกัด
7. ให้ H เป็นกรุปย่อยของกรุป G และ N เป็นกรุปย่อยปรกติของ G จงพิสูจน์ว่า
   7.1 ถ้า $[G:N]$ และ $|H|$ ต่างเป็นจำนวนจำกัดซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กันแล้ว H เป็นกรุปย่อยของ N
   7.2 ถ้า $[G:H]$ และ $|N|$ ต่างเป็นจำนวนจำกัดซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กันแล้ว N เป็นกรุปย่อยของ H
8. ให้ H เป็นกรุปย่อยวัฏจักรของกรุป G จงพิสูจน์ว่าถ้า H เป็นกรุปย่อยปรกติแล้วทุกๆ กรุปย่อยของ H เป็นกรุปย่อยปรกติของ G

1.5 กรุปสมสัณฐาน

ความเข้าใจได้ของมนุษย์เกิดจากความสามารถในการแยกแยะและจดจำ ความเหมือนหรือความแตกต่างและความสัมพันธ์กันของสรรพสิ่ง ในพจนานุกรมบอกเราว่าสิ่งสองสิ่งสัมพันธ์กันแบบสมสัณฐาน ถ้าสองสิ่งนั้นมีโครงสร้างเหมือนกัน สมสัณฐานจึงเป็นศูนย์กลางของการศึกษาในหลายๆ สาขาของวิชาคณิตศาสตร์และซึมแทรกอยู่ในทุกๆ การให้เหตุผลเชิงนามธรรม ตัวอย่างเช่น สมสัณฐานในวิชาเรขาคณิตมีหลายชนิด ชนิดง่ายที่สุดและคุ้นเคยกันดีคือ "การเท่ากันทุกประการ (congruence)" และ "รูปคล้าย (similar)" รูปเรขาคณิตสองรูปเท่ากันทุกประการถ้ามีการเคลื่อนย้ายบนระนาบส่งรูปหนึ่งไปบนอีกรูปหนึ่ง และรูปเรขาคณิตสองรูปคล้ายกันถ้ามีการเลื่อนทางขนานบนระนาบส่งรูปหนึ่งไปบนอีกรูปหนึ่งในลักษณะ"หด" หรือ "ยืด" ด้วยอัตราส่วนคงตัว ดังรูปข้างล่างนี้



ถ้าสังเกตให้ดีจะเห็นว่า "การเคลื่อนย้าย" หรือ "การเลื่อนทางขนาน" ที่กล่าวถึงในสมสัณฐานของวิชาเรขาคณิตทั้งสองตัวอย่างก็คือฟังก์ชันระหว่างเซตสองเซตที่เป็นแบบหนึ่งต่อหนึ่งและทั่วถึงซึ่งยืนยงโครงสร้างตามลำดับ

ในเรื่องกรุป ถ้า $G_1 = \{0,1,2\}$ และ $G_2 = \{e,a,b\}$ เป็นกรุปสองกรุปภายใต้การดำเนินการ $+$ บน G_1 และการดำเนินการ $\cdot$ บน G_2 ดังแสดงในตารางข้างล่างนี้

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

ตารางของ G_1

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

ตารางของ G_2

แม้ว่า G_1 และ G_2 ไม่ใช่กรุปเดียวกัน แต่มีโครงสร้างเหมือนกันซึ่งจะกล่าวว่าสมสัณฐานกัน และโดยความเป็นจริง เรามีฟังก์ชันจาก G_1 ไปยัง G_2 ที่เป็นแบบหนึ่งต่อหนึ่งและทั่วถึงซึ่งยืนยงการดำเนินการของทั้งสองกรุป ดังนี้

$$\begin{pmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ e & a & b \end{pmatrix}$$

โดยทั่วไป การสมสัณฐานกันของกรุปสองกรุป จะต้องมีฟังก์ชัน θ ชนิดหนึ่งต่อหนึ่งและทั่วถึงระหว่างกรุปทั้งสองในลักษณะที่ยืนยงการดำเนินการของทั้งสองกรุป กล่าวคือสำหรับทุกๆ คู่ $a,b \in G_1$ ถ้า $\theta(a) = a'$ และ $\theta(b) = b'$ แล้ว $\theta(ab) = a'b'$ นั่นคือถ้า θ ส่ง a ไปยัง a' และส่ง b ไปยัง b' แล้ว θ ต้องส่ง ab ไปยัง $a'b'$ เพราะจะทำให้ θ แปลงตารางการคูณของ G_1 ไปเป็นตารางการคูณของ G_2 ดังนี้

G_1		b		G_2		b'
		$\vdots$				$\vdots$
a	$\cdots$	ab	$\xrightarrow[\text{แทน } x \text{ ด้วย } \theta(x) \text{ สำหรับทุกๆ } x]{}$	a'	$\cdots$	$a'b'$

เราอาจกล่าวสถานการณ์ของการสมสัณฐานกันของกรุปได้อีกอย่างหนึ่งว่า กรุปสองกรุปจะสมสัณฐานกัน ถ้ากรุปทั้งสองเป็นเสมือนกรุปเดียวกัน ต่างกันเฉพาะชื่อของสมาชิกในแต่ละกรุป ดังนั้นถ้าเปลี่ยนชื่อสมาชิกในกรุปหนึ่งให้เหมือนกับของอีกกรุปหนึ่งแล้ว กรุปทั้งสองจะเป็นกรุปเดียวกันและฟังก์ชันที่ส่งแบบยืนยงการดำเนินการก็คือเครื่องมือการเปลี่ยนชื่อนั่นเอง

1.5.1 **บทนิยาม** ให้ G และ H เป็นกรุปและ $\theta : G \to H$ เรียก θ ว่า *สมสัณฐาน (isomorphism)* ถ้า θ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึงซึ่ง $\theta(ab) = \theta(a)\theta(b)$ ทุกๆ $a,b \in G$ และถ้ามีสมสัณฐานจาก G ไปทั่วถึง H จะกล่าวว่า G *สมสัณฐานกับ (isomorphic)* H และเขียนแทนด้วยสัญลักษณ์ $G \cong H$

ขอให้สังเกตว่าในสมการ $\theta(ab) = \theta(a)\theta(b)$ นั้น ab เป็นผลการดำเนินการของ G ส่วน $\theta(a)\theta(b)$ เป็นผลการดำเนินการใน H

ปัญหาที่ตามมาก็คือ จะทราบได้อย่างไร หรือแสดงได้อย่างไรว่า กรุปสองกรุป G และ H สมสัณฐานกันหรือไม่ สำหรับในกรณีที่กรุปสองกรุปสมสัณฐานกันอาจแสดงได้ไม่ยาก เพราะตามความหมายหรือบทนิยามบอกให้เรากระทำตามขั้นตอนต่อไปนี้

1. "หา" หรือ "สร้าง" ฟังก์ชัน $\theta : G \to H$ (ในการสร้าง เราอาจคาดเดามาก่อนแล้วว่า θ น่าจะเป็นสมสัณฐาน)
2. พิสูจน์ว่า θ ในข้อ 1 เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง
3. พิสูจน์ว่า θ ในข้อ 1 สอดคล้องสมการ $\theta(ab) = \theta(a)\theta(b)$ ทุกๆ $a,b \in G$

ตัวอย่างเช่นถ้าให้ $\mathbb{R}$ แทนกรุปของจำนวนจริงทั้งหมดภายใต้ "การบวก +" แบบปกติและ $\mathbb{R}^+$ แทนกรุปของจำนวนจริงบวกทั้งหมดภายใต้ "การคูณ" แบบปกติ แล้วเป็นที่น่าสนใจว่ากรุปทั้งสองนี้สมสัณฐานกันหรือไม่ซึ่งเราอาจเดาว่ากรุปทั้งสองสมสัณฐานกัน ทำให้เราต้องพิสูจน์ข้อคาดเดานี้ด้วยขั้นตอนที่กล่าวไว้ในย่อหน้าก่อน ดังนี้

1. เราคาดเดาด้วยสมบัติของฟังก์ชันเชิงกำลังจากที่เคยศึกษามาว่า $\theta : \mathbb{R} \to \mathbb{R}^+$ ซึ่งนิยามโดย $\theta(x) = e^x$ ทุกๆ จำนวนจริง x **อาจ**เป็นสมสัณฐานที่ต้องการ
2. ตรวจสอบว่า θ ที่คาดเดาในข้อ 1 เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งโดยให้ a และ b เป็นจำนวนจริงซึ่ง $e^a = e^b$ แล้วโดยการหาภาพของฟังก์ชันลอการิทึมธรรมชาติจะได้ $a = b$ ต่อไปตรวจสอบว่า θ เป็นฟังก์ชันชนิดทั่วถึงโดยให้ y เป็นจำนวนจริงบวกแล้ว $y = e^{\ln y} = \theta(\ln y)$ ดังนั้นมีจำนวนจริง $x = \ln y$ ซึ่ง $\theta(x) = y$ เพราะฉะนั้น θ ที่คาดเดาไว้เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง
3. ตรวจสอบหรือพิสูจน์ว่า θ สอดคล้องสมการ $\theta(ab) = \theta(a)\theta(b)$ สำหรับทุกๆ จำนวนจริง a และ b ด้วยการประยุกต์ความจริงที่รู้จักกันเป็นอย่างดีว่า $e^{a+b} = e^a e^b$ (และด้วยเหตุผลนี้ จึงอาจตอบคำถามว่าทำไมจึงเลือกฟังก์ชันเชิงกำลังเป็นสมสัณฐาน)

เพราะฉะนั้น $(\mathbb{R};+) \cong (\mathbb{R}^+;\cdot)$

สำหรับตัวอย่างกรณีกรุปจำกัด เราอาจบอกความเป็นสมสัณฐานกันโดยดูง่ายๆ จากตารางการดำเนินการของทั้งสองกรุป เช่นกรุป $G=\{1,-1,i,-i\}$ กับกรุป $\mathbb{Z}_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$ ซึ่งมีตารางการคูณและตารางการบวกแสดงตามลำดับ ดังข้างล่างนี้

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

จะเห็นว่าถ้าเราแทน $\bar{0}$ ด้วย 1 แทน $\bar{1}$ ด้วย i แทน $\bar{2}$ ด้วย -1 และแทน $\bar{3}$ ด้วย $-i$ แล้วตารางการดำเนินการทั้งสองจะเป็นตารางเดียวกัน นั่นคือเราได้มีการกำหนดฟังก์ชัน $\theta:\mathbb{Z}_4\to G$ โดย $\theta(\bar{0})=1,\ \theta(\bar{1})=i,\ \theta(\bar{2})=-1$ และ $\theta(\bar{3})=-i$ แล้วเห็นได้ชัดว่า θ เป็นสมสัณฐาน

ขอให้สังเกตว่า $\bar{\theta}:\mathbb{Z}_4\to G$ ซึ่งนิยามโดย $\bar{\theta}(\bar{0})=1,\ \ \bar{\theta}(\bar{1})=-i,\ \ \bar{\theta}(\bar{2})=-1$ และ $\bar{\theta}(\bar{3})=i$ ก็เป็นสมสัณฐานเช่นเดียวกัน

สำหรับกรณีกรุปสองกรุป**ไม่**สมสัณฐานกัน เราต้องแสดงว่า**ทุก ๆ** ฟังก์ชันที่ส่งจากกรุปหนึ่งไปยังอีกกรุปหนึ่งไม่เป็นสมสัณฐาน นั่นคือไม่ใช่ฟังก์ชันหนึ่งต่อหนึ่ง หรือไม่ใช่ฟังก์ชันทั่วถึง หรือมีคู่สมาชิกในกรุปซึ่งเป็นโดเมนที่ทำให้ฟังก์ชันไม่สอดคล้องสมการ $\theta(ab)=\theta(a)\theta(b)$ จะเห็นว่าอาจเป็นการยากในทางปฏิบัติที่จะแสดงให้ครบทุกๆ ฟังก์ชันได้ เราจึงต้องหาวิธีการอื่นเพื่อแสดงว่ากรุปสองกรุปไม่สมสัณฐานกัน

เมื่อพิจารณาความหมายของการเป็นกรุปที่สมสัณฐานกัน ซึ่งดังกล่าวไว้แล้วว่ากรุปทั้งสองนั้นเป็นเสมือนกรุปเดียวกัน ต่างกันเฉพาะชื่อของสมาชิกในแต่ละกรุปเท่านั้น แสดงว่ากรุปทั้งสองมีสมบัติต่างๆ เหมือนๆ กัน ดังนั้นถ้ากรุปหนึ่งมีสมบัติอย่างหนึ่งที่อีกกรุปหนึ่งไม่มีสมบัตินั้น จะแสดงว่ากรุปทั้งสองไม่สมสัณฐานกัน และตัวอย่างของสมบัติที่เรานิยมอ้าง เพื่อแสดงว่ากรุปสองกรุปไม่สมสัณฐานกัน ตัวอย่างเช่น

1. กรุปหนึ่งเป็นอาบีเลียนกรุป แต่อีกกรุปหนึ่งไม่เป็น
2. แต่ละสมาชิกในกรุปหนึ่งเป็นตัวผกผันของตัวเอง แต่สมาชิกของอีกกรุปหนึ่งไม่เป็น
3. กรุปหนึ่งก่อกำเนิดโดยสมาชิกสองตัว แต่สมาชิกสองตัวใดๆ ในอีกกรุปหนึ่งจะไม่ก่อกำเนิดกรุปนั้น

ตัวอย่างเช่นถ้า $\mathbb{R}^*$ แทนเซตของจำนวนจริงที่ไม่ใช่ศูนย์ทั้งหมดแล้ว $\mathbb{R}^*$ กับการคูณแบบปกติเป็นกรุปซึ่งไม่สมสัณฐานกับกรุป $\mathbb{R}$ กับการบวกแบบปกติ เพราะว่า 1 เป็นเอกลักษณ์ของ $\mathbb{R}^*$

และมี $-1 \in \mathbb{R}^*$ ซึ่ง $(-1)(-1)=1$ ในขณะที่ 0 เป็นเอกลักษณ์ของ $\mathbb{R}$ แต่ไม่มีสมาชิก x ใดๆ ใน $\mathbb{R}$ ซึ่ง $x+x=0$ เป็นต้น

อย่างไรก็ตาม เราอาจแสดงว่า $\mathbb{R}$ ไม่สมสัณฐานกับ $\mathbb{R}^*$ อีกวิธีหนึ่งโดยสมมติว่ามีสมสัณฐาน $\theta : \mathbb{R} \to \mathbb{R}^*$ และสังเกตว่าสมสัณฐานจะส่งเอกลักษณ์ไปยังเอกลักษณ์ (แบบฝึกหัด 1.5 ข้อ 1) ดังนั้น $\theta(0)=1$ และเพราะ $-1 \in \mathbb{R}^*$ และ θ เป็นฟังก์ชันทั่วถึง ทำให้มี $x \in \mathbb{R}$ ซึ่ง $\theta(x)=-1$ และได้ $\theta(2x)=\theta(x+x)=\theta(x)\theta(x)=(-1)(-1)=1=\theta(0)$ แต่ θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง จึงได้ $2x=0$ นั่นคือ $x=0$ ดังนั้น $\theta(0)=-1$ และ $\theta(0)=1$ ทำให้ θ ไม่เป็นฟังก์ชัน เกิดเป็นข้อขัดแย้งกันเอง เพราะฉะนั้นไม่มีสมสัณฐานจาก $\mathbb{R}$ ไปยัง $\mathbb{R}^*$

ถ้า G เป็นกรุป เห็นได้ชัดว่าฟังก์ชันเอกลักษณ์ 1_G เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G ไปทั่วถึง G และ $1_G(ab)=ab=1_G(a)1_G(b)$ ทุกๆ $a,b \in G$ ดังนั้น $G \cong G$

ถ้า G และ H เป็นกรุปซึ่ง $G \cong H$ แล้วมีสมสัณฐาน $\theta : G \to H$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ทำให้มี θ^{-1} เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก H ไปทั่วถึง G ยิ่งไปกว่านั้นแต่ละ $c,d \in H$ มี $a,b \in G$ ซึ่ง $\theta^{-1}(c)=a$ และ $\theta^{-1}(d)=b$ ทำให้ได้ $\theta(ab)=\theta(\theta^{-1}(c))\theta(\theta^{-1}(d))=cd$ ดังนั้น $\theta^{-1}(cd)=ab=\theta^{-1}(c)\theta^{-1}(d)$ ซึ่งแสดงว่า θ^{-1} เป็นสมสัณฐานทำให้ได้ $H \cong G$

ถ้า G, H และ K เป็นกรุปซึ่ง $G \cong H$ และ $H \cong K$ แล้วมีสมสัณฐาน $\theta : G \to H$ และ $\varphi : H \to K$ ดังนั้นฟังก์ชันประกอบ $\varphi \circ \theta : G \to K$ เป็นชนิดหนึ่งต่อหนึ่งและทั่วถึง และถ้า $a,b \in G$ แล้ว $\theta(ab)=\theta(a)\theta(b)$ โดยที่ $\theta(a)$ และ $\theta(b)$ เป็นสมาชิกของกรุป H จะทำให้ได้ $(\varphi \circ \theta)(ab)$ $=\varphi(\theta(ab))=\varphi(\theta(a)\theta(b))=\varphi(\theta(a))\varphi(\theta(b))=(\varphi \circ \theta)(a)(\varphi \circ \theta)(b)$ ดังนั้น $G \cong K$ จึงสรุปได้เป็นทฤษฎีบทต่อไปนี้

1.5.2 **ทฤษฎีบท** ให้ G, H และ K เป็นกรุป แล้ว

1. $G \cong G$
2. ถ้า $G \cong H$ แล้ว $H \cong G$
3. ถ้า $G \cong H$ และ $H \cong K$ แล้ว $G \cong K$ ❐

ความสำคัญของการสมสัณฐานกันของกรุปคือการกล่าวในเชิงนามธรรมว่ากรุปทั้งสองเปรียบเสมือนเป็นกรุปเดียวกัน จึงเป็นที่น่าสนใจที่จะถามหากรุปทั้งหมดที่สมสัณฐานกับกรุปที่รู้จักหรือกรุปที่กำหนด เราจึงสนใจศึกษาหาวิธีกำหนดรูปแบบทั่วไปของกรุป

สมมติเราพิจารณาตารางการคูณของกรุปๆ หนึ่ง โดยพิจารณาการคูณของสมาชิกสองตัวที่ไม่ใช่เอกลักษณ์ทั้งคู่ซึ่งขอกำหนดเป็นสัญลักษณ์ a และ b ถ้าความสัมพันธ์ของสมาชิกทั้งสองคือ $a^3=b^2=e$ และ $ba=a^2b$ จะเห็นว่าไม่ว่าจะกำหนดแถวผลคูณในรูปใดมาก็ตาม จะได้ผลคูณเป็น

e, a, a^2, b หรือ a^2b ตัวใดตัวหนึ่งเสมอ (เช่นผลคูณ $aba^2b^2a^3b^5a^4$ คือ $aba^2eeba = aba^2ba = aba^2a^2b = aba^4b = abab = aa^2bb = a^3b^2 = ee = e$ เป็นต้น) และสมาชิกทั้งหกตัวนี้ต่างกันทั้งหมด ตัวอย่างเช่นถ้า $ab = a^2b$ แล้วโดยกฎการตัดออกจะได้ $b = ab$ และได้ $a = e$ ซึ่งเกิดเป็นข้อขัดแย้งกันเองเป็นต้น และสังเกตว่าในการประยุกต์ความสัมพันธ์ดังกล่าวเพื่อคำนวณผลคูณในรูปใดก็ตาม จะเป็นไปตามข้อสมมติว่ากฎการเปลี่ยนหมู่เป็นจริง ดังนั้นตารางการคูณนี้จึงกำหนดกรุปที่สมสัณฐานกับกรุปสมมาตร S_3 หรือกรุปการสมมาตร D_3 และจะเห็นว่าการกล่าวถึงกรุปในย่อหน้านี้ก็ไม่ได้ชี้เฉพาะด้วยสมาชิกของ S_3 หรือ D_3 ดังนั้นการกล่าวถึงกรุปที่สมสัณฐานกับ S_3 หรือ D_3 เราจึงนิยมใช้สัญลักษณ์แทนด้วย

$$< a,b \mid a^3 = b^2 = e, ba = a^2b >$$

และสำหรับกรุปนามธรรมอื่นๆ เราก็สามารถกระทำได้ในลักษณะเช่นเดียวกัน

1.5.3 **บทนิยาม** ให้ $a,b,c,...$ เป็นสัญลักษณ์และ $R_1, R_2, ...$ เป็นความสัมพันธ์ของ $a,b,c,...$ เราใช้สัญลักษณ์ $< a,b,c,... \mid R_1, R_2, ... >$ แทนกรุปเล็กสุดที่ทำให้ความสัมพันธ์ $R_1, R_2, ...$ เหล่านี้กำหนดการคูณบนเซตที่ประกอบด้วย $a,b,c,...$ กับเซตนี้เป็นกรุป

เราเรียกกรุปเช่นนี้ว่ากรุป *ก่อกำเนิดโดย (generated by)* $a,b,c,...$ และเรียก $a,b,c,...$ ว่า *ตัวก่อกำเนิด (generators)*

สังเกตว่า โดยความเป็นจริงผลคูณของสมาชิกในกรุปที่ก่อกำเนิดโดย $a,b,c,...$ ประกอบด้วยสัญลักษณ์ $a^{-1}, b^{-1}, c^{-1}, ...$ ด้วย แต่เพื่อหลีกเลี่ยงสัญลักษณ์เหล่านี้ จึงใช้ความสัมพันธ์ในรูป $a^r = e$ เมื่อ r เป็นจำนวนเต็มบวกซึ่งทำให้ได้ $a^{-1} = a^{r-1}$

เราทราบจากหัวข้อ 1.3 แล้วว่า *กรุปวัฏจักร (cyclic groups)* คือกรุปที่ประกอบด้วยสมาชิกที่เขียนได้ในรูปกำลังต่างๆ ของสมาชิกตัวหนึ่งของกรุป ดังนั้นกรุปวัฏจักรอันดับ n คือกรุปที่มีเอกภพคือเซตในรูป $\{e, a, a^2, ..., a^{n-1}\}$ และสอดคล้องความสัมพันธ์ $ae = a = ea$, $a^n = e$ และกฎการคูณ $a^{r+s} = a^r a^s$ โดยที่ $r+s$ หมายถึงผลบวกที่ลดทอนโดยความสัมพันธ์มอดูโล n [เช่นถ้า $n = 6$, $r = 3, s = 5$ แล้ว $r+s = 8$ ซึ่งลดทอนโดยความสัมพันธ์มอดูโล 6 แล้วเท่ากับ 2 เป็นต้น ในกรณีทั่วไปเราเขียน $r+s = qn+t$ แล้ว t จะคือจำนวนที่ลดทอนโดยความสัมพันธ์มอดูโล n ของ $r+s$] และถ้า $t = 0$ จะเขียน $a^t = a^0 = e$

กฎการคูณของกรุปวัฏจักรอันดับ n ในย่อหน้าก่อนสอดคล้องกับกฎการเปลี่ยนหมู่ เพราะ $a^t(a^r a^s) = a^t a^{r+s} = a^{t+(r+s)} = a^{(t+r)+s} = a^{t+r} a^s = (a^t a^r) a^s$ นอกจากนี้ตัวผกผันของ a^r คือ a^{n-r}

ถ้าใช้สัญลักษณ์ C_n แทน *กรุปวัฏจักรอันดับ* n แล้ว C_n เป็นกรุปจำกัดที่เขียนได้ในรูปของตัวก่อกำเนิดและความสัมพันธ์ของตัวก่อกำเนิด ดังนี้

$$C_n = <a|a^n = e>$$

ส่วนกรุปวัฏจักรอันดับอนันต์ที่มี a เป็นตัวก่อกำเนิด เราแทนด้วยสัญลักษณ์ C_∞ ซึ่งเขียนได้ในรูปแบบดังนี้

$$C_\infty = <e, a^{\pm r}|r = 0,1,2,\ldots>$$

ทฤษฎีบทต่อไป แสดงการจำแนกกรุปวัฏจักรทั้งหมด

1.5.4 **ทฤษฎีบท** กรุปวัฏจักรอันดับ n สมสัณฐานกับกรุปการบวก $(\mathbb{Z}_n;+)$ ของจำนวนเต็มมอดุโล n และกรุปวัฏจักรอันดับอนันต์สมสัณฐานกับกรุปการบวก $(\mathbb{Z};+)$ ของจำนวนเต็มทั้งหมด

บทพิสูจน์ ให้ $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$ และนิยาม $f: C_n \to Z_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ โดย $f(a^r)$ $= \overline{r}$ ซึ่งทำให้ได้ $f: \begin{array}{lll} e \to \overline{0} & a^3 \to \overline{3} & a^6 \to \overline{6} \\ a \to \overline{1}, & a^4 \to \overline{4}, & \vdots \\ a^2 \to \overline{2} & a^5 \to \overline{5} & a^r \to \overline{r} \end{array}$ และอื่นๆ ซึ่งเห็นได้ชัดว่า f เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง นอกจากนี้

$$f(a^r a^s) = f(a^{r+s}) = f(a^t) \quad [\text{โดยที่ } 0 \le t \le n-1 \text{ และ } r+s \equiv t(\bmod n)]$$

$$= \overline{t} = \overline{r} + \overline{s} \quad [\text{เพราะว่า } r+s \equiv t(\bmod n)] \quad = f(a^r) + f(a^s)$$

ขอให้สังเกตว่าเราใช้ + แทนการคูณในกรุป $(Z_n;+)$ ดังนั้น f เป็นฟังก์ชันสมสัณฐาน

ต่อไปให้ $C_\infty = \{e, a^{\pm 1}, a^{\pm 2}, \ldots\}$ เป็นกรุปวัฏจักรอันดับอนันต์และนิยาม $f: C_\infty \to Z$ ในทำนองเดียวกันโดย $f(a^r) = r$ ซึ่งทำให้ได้ $f: \begin{array}{lll} e \to 0 & a^2 \to \overline{2} & a^{-3} \to -3 \\ a \to 1, & a^{-2} \to -2, & a^4 \to 4 \\ a^{-1} \to -1 & a^3 \to 3 & a^{-4} \to -4 \end{array}$ และอื่นๆ ซึ่งเห็นได้ชัดว่า f เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง ยิ่งไปกว่านั้น

$$f(a^r a^s) = f(a^{r+s}) = r + s = f(a^r) + f(a^s)$$

ดังนั้น f เป็นฟังก์ชันสมสัณฐาน ❐

ขอปิดท้ายหัวข้อนี้ด้วยการจำแนกกรุป (ภายใต้การสมสัณฐาน) อันดับ 1 ถึง 5

กรุปอันดับ 1 อันดับ 2 อันดับ 3 และอันดับ 5 :

โดยทฤษฎีบทของลากรองจ์และภายใต้เงื่อนไขการสมสัณฐาน มีกรุปอันดับ 1,2,3 และ 5 เพียงอย่างละกรุปเดียวคือกรุปวัฏจักร $C_1 = \{e\}$, $C_2 = \{e, a\} \cong \mathbb{Z}_2$, $C_3 = \{e, a, a^2\} \cong \mathbb{Z}_3$ และ $C_5 = \{e, a, a^2, a^3, a^4\} \cong \mathbb{Z}_5$ ตามลำดับ

กรุปอันดับ 4: โดยการประยุกต์ทฤษฎีบท 1.3.4 มีกรุปอันดับ 4 ซึ่งเป็นกรุปวัฏจักร $G = C_4 = <a|a^4 = e> = \{e, a, a^2, a^3\} = \mathbb{Z}_4$ เมื่อมี $a \in G$ ซึ่ง $a^4 = e$ แต่ถ้าไม่มีสมาชิกตัวใดใน G ที่มีอันดับ 4 โดยทฤษฎีบทของลากรองจ์ ทุกๆ สมาชิกของ G ที่ไม่ใช่เอกลักษณ์มีอันดับ 2 ดังนั้น $G =$

$\{e, a, b, c\}$ โดยที่ $a^2 = b^2 = c^2 = e$ เพราะฉะนั้น $c = ab$ และ $c^2 = (ab)^2 = e$ ทำให้ได้ $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ นั่นคือ

$$G = < a, b | a^2 = b^2 = e, ab = ba > = \{e, a, b, ab\}$$

เราเรียกชื่อกรุปนี้ตามชื่อของท่านผู้ค้นพบว่า *กรุปไคลน์-4 (Klein 4-group)* และแทนด้วยสัญลักษณ์ K_4 โดยมีตารางการคูณของ K_4 แสดงดังนี้

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

ตัวอย่างรูปธรรมของกรุปไคลน์-4 เช่นกรุปของวิธีเรียงสับเปลี่ยนซึ่งเป็นกรุปย่อยของกรุปการสมมาตร S_4 ดังนั้นตารางการคูณจึงเป็นไปตามกฎการคูณของ S_4 ดังแสดงตามตารางข้างล่างนี้ และจะเห็นว่าเป็นตารางการคูณเดียวกันกับของ K_4 ข้างต้น

	(1)	(1 2)	(3 4)	(1 2)(3 4)
(1)	(1)	(1 2)	(3 4)	(1 2)(3 4)
(1 2)	(1 2)	(1)	(1 2)(3 4)	(3 4)
(3 4)	(3 4)	(1 2)(3 4)	(1)	(1 2)
(1 2)(3 4)	(1 2)(3 4)	(3 4)	(1 2)	(1)

แบบฝึกหัด 1.5

1. ให้ G และ H เป็นกรุปและ $\theta : G \to H$ เป็นสมสัณฐาน จงพิสูจน์ว่า
   1.1 $\theta(e_G) = e_H$ [นั่นคือสมสัณฐานส่งเอกลักษณ์ไปยังเอกลักษณ์]
   1.2 $\theta(a^{-1}) = \theta(a)^{-1}$ ทุกๆ $a \in G$ [นั่นคือสมสัณฐานส่งตัวผกผันของ $a \in G$ ไปยังตัวผกผันของ $\theta(a) \in H$ หรือกล่าวอีกนัยหนึ่งคือ $\theta(a) = b \Leftrightarrow \theta(a^{-1}) = b^{-1}$]
   1.3 ถ้า $G = < a >$ เป็นกรุปวัฏจักรแล้ว H เป็นกรุปวัฏจักรซึ่ง $H = < \theta(a) >$ [นั่นคือสมสัณฐานส่งตัวก่อกำเนิดไปยังตัวก่อกำเนิด]

2. ให้ $G=\{x\in\mathbb{R}|x\neq -1\}$ และ $*$ เป็นการดำเนินการบน G ซึ่งนิยามสำหรับทุกๆ $x,y\in G$ โดย $x*y=x+y+xy$ จงแสดงว่า $\theta:\mathbb{R}^*\to G$ นิยามโดย $\theta(x)=x-1$ สำหรับทุกๆ $x\in\mathbb{R}^*$ เป็นสมสัณฐาน
3. ให้ G เป็นกรุปของจำนวนจริง $\mathbb{R}$ ทั้งหมดกับการดำเนินการ $*$ ซึ่งนิยามโดย $x*y=x+y+1$ สำหรับทุกๆ $x,y\in R$ จงแสดงว่ากรุป $\mathbb{R}$ สมสัณฐานกับ G
4. จงแสดงว่ากรุปสองกรุปที่กำหนดในแต่ละข้อต่อไปนี้ สมสัณฐานกันหรือไม่

   4.1 $\mathbb{Z}_6$ และ $\mathbb{Z}_2\times\mathbb{Z}_3$ 4.2 $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ และ D_4

   4.3 S_3 และกรุป $G=\{e,a,a^2,b,c,d\}$ ซึ่งมีตารางการคูณแสดงดังนี้

$\cdot$	e	a	a^2	b	c	d
e	e	a	a^2	b	c	d
a	a	a^2	e	c	d	b
a^2	a^2	e	a	d	b	c
b	b	d	c	e	a^2	a
c	c	b	d	a	e	a^2
d	d	c	b	a^2	a	e

   [**หมายเหตุ** ขอให้สังเกตว่า $c=ab$ และ $d=a^2b$ เราจึงอาจเขียน G ได้ใหม่เป็น $G=\{e,a,a^2,b,ab,a^2b\}$ ซึ่งแสดงว่า G ก่อกำเนิดโดย $\{a,b\}$ โดยที่ a และ b สอดคล้องความสัมพันธ์ $a^3=e=b^2$ และ $ba=a^2b$ นั่นคือ

$$G=\ <a,b|a^3=e=b^2,ba=a^2b>]$$

   4.4 กรุปการบวกของจำนวนเต็มทั้งหมด $\mathbb{Z}$ และของจำนวนตรรกยะทั้งหมด $\mathbb{Q}$

   4.5 กรุปของจำนวนตรรกยะทั้งหมด $\mathbb{Q}$ ภายใต้การบวกและกรุปของจำนวนตรรกยะบวกทั้งหมด $\mathbb{Q}^+$ ภายใต้การคูณ
5. จงพิสูจน์ว่ากรุปควอเทอร์เนียนสมสัณฐานกับกรุป $G=<a,b|a^4=e,a^2=b^2,ba=a^3b>$
6. ให้ n เป็นจำนวนเต็มบวกคงตัว จงพิสูจน์ว่ากรุป $\{kn|k\in\mathbb{Z}\}\subseteq\mathbb{Z}$ ภายใต้การบวกปกติสมสัณฐานกับกรุปการบวก $\mathbb{Z}$
7. จงพิสูจน์ว่าเซต $\{\sigma\in S_n|\sigma(n)=n\}$ เป็นกรุปย่อยของ S_n ซึ่งสมสัณฐานกับ S_{n-1}
8. จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_2\times\mathbb{Z}_2$ พร้อมทั้งแสดงว่า $\mathbb{Z}_2\times\mathbb{Z}_2$ สมสัณฐานกับ $\mathbb{Z}_4$ หรือไม่

9. ให้ G, H, K และ T เป็นกรุป จงพิสูจน์ว่า

9.1 $G \times H \cong H \times G$ และถ้า $G \cong H$ และ $K \cong T$ แล้ว $G \times K \cong H \times T$

9.2 $G \cong G \times \{e_H\}$ และ $H \cong \{e_G\} \times H$

9.3 G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $\theta : G \to G$ นิยามโดย $\theta(x) = x^{-1}$ ทุกๆ $x \in G$ เป็นสมสัณฐาน

10. ให้ G และ H เป็นกรุปและ $\theta : G \to H$ เป็นสมสัณฐาน จงพิสูจน์ว่า

10.1 G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ H เป็นกรุปอาบีเลียน

10.2 G เป็นกรุปวัฏจักร ก็ต่อเมื่อ H เป็นกรุปวัฏจักร

10.3 G เป็นกรุปก่อกำเนิดแบบจำกัด ก็ต่อเมื่อ H เป็นกรุปก่อกำเนิดแบบจำกัด

10.4 G เป็นกรุปเชิงเดียว ก็ต่อเมื่อ H เป็นกรุปเชิงเดียว

[**บทนิยาม** เรากล่าวว่า G เป็น *กรุปเชิงเดียว (simple group)* ถ้า G และ $\{e\}$ เท่านั้นที่เป็นกรุปย่อยปรกติของ G]

11. ให้ K และ N เป็นกรุปย่อยปรกติของกรุป G จงพิสูจน์ว่า

11.1 $< N \cup K >$ เป็นกรุปย่อยปรกติของ G

11.2 ถ้า $N \cap K = \{e\}$ และ $G = < N \cup K >$ แล้ว $G/N \cong K$

12. ให้ N_1 เป็นกรุปย่อยปรกติของกรุป G_1 และ N_2 เป็นกรุปย่อยปรกติของกรุป G_2 จงพิสูจน์ว่า $N_1 \times N_2$ เป็นกรุปย่อยปรกติของ $G_1 \times G_2$ และ $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$

1.6 ทฤษฎีบทการแทนของกรุป

หัวข้อ 1.5 ได้แสดงให้เห็นว่ากรุปวัฏจักรไม่ใช่กรุปนามธรรมภายใต้การสมสัณฐานหรือกล่าวอีกนัยหนึ่งได้ว่า แม้จะกำหนดกรุปวัฏจักรนามธรรม เราจะทราบโครงสร้างของกรุปนั้น และเมื่อเริ่มต้นกำเนิดทฤษฎีกรุปได้นิยามว่ากรุปคือกรุปของวิธีเรียงสับเปลี่ยนและได้ศึกษาสมบัติของกรุปเหล่านี้มาอย่างยาวนาน ทำให้เรารู้จักกรุปของวิธีเรียงสับเปลี่ยนกันเป็นอย่างดี และต่อมาแม้จะขยายนิยามกรุปในเชิงนามธรรม เรายังต้องการเห็นตัวอย่างรูปธรรมของกรุปเพื่อให้เข้าใจโครงสร้างของกรุปนามธรรมเหล่านั้น จนกระทั่งนักคณิตศาสตร์ชาวอังกฤษนามว่า อาร์เทอร์ เคย์เลย์ (Arthur Cayley) ซึ่งมีชีวิตในช่วงคริสตศักราช 1821 – 1895 ได้พิสูจน์ทฤษฎีบทตัวแทนของกรุปนามธรรมซึ่งกล่าวว่า "ทุกๆ กรุปสมสัณฐานกับกรุปของวิธีเรียงสับเปลี่ยน" ทำให้เห็นว่าแม้จะนิยามกรุปเชิงนามธรรมอย่างไร กรุปทั้งหมดก็คือกรุปของวิธีเรียงสับเปลี่ยนดังที่ศึกษากันมาแต่เดิม ทำให้สมบัติต่างๆ ของกรุปที่ศึกษากันมาอย่างยาวนานเป็นสมบัติของกรุปนามธรรมด้วย

ในหัวข้อนี้ เราแสดงการพิสูจน์ทฤษฎีบทของเคย์เลย์ และตัวอย่างการประยุกต์ทฤษฎีบทของเคย์เลย์ ในการหากรุปของวิธีเรียงสับเปลี่ยนซึ่งเป็นตัวแทนของกรุปที่กำหนด

1.6.1 ทฤษฎีบทของเคย์เลย์ (Cayley's Theorem) สำหรับแต่ละกรุป G จะมีกรุปย่อย $\bar{G}$ ของกรุปสมมาตร $A(G)$ ซึ่ง $G \cong \bar{G}$

บทพิสูจน์ ให้ G เป็นกรุป เราต้องการหากรุป $\bar{G}$ ซึ่งเป็นกรุปย่อยของ $A(G)$ ที่ทำให้ $G \cong \bar{G}$ ดังนั้นขนาดของ $\bar{G}$ ต้องเท่ากับขนาดของ G และสมาชิกของ $\bar{G}$ จะเป็นวิธีเรียงสับเปลี่ยนบน G นั่นคือ แต่ละ $a \in G$ เคย์เลย์สร้างฟังก์ชัน(ที่ขึ้นกับ a) จาก G ไปยัง G ซึ่งเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงโดยใช้สัญลักษณ์แทนด้วย π_a และนิยามให้ $\pi_a(x) = ax$ ทุกๆ $x \in G$ และพิสูจน์ว่า

1. $\pi_a \in A(G)$ สำหรับแต่ละ $a \in G$

1.1 π_a เป็นฟังก์ชันหนึ่งต่อหนึ่ง:ให้ $x_1, x_2 \in G$ โดยที่ $\pi_a(x_1) = \pi_a(x_2)$ แล้วโดยนิยามของ π_a จะได้ $ax_1 = ax_2$ ซึ่งทำให้ได้โดยกฎการตัดออกในกรุปว่า $x_1 = x_2$

1.2 π_a เป็นฟังก์ชันทั่วถึง: ให้ $y \in G$ แล้ว $y = ey = (aa^{-1})y = a(a^{-1}y)$ และเพราะ $a^{-1}y \in G$ ดังนั้นมี $x = a^{-1}y \in G$ ซึ่ง $\pi_a(x) = \pi_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = ey = y$

เมื่อทราบว่า $\pi_a \in A(G)$ ทุกๆ $a \in G$ จึงให้ $\bar{G} = \{\pi_a | a \in G\}$

2. จะแสดงว่า $\bar{G}$ เป็นกรุปย่อยของ $A(G)$

2.1 ให้ $a, b \in G$ และ $x \in G$ แล้ว $(\pi_a \circ \pi_b)(x) = \pi_a(\pi_b(x)) = a(bx) = a(bx) = \pi_{ab}(x)$ เพราะฉะนั้น $\pi_a \circ \pi_b = \pi_{ab} \in A(G)$ นั่นคือ $\bar{G}$ มีสมบัติปิดการคูณของ $A(G)$

2.2 $\pi_e(x) = ex = x$ ทุกๆ $x \in G$ ซึ่งแสดงว่า π_e เป็นฟังก์ชันเอกลักษณ์ ดังนั้น π_e เป็นเอกลักษณ์ของ $\bar{G}$ และของ $A(G)$

2.3 จะได้โดยข้อ 2.1 ว่า $\pi_a \circ \pi_{a^{-1}} = \pi_{aa^{-1}} = \pi_e$ ทุกๆ $a \in G$ ดังนั้น $\pi_{a^{-1}}$ เป็นตัวผกผันของ π_a ซึ่งแสดงว่า $\pi_a^{-1} = \pi_{a^{-1}} \in \bar{G}$

2.4 เห็นได้ชัดว่า $\pi_a \circ \pi_{b^{-1}} = \pi_{ab^{-1}} \in \bar{G}$ ทุกๆ $a, b \in G$

3. จะแสดงว่า $\bar{G}$ สมสัณฐานกับ G ให้ $f : G \to \bar{G}$ นิยามโดย $f(a) = \pi_a$ ทุกๆ $a \in G$

3.1 f เป็นฟังก์ชันหนึ่งต่อหนึ่ง: ให้ $a, b \in G$ ซึ่ง $f(a) = f(b)$ แล้วโดยนิยามของ f จะได้ $\pi_a = \pi_b$ นั่นคือ $\pi_a(x) = \pi_b(x)$ ทุกๆ $x \in G$ จึงเลือก $e \in G$ ทำให้ได้ $\pi_a(e) = \pi_b(e)$ จึงได้ $a = ae = \pi_a(e) = \pi_b(e) = be = b$

3.2 เห็นได้ชัดจากนิยามของ $\bar{G}$ ว่า f เป็นฟังก์ชันทั่วถึง

3.3 สำหรับแต่ละ $a, b \in G$ จะได้ว่า $f(ab) = \pi_{ab} = \pi_a \circ \pi_b = f(a) \circ f(b)$

เพราะฉะนั้น f เป็นสมสัณฐาน ซึ่งเป็นอันจบการพิสูจน์ $\square$

1.6.2 **บทแทรก** ถ้า G เป็นกรุปจำกัด แล้วมีจำนวนเต็มบวก n ซึ่ง G สมสัณฐานกับกรุปย่อยของ S_n

บทพิสูจน์ ให้ $n = |G|$ และ $A(G) = S_n$ แล้วดำเนินการพิสูจน์เช่นเดียวกับทฤษฎีบทของเคย์เลย์ $\square$

1.6.3 **ตัวอย่าง** จะแสดงว่ากรุปไคลน์-4 $K_4 = \{e, a, b, ab\}$ ซึ่งมีตารางการคูณแสดงดังในหัวข้อ 1.5 สมสัณฐานกับกรุปย่อยของกรุปสมมาตร S_4 โดยจะสร้างกรุปย่อย $\overline{G}$ ของ S_4 เช่นเดียวกับในบทพิสูจน์ทฤษฎีบทของเคย์เลย์ นั่นคือแต่ละ $x \in K_4$ กำหนด $\pi_x : K_4 \to K_4$ โดยการคูณทางซ้ายด้วย x กับทุกๆ สมาชิกในโดเมน ซึ่งทำให้ได้สมาชิกทั้งหมดของ $\overline{G}$ เป็นดังนี้

$$\pi_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = \iota_{K_4}, \qquad \pi_a = \begin{pmatrix} e & a & b & c \\ e & a & c & b \end{pmatrix} = (e\ a)(b\ c),$$

$$\pi_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (e\ b)(a\ c), \qquad \pi_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = (e\ c)(a\ b)$$

โดยผลการพิสูจน์ในทฤษฎีบทของเคย์เลย์ จะได้ $\overline{G} = \{\pi_e, \pi_a, \pi_b, \pi_c\}$ เป็นกรุปย่อยของ S_4 ซึ่งสมสัณฐานกับ K_4 โดยที่ $\{\pi_e, \pi_a, \pi_b, \pi_c\} = \{\iota, (e\ a)(b\ c), (e\ b)(a\ c), (e\ c)(a\ b)\}$ สมสัณฐานกับกรุปย่อย $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ ของ S_4 ดังนั้น

$$K_4 \cong \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$ ○

1.6.4 **ตัวอย่าง** เซตกำลัง $P(\{a,b,c\}) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$ กับการดำเนินการ "ผลต่างสมมาตร" เป็นกรุปจำกัด และเราจะหา n และกรุปย่อย H ของ S_n ซึ่ง $H \cong P(\{a,b,c\})$ ซึ่งโดยทฤษฎีบทของเคย์เลย์ n คือขนาดของ $P(\{a,b,c\})$ ซึ่งเท่ากับ $2^3 = 8$ และดำเนินการสร้าง H ดังนี้

$$\pi_e = \iota, \quad \pi_{\{a\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a\} & \phi & \{a,b\} & \{a,c\} & \{b\} & \{c\} & \{a,b,c\} & \{b,c\} \end{pmatrix},$$

$$\pi_{\{b\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{b\} & \{a,b\} & \phi & \{b,c\} & \{a\} & \{a,b,c\} & \{c\} & \{a,c\} \end{pmatrix},$$

$$\pi_{\{c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{c\} & \{a,c\} & \{b,c\} & \phi & \{a,b,c\} & \{a\} & \{b\} & \{a,b\} \end{pmatrix},$$

$$\pi_{\{a,b\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a,b\} & \{b\} & \{a\} & \{a,b,c\} & \phi & \{b,c\} & \{a,c\} & \{c\} \end{pmatrix},$$

$$\pi_{\{a,c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a,c\} & \{c\} & \{a,b,c\} & \{a\} & \{b,c\} & \phi & \{a,b\} & \{b\} \end{pmatrix},$$

$$\pi_{\{b,c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{b,c\} & \{a,b,c\} & \{c\} & \{b\} & \{a,c\} & \{a,b\} & \phi & \{a\} \end{pmatrix},$$

$$\pi_{\{a,b,c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a,b,c\} & \{b,c\} & \{a,c\} & \{a,b\} & \{c\} & \{b\} & \{a\} & \phi \end{pmatrix}$$

ถ้าแทน $\phi \leftrightarrow 1$, $\{a\} \leftrightarrow 2$, $\{b\} \leftrightarrow 3$, $\{c\} \leftrightarrow 4$, $\{a,b\} \leftrightarrow 5$, $\{a,c\} \leftrightarrow 6$, $\{b,c\} \leftrightarrow 7$ และ $\{a,b,c\} \leftrightarrow 8$ จะได้ $\pi_e = (1)$,

$$\pi_{\{a\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 6 & 3 & 4 & 8 & 7 \end{pmatrix} = (12)(35)(46)(78),$$

$$\pi_{\{b\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 7 & 2 & 8 & 4 & 6 \end{pmatrix} = (13)(25)(47)(68),$$

$$\pi_{\{c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 1 & 8 & 2 & 3 & 5 \end{pmatrix} = (14)(26)(37)(58),$$

$$\pi_{\{a,b\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 8 & 1 & 7 & 6 & 4 \end{pmatrix} = (15)(23)(48)(67),$$

$$\pi_{\{a,c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 8 & 2 & 7 & 1 & 5 & 3 \end{pmatrix} = (16)(24)(38)(57),$$

$$\pi_{\{b,c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} = (17)(28)(34)(56),$$

และ $$\pi_{\{a,b,c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (18)(27)(36)(45)$$

ดังนั้นกรุปย่อย H ของ S_8 ซึ่ง $H \cong P(\{a,b,c\})$ คือ

$$H = \{(1),(12)(35)(46)(78),(13)(25)(47)(68),(14)(26)(37)(58),(15)(23)(48)(67),$$
$$(16)(24)(38)(57),(17)(28)(34)(56),(18)(27)(36)(45)\}$$

สังเกตว่าทุกๆ สมาชิกของ H มีอันดับ 2 และเราพิสูจน์ได้ไม่ยากว่า H สมสัณฐานกับกรุป $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ❍

แบบฝึกหัด 1.6

1. การพิสูจน์ทฤษฎีบทของเคย์เลย์ เราจับคู่แต่ละสมาชิก a ในกรุป G ด้วยวิธีเรียงสับเปลี่ยน π_a ซึ่งนิยามโดย $\pi_a(x) = ax$ ทุกๆ $x \in G$ นั่นคือกำหนดด้วยกฎการคูณทางซ้ายทุกๆ สมาชิกของ G ด้วย a จึงเรียก $\overline{G} = \{\pi_a | a \in G\}$ ว่า "*การแทนทางซ้าย (the left representtation)* ของ G" ในทำนองเดียวกันเราอาจกำหนดวิธีเรียงสับเปลี่ยน ρ_a โดยนิยาม $\rho_a(x) = xa$ ทุกๆ $x \in G$ นั่นคือกำหนดด้วยกฎการคูณทางขวาทุกๆ สมาชิกของ G ด้วย a และเรียก $G^* = \{\rho_a | a \in G\}$ ว่า "*การแทนทางขวา (the right representation)* ของ G" และสังเกตว่าการแทนทั้งสองเป็นการแทนเดียวกันสำหรับกรุปอาบีเลียน

   จงพิสูจน์ทฤษฎีบทของเคย์เลย์ด้วยการแทนทางขวา

2. จงหาการแทนทางซ้ายและการแทนทางขวาของกรุปในข้อต่อไปนี้

   2.1 $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$ และ $\mathbb{Z}_2 \times S_3$

   2.2 กรุป P_2 ของเซตย่อยทั้งหมดบนเซต 2 สมาชิก

   2.3 กรุปซึ่งประกอบด้วยเมทริกซ์ 6 ตัวคือ $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $C = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$, $D = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ และ $K = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$ ซึ่งมีตารางการคูณดังนี้

	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	B	A
K	K	B	A	D	C	I

3. จงหาจำนวนเต็มบวก n และกรุปย่อยของ S_n ซึ่งสมสัณฐานกับกรุป $\mathbb{Z}_7^*$ (นั่นคือกรุป $\mathbb{Z}_7 \setminus \{\overline{0}\}$) และกรุป $\mathbb{Z}_2 \times S_3$

1.7 สาทิสสัณฐานและทฤษฎีบทสมสัณฐาน

การศึกษาโครงสร้างพีชคณิตที่มีขนาดใหญ่แต่ซับซ้อนวิธีหนึ่งคือ ศึกษาโครงสร้างพีชคณิตที่มีขนาดเล็กกว่าและซับซ้อนน้อยกว่า เพื่อให้เห็นสมบัติที่ต้องการศึกษานั้นชัดเจนขึ้น สาทิสสัณฐาน

เป็นเครื่องมือสำคัญของวิธีการดังกล่าว เพราะสาทิสสัณฐานเป็นฟังก์ชันจากโครงสร้างคณิตศาสตร์ระบบหนึ่งไปยังอีกระบบหนึ่งที่มีสมบัติยืนยงหรือไม่แปรเปลี่ยนโครงสร้างและไม่จำเป็นต้องเป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้นภาพของสาทิสสัณฐานจะมีขนาดเล็กกว่าหรือเท่ากับโดเมน แต่จะสะท้อนสมบัติบางประการของโดเมน โดยเฉพาะเมื่อต้องการศึกษาสมบัติใดของโครงสร้างโดเมน เราจะหาภาพสาทิสสัณฐานของโดเมนที่มีสมบัตินั้นๆ และศึกษาภาพสาทิสสัณฐานแทน ในหัวข้อนี้ เราจะกล่าวถึงสาทิสสัณฐานระหว่างกรุป สมบัติที่ถ่ายทอดผ่านทางสาทิสสัณฐาน พิสูจน์ทฤษฎีบทหลักมูลของพีชคณิตและทฤษฎีบทสมสัณฐานสามทฤษฎีบท

เราเห็นแล้วว่ากรุปสองกรุปจะสมสัณฐานกัน ถ้ามีฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึงซึ่งแปลงสมาชิกของกรุปหนึ่งไปทั่วถึงอีกกรุปหนึ่ง ในลักษณะที่ทำให้เห็นว่าโครงสร้างของทั้งสองกรุปเหมือนกัน และเพราะภายใต้การแปลงดังกล่าวจะไม่แปรเปลี่ยนโครงสร้างของกรุปทั้งสอง ดังนั้นสำหรับกรุปสองกรุปใดๆ ที่อาจไม่สมสัณฐานกัน เราก็อาจเห็นการแปลงที่ไม่แปรเปลี่ยนโครงสร้างระหว่างกรุปทั้งสองโดยที่การแปลงนั้นอาจไม่เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งหรือไม่เป็นฟังก์ชันทั่วถึง ตัวอย่างเช่นการแปลง θ จากกรุป $\mathbb{Z}_6$ ไปยังกรุป $\mathbb{Z}_3$ ซึ่งกำหนดดังนี้

$$\theta = \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} \\ \bar{0} & \bar{1} & \bar{2} & \bar{0} & \bar{1} & \bar{2} \end{pmatrix}$$

แม้ว่า θ เป็นฟังก์ชันทั่วถึง แต่ก็ไม่ใช่ฟังก์ชันหนึ่งต่อหนึ่งและถ้าเปรียบเทียบตารางการคูณของ $\mathbb{Z}_6$ กับภาพของ $\mathbb{Z}_6$ ภายใต้ θ ดังตารางข้างล่างนี้ จะเห็นว่าตารางของภาพของ $\mathbb{Z}_6$ ภายใต้ θ เป็น

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\xrightarrow[x \text{ ด้วย } f(x)]{\text{แทนที่}}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\xrightarrow[\text{เช่น } 2+2=1 \text{ ปรากฏ 4 ครั้ง}]{\text{กำจัดตัวซ้ำ}}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

ตารางการคูณของ $\mathbb{Z}_3$ ปรากฏซ้ำสี่ครั้งซึ่งแสดงว่า θ ยืนยงการดำเนินการของ $\mathbb{Z}_6$ ทำให้เห็นว่า $\mathbb{Z}_3$ เป็นโครงสร้างบางส่วนของ $\mathbb{Z}_6$

โดยทั่วไปถ้า G และ $\overline{G}$ เป็นกรุปและมีฟังก์ชัน θ ซึ่งแปลง G ไปยัง $\overline{G}$ ในลักษณะยืนยงหรือไม่แปรเปลี่ยนโครงสร้างบางส่วนของ G เราหมายความว่า θ แปลงตารางการคูณของ G ไปเป็นตารางการคูณของ $\overline{G}$ ในลักษณะที่ถ้า $a,b \in G$ ซึ่ง $\theta(a)=a'$ และ $\theta(b)=b'$ แล้ว $\theta(ab)=\theta(a)\theta(b)$ ใน $\overline{G}$ เช่นเดียวกับการแปลงสมสัณฐาน

1.7.1 **บทนิยาม** ให้ G และ $\overline{G}$ เป็นกรุป เรากล่าวว่า $\theta : G \to \overline{G}$ เป็น *สาทิสสัณฐาน (homomorphism)* ถ้า $\theta(ab)=\theta(a)\theta(b)$ สำหรับทุกๆ $a,b \in G$

สังเกตว่า ab ในสมการ $\theta(ab)=\theta(a)\theta(b)$ เป็นผลคูณของสมาชิกในกรุป G ในขณะที่ $\theta(a)\theta(b)$ เป็นผลคูณของสมาชิกในกรุป $\overline{G}$ ดังนั้นสมการ $\theta(ab)=\theta(a)\theta(b)$ แสดงให้ทราบว่าภาพภายใต้สาทิสสัณฐาน θ ของผลคูณใน G เป็นผลคูณของภาพภายใต้ θ ใน $\overline{G}$ จึงเรียกสมบัตินี้ของ θ ว่า "สมบัติยืนยงการดำเนินการ"

ความสัมพันธ์ของสาทิสสัณฐาน θ กับการดำเนินการของ G และ $\overline{G}$ อาจแสดงได้ด้วยแผนภาพต่อไปนี้

$$\begin{tikzcd}
(a,b) \arrow[r, "\cdot"] \arrow[d, "\theta"'] & a\cdot b \arrow[d, "\theta"] \\
(\theta(a),\theta(b)) \arrow[r, "\cdot"'] & \theta(a)\theta(b)=\theta(ab)
\end{tikzcd}$$

จากแผนภาพจะเห็นว่า ถ้าเริ่มต้นที่คู่อันดับ (a,b) แล้วไม่ว่าจะไปทางซ้ายหรือทางขวาของแผนภาพ จะไปสิ้นสุดด้วยผลอย่างเดียวกันโดยสมบัติยืนยงการดำเนินการ เราจึงเรียกแผนภาพในลักษณะนี้ว่า *แผนภาพสลับที่ (commutative diagram)*

สังเกตว่าทุกๆ สมสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ เป็นสาทิสสัณฐาน ดังนั้นตัวอย่างของสมสัณฐานในหัวข้อ 1.5 จึงเป็นตัวอย่างของสาทิสสัณฐาน

1.7.2 **ตัวอย่าง** ให้ θ เป็นฟังก์ชันจากกรุปการบวก $\mathbb{Z}$ ของจำนวนเต็มทั้งหมดไปยังกรุปการบวก $\mathbb{Z}_n$ ของเรซิดิวคลาส มอดูโล n เมื่อ n เป็นจำนวนเต็มบวกซึ่งนิยามโดย $\theta(a)=\overline{a}$ ทุกๆ จำนวนเต็ม a [นั่นคือ θ ส่งแต่ละจำนวนเต็มไปยังเซตสมมูลที่บรรจุ a] แล้ว θ เป็นสาทิสสัณฐานเพราะ $\theta(a+b)=\overline{a+b}=\overline{a}\oplus\overline{b}=\theta(a)\oplus\theta(b)$ ทุกๆ จำนวนเต็ม a และ b ○

1.7.3 **ตัวอย่าง** ให้ G และ H เป็นกรุป แล้ว

1. ถ้า $\theta : G \to H$ นิยามโดย $\theta(a) = e_H$ ทุกๆ $a \in G$ แล้ว θ เป็นสาทิสสัณฐาน เพราะ $\theta(ab) = e_H = e_H \cdot e_H = \theta(a)\theta(b)$ ทุกๆ $a,b \in G$ ยิ่งไปกว่านั้น θ เป็นฟังก์ชันคงตัวเพียงฟังก์ชันเดียวที่เป็นสาทิสสัณฐาน เราจึงเรียก θ ว่า *สาทิสสัณฐานคงตัว (constant homomorphism)*

2. มีสาทิสสัณฐาน $G \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} G \times H \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} H$ สี่ฟังก์ชันซึ่งนิยามตามลำดับโดย $\iota_1(g) = (g,e)$, $\iota_2(h) = (e,h)$, $\pi_1(g,h) = g$ และ $\pi_2(g,h) = h$ ทุกๆ $g \in G$ และ $h \in H$ โดยที่ ι_i เป็นฟังก์ชันหนึ่งต่อหนึ่งและ π_i เป็นฟังก์ชันทั่วถึง สำหรับ $i = 1,2$ ○

ทฤษฎีบทต่อไป แสดงโครงสร้างที่จะไม่แปรเปลี่ยนภายใต้สาทิสสัณฐาน

1.7.4 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ แล้ว

1. $\theta(e) = \bar{e}$ เมื่อ e และ $\bar{e}$ เป็นเอกลักษณ์ของ G และ $\bar{G}$ ตามลำดับ
2. $\theta(a^{-1}) = \theta(a)^{-1}$ สำหรับแต่ละ $a \in G$

บทพิสูจน์ 1. เนื่องจาก $\theta(e)\bar{e} = \theta(e) = \theta(e \cdot e) = \theta(e)\theta(e) = \bar{e} \cdot \bar{e}$ ดังนั้นโดยกฎการตัดออกในกรุป $\bar{G}$ จะได้ $\theta(e) = \bar{e}$

2. ให้ $a \in G$ แล้ว $\theta(a)\theta(a^{-1}) = \theta(aa^{-1}) = \theta(e) = \bar{e}$ ซึ่งแสดงว่า $\theta(a^{-1})$ เป็นตัวผกผันของ $\theta(a)$ แต่ตัวผกผันของ $\theta(a)$ มีเพียงหนึ่งเดียว จึงสรุปได้ว่า $\theta(a^{-1}) = \theta(a)^{-1}$ □

1.7.5 **ตัวอย่าง** เพื่อให้เห็นการประยุกต์ทฤษฎีบท 1.7.4 จะแสดงว่าแต่ละจำนวนจริง $r \neq 0$ มีสาทิสสัณฐาน θ จากกรุปการบวก $\mathbb{Z}$ ไปยังกรุปการคูณ $\mathbb{R}^+$ ของจำนวนจริงบวกทั้งหมดเพียงฟังก์ชันเดียวซึ่ง $\theta(1) = r$

วิธีทำ สำหรับจำนวนจริง $r \neq 0$ ให้ $\bar{\theta} : \mathbb{R} \to \mathbb{R}^+$ นิยามโดย $\bar{\theta}(x) = r^x$ ทุกๆ $x \in \mathbb{R}$ แล้วพิสูจน์ว่า $\bar{\theta}$ เป็นสมสัณฐานได้ทำนองเดียวกับในหัวข้อ 1.5 และถ้า θ เป็นฟังก์ชันกำกัดของ $\bar{\theta}$ ลงบน $\mathbb{Z}$ แล้ว θ เป็นสาทิสสัณฐาน ส่วนการพิสูจน์ว่า θ เป็นเพียงฟังก์ชันเดียวซึ่ง $\theta(1) = r$ เราสมมติให้ $\varphi : \mathbb{R} \to \mathbb{R}^+$ เป็นสาทิสสัณฐานซึ่ง $\varphi(1) = r$ และจะแสดงว่า $\theta = \varphi$

ถ้า n เป็นจำนวนเต็มบวกแล้ว $n = \underbrace{1+1+\ldots+1}_{n \text{ time}}$ และด้วยสมบัติยืนยงการดำเนินการของ θ และ φ จะได้ $\theta(n) = \theta(1+\cdots+1) = \theta(1)^n = r^n = \varphi(1)^n = \varphi(1+\cdots+1) = \varphi(n)$ แต่ถ้า n เป็นจำนวน เต็มลบแล้ว $-n$ เป็นจำนวนเต็มบวก ทำให้ได้โดยกรณีของจำนวนเต็มบวกว่า $\theta(-n) = \varphi(-n)$ ดังนั้น $\theta(n) = \theta(-(-n)) = -\theta(-n) = -\varphi(-n) = \varphi(-(-n)) = \varphi(n)$ และเพราะ 0 และ 1 เป็นเอกลักษณ์ของกรุป $\mathbb{Z}$ และ $\mathbb{R}^+$ ตามลำดับ จึงได้ $\theta(0) = 1 = \varphi(0)$ จากทั้งสามกรณีดังกล่าว

สรุปได้ว่า $\theta(n)=\varphi(n)$ ทุกๆ จำนวนเต็ม n ดังนั้น $\theta=\varphi$ ○

ทฤษฎีบทต่อไป แสดงว่าภาพของสาทิสสัณฐานเป็นกรุป ยิ่งไปกว่านั้นสาทิสสัณฐานยังส่งโครงสร้างบางส่วนของโดเมนไปยังภาพของสาทิสสัณฐานและโดยกลับกัน

1.7.6 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$

1. ถ้า H เป็นกรุปย่อยของ G แล้ว $\theta(H)$ เป็นกรุปย่อยของ $\bar{G}$
2. ถ้า $\bar{H}$ เป็นกรุปย่อยของ $\bar{G}$ แล้ว $\theta^{-1}(\bar{H})$ เป็นกรุปย่อยของ G

บทพิสูจน์ 1. ให้ H เป็นกรุปย่อยของ G ขอทบทวนว่า $\theta(H)=\{\theta(h)|h\in H\}$ ให้ $x,y\in\theta(H)$ แล้วมี $h_1,h_2\in H$ ซึ่ง $x=\theta(h_1)$ และ $y=\theta(h_2)$ แต่ $h_1h_2^{-1}\in H$ และ $xy^{-1}=\theta(h_1)\theta(h_2)^{-1}=\theta(h_1h_2^{-1})\in\theta(H)$ ทำให้ได้ $\theta(H)$ เป็นกรุปย่อยของ $\bar{G}$

2. ให้ $\bar{H}$ เป็นกรุปย่อยของ $\bar{G}$ และขอทบทวนว่า $\theta^{-1}(\bar{H})=\{a\in G|\theta(a)\in\bar{H}\}$ ให้ $a,b\in\theta^{-1}(\bar{H})$ แล้ว $\theta(a),\theta(b)\in\bar{H}$ ทำให้ได้ $\theta(ab^{-1})=\theta(a)\theta(b)^{-1}\in\bar{H}$ ซึ่งแสดงว่า $ab^{-1}\in\theta^{-1}(\bar{H})$ ดังนั้น $\theta^{-1}(\bar{H})$ เป็นกรุปย่อยของ G □

1.7.6 **บทแทรก** ถ้า θ, G และ $\bar{G}$ เป็นดังทฤษฎีบท 1.7.6 แล้ว $\theta(G)$ เป็นกรุปย่อยของ $\bar{G}$ □

1.7.8 **บทแทรก** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$

1. ถ้า $\bar{N}$ เป็นกรุปย่อยปรกติของ $\bar{G}$ แล้ว $\theta^{-1}(\bar{N})$ เป็นกรุปย่อยปรกติของ G
2. ถ้า $\theta(G)=\bar{G}$ แล้ว $\theta(N)$ เป็นกรุปย่อยปรกติของ $\bar{G}$ สำหรับแต่ละกรุปย่อยปรกติ N ของ G

บทพิสูจน์ 1. ให้ $n\in\theta^{-1}(\bar{N})$ และ $a\in G$ แล้ว $\theta(n)\in\bar{N}$ และเพราะ $\bar{N}$ เป็นกรุปย่อยปรกติของ $\bar{G}$ จึงได้ $\theta(ana^{-1})=\theta(a)\theta(n)\theta(a^{-1})\in\bar{N}$ ซึ่งแสดงว่า $ana^{-1}\in\theta^{-1}(\bar{N})$ ดังนั้น $\theta^{-1}(\bar{N})$ เป็นกรุปย่อยปรกติของ G

2. ให้ N เป็นกรุปย่อยปรกติของ G และ $\theta(G)=\bar{G}$ ให้ $n'\in\theta(N)$ และ $x\in\bar{G}$ แล้วมี $n\in N$ และ $a\in G$ ซึ่ง $\theta(n)=n'$, $\theta(a)=x$ และ $ana^{-1}\in N$ ทำให้ได้ $xn'x^{-1}=\theta(a)\theta(n)\theta(a)^{-1}=\theta(ana^{-1})\in\theta(N)$ ซึ่งแสดงว่า $\theta(N)$ เป็นกรุปย่อยปรกติของ $\bar{G}$ □

สังเกตว่าแต่ละกรุป G ที่มี e เป็นเอกลักษณ์ เราแสดงได้อย่างง่ายๆ ว่า $a\{e\}a^{-1}=\{e\}$ และ $aGa^{-1}=G$ ทุกๆ $a\in G$ ซึ่งแสดงว่า $\{e\}$ และ G เป็นกรุปย่อยปรกติของ G เราจึงเรียก {e} และ G ว่า *กรุปย่อยชัด (trivial subgroup)* และ *กรุปย่อยปรกติชัด (trivial normal subgroup)* ของ G ตามลำดับ

ในทางกลับกัน อาจมีคำถามว่าถ้า θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ แล้ว ภาพผกผันของ $\bar{e}$ จะเป็นกรุปย่อยและเป็นกรุปย่อยปรกติของ G หรือไม่ เราจะพิสูจน์คำตอบเชิงบวกของคำถามดังกล่าว กล่าวคือทุกๆ ภาพผกผันของ $\bar{e}$ เป็นกรุปย่อยปรกติของ G และโดยกลับกัน แต่ละกรุปย่อยปรกติ N ของ G จะมีกรุป $\bar{G}$ และสาทิสสัณฐานจาก G ไปยัง $\bar{G}$ ซึ่งภาพผกผันของ $\bar{e}$ ใน $\bar{G}$ คือ N

1.7.9 **บทนิยาม** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ เรียกเซตของสมาชิกใน G ซึ่งถูกส่งโดย θ ไปยังเอกลักษณ์ $\bar{e}$ ใน $\bar{G}$ ว่า *ส่วนกลาง (kernel)* ของ θ และเขียนแทนเซตนี้ดังนี้

$$\ker\theta = \{a \in G | \theta(a) = \bar{e}\} = \theta^{-1}(\{\bar{e}\})$$

โดยทฤษฎีบท 1.7.4 จะเห็นว่า $\ker\theta$ ไม่เป็นเซตว่างเพราะเอกลักษณ์ของกรุป G เป็นสมาชิกของ $\ker\theta$ และเพราะ $\{\bar{e}\}$ เป็นกรุปย่อยปรกติของ $\bar{G}$ โดยบทแทรก 1.7.7 จึงได้ว่า $\ker\theta = \theta^{-1}(\{\bar{e}\})$ เป็นกรุปย่อยปรกติของ G

1.7.10 **ทฤษฎีบท** ถ้า θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ แล้ว $\ker\theta$ เป็นกรุปย่อยปรกติของ G ❐

เนื่องจากเอกลักษณ์ $\bar{e}$ ของกรุป $\bar{G}$ เป็นสมาชิกของทุกๆ กรุปย่อย $\bar{H}$ ของ $\bar{G}$ ดังนั้น $\theta^{-1}(\{\bar{e}\})$ เป็นเซตย่อยของ $\theta^{-1}(\bar{H})$ เราจึงได้บทแทรกต่อไปนี้

1.7.11 **บทแทรก** ถ้า θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ แล้ว $\theta^{-1}(\bar{H})$ เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq \theta^{-1}(H)$ ทุกๆ กรุปย่อย $\bar{H}$ ของ $\bar{G}$ ❐

1.7.12 **ตัวอย่าง** เห็นชัดว่า $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ เป็นกรุปภายใต้การคูณแบบปกติ ให้ $\theta : \mathbb{Z} \to \mathbb{R}^*$ นิยามโดย $\theta(n) = 1$ ถ้า n เป็นจำนวนเต็มคู่และ $\theta(n) = -1$ ถ้า n เป็นจำนวนเต็มคี่ จะเห็นว่าถ้า m และ n ต่างเป็นจำนวนเต็มคู่หรือต่างเป็นจำนวนคี่ แล้ว $\theta(mn) = 1 = (1)(1) = (-1)(-1) = \theta(m)\theta(n)$ แต่ถ้า m หรือ n ตัวหนึ่งเป็นจำนวนคู่และอีกตัวหนึ่งจำนวนคี่ แล้ว $\theta(mn) = -1 = (-1)(1) = (1)(-1) = \theta(m)\theta(n)$ ซึ่งแสดงว่า θ เป็นสาทิสสัณฐาน ทำให้ได้

$$\ker\theta = \{n \in \mathbb{Z} | \theta(n) = 1\}$$

ซึ่งคือเซตของจำนวนเต็มคู่ทั้งหมด เป็นกรุปย่อยปรกติของ $\mathbb{Z}$ ❍

ถ้า θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ และ $y \in \theta(G)$ แล้วมี $x \in G$ ซึ่ง $y = \theta(x)$ โดยเรียก x ว่าภาพผกผันของ y ภายใต้ θ และถ้า $y = \bar{e}$ เป็นเอกลักษณ์ของ $\bar{G}$ แล้ว

$K = \ker\theta = \theta^{-1}(\{\bar{e}\})$ เป็นกรุปย่อยปรกติของ G ดังนั้นเซตของโคเซตซ้ายทั้งหมดของ K ใน G เป็นเซตเดียวกับเซตของโคเซตขวาทั้งหมดของ K ใน G ทำให้กล่าวถึงเซตนี้ได้อย่างสั้นๆ ว่าเซตของโคเซตทั้งหมดของ K ใน G จึงเกิดคำถามว่าแต่ละโคเซตของ K ใน G จะเป็นภาพผกผันของสมาชิกใน $\bar{G}$ เช่นเดียวกับ K หรือไม่ ทฤษฎีบทต่อไปจะพิสูจน์ความจริงนี้

1.7.13 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ และ $K = \ker\theta$ แล้วโคเซต xK เป็นภาพผกผันของ $\theta(x) \in \theta(G)$ ทุกๆ $x \in G$

บทพิสูจน์ ให้ $x \in G$ แล้ว $y = \theta(x) \in \theta(G)$ ให้ $t \in \theta^{-1}(\{y\})$ แล้ว $\theta(t) = y = \theta(x)$ จะได้ $\bar{e} = \theta(x)^{-1}\theta(t) = \theta(x^{-1}t)$ ทำให้ได้ $x^{-1}t \in K$ นั่นคือ $xK = tK$ ดังนั้น $t \in xK$ จึงได้ $\theta^{-1}(\{y\}) \subseteq xK$ ในทางกลับกันถ้า $t \in xK$ จะมี $k \in K$ ซึ่ง $t = xk$ จึงได้ $\theta(t) = \theta(xk) = \theta(x)\theta(k) = \theta(x)\bar{e} = \theta(x) = y$ ดังนั้น $t \in \theta^{-1}(\{y\})$ ซึ่งแสดงว่า $xK \subseteq \theta^{-1}(\{y\})$ เป็นภาพผกผันของ $\theta(x)$ ❐

เราได้แสดงในหัวข้อ 1.4 แล้วว่า ทุกๆ โคเซต (ซ้ายหรือขวาก็ตาม) ของ K ใน G มีขนาดเท่ากันและเท่ากับขนาดของ K ดังนั้นสำหรับเซตโทน $K = \{e\}$ ที่ประกอบด้วยเอกลักษณ์ของ G เพียงตัวเดียว ภาพผกผันของแต่ละสมาชิกใน $\theta(G)$ จะประกอบด้วยสมาชิกเพียงหนึ่งเดียวด้วยเช่นกันซึ่งแสดงว่า θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง เราจึงได้บทแทรกต่อไปนี้

1.7.14 **บทแทรก** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ แล้ว

1. θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ $\ker\theta = \{e\}$
2. θ เป็นสมสัณฐาน ก็ต่อเมื่อ มีสาทิสสัณฐาน $\theta^{-1} : \bar{G} \to G$ ซึ่ง $\theta \circ \theta^{-1} = 1_{\bar{G}}$ และ $\theta^{-1} \circ \theta = 1_G$ ❐

ในหัวข้อ 1.4 เราได้เห็นแล้วว่า แต่ละกรุปย่อยปรกติ N ของกรุป G กำหนดกรุปผลหาร G/N ที่ประกอบด้วยโคเซตทั้งหมดของ N ใน G และเมื่อพิจารณากรุป G และ G/N ก็อาจมีคำถามว่า จะมีสาทิสสัณฐานระหว่างกรุปทั้งสองนี้หรือไม่ และเพื่อหาคำตอบ เราอาจลองส่งแต่ละสมาชิกใน G แบบเป็นธรรมชาติไปยังโคเซตที่บรรจุสมาชิกนั้น ทฤษฎีบทต่อไปจะแสดงว่าการส่งดังกล่าวเป็นสาทิสสัณฐานซึ่งจะทำให้เราได้ด้วยว่า ทุกๆ กรุปย่อยปรกติของกรุป G เป็นส่วนกลางของสาทิสสัณฐาน

1.7.15 **ทฤษฎีบท** แต่ละกรุปย่อยปรกติ N ของกรุป G จะมีกรุป $\bar{G}$ และสาทิสสัณฐาน θ จาก G ไปทั่วถึง $\bar{G}$ ซึ่ง N เป็นส่วนกลางของ θ

บทพิสูจน์ ให้ N เป็นกรุปย่อยปรกติของ G และให้ $\eta : G \to G/N$ นิยามโดย $\eta(a) = aN$ ทุกๆ $a \in G$ แล้วจะแสดงว่า η เป็นสาทิสสัณฐาน

เนื่องจากกรุปผลหาร G/N เป็นผลแบ่งกั้น G ดังนั้น η เป็นฟังก์ชันและเห็นได้ชัดโดยนิยามของโคเซตว่า η เป็นฟังก์ชันทั่วถึง และถ้า $a,b \in G$ แล้วโดยนิยามการคูณของโคเซต จะได้ $\eta(ab) \quad abN = (aN)(bN) = \eta(a)\eta(b)$ เพราะฉะนั้น η เป็นสาทิสสัณฐาน

สุดท้ายเพราะว่าโคเซต $N = eN$ เป็นเอกลักษณ์ของกรุปผลหาร G/N จึงได้ว่า

$$a \in \ker\eta \iff \eta(a) = N \iff aN = N \iff a \in N$$

ทุกๆ $a \in G$ เพราะฉะนั้น $N = \ker\eta$ □

1.7.16 หมายเหตุ เราเรียกฟังก์ชัน η ในทฤษฎีบท 1.7.15 ว่า *สาทิสสัณฐานธรรมชาติ (natural homomorphism)*

ขอให้สังเกตว่าทฤษฎีบท 1.7.15 ยังแสดงว่าแต่ละกรุปย่อยปรกติของกรุปจะกำหนดกรุปผลหารซึ่งเป็นภาพสาทิสสัณฐานของกรุปนั้น แต่อาจมีคำถามว่าภาพของกรุปภายใต้สาทิสสัณฐานสำคัญอย่างไร เราจะพิจารณาจากตัวอย่างต่อไปนี้

ให้ $P = \{e, o\}$ แล้ว P เป็นกรุปภายใต้การดำเนินการกำหนดบนดังตารางข้างล่างนี้

$+$	e	o
e	e	o
o	o	e

ให้ $f : \mathbb{Z} \to P$ โดย f ส่งทุกๆ จำนวนคู่ไปยัง e และส่งทุกๆ จำนวนคี่ไปยัง o [นั่นคือเราให้ e แทน "คู่ (even)" และให้ o แทน "คี่ (odd)"] จึงเรียกกรุป P ว่า *กรุปภาวะ (parity group)* แล้วการพิสูจน์ทำนองเดียวกับตัวอย่าง 1.7.11 แสดงว่า f เป็นสาทิสสัณฐานซึ่งเห็นชัดว่า f เป็นฟังก์ชันทั่วถึง ดังนั้น P เป็นภาพภายใต้สาทิสสัณฐานของกรุป $\mathbb{Z}$ ที่มีขนาดเล็กกว่าและมีความซับซ้อนน้อยกว่า $\mathbb{Z}$ อย่างไรก็ตาม P และ $\mathbb{Z}$ มีสมบัติที่เหมือนกันอย่างหนึ่งคือภาวะแสดงความเป็นคู่และคี่ แสดงให้เห็นว่าสาทิสสัณฐานแปลงสมบัติจากกรุปที่เป็นโดเมน (ซึ่งอาจมีความยุ่งยากซับซ้อน) มายังกรุปซึ่งเป็นภาพของสาทิสสัณฐานที่มีขนาดเล็กกว่า(จึงมีความซับซ้อนน้อยกว่า) ทำให้เห็นสมบัตินั้นอย่างชัดเจน

เราจึงต้องการหาภาพภายใต้สาทิสสัณฐานทั้งหมดของแต่ละกรุป และทฎษฎีบท 1.7.15 ได้พิสูจน์แล้วว่าทุกๆ กรุปผลหารของกรุปเป็นภาพภายใต้สาทิสสัณฐานของกรุปนั้น เราจึงต้องการทราบว่า จะมีภาพภายใต้สาทิสสัณฐานของกรุปที่นอกเหนือจากกรุปผลหารหรือไม่ ทฤษฎีบทต่อไป

พิสูจน์ว่าจะไม่มีภาพภายใต้สาทิสสัณฐานของกรุปที่นอกเหนือจากกรุปผลหาร ทฤษฎีบทนี้จึงสำคัญในวิชาพีชคณิต จึงเรียกทฤษฎีบทนี้ว่า "ทฤษฎีบทหลักมูลของสาทิสสัณฐาน"

1.7.17 **ทฤษฎีบทหลักมูลของสาทิสสัณฐาน** (The fundamental homomorphism theorem)

ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ และ $K = \ker\theta$ ถ้า N เป็นกรุปย่อยปรกติของ G ซึ่ง $N \subseteq K$ แล้วมีสาทิสสัณฐาน $\bar{\theta} : G/N \to \bar{G}$ เพียงหนึ่งเดียวที่ทำให้

1. $\bar{\theta}(aN) = \theta(a)$ สำหรับทุกๆ $a \in G$
2. $\operatorname{Im}\theta = \operatorname{Im}\bar{\theta}$ และ $\ker\bar{\theta} = (\ker\theta)/N$
3. $\bar{\theta}$ เป็นสมสัณฐาน ก็ต่อเมื่อ θ เป็นฟังก์ชันทั่วถึงและ $N = K$

บทพิสูจน์ 1. นิยาม $\bar{\theta} : G/N \to \bar{G}$ โดย $\bar{\theta}(xK) = \theta(x)$ ทุกๆ $x \in G$ และให้ $x_1, x_2 \in G$ ซึ่ง $x_1N = x_2N$ แล้ว $x_2x_1^{-1} \in N \subseteq K$ ทำให้ $x_1K = x_2K$ และโดยทฤษฎีบท 1.7.13 จะได้ $\theta(x_1) = \theta(x_1K) = \theta(x_2K) = \theta(x_2)$ ดังนั้น $\bar{\theta}$ กำหนดแจ่มชัด ต่อไปให้ $x_1, x_2 \in G$ แล้ว

$$\bar{\theta}((x_1N)(x_2N)) = \bar{\theta}(x_1x_2N) = \theta(x_1x_2) = \theta(x_1)\theta(x_2) = \bar{\theta}(x_1N)\bar{\theta}(x_2N)$$

ดังนั้น $\bar{\theta}$ เป็นสาทิสสัณฐาน

2. เห็นได้ชัดว่า $\operatorname{Im}\theta = \operatorname{Im}\bar{\theta}$ และเพราะ $aN \in \ker\bar{\theta} \Leftrightarrow \theta(a) = e \Leftrightarrow a \in \ker\theta$ ดังนั้น $\ker\bar{\theta} = \{aN | a \in \ker\theta\} = (\ker\theta)/N$

3. $\bar{\theta}$ เป็นสมสัณฐาน ก็ต่อเมื่อ $\operatorname{Im}\theta = \operatorname{Im}\bar{\theta} = \bar{G}$ และ $\{N\} = \ker\bar{\theta} = (\ker\theta)/N$ ซึ่งเกิดขึ้นเมื่อ $N = K$

สุดท้ายขอละการพิสูจน์ว่า $\bar{\theta}$ เป็นสาทิสสัณฐาน เพียงหนึ่งเดียวซึ่งสอดคล้องข้อ 1, 2 และ 3 ไว้เป็นแบบฝึกหัด ❐

1.7.18 **บทแทรก** ถ้า θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\bar{G}$ และ $K = \ker\theta$ แล้ว $\theta(G) \cong G/K$ ❐

1.7.19 **บทแทรก** ให้ N และ M เป็นกรุปย่อยปรกติของกรุป G และ $\bar{G}$ ตามลำดับ ถ้า θ เป็นสาทิสสัณฐานจาก G ไปยัง $\bar{G}$ โดยที่ $\theta(N)$ เป็นกรุปย่อยของ M แล้ว

1. θ ชักนำสาทิสสัณฐาน $\bar{\theta} : G/N \to \bar{G}/M$ ซึ่งนิยามโดย $\bar{\theta}(aN) = \theta(a)N$ ทุกๆ $a \in G$
2. $\bar{\theta}$ ในข้อ 1 เป็นสมสัณฐาน ก็ต่อเมื่อ $\bar{G} = \langle \operatorname{Im}\theta \cup M \rangle$ และ $\theta^{-1}(N) \subseteq M$
3. ถ้า θ เป็นสาทิสสัณฐานชนิดทั่วถึงซึ่ง $\theta(N) = M$ แล้ว $\bar{\theta}$ เป็นสมสัณฐาน

บทพิสูจน์ ให้ η เป็นสาทิสสัณฐานธรรมชาติจาก $\bar{G}$ ไปทั่วถึง $\bar{G}/M$ แล้วฟังก์ชันประกอบ $\eta \circ \theta$ เป็นสาทิสสัณฐานจาก G ไปยัง $\bar{G}/M$ โดยที่ $N \subseteq \theta^{-1}(M) = \ker(\eta \circ \theta)$ ดังนั้นโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ว่า

1. $\bar{\theta} : G/N \to \bar{G}/M$ ซึ่งนิยามโดย $\bar{\theta}(aN) = \theta(a)N$ ทุกๆ $a \in G$ เป็นสาทิสสัณฐาน
2. $\bar{\theta}$ ในข้อ 1 เป็นสมสัณฐาน $\Leftrightarrow$ $\eta \circ \theta$ เป็นชนิดทั่วถึงและ $N = \ker(\eta \circ \theta)$
   $\Leftrightarrow$ $\bar{G} = <\operatorname{Im}\theta \cup M>$ และ $\theta^{-1}(N) \subseteq M$
3. ถ้า θ เป็นชนิดทั่วถึงแล้ว $\bar{G} = \operatorname{Im}\theta = <\operatorname{Im}\theta \cup M>$ และถ้า $\theta(N) = M$ แล้ว $\ker\theta \subseteq N$ ซึ่งทำให้ได้ $\bar{\theta}$ เป็นสมสัณฐาน ❐

1.7.20 **ตัวอย่าง** เราได้แสดงแล้วว่าทุกๆ กรุปวัฏจักรสมสัณฐานกับกรุป $\mathbb{Z}$ หรือ $\mathbb{Z}_n$ เมื่อ n เป็นจำนวนเต็มบวก แต่เราอาจพิสูจน์ความจริงนี้ได้อีกวิธีหนึ่งโดยประยุกต์ทฤษฎีบทหลักมูล ดังนี้

ให้ G เป็นกรุปและสำหรับแต่ละ $a \in G$ นิยาม $\theta : \mathbb{Z} \to G$ โดย $\theta(n) = a^n$ ทุกๆ จำนวนเต็ม n จะขอละการพิสูจน์ว่า θ เป็นสาทิสสัณฐานไว้เป็นแบบฝึกหัด แล้วโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $\theta(G) \cong \mathbb{Z}/K$ เมื่อ $K = \ker\theta$ และสังเกตว่า $\theta(G) = \{a^n | n \in \mathbb{Z}\} = <a>$ เป็นกรุปวัฏจักรก่อกำเนิดโดย a

จาก $K = \{n \in \mathbb{Z} | a^n = e\}$ ถ้า $K = \{0\}$ แล้ว $<a> = \theta(G) \cong \mathbb{Z}/K = \mathbb{Z}/\{0\} \cong \mathbb{Z}$ เป็นกรุปวัฏจักรอันดับอนันต์ และถ้า $K \neq \{0\}$ แล้วมีจำนวนต็มบวก n น้อยสุดซึ่ง $a^n = e$ ในกรณีเช่นนี้ $K = <n>$ และได้ $<a> = \theta(G) \cong \mathbb{Z}/K = \mathbb{Z}/<n> \cong \mathbb{Z}_n$ ❍

1.7.21 **ตัวอย่าง** จะแสดงว่าสำหรับแต่ละจำนวนเต็มบวก n ขนาดของกรุปสลับ A_n เป็นครึ่งหนึ่งของขนาดของกรุปสมมาตร S_n อีกวิธีหนึ่งโดยประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐานดังนี้

ให้ P เป็นกรุปภาวะและ n เป็นจำนวนเต็มบวก และนิยาม $\theta : S_n \to P$ โดย $\theta(\alpha) = \begin{cases} e, \alpha \in A_n \\ o, \alpha \notin A_n \end{cases}$ แล้วเห็นชัดว่า θ เป็นสาทิสสัณฐานจาก S_n ไปทั่วถึง P ดังนั้นโดยทฤษฎีบทหลักมูล จะได้ $P \cong S_n/K$ เมื่อ $K = \ker\theta = \{\alpha \in S_n | \theta(\alpha) = e\} = A_n$ ดังนั้น $2 = |P| = |S_n/K| = \dfrac{|S_n|}{|K|} = \dfrac{|S_n|}{|A_n|}$ ทำให้ได้ $|A_n| = \dfrac{|S_n|}{2}$ ❍

1.7.22 **ตัวอย่าง** ให้ G เป็นกรุปของการหมุนระนาบรอบจุดคงที่ p และแต่ละจำนวนจริง r ให้ $\theta(r)$ แทนสมาชิกใน G ซึ่งเป็นการหมุนรอบ p ตามเข็มนาฬิกาไป r เรเดียนแล้ว θ เป็นสาทิสสัณฐานจากกรุปการบวก $\mathbb{R}$ ของจำนวนจริงทั้งหมดไปทั่วถึง G ดังนั้นโดยทฤษฎีบทหลักมูล จะได้

$G \cong \mathbb{R}/K$ เมื่อ $K = \ker\theta = \{2k\pi | k \in \mathbb{Z}\} = <2\pi>$ เพราะฉะนั้น $G \cong \mathbb{R}/<2\pi>$ ❍

ถ้า θ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ เราได้พิสูจน์แล้วว่าแต่ละกรุปย่อย H ของ G กำหนดกรุปย่อย $\theta(H)$ ของ $\overline{G}$ และถ้า H และ K เป็นกรุปย่อยของ G ซึ่ง $H \subseteq K \subseteq \ker\theta$ แล้ว $\theta(H) = \theta(K)$ นั่นคือทุกๆ กรุปย่อยของ G ซึ่งเป็นเซตย่อยของส่วนกลางของสาทิสสัณฐานกำหนดกรุปย่อยของ $\overline{G}$ เป็นกรุปย่อยเดียวกัน ทำให้ได้ว่าไม่มีฟังก์ชันสมนัยหนึ่งต่อหนึ่งระหว่างเซตของกรุปย่อยทั้งหมดของ G กับเซตของกรุปย่อยทั้งหมดของ $\overline{G}$ แต่ทฤษฎีบทต่อไปแสดงว่าถ้าสาทิสสัณฐานเป็นชนิดทั่วถึงแล้วมีฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงระหว่างเซตของกรุปย่อยทั้งหมดของ G ที่มีส่วนกลางของสาทิสสัณฐานเป็นเซตย่อยกับเซตของกรุปย่อยทั้งหมดของ $\overline{G}$

1.7.23 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปทั่วถึงกรุป $\overline{G}$

1. ถ้า H เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq H$ แล้ว $H = \theta^{-1}(\theta(H))$

2. ขนาดของเซตของกรุปย่อย H ทั้งหมดของ G ซึ่ง $\ker\theta \subseteq H$ เท่ากับขนาดของเซตของกรุปย่อยทั้งหมดของ $\overline{G}$

บทพิสูจน์ 1. $H \subseteq \theta^{-1}(\theta(H))$ โดยสมบัติของฟังก์ชันทั่วไป จึงเหลือเพียงแสดงว่า $\theta^{-1}(\theta(H)) \subseteq H$ โดยให้ $a \in \theta^{-1}(\theta(H))$ แล้ว $\theta(a) \in \theta(H)$ ดังนั้นมี $h \in H$ ซึ่ง $\theta(a) = \theta(h)$ ทำให้ได้ $\overline{e} = \theta(a)\theta(h^{-1}) = \theta(ah^{-1})$ ซึ่งแสดงว่า $ah^{-1} \in \ker\theta \subseteq H$ นั่นคือมี $h' \in H$ ซึ่ง $ah^{-1} = h'$ ดังนั้น $a = h'h \in H$

2. ให้ A เป็นเซตของกรุปย่อย H ทั้งหมดของ G ซึ่ง $\ker\theta \subseteq H$ และ B เป็นเซตของกรุปย่อยทั้งหมดของ $\overline{G}$ และให้ $\sigma : A \to B$ นิยามโดย $\sigma(H) = \theta(H)$ ทุกๆ $H \in A$ จะแสดงก่อนว่า σ เป็นฟังก์ชันทั่วถึง โดยให้ $\overline{H}$ เป็นกรุปย่อยของ $\overline{G}$ แล้ว $\theta^{-1}(\overline{H})$ เป็นกรุปย่อยของ G และเพราะ $\overline{e} \in \overline{H}$ ดังนั้น $\ker\theta = \theta^{-1}(\{\overline{e}\}) \subseteq \theta^{-1}(\overline{H})$ ให้ $H = \theta^{-1}(\overline{H})$ แล้ว $H \in A$ ทำให้ได้ $\sigma(H) = \theta(H) = \theta(\theta^{-1}(\overline{H}) = \overline{H}$

ต่อไปจะแสดงว่า σ เป็นฟังก์ชันหนึ่งต่อหนึ่ง โดยให้ H และ K เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq H \cap K$ และ $\theta(H) = \theta(K)$ แล้วโดยข้อ 1 จะได้ $H = \theta^{-1}(\theta(H)) = \theta^{-1}(\theta(K)) = K$

❐

โดยทฤษฎีบท 1.7.23 เมื่อประยุกต์สาทิสสัณฐานธรรมชาติกับกรุปผลหารซึ่งกำหนดโดยแต่ละกรุปย่อยปรกติของกรุป จะได้บทแทรกต่อไปนี้

1.7.24 **บทแทรก** ให้ N เป็นกรุปย่อยปรกติของกรุป G

1. $|A| = |B|$ ถ้า A เป็นเซตของกรุปย่อย H ทั้งหมดของ G ซึ่ง $N \subseteq H$ และ B เป็นเซตของกรุปย่อยทั้งหมดของ G/N

2. ถ้า K กรุปย่อยของ G/N แล้วมีกรุปย่อย H ของ G ซึ่ง $N \subseteq H$ และ $K = H/N$

3. H/N ในข้อ 2 เป็นกรุปย่อยปรกติของ G/N ก็ต่อเมื่อ H เป็นกรุปย่อยปรกติของ G ❐

เราจะปิดท้ายหัวข้อนี้ ด้วยการประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐานเพื่อพิสูจน์ทฤษฎีบทสำคัญเกี่ยวกับสมสัณฐานที่รู้จักกันเป็นอย่างดี

1.7.25 **ทฤษฎีบท** ให้ G เป็นกรุป N เป็นกรุปย่อยปรกติของ G และ H เป็นกรุปย่อยของ G

1. NH เป็นกรุปย่อยของ G
2. $H \cap N$ เป็นกรุปย่อยปรกติของ H
3. N เป็นกรุปย่อยปรกติของ NH

บทพิสูจน์ 1. เพียงพอที่จะแสดงว่า $NH = HN$ ให้ $n \in N$ และ $h \in H$ เพราะ $h^{-1} \in H \subseteq G$ และ N เป็นกรุปย่อยปรกติของ G ดังนั้น $h^{-1}nh = h^{-1}n(h^{-1})^{-1} \in N$ จะได้ $nh = h(h^{-1}nh) \in HN$ ทำให้ได้ $NH \subseteq HN$ และโดยการพิสูจน์ในทำนองคล้ายกัน จะได้ $HN \subseteq NH$

2. เห็นชัดว่า $H \cap N$ เป็นกรุปย่อยของ H จึงให้ $t \in H \cap N$ และ $h \in H$ แล้ว $t \in H$ ทำให้ได้ $hth^{-1} \in H$ แต่เพราะ $t \in N$, $h \in H \subseteq G$ และ N เป็นกรุปย่อยปรกติของ G ดังนั้น $hth^{-1} \in N$ เพราะฉะนั้น $hth^{-1} \in H \cap N$

3. เพราะว่า N เป็นกรุปย่อยปรกติของ G ดังนั้น $ana^{-1} \in N$ ทุกๆ $n \in N$ และ $a \in G$ แต่ $NH \subseteq G$ ทำให้ได้ $ana^{-1} \in N$ ทุกๆ $n \in N$ และ $a \in NH$ เพราะฉะนั้น N เป็นกรุปย่อยปรกติของ NH ❐

1.7.26 **ทฤษฎีบทที่หนึ่งของสมสัณฐาน** (The First Isomorphism Theorem)

ถ้า N เป็นกรุปย่อยปรกติของกรุป G และ H เป็นกรุปย่อยของ G แล้ว

$H/(H \cap N) \cong NH/N$

บทพิสูจน์ NH เป็นกรุปย่อยของ G และ $H \cap N$ เป็นกรุปย่อยปรกติของ H และ N เป็นกรุปย่อยปรกติของ NH โดยทฤษฎีบท 1.7.25 ดังนั้น $H/(H \cap N)$ และ NH/N ต่างเป็นกรุปผลหาร

เพื่อหาสาทิสสัณฐาน θ จาก H ไปทั่วถึง NH/N โดยมีส่วนกลางคือ $H \cap N$ และประยุกต์ทฤษฎีบทหลักมูลให้ได้ว่า $H/(H \cap N) \cong NH/N$ ดังนั้น θ จะต้องส่งแต่ละ $h \in H$ ไปยังโคเซตใน NH/N

แต่เพราะ $H \subseteq NH$ และสาทิสสัณฐานธรรมชาติ η ส่งจาก NH ไปทั่วถึง NH/N จึงให้ θ เป็นฟังก์ชันประกอบของฟังก์ชันเอกลักษณ์ ι_H ซึ่งกำกัดลงบน H กับ η นั่นคือ $\theta = \eta \circ \iota_H$ โดยมีแผนภาพการส่งแสดงดังนี้

$$\begin{tikzcd} H \arrow[rr, "\iota_H"] \arrow[dr, "\theta"'] & & HK \arrow[dl, "\eta"] \\ & HK/H & \end{tikzcd}$$

แล้ว θ เป็นสาทิสสัณฐานชนิดทั่วถึง และ

$$\begin{aligned} a \in \ker\theta \quad &\Leftrightarrow \quad h \in H \text{ และ } \theta(a) = N \\ &\Leftrightarrow \quad h \in H \text{ และ } N = (\eta \circ \iota_H)(a) = (\eta(\iota_H(a)) = \eta(a) = aN \\ &\Leftrightarrow \quad h \in H \text{ และ } a \in N \qquad \Leftrightarrow \qquad a \in H \cap N \end{aligned}$$

ทำให้ได้ $\ker\theta = H \cap N$ ตามต้องการ ❐

1.7.27 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปทั่วถึงกรุป $\bar{G}$

1. ถ้า N เป็นกรุปย่อยปรกติของ G ซึ่ง $\ker\theta \subseteq N$ แล้ว $G/N \cong \bar{G}/\theta(N)$
2. ถ้า $\bar{N}$ เป็นกรุปย่อยปรกติของ $\bar{G}$ แล้ว $G/\theta^{-1}(\bar{N}) \cong \bar{G}/\bar{N}$

บทพิสูจน์ 1. เนื่องจาก $\theta(N)$ เป็นกรุปย่อยปรกติของ $\bar{G}$ จึงให้ $\bar{\eta}$ เป็นสาทิสสัณฐานธรรมชาติจาก $\bar{G}$ ไปทั่วถึง $\bar{G}/\theta(N)$ และให้ σ เป็นฟังก์ชันประกอบของ θ และ $\bar{\eta}$ ซึ่งมีแผนภาพของฟังก์ชันประกอบดังแสดงข้างล่างนี้ แล้วเพราะ θ และ $\bar{\eta}$ เป็นสาทิสสัณฐาน ดังนั้น σ เป็นสาทิสสัณฐาน และเพราะ $\bar{\eta}$ เป็นฟังก์ชันทั่วถึง ดังนั้น σ เป็นฟังก์ชันทั่วถึง แต่โดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $G/\ker\sigma \cong \bar{G}/\theta(N)$ จึงเหลือเพียงแสดงว่า $\ker\sigma = N$

$$\begin{tikzcd} G \arrow[rr, "\theta"] \arrow[dr, "\sigma"'] & & \bar{G} \arrow[dl, "\bar{\eta}"] \\ & \bar{G}/\sigma(N) & \end{tikzcd}$$

เนื่องจากเอกลักษณ์ของกรุปผลหาร $\bar{G}/\theta(N)$ คือโคเซต $\bar{e}\theta(N) = \theta(N)$ เราจะได้

$$a \in \ker\sigma \quad \Leftrightarrow \quad \sigma(a) = \theta(N)$$

$\Leftrightarrow \quad \theta(N) = (\bar{\eta} \circ \theta)(a) = \bar{\eta}(\theta(a)) = \theta(a)\theta(N)$ (โดยนิยามของ $\bar{\eta}$)

$\Leftrightarrow \quad \theta(a) \in \theta(N) \quad \Leftrightarrow \quad a \in \theta^{-1}(\theta(N)) = N$ (เพราะว่า $\ker\theta \subseteq N$)

ดังนั้น $\ker\theta = N$ และได้ $G/N \cong \bar{G}/\theta(N)$ ตามต้องการ

2. ให้ $\bar{N}$ เป็นกรุปย่อยปรกติของ $\bar{G}$ แล้ว $\theta^{-1}(\bar{N})$ เป็นกรุปย่อยปรกติของ G ยิ่งไปกว่านั้น $\ker\theta \subseteq \theta^{-1}(\bar{N})$ ดังนั้นโดยข้อ 1 จะได้ $G/\theta^{-1}(\bar{N}) \cong \bar{G}/\theta(\theta^{-1}(\bar{N})) = \bar{G}/\bar{N}$ ❐

1.7.28 ทฤษฎีบทที่สองของสมสัณฐาน (The Second Isomorphism Theorem)

ถ้า N และ H เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $N \subseteq H$ แล้ว $\dfrac{G/N}{H/N} \cong G/H$

บทพิสูจน์ ให้ N และ H เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $N \subseteq H$ และให้ η เป็นสาทิสสัณฐานธรรมชาติจาก G ไปทั่วถึง G/N แล้วเพราะ H เป็นกรุปย่อยปรกติของ G ดังนั้น $\eta(H)$ เป็นกรุปย่อยปรกติของ G/N ซึ่ง $\eta(H) = H/N$ และเพราะว่า $\ker\eta = N \subseteq H$ จะได้โดยทฤษฎีบท 1.7.26 ว่า $G/H \cong \dfrac{G/N}{\eta(H)} = \dfrac{G/N}{H/N}$ ตามต้องการ ❐

แบบฝึกหัด 1.7

1. ฟังก์ชันซึ่งนิยามระหว่างกรุปในข้อต่อไปนี้เป็นสาทิสสัณฐานหรือไม่ พร้อมหาส่วนกลาง

   1.1 $f : \mathbb{Z}_8 \to \mathbb{Z}_4$ กำหนดโดย $f = \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} \\ \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{0} & \bar{1} & \bar{2} & \bar{3} \end{pmatrix}$

   1.2 $f : \mathbb{R} \to \mathbb{R}^*$ กำหนดโดย $f(a) = 2^a$

2. ให้ $\Im(\mathbb{R})$ แทนกรุปของฟังก์ชันค่าจริงทั้งหมดภายใต้การบวกของฟังก์ชัน จงแสดงว่า $\varphi : \Im(\mathbb{R}) \to \mathbb{R}$ นิยามโดย $\varphi(f) = f(0)$ ทุกๆ $f \in \Im(\mathbb{R})$ เป็นสาทิสสัณฐาน

3. ให้ $A \subset B$ เป็นเซตและนิยาม $h : P(A) \to P(B)$ โดย $h(C) = A \subset B$ ทุกๆ $C \subset A$ จงพิสูจน์ว่า h เป็นสาทิสสัณฐาน

4. จงแสดงว่าถ้า G และ $\bar{G}$ เป็นกรุป $\varphi_1 : G \times \bar{G} \to G$ และ $\varphi_2 : G \times \bar{G} \to \bar{G}$ นิยามตามลำดับโดย $\varphi_1(a,b) = a$ และ $\varphi_2(a,b) = b$ แล้ว φ_1 และ φ_2 เป็นสาทิสสัณฐาน

5. จงพิสูจน์ว่า G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $f : G \to G$ นิยามโดย $f(x) = x^{-1}$ ทุกๆ $x \in G$ เป็นสาทิสสัณฐาน

6. ให้ G และ $\bar{G}$ เป็นกรุปและ $f : G \to \bar{G}$ เป็นสาทิสสัณฐาน จงพิสูจน์ว่า

   6.1 ถ้า $a \in G$ และ $f(a) \in \bar{G}$ มีอันดับจำกัด แล้ว $|a|$ เป็นอนันต์หรือ $|f(a)|$ เป็นตัวหารของ $|a|$

6.2 ถ้า $S \subseteq G$ ซึ่ง $G = < S >$ แล้ว $\bar{G} = < f(S) >$

7. ให้ G เป็นกรุปวัฏจักรอันดับจำกัด n และ k เป็นจำนวนเต็มบวกซึ่ง $(n,k)=1$ จงพิสูจน์ว่า $\theta : G \to G$ นิยามโดย $\theta(x) = x^k$ ทุกๆ $x \in G$ เป็นสาทิสสัณฐาน

8. จงประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐาน เพื่อแสดงว่าข้อต่อไปนี้เป็นจริง

   8.1 $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong G_S / < r_2 >$ 8.2 $\mathbb{Z}_k \cong \mathbb{Z}_n / < \bar{k} >$ เมื่อ k เป็นตัวหารของ n

   8.3 $\mathbb{Z}_3 \cong (\mathbb{Z}_3 \times \mathbb{Z}_3)/K$ เมื่อ $K = \{(0,0),(1,1),(2,2)\}$

   8.4 $P_2 \cong P_3 / K$ เมื่อ P_2 และ P_3 คือเซตกำลังของ $\{1,2\}$ และ $\{1,2,3\}$ และ $K = \{\phi, \{1\}\}$

9. ให้ J และ K เป็นกรุปย่อยปรกติของกรุป G และ H ตามลำดับ จงพิสูจน์ว่าฟังก์ชัน f ซึ่งกำหนดการส่งโดย $f(x,y) = (xJ, yK)$ เป็นสาทิสสัณฐานจาก $G \times H$ ไปทั่วถึง $(G/J) \times (H/K)$ และ $(G \times H)/(J \times K) \cong (G/J) \times (H/K)$

10. ให้ $\alpha : \Im(\mathbb{R}) \to \mathbb{R}$ และ $\beta : \Im(\mathbb{R}) \to \mathbb{R}$ นิยามโดย $\alpha(f) = f(1)$ และ $\beta(f) = f(2)$ ทุกๆ $f \in \Im(\mathbb{R})$ จงพิสูจน์ว่า α และ β เป็นสาทิสสัณฐานและถ้า J เป็นเซตของฟังก์ชันทั้งหมดจาก $\mathbb{R}$ ไปยัง $\mathbb{R}$ ที่มีกราฟผ่านจุด $(1,0)$ และ K เป็นเซตของฟังก์ชันทั้งหมดจาก $\mathbb{R}$ ไปยัง $\mathbb{R}$ ที่มีกราฟผ่านจุด $(2,0)$ แล้ว $\Im(\mathbb{R})/J \cong \mathbb{R} \cong \Im(\mathbb{R})/K$

11. ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $H \subseteq K$ และนิยาม $\alpha : G/H \to G/K$ โดย $\alpha(aH) = aK$ จงพิสูจน์ว่า α เป็นฟังก์ชันและเป็นสาทิสสัณฐานชนิดทั่วถึงซึ่ง $\ker \alpha = K/H$ พร้อมสรุปผลตามทฤษฎีบทหลักมูลของสาทิสสัณฐาน

12. ให้ H, H_1, K และ K_1 เป็นกรุปย่อยของกรุป G จงพิสูจน์ว่าถ้า H_1 เป็นกรุปย่อยปรกติของ H และ K_1 เป็นกรุปย่อยปรกติของ K แล้ว $(H \cap K)H_1/(H \cap K_1)H_1 \cong (H \cap K)K_1/(H_1 \cap K)K_1$

1.8 ผลคูณตรงของกรุป

ในหัวข้อนี้ เราศึกษาการสร้างกรุปจากกรุปจำนวนจำกัดกรุปในลักษณะเป็นภาคขยายของตัวอย่าง 1.1.8 พร้อมจำแนกและพิสูจน์สมบัติสำคัญของกรุปผลคูณตรง

1.8.1 **ทฤษฎีบท** ให้ $G_1, G_2, ..., G_n$ เป็นกรุป แล้วผลคูณคาร์ทีเซียนของ $G_1, G_2, ..., G_n$ ซึ่งคือเซต $G_1 \times G_2 \times ... \times G_n = \{(g_1, g_2, ..., g_n) \mid g_i \in G_i ; i = 1,2,...,n\}$ กับการดำเนินการตามองค์

ประกอบคือ $(g_1, g_2, ..., g_n)(h_1, h_2, ..., h_n) = (g_1h_1, g_2h_2, ..., g_nh_n)$ ทุกๆ $(g_1, g_2, ..., g_n)$ และ $(h_1, h_2, ..., h_n)$ ใน $G_1 \times G_2 \times ... \times G_n$ เป็นกรุป ❐

1.8.2 บทนิยาม เรียกกรุป $G_1 \times G_2 \times ... \times G_n$ ในทฤษฎีบท 1.8.1 ว่า *ผลคูณตรง (direct product)* ของกรุป $G_1, G_2, ..., G_n$

1.8.3 บทนิยาม ให้ $G, G_1, G_2, ..., G_n$ เป็นกรุป เรากล่าวว่า G เป็น *ผลคูณภายนอก (external direct product)* ของ $G_1, G_2, ..., G_n$ ถ้า G สมสัณฐานกับผลคูณตรง $G_1 \times G_2 \times ... \times G_n$

1.8.4 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวกและ $G_1, G_2, ..., G_n$ เป็นกรุป แล้วแต่ละ $1 \le i \le n$ มีกรุปย่อยปรกติ $\overline{G_i}$ ของกรุป $G_1 \times G_2 \times ... \times G_n$ ซึ่ง

1. $\overline{G_i}$ สมสัณฐานกับ G_i ทุกๆ $1 \le i \le n$,
2. $\overline{G_i} \cap \left(\overline{G_1}\,\overline{G_2}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}\right) = \{(e_1, e_2, ..., e_n)\}$ สำหรับแต่ละ $1 \le i \le n$
3. $G_1 \times G_2 \times ... \times G_n = \overline{G_1}\,\overline{G_2}...\overline{G_n}$

บทพิสูจน์ ให้ $1 \le i \le n$ และนิยาม $\overline{G_i} = \{\, (e_1, e_2, ..., e_{i-1}, g_i, e_{i+1}, ..., e_n) \mid g_i \in G_i \}$ แล้ว $\overline{g_i} \in \overline{G_i}$ ก็ต่อเมื่อมี $g_i \in G_i$ ซึ่ง $\overline{g_i} = (e_1, e_2, ..., e_{i-1}, g_i, e_{i+1}, ..., e_n)$ และเพราะ $(e_1, e_2, ..., e_n) \in \overline{G_i}$ เป็นเอกลักษณ์ของ $G_1 \times G_2 \times ... \times G_n$ เมื่อ e_i เป็นเอกลักษณ์ของ G_i ดังนั้น $\overline{G_i} \ne \phi$ และขอให้พิสูจน์เป็นแบบฝึกหัดว่า $\overline{G_i}$ เป็นกรุปย่อยปรกติของ $G_1 \times G_2 \times ... \times G_n$

1. เห็นชัดว่า $\alpha : \overline{G_i} \to G_i$ ซึ่งนิยามโดย $\alpha(e_1, e_2, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n) = a_i$ ทุกๆ $a_i \in G_i$ เป็นสมสัณฐาน

2. ให้ $(g_1, g_2, ..., g_n) \in \overline{G_i} \cap \left(\overline{G_1}\,\overline{G_2}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}\right)$ แล้ว $(g_1, g_2, ..., g_n) \in \overline{G_i}$ ดังนั้น $(g_1, g_2, ..., g_n) = (e_1, e_2, ..., e_{i-1}, g_i, e_{i+1}, ..., e_n)$ ทำให้ $g_k = e_k$ ทุกๆ $k \in \{1, 2, ..., n\} \setminus \{i\}$ และจาก $(g_1, g_2, ..., g_n) \in \overline{G_1}\,\overline{G_2}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}$ จะมี $\overline{g_k} = \overline{G_k}$ สำหรับ $1 \le k \ne i \le n$ ซึ่ง

$$(g_1, g_2, ..., g_n) = \overline{g_1}...\overline{g_{i-1}}\,\overline{g_{i+1}}...\overline{g_n} = \overline{g_1}...\overline{g_{i-1}}\,\overline{e_i}\,\overline{g_{i+1}}...\overline{g_n} = (g_1, g_2, ..., g_{i-1}, e_i, g_{i+1}, ..., g_n)$$

ดังนั้น $g_k = e_k$ ทุกๆ $1 \le k \le n$ จะได้ $(g_1, g_2, ..., g_n) = (e_1, e_2, ..., e_n)$ และเห็นชัดว่า $(e_1, ..., e_n) \in \overline{G_i} \cap \left(\overline{G_1}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}\right)$ ดังนั้น $\overline{G_i} \cap \left(\overline{G_1}\,\overline{G_2}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}\right) = \{(e_1, e_2, ..., e_n)\}$

เพราะว่า $(g_1, g_2, ..., g_n) = (g_1, e_2, ..., e_n)(e_1, g_2, e_3, ..., e_n)...(e_1, e_2, ..., g_n) = \overline{g_1}\,\overline{g_2}...\overline{g_n}$ ทุกๆ $g_i \in G_i$ และ $1 \le i \le n$ จึงเห็นชัดว่า $G_1 \times G_2 \times ... \times G_n = \overline{G_1}\,\overline{G_2}...\overline{G_n}$ ❐

ทฤษฎีบท 1.8.1 และ 1.8.4 แสดงว่าผลคูณ $G_1 \times G_2 \times ... \times G_n$ และ $G_1G_2...G_n$ เป็นกรุปสำหรับทุกๆ หมู่ของกรุป $G_1, G_2, ..., G_n$ ซึ่งเราเรียก $G_1 \times G_2 \times ... \times G_n$ ว่าผลคูณภายนอกของ $G_1, G_2, ..., G_n$ เราจึงจะกำหนดผลคูณภายในของ $G_1, G_2, ..., G_n$ ดังในบทนิยามต่อไปนี้

1.8.5 **บทนิยาม** ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์และ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปรกติของ G เรากล่าวว่า G เป็น *ผลคูณภายใน (internal direct product)* ของ $G_1, G_2, ..., G_n$ ถ้า

1. $G = G_1G_2 ...G_n$

และ 2. $G_i \cap (G_1G_2 ...G_{i-1}G_{i+1}...G_n) = \{e\}$ สำหรับแต่ละ $1 \le i \le n$

จะเขียนแทน G ซึ่งเป็นผลคูณตรงภายในของกรุปย่อยปรกติ $G_1, G_2, ..., G_n$ ด้วยสัญลักษณ์ $G_1 \otimes G_2 \otimes ... \otimes G_n$

สังเกตว่าถ้า $n = 2$ แล้วกรุป G เป็นผลคูณภายในของกรุปย่อยปรกติ G_1 และ G_2 ของ G ก็ต่อเมื่อ $G = G_1G_2$ และ $G_1 \cap G_2 = \{e\}$ เมื่อ e แทนเอกลักษณ์ของ G

1.8.6 **ตัวอย่าง** กรุปไคลน์ $-K_4 = <a,b | a^2 = e = b^2, ab = ba> = \{e,a,b,ab\}$ เป็นกรุปอาบีเลียน ดังนั้นกรุปย่อย $H = <a>$ และ $K = <b>$ เป็นกรุปย่อยปรกติของ K_4 โดยที่ $K_4 = HK$ และ $H \cap K = \{e\}$ ดังนั้น $K_4 = H \otimes K$ เป็นผลคูณตรงภายในของกรุปย่อยวัฏจักรอันดับสอง ❍

1.8.7 **ตัวอย่าง** ให้ $G = <a>$ เป็นกรุปวัฏจักรอันดับอนันต์ H และ K เป็นกรุปย่อยของ G ที่ไม่ใช่กรุปย่อยชัดแล้ว H และ K เป็นกรุปย่อยวัฏจักร จะมีจำนวนเต็ม $m > 1$ และ $n > 1$ ซึ่ง $H = <a^m>$ และ $K = <a^n>$ ทำให้ได้ $a^{mn} \in H \cap K$ ทั้งนี้เพราะ $a^{mn} = (a^m)^n \in H$ และ $a^{mn} = (a^n)^m \in K$ แต่เพราะ $G = <a>$ มีอันดับอนันต์ ดังนั้น $a^k \ne e$ ทุกๆ จำนวนเต็ม $k \ge 1$ ทำให้ $a^{mn} \ne e$ ซึ่งแสดงว่า $H \cap K \ne \{e\}$ เพราะฉะนั้น G ไม่เป็นกรุปผลคูณภายใน ❍

เมื่อมีทั้งตัวอย่างของกรุปผลคูณภายในและกรุปที่ไม่เป็นกรุปผลคูณภายใน เราจึงจะกล่าวเกณฑ์สำหรับพิจารณาว่ากรุปใดเป็นกรุปผลคูณภายใน

1.8.8 **ทฤษฎีบท** ให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปรกติของกรุป G ที่มี e เป็นเอกลักษณ์ ถ้า G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ แล้ว

1. $G_i \cap G_j = \{e\}$ สำหรับทุกๆ $1 \le i \ne j \le n$
2. $h_ih_j = h_jh_i$ สำหรับทุกๆ $h_i \in G_i$ และ $h_j \in G_j$ และ $1 \le i, j \le n$

บทพิสูจน์ 1. ให้ $1 \le i < j \le n$ และให้ $k \in G_i \cap G_j$ แล้ว $k \in G_i$ และ $k \in G_j$ ให้ $e_s = e$ ทุกๆ $s = 1,2,...,n$ แล้ว $k = e_1e_2...e_{i-1}e_{i+1}...e_{j-1}ke_{j+1}...e_n \in G_1G_2...G_{i-1}G_{i+1}...G_n$ เพราะฉะนั้น $k \in G_i \cap (G_1G_2...G_{i-1}G_{i+1}...G_n)$ ทำให้ได้ $k = e$

2. ให้ $1 \le i, j \le n$ และให้ $h_i \in G_i$ และ $h_j \in G_j$ เพราะ $h_i^{-1} \in G_i$ และ $h_j \in G$ และ G_i เป็นกรุปย่อยปรกติของ G ดังนั้น $h_jh_i^{-1}h_j^{-1} \in G_i$ จึงได้ $h_i(h_jh_i^{-1}h_j^{-1}) \in G_i$ ในทำนองเดียวกันเพราะ

$h_j \in G_j$ และ $h_i \in G$ และG_j เป็นกรุปย่อยปรกติของ G ดังนั้น $h_i h_j h_i^{-1} \in G_j$ จะได้ $(h_i h_j h_i^{-1})h_j^{-1}$ $\in G_j$ เพราะฉะนั้น $h_i h_j h_i^{-1} h_j^{-1} \in G_i \cap G_j = \{e\}$ ทำให้ได้ $h_i h_j h_i^{-1} h_j^{-1} = e$ นั่นคือ $h_i h_j = h_j h_i$ ❐

ถ้า G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ แล้ว $G = G_1 G_2 ... G_n$ ดังนั้นแต่ละ $g \in G$ เขียนได้ในรูปผลคูณของสมาชิกจากแต่ละ $G_1, ..., G_n$ นั่นคือ $g = g_1 g_2 ... g_n$ เมื่อ $g_i \in G_i$ ทุกๆ $1 \le i \le n$ ทฤษฎีบทต่อไปจะแสดงว่าผลคูณดังกล่าวมีได้เพียงชุดเดียวเท่านั้น

1.8.9 **ทฤษฎีบท** กรุป G เป็นผลคูณภายในของกรุปย่อยปรกติ $G_1, G_2, ..., G_n$ ของ G ก็ต่อเมื่อแต่ละ $g \in G$ เขียนได้แบบเดียวในรูป $g = g_1 g_2 ... g_n$ โดยที่ $g_i \in G_i$ ทุกๆ $1 \le i \le n$

บทพิสูจน์ ให้ $g \in G$ และสำหรับแต่ละ $1 \le i \le n$ มี $g_i, h_i \in G_i$ ซึ่ง $g = g_1 g_2 ... g_n = h_1 h_2 ... h_n$ จะแสดงว่า $g_i = h_i$ ทุกๆ $1 \le i \le n$ โดยให้ $i \in \{1, 2, ..., n\}$ จาก $g_1 g_2 ... g_n = h_1 h_2 ... h_n$ จะได้ว่า

$$g_i = g_{i-1}^{-1} g_{i-2}^{-1} ... g_1^{-1} h_1 h_2 ... h_n g_n^{-1} g_{n-1}^{-1} ... g_{i+1}^{-1}$$

แต่เพราะ $h_i h_j = h_j h_i$ ทุกๆ $h_i \in G_i$ และ $h_j \in G_j$ และ $1 \le i, j \le n$ ดังนั้น

$$g_i = h_i \left(h_1 g_1^{-1}\right)\left(h_2 g_2^{-1}\right) ... \left(h_{i-1} g_{i-1}^{-1}\right)\left(h_{i+1} g_{i+1}^{-1}\right) ... \left(h_n g_n^{-1}\right)$$

จึงได้ $h_i^{-1} g_i = \left(h_1 g_1^{-1}\right)\left(h_2 g_2^{-1}\right) ... \left(h_{i-1} g_{i-1}^{-1}\right)\left(h_{i+1} g_{i+1}^{-1}\right) ... \left(h_n g_n^{-1}\right) \in G_1 G_2 ... G_{i-1} G_{i+1} ... G_n$ แต่ $h_i^{-1} g_i$ $\in G_i$ ดังนั้น $h_i^{-1} g_i \in G_i \cap \left(G_1 G_2 ... G_{i-1} G_{i+1} ... G_n\right) = \{e\}$ ซึ่งแสดงว่า $h_i^{-1} g_i = e$ นั่นคือ $g_i = h_i$

สำหรับบทกลับ เห็นชัดว่า $G = G_1 G_2 ... G_n$ จึงให้ $h \in G_i \cap \left(G_1 G_2 ... G_{i-1} G_{i+1} ... G_n\right)$ สำหรับ $1 \le i \le n$ แล้ว $h \in G_i$ และ $h = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ สำหรับบาง $h_j \in G_j$ เมื่อ $1 \le j \ne i \le n$ ทำให้ได้ $\underbrace{e \cdots e}_{i-1} h \underbrace{e \cdots e}_{n-i} = h = h_1 \cdots h_{i-1} e h_{i+1} \cdots h_n \in G$ แต่โดยสมมติฐานว่า h เขียนได้วิธีเดียวในรูปผลคูณของสมาชิกจาก $G_1, G_2, ..., G_n$ ทำให้ได้ $h = e$ ซึ่งเป็นอันจบการพิสูจน์ ❐

ทฤษฎีบทต่อไปแสดงความสัมพันธ์ของผลคูณภายนอกและผลคูณภายใน

1.8.10 **ทฤษฎีบท** กรุป G เป็นผลคูณภายนอกของกรุป $G_1, G_2, ..., G_n$ ก็ต่อเมื่อมีกรุปย่อยปรกติ $N_1, ..., N_n$ ของ G ซึ่ง $G_i \cong N_i$ ทุกๆ $1 \le i \le n$ และ G เป็นผลคูณภายในของ $N_1, N_2, ..., N_n$

บทพิสูจน์ ให้ α เป็นสมสัณฐานจาก G ไปทั่วถึง $G_1 \times ... \times G_n$ และให้ $1 \le i \le n$ และนิยาม $\overline{G_i}$ ดังบทพิสูจน์ของทฤษฎีบท 1.8.4 แล้ว $\overline{G_i}$ เป็นกรุปย่อยปรกติของ $G_1 \times ... \times G_n$ ซึ่ง $\overline{G_i} \cong G_i$ และให้ $N_i = \alpha^{-1}\left(\overline{G_i}\right)$ แล้วเพราะภาพผกผันภายใต้สาทิสสัณฐานของกรุปย่อยปรกติเป็นกรุปย่อยปรกติ ดังนั้น N_i เป็นกรุปย่อยปรกติของ G นอกจากนี้ $N_i = \alpha\left(N_i\right) = \overline{G_i} \cong G_i$ ต่อไปจะแสดงว่า G เป็นผลคูณภายในของ $N_1, ..., N_n$

1. ให้ $g \in G$ แล้ว $\alpha(g) \in G_1 \times G_2 \times \ldots \times G_n$ ดังนั้นแต่ละ $1 \le i \le n$ มี $\overline{g_i} \in \overline{G_i}$ ซึ่ง $\alpha(g) = \overline{g_1}\,\overline{g_2}\ldots\overline{g_n}$ แต่ $\overline{g_i} \in \overline{G_i} = \alpha(N_i)$ ทุกๆ $1 \le i \le n$ จึงมี $x_i \in N_i$ ซึ่ง $\overline{g_i} = \alpha(x_i)$ ทุกๆ $1 \le i \le n$ ทำให้ได้ $\alpha(g) = \overline{g_1}\,\overline{g_2}\ldots\overline{g_n} = \alpha(x_1)\alpha(x_2)\ldots\alpha(x_n) = \alpha(x_1x_2\ldots x_n)$ และเพราะ α เป็นฟังก์ชันหนึ่งต่อหนึ่ง จึงได้ $g = x_1x_2\ldots x_n$ เพราะฉะนั้น $G = N_1N_2\ldots N_n$

2. ให้ $1 \le i \le n$ และ $y \in N_i \cap (N_1 \ldots N_{i-1}N_{i+1}\ldots N_n)$ แล้ว $y \in N_i = \alpha^{-1}(\overline{G_i})$ และ $y \in N_1 \ldots N_{i-1}N_{i+1}\ldots N_n$ ดังนั้น $\alpha(y) \in \overline{G_i}$ และแต่ละ $1 \le j \ne i \le n$ มี $x_j \in N_j$ ซึ่ง $y = x_1 \ldots x_{i-1}x_{i+1}\ldots x_n$ ทำให้ $\alpha(y) = \alpha(x_1\ldots x_{i-1}x_{i+1}\ldots x_n) = \alpha(x_1)\ldots\alpha(x_{i-1})\alpha(x_{i+1})\ldots\alpha(x_n)$ และเพราะ $x_j \in N_j = \alpha^{-1}(\overline{G_j})$ จึงได้ $\alpha(x_j) \in \overline{G_j}$ ทุกๆ $1 \le j \ne i \le n$ ทำให้ $\alpha(y) \in \overline{G_1}\ldots\overline{G_{i-1}}\,\overline{G_{i+1}}\ldots\overline{G_n}$ นั่นคือ $\alpha(y) \in \overline{G_i} \cap (\overline{G_1}\ldots\overline{G_{i-1}}\,\overline{G_{i+1}}\ldots\overline{G_n}) = \{(e_1, e_2, \ldots, e_n)\}$ เมื่อ $e_k \in G_k$ ทุกๆ $1 \le k \le n$ จึงได้ $\alpha(y) = (e_1, e_2, \ldots, e_n) = \alpha(e)$ เป็นเอกลักษณ์ใน $G_1 \times \ldots \times G_n$ ดังนั้น $y = e$

ในทางกลับกัน สมมติมีกรุปย่อยปรกติ $N_1, \ldots, N_n$ ของ G ซึ่ง $G_i \cong N_i$ โดยสมสัณฐาน $\alpha_i : N_i \to G_i$ สำหรับ $1 \le i \le n$ และ G เป็นผลคูณภายในของ $N_1, \ldots, N_n$ สังเกตว่าแต่ละ $g \in G$ มี $x_i \in N_i$ ทุกๆ $1 \le i \le n$ ซึ่ง $g = x_1x_2\ldots x_n$ จึงให้ $\alpha : G \to G_1 \times \ldots \times G_n$ นิยามโดย $\alpha(g) = (\alpha_1(x_1), \alpha_2(x_2), \ldots, \alpha_n(x_n))$ ทุกๆ $g = x_1x_2\ldots x_n \in G$ แล้วเพราะแต่ละ $g \in G$ มี $x_i \in N_i$ ทุกๆ $1 \le i \le n$ เพียงชุดเดียวซึ่ง $g = x_1x_2\ldots x_n$ จะได้ว่า α กำหนดแจ่มชัด

ให้ $g, h \in G$ แล้วมี $x_i, y_i \in N_i$ ทุกๆ $1 \le i \le n$ ซึ่ง $g = x_1x_2\ldots x_n$ และ $h = y_1y_2\ldots y_n$ และโดยทฤษฎีบท1.8.6 ข้อ 2 จะได้ $gh = x_1x_2\ldots x_ny_1y_2\ldots y_n = (x_1y_1)(x_2y_2)\ldots(x_ny_n)$ แต่โดยนิยามของ α และการดำเนินการในกรุปผลคูณตรงจะได้

$$\begin{aligned}\alpha(gh) &= \alpha((x_1y_1)(x_2y_2)\ldots(x_ny_n)) = (\alpha_1(x_1y_1), \alpha_2(x_2y_2), \ldots, \alpha_n(x_ny_n)) \\ &= (\alpha_1(x_1)\alpha_1(y_1), \alpha_2(x_2)\alpha_2(y_2), \ldots, \alpha_n(x_n)\alpha_n(y_n)) \\ &= (\alpha_1(x_1), \alpha_2(x_2), \ldots, \alpha_n(x_n))(\alpha_1(y_1), \alpha_2(y_2), \ldots, \alpha_n(y_n)) = \alpha(g)\alpha(h)\end{aligned}$$

ดังนั้น α เป็นสาทิสสัณฐาน

ต่อไปให้ $g, h \in G$ โดยที่ $\alpha(g) = \alpha(h)$ แล้วมี $x_i, y_i \in N_i$ ทุกๆ $1 \le i \le n$ ซึ่ง $g = x_1x_2\ldots x_n$ และ $h = y_1y_2\ldots y_n$ ทำให้ได้ $\alpha(x_1, x_2, \ldots, x_n) = \alpha(g) = \alpha(h) = \alpha(y_1, y_2, \ldots, y_n)$ จึงได้ $(\alpha_1(x_1), \alpha_2(x_2), \ldots, \alpha_n(x_n)) = (\alpha_1(y_1), \alpha_2(y_2), \ldots, \alpha_n(y_n))$ ดังนั้น $\alpha_i(x_i) = \alpha_i(y_i)$ ทุกๆ $1 \le i \le n$ แต่ α_i เป็นฟังก์ชันหนึ่งต่อหนึ่งทุกๆ $1 \le i \le n$ จึงได้ว่า $x_i = y_i$ ทุกๆ $1 \le i \le n$ เพราะฉะนั้น $g = h$ ซึ่งแสดงว่า α เป็นฟังก์ชันหนึ่งต่อหนึ่ง

สุดท้ายให้ $(g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \ldots \times G_n$ แล้ว $g_i \in G_i$ ทุกๆ $1 \le i \le n$ และเพราะ α_i เป็นฟังก์ชันทั่วถึงทุกๆ $1 \le i \le n$ ทำให้แต่ละ $1 \le i \le n$ มี $x_i \in N_i$ ซึ่ง $\alpha_i(x_i) = g_i$

ให้ $g = x_1x_2...x_n$ แล้ว $g \in G$ โดยที่ $\alpha(g) = \alpha(x_1x_2...x_n) = (\alpha_1(x_1), \alpha_2(x_2), ..., \alpha_n(x_n)) = (g_1, g_2, ..., g_n)$ ดังนั้น α เป็นฟังก์ชันทั่วถึง

เพราะฉะนั้น α เป็นสมสัณฐาน ทำให้ได้ $G \cong G_1 \times G_2 \times ... \times G_n$ ❐

1.8.11 บทแทรก ให้ G เป็นผลคูณภายในของกรุปย่อย $G_1, G_2, ..., G_n$ ของ G ถ้า N เป็นผลคูณภายนอกของกรุป $N_1, N_2, ..., N_n$ ซึ่ง $G_i \cong N_i$ สำหรับแต่ละ $1 \le i \le n$ แล้ว $G \cong N$ ❐

1.8.12 บทแทรก ให้ G เป็นกรุปและ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปรกติของ G แล้ว G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ ก็ต่อเมื่อ G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ ❐

แบบฝึกหัด 1.8

1. ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $G = H \otimes K$ จงพิสูจน์ว่า
   1.1 $(G/H) \cong K$ และ $(G/K) \cong H$
   1.2 ถ้า N เป็นกรุปย่อยปรกติของ H แล้ว N เป็นกรุปย่อยปรกติของ G และ $(G/N) \cong (H/N) \times K$
   1.3 ถ้า G เป็นกรุปจำกัดซึ่ง $G = HK$ หรือ $H \cap K = \{e\}$ หรือ $(|H|, |K|) = 1$ แล้ว $G = H \otimes K$
2. จงแสดงว่า $\mathbb{Z}_{15}$ เป็นกรุปผลคูณตรงภายใน แต่ G_S และ S_3 ไม่เป็นกรุปผลคูณตรงภายใน
3. ให้ θ เป็นสาทิสสัณฐานจากกรุป G ไปทั่วถึงกรุป $\bar{G}$ และ H เป็นกรุปย่อยปรกติของ G จงแสดงว่าถ้าฟังก์ชันกำกัดของ θ ลงบน H เป็นสมสัณฐานจาก H ไปทั่วถึง $\bar{G}$ แล้ว $G = H \otimes \ker\theta$
4. ให้ n เป็นจำนวนเต็มบวกและ $G_1, G_2, ..., G_n$ เป็นกรุป จงพิสูจน์ว่า
   4.1 $G_1 \times ... \times G_n$ สมสัณฐานกับ $G_{\sigma(1)} \times ... \times G_{\sigma(n)}$ ทุกๆ วิธีเรียงสับเปลี่ยน σ บน $\{1, \ldots, n\}$
   4.2 $|(g_1, g_2, ..., g_n)|$ เท่ากับตัวคูณร่วมน้อยของ $|g_1|, |g_2|, \ldots, |g_n|$ ทุกๆ $(g_1, g_2, ..., g_n)$ ใน $G_1 \times G_2 \times ... \times G_n$
   4.3 $G_1 \times G_2 \times ... \times G_n$ เป็นกรุปวัฏจักร ก็ต่อเมื่อ $|g_1|, |g_2|, \ldots, |g_n|$ เป็นจำนวนเฉพาะสัมพัทธ์

บทที่ 2
โครงสร้างของกรุปอาบีเลียน

การศึกษาเรื่องกรุป นอกจากเราสนใจศึกษาสาระของทฤษฎีกรุปดังกล่าวในบทที่ 1 แล้ว ปัญหาเปิดที่สำคัญซึ่งอยู่ในความสนใจมาเป็นเวลาช้านานและคงจะอยู่ในความสนใจต่อไปจนกว่าจะได้คำตอบก็คือการจำแนกกรุปทั้งหมด อย่างไรก็ตาม ณ ปัจจุบันเราสามารถจำแนกกรุปอาบีเลียนชนิดก่อกำเนิดแบบจำกัดได้ทั้งหมดแล้ว

เมื่อเริ่มต้น เราได้ศึกษาการจำแนกกรุปอาบีเลียนอันดับจำกัด ทั้งในกรณีของกรุปที่มีอันดับเป็นกำลังสองของจำนวนเฉพาะและกรณีของกรุปที่มีอันดับเป็นจำนวนเต็มบวกใดๆ ปรากฏว่าการศึกษาดังกล่าว ทำให้ได้แนวทางสำหรับการศึกษาโครงสร้างของกรุปอาบีเลียนในหมู่ที่กว้างขึ้น นั่นคือหมู่ของกรุปอาบีเลียนก่อกำเนิดโดยเซตย่อยจำกัดของกรุปนั้นๆ ซึ่งเราเรียกกรุปในหมู่นี้ว่ากรุปอาบีเลียนก่อกำเนิดแบบจำกัด

ดังกล่าวไว้ในบทที่ 1 แล้วว่า แนวทางหนึ่งที่เราสามารถอธิบายลักษณะหรือชนิดของกรุปที่กำลังศึกษา คือการบรรยายด้วยตัวก่อกำเนิดและความสัมพันธ์ของตัวก่อกำเนิดเหล่านั้น ตัวอย่างเช่นกรุปอาบีเลียนไคลน์–4 ถูกบรรยายโดย $K_4 = < a,b \mid a^2 = b^2 = e, ab = ba >$ เราจึงดำเนินตามแนวคิดนี้ในการบรรยายกรุปอาบีเลียน (ที่จะศึกษาต่อไป) แต่สำหรับกรุปทั่วไป แนวคิดที่ทำให้สะดวกในการกล่าวถึงคือการกล่าวว่ากรุปเป็นภาพของกรุปเสรี

ในบทนี้ เราศึกษากรุปอาบีเลียนเสรีและศึกษาแนวคิดของนักคณิตศาสตร์ในการจำแนกกรุปอาบีเลียนก่อกำเนิดแบบจำกัดซึ่งต้องกล่าวในรูปของผลคูณตรง แต่เพื่อเน้นความเป็นกรุปอาบีเลียน เราจะใช้สัญลักษณ์ "การบวก +" แทนการดำเนินการของกรุป และเพื่อให้สัญลักษณ์สอดคล้องกัน จึงใช้ "0" และ "$-x$" แทน "เอกลักษณ์" และ "ตัวผกผัน" ของแต่ละสมาชิก x ในกรุปตามลำดับ ดังนั้น "ผลคูณตรง" จึงเรียกเป็น "ผลบวกตรง"

2.1 การวางนัยผลคูณตรงและผลบวกตรง

ในหัวข้อนี้ เราศึกษาการขยายบทนิยามของผลคูณตรง $G \times H$ ของกรุป G และ H ไปยังผลคูณตรงของหมู่ $\{G_i \mid i \in I\}$ ของกรุปซึ่งดรรชนีโดยเซต $I \neq \phi$ ที่อาจเป็นเซตจำกัดหรือเซตอนันต์

เราเริ่มด้วยการนิยามผลคูณคาร์ทีเซียนของหมู่ $\{G_i \mid i \in I\}$ ของกรุป โดยสังเกตจาก $G \times H$ ซึ่งเป็นผลคูณคาร์ทีเซียนของหมู่ $\{G, H\}$ ที่ดรรชนีโดยเซต $I = \{1,2\}$ แล้วแต่ละ $(g,h) \in G \times H$ อาจหมายถึงฟังก์ชันจากเซตดรรชนี I ไปยัง $G \cup H$ ที่นิยามโดย $(g,h)(1) = g$ และ $(g,h)(2) = h$ เราจึงขยายแนวคิดนี้ในการให้นิยามผลคูณคาร์ทีเซียนของ $\{G_i \mid i \in I\}$

2.1.1 **บทนิยาม** ให้ $\{G_i | i \in I\}$ เป็นหมู่ของกรุปซึ่งดรรชนีโดยเซต $I \neq \phi$ เรียกเซตของฟังก์ชัน f ทั้งหลายจาก I ไปยัง $\bigcup_{i\in I} G_i$ ซึ่ง $f(i) \in G_i$ ทุกๆ $i \in I$ ว่า *ผลคูณคาร์ทีเซียน (cartesian product)* ของ $\{G_i | i \in I\}$ และเขียนแทนด้วยสัญลักษณ์ $\prod_{i\in I} G_i$

ให้ $\{G_i | i \in I\}$ เป็นหมู่ของกรุปและนิยามการดำเนินการบน $\prod_{i\in I} G_i$ ในลักษณะขยายการนิยามการดำเนินการตามองค์ประกอบ (component wise) บน $G \times H$ โดยแต่ละคู่ $f, g \in \prod_{i\in I} G_i$ ให้ $fg : I \to \prod_{i\in I} G_i$ นิยามโดย $fg(i) = f(i)g(i)$ ทุกๆ $i \in I$ แล้วการคำนวณโดยตรงเช่นเดียวกับกรณีของ $G \times H$ พิสูจน์ได้ว่า $\prod_{i\in I} G_i$ เป็นกรุป และเพื่อให้เป็นไปในแนวเดียวกันกับสัญลักษณ์ $(g,h) \in G \times H$ หรือ $(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$ จะเขียน $f \in \prod_{i\in I} G_i$ ในรูปแบบของภาพของ f เป็น $(a_i)_{i\in I}$ ดังนั้นผลคูณ fg จึงแทนด้วย $(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}$

ทฤษฎีบทต่อไป พิสูจน์ได้ในทำนองเดียวกับในหัวข้อ 1.8 จึงละการพิสูจน์ไว้เป็นแบบฝึกหัด

2.1.2 **ทฤษฎีบท** ให้ $\{G_i | i \in I\}$ เป็นหมู่ของกรุปซึ่ง $I \neq \phi$ แล้ว

1. $\prod_{i\in I} G_i$ เป็นกรุป
2. $\pi_k : \prod_{i\in I} G_i \to G_k$ ซึ่งนิยามโดย $\pi_k(f) = f(k)$ [หรือ $\pi_k((a_i)_{i\in I}) = a_k$] ทุกๆ $k \in I$ เป็นสาทิสสัณฐานชนิดทั่วถึง และเรียก π_k ทุกๆ $k \in I$ ว่า *การฉาย (projection)* ❑

2.1.3 **บทนิยาม** ให้ $I \neq \phi$ จะกล่าวว่ากรุป G เป็น*ผลคูณตรง (direct product)* ของหมู่ $\{G_i | i \in I\}$ ของกรุปถ้า G สมสัณฐานกับ $\prod_{i\in I} G_i$

ในกรณีที่ $\{G_i | i \in I\}$ เป็นหมู่ของกรุปอาบีเลียน จะแทน $\prod_{i\in I} G_i$ ด้วยสัญลักษณ์ $\sum_{i\in I} G_i$ และเรียกว่า *ผลบวกตรง (direct sum)* ของ $\{G_i | i \in I\}$ ทำให้ผลคูณ $(a_i)_{i\in I}(b_i)_{i\in I}$ เขียนแทนด้วยผลบวก $(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I}$

สังเกตว่าทฤษฎีบทต่างๆ ที่เกี่ยวกับผลคูณตรงของกรุปจำนวนจำกัดในหัวข้อ 1.8 เป็นจริงสำหรับผลคูณตรงของหมู่ของกรุป จึงขอละการเขียนและการพิสูจน์ไว้เป็นแบบฝึกหัด

ทฤษฎีบทต่อไปเป็นทฤษฎีบทสำคัญในการประยุกต์เพื่อพิสูจน์ทฤษฎีบทหลักมูลของกรุปอาบีเลียนก่อกำเนิดแบบจำกัด ซึ่งจะศึกษากันในหัวข้อต่อๆ ไป

2.1.4 **ทฤษฎีบท** 1. $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ ทุกๆ จำนวนเต็มบวก m และ n ซึ่ง $(m,n) = 1$

2. ถ้า $n>1$ และ $r,n_1,n_2,\ldots,n_r$ เป็นจำนวนเต็มบวกซึ่ง $n=n_1n_2\cdots n_r$ และ $(n_i,n_j)=1$ ทุกๆ $1\le i\ne j\le r$ แล้ว $\mathbb{Z}_n\cong\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_r}$

บทพิสูจน์ 1. ให้ m และ n เป็นจำนวนเต็มบวกซึ่ง $(m,n)=1$ แล้วมีจำนวนเต็มบวก s และ t ซึ่ง $1=ms+nt$ ให้ $H=<m1>$ และ $K=<n1>$ เป็นกรุปย่อยของ $\mathbb{Z}_{mn}=<1>$ แล้วจะแสดงก่อนว่า $H\cong\mathbb{Z}_n$ และ $K\cong\mathbb{Z}_m$

เพราะว่า $(mn)1=0\in\mathbb{Z}_{mn}$ ดังนั้น $\{0,m1,(2m)1,\ldots,(n-1)m1\}\subseteq H$ และสำหรับ $x\in H$ มีจำนวนเต็ม a ซึ่ง $x=a(m1)$ แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม q และ r ซึ่ง $x=a(m1)$ $=(nq+r)m1=(nq)m1+r(m1)=r(m1)$ โดยที่ $0\le r<n$ ทำให้ได้ $x=a(m1)=r(m1)\in$ $\{0,m1,(2m)1,\ldots,(n-1)m1\}$ ดังนั้น $H=\{0,m1,2m1,\ldots,(n-1)m1\}\cong\mathbb{Z}_n$ และด้วยการพิสูจน์ในทำนองเดียวกัน จะได้ $K=\{0,n1,2n1,\ldots,(m-1)n1\}\cong\mathbb{Z}_m$ เพราะฉะนั้น $nv=0$ ทุกๆ $v\in H$ และ $mv=0$ ทุกๆ $v\in K$

ต่อไปให้ $u\in\mathbb{Z}_{mn}$ แล้ว $u=u1=u(ms+nt)=(us)m+(ut)n$ โดยที่ $(us)m\in H$ และ $(ut)n\in K$ จึงได้ $\mathbb{Z}_{mn}=H+K$ สุดท้ายให้ $v\in H\cap K$ แล้ว $v\in H$ และ $v\in K$ ดังนั้น $nv=0$ และ $mv=0$ แต่ $v=v1=v(ms+nt)=(mv)s+(nv)t=0$ ทำให้ได้ $H\cap K=\{0\}$ ซึ่งแสดงว่า $\mathbb{Z}_{mn}=H\oplus K$

เพราะฉะนั้น $\mathbb{Z}_{mn}=H\oplus K\cong\mathbb{Z}_m\oplus\mathbb{Z}_n$

2. จะพิสูจน์โดยอุปนัยเชิงคณิตศาสตร์บน r ซึ่งเห็นชัดว่าทฤษฎีบทเป็นจริงถ้า $r=1$ จึงสมมติว่าทฤษฎีบทเป็นจริงสำหรับจำนวนเต็มบวก r และให้ $n_1,n_2,\cdots,n_{r+1}$ เป็นจำนวนเต็มบวกซึ่ง $(n_i,n_j)=1$ ทุกๆ $1\le i\ne j\le r+1$ และ $n=n_1n_2\cdots n_{r+1}$ ให้ $s=n_{r+1}$ และ $m=n_1n_2\cdots n_r$ แล้ว $(m,s)=1$ ทำให้ได้โดยข้อ 1 ว่า $\mathbb{Z}_n=\mathbb{Z}_{ms}\cong\mathbb{Z}_m\oplus\mathbb{Z}_s$ แต่โดยสมมติฐานของอุปนัยซึ่ง $m=$ $n_1n_2\cdots n_r$ จะได้ $\mathbb{Z}_m\cong\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_r}$ ดังนั้น $\mathbb{Z}_n=\mathbb{Z}_{ms}\cong\mathbb{Z}_m\oplus\mathbb{Z}_s\cong\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_r}\oplus\mathbb{Z}_{n_{r+1}}$ ❑

2.1.5 **บทแทรก** ถ้า n เป็นจำนวนเต็มซึ่ง $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ โดยที่ $r,k_1,\ldots,k_r$ เป็นจำนวนเต็มบวกและ $p_1,\ldots,p_r$ เป็นจำนวนเฉพาะที่ต่างกันทั้งหมด แล้ว $\mathbb{Z}_n\cong\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_r}$ เมื่อ $n_i=p_i^{k_i}$ ทุกๆ $1\le i\le r$ ❑

สังเกตว่าบทแทรก 2.1.5 กล่าวว่าทุกๆ กรุปวัฏจักรอันดับจำกัดเขียนได้ในรูปผลบวกตรงของกรุปวัฏจักรที่มีอันดับเป็นกำลังของจำนวนเฉพาะซึ่งเป็นกรณีเฉพาะของทฤษฎีบทหลักมูลของกรุปอาบีเลียนก่อกำเนิดแบบจำกัดที่จะศึกษากันต่อไปในบทนี้

แบบฝึกหัด 2.1

1. ให้ G เป็นกรุปอาบีเลียน m เป็นจำนวนเต็มบวกและ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่าเซตในข้อต่อไปนี้เป็นกรุปย่อยของ G

   1.1 $mG = \{mu | u \in G\}$ 1.2 $G[m] = \{u \in G | mu = 0\}$

   1.3 $G(p) = \{u \in G | (\exists n \geq 0)(|u| = p^n)\}$

   1.4 $G_t = \{u \in G \mid |u|$ เป็นจำนวนจำกัด$\}$ [**หมายเหตุ**: เราเรียก G_t ว่า *กรุปย่อยทอร์ชัน (torsion subgroup)* ของ G แต่ถ้า $G_t = G$ เราเรียก G ว่า *กรุปทอร์ชัน (torsion group)* และถ้า $G_t = \{0\}$ เราเรียก G ว่า *กรุปทอร์ชันเสรี (torsion free group)*]

2. ให้ $I \neq \phi$ และ $\{G_i | i \in I\}$ เป็นหมู่ของกรุปอาบีเลียนและ m เป็นจำนวนเต็มบวก จงพิสูจน์ว่าถ้า $G \cong \prod_{i \in I} G_i$ แล้ว $mG \cong \prod_{i \in I} mG_i$ และ $(G/mG) \cong \prod_{i \in I}(G_i/mG_i)$

3. ให้ $I \neq \phi$ และ $\{G_i | i \in I\}$ เป็นหมู่ของกรุปอาบีเลียนและสำหรับแต่ละ $i \in I$ ให้ H_i เป็นกรุปย่อยปรกติของ G_i จงพิสูจน์ว่า $\prod_{i \in I} H_i$ เป็นกรุปย่อยปรกติของ $\prod_{i \in I} G_i$ และ $(\prod_{i \in I} G_i / \prod_{i \in I} H_i) \cong \prod_{i \in I}(G_i/H_i)$

4. ให้ $I \neq \phi$ และ $\{G_i | i \in I\}$ เป็นหมู่ของกรุป H เป็นกรุปและ $\{\varphi_i : H \to G_i | i \in I\}$ เป็นหมู่ของสาทิสสัณฐาน จงพิสูจน์ว่ามีสาทิสสัณฐาน $\varphi : H \to \prod_{i \in I} G_i$ เพียงหนึ่งเดียวซึ่ง $\pi_i \circ \varphi = \varphi_i$ ทุกๆ $i \in I$

5. ให้ $I \neq \phi$ และ $\{A_i | i \in I\}$ เป็นหมู่ของกรุปอาบีเลียน B เป็นกรุปอาบีเลียนและ $\{\psi_i : A_i \to B | i \in I\}$ เป็นหมู่ของสาทิสสัณฐาน จงพิสูจน์ว่ามีสาทิสสัณฐาน $\psi : \sum_{i \in I} A_i \to B$ เพียงหนึ่งเดียวซึ่ง $\psi \circ \iota_i = \psi_i$ ทุกๆ $i \in I$ โดยที่ $\iota_k : A_k \to \sum_{i \in I} A_i$ นิยามโดย $\iota_k(a) = (a_i)_{i \in I}$ เมื่อ $a_i = a$ ถ้า $i = k$ และ $a_i = e$ ถ้า $i \neq k$ ทุกๆ $a \in A_k$ และทุกๆ $k \in I$

6. จงพิสูจน์ว่าถ้า $I \neq \phi$ และ G เป็นผลคูณตรงของหมู่ของกรุป $\{G_i | i \in I\}$ แล้วมีหมู่ของกรุปย่อยปรกติ $\{N_i | i \in I\}$ ของ G ซึ่ง (i) $G = < \bigcup_{i \in I} N_i >$ (ii) $N_i \cong G_i$ ทุกๆ $i \in I$ และ (iii) $N_k \cap < \bigcup_{i \neq k} N_i > = \{e\}$ ทุกๆ $k \in I$

7. ให้ $\{G_i | i \in I\}$ เป็นหมู่ของกรุป $J \subseteq I$ และ $\alpha : \prod_{i \in J} G_i \to \prod_{i \in I} G_i$ นิยามโดย $\alpha((a_i)_{i \in J}) = (b_i)_{i \in I}$ โดยที่ $b_j = a_j$ สำหรับ $j \in J$ และ $b_i = e_i$ (เอกลักษณ์ของ G_i) สำหรับ $i \notin J$ จงพิสูจน์ว่า α เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่งและ $\prod_{i \in I} G_i \Big/ \alpha\left(\prod_{j \in J} G_j\right) \cong \prod_{i \in I \setminus J} G_i$

8. จงวางนัยทั่วไปของทฤษฎีบทและแบบฝึกหัดในหัวข้อ 1.8 สำหรับหมู่ของกรุป $\{G_i | i \in I\}$

2.2 ทฤษฎีบทเศษเหลือของจีน

มีเรื่องเล่าต่อๆ กันมา(โดยไม่ปรากฏหลักฐาน)ว่า แม่ทัพชาวจีนสมัยสงครามสามก๊กท่านหนึ่งชื่นชอบวิชาการคำนวณ ทุกครั้งหลังการสู้รบจะนับจำนวนทหารที่อยู่ในความรับผิดชอบซึ่งไม่บาดเจ็บหรือล้มตาย เช่นครั้งหนึ่งท่านคาดคะเนว่าเหลือทหารอยู่ไม่เกิน 15,000 นาย และเพราะ $15{,}000 < 17{,}017$ โดยที่ $17017 = 7\times 11\times 13\times 17$ ท่านจึงสั่งให้ทหารทุกคนเข้าแถวสี่แบบคือ เมื่อเข้าแถว แถวละ 7 นายปรากฏว่าเหลือเศษ 6 นาย เมื่อเข้าแถว แถวละ 11 นาย ปรากฏว่าเหลือเศษ 7 นาย เมื่อเข้าแถว แถวละ 13 นายปรากฏว่าเหลือเศษ 5 นาย และเมื่อเข้าแถว แถวละ 17 นายปรากฏว่าเหลือเศษ 2 นาย หลังจากนั้นท่านก็คำนวณอยู่สักครู่ก็สามารถบอกได้ว่า มีทหารที่ไม่บาดเจ็บหรือล้มตายในกองทัพของท่านเหลืออยู่ 14,384 นาย

นักคณิตศาสตร์ในยุคต่อมา สนใจศึกษาวิธีการคำนวณของท่านและได้พิสูจน์เป็นหลักการคำนวณไว้ในหลายสาขาวิชา เช่นวิชาทฤษฎีจำนวนและวิชาพีชคณิต โดยให้ชื่อหลักการเพื่อเป็นเกียรติแด่ท่านแม่ทัพจีนผู้นี้ว่า "ทฤษฎีบทเศษเหลือของจีน (The Chinese Remainder Theorem)"

สังเกตว่าท่านแม่ทัพเริ่มต้นด้วยการแยกตัวประกอบของ $N = 17017$ ในรูปผลคูณของจำนวนเต็มซึ่งแต่ละคู่เป็นจำนวนเฉพาะสัมพัทธ์ ทำให้ได้โดยทฤษฎีบท 2.1.4 ว่า $\mathbb{Z}_{17017} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{13} \oplus \mathbb{Z}_{17}$ แต่ทฤษฎีบท 2.1.4 ยังไม่ได้แสดงสมสัณฐาน เราจึงสังเกตต่อไปว่า $14{,}384 \equiv 6 \pmod 7$, $14{,}384 \equiv 7 \pmod{11}$, $14{,}384 \equiv 5 \pmod{13}$ และ $14{,}384 \equiv 2 \pmod{17}$ นั่นคือ $14{,}384 \in \mathbb{Z}_{17017}$ เป็นคำตอบของระบบสมการสมภาค $z \equiv 6 \pmod 7$, $z \equiv 7 \pmod{11}$, $z \equiv 5 \pmod{13}$ และ $z \equiv 2 \pmod{17}$

นอกจากนี้ยังอาจสังเกตว่า การส่งต่อไปนี้เป็นสมสัณฐาน

1. $12 = 4\times 3$ โดยที่ $(4,3) = 1$ แล้วการส่ง $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4 \oplus \mathbb{Z}_3$ ซึ่งนิยามโดย $\phi([z]_{12}) = ([z]_4, [z]_3)$ [ตัวอย่างเช่น $\phi([5]_{12}) = ([5]_4, [5]_3) = ([1]_4, [2]_3)$ เป็นต้น] เป็นสมสัณฐาน

2. $210 = 14\times 15$ โดยที่ $(14,15) = 1$ แล้ว $\phi : \mathbb{Z}_{210} \to \mathbb{Z}_{14} \oplus \mathbb{Z}_{15}$ ซึ่งนิยามโดย $\phi([z]_{210}) = ([z]_{14}, [z]_{15})$ [เช่น $\phi([150]_{210}) = ([150]_{14}, [150]_{15}) = ([10]_{14}, [0]_{15})$ เป็นต้น] เป็นสมสัณฐาน

3. $720 = 16\times 9\times 5$ โดยที่ $(16,9) = 1$, $(16,5) = 1$ และ $(9,5) = 1$ แล้ว $\phi : Z_{720} \to Z_{16} \oplus Z_9 \oplus Z_5$ นิยามโดย $\phi([z]_{210}) = ([z]_{14}, [z]_{15})$ [เช่น $\phi([516]_{720}) = ([516]_{16}, [516]_9, [516]_5) = ([4]_{16}, [3]_9, [1]_5)$ เป็นต้น] เป็นสมสัณฐาน

การเป็นฟังก์ชันทั่วถึงของสมสัณฐาน จะทำให้ได้คำตอบของระบบสมการสมภาคและการเป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งจะทำให้ได้ว่าคำตอบมีเพียงคำตอบเดียว เราจึงได้ทฤษฎีบทเศษเหลือ

ของจีนต่อไปนี้แสดงการมีคำตอบเพียงหนึ่งเดียวของระบบสมการสมภาคเชิงเส้น $z \equiv z_1 \pmod{n_1}$, $\ldots$, $z \equiv z_r \pmod{n_r}$

2.2.1 **ทฤษฎีบทเศษเหลือของจีน** (The Chinese Remainder Theorem)

ให้ $r, n, n_1, \ldots, n_r$ เป็นจำนวนเต็มบวกซึ่ง $n = n_1 \cdot n_2 \cdots n_r$ ถ้า $(n_i, n_j) = 1$ ทุกๆ $1 \le i \ne j \le r$ แล้ว $\phi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ ซึ่งนิยามโดย $\phi([z]_n) = ([z]_{n_1}, [z]_{n_2}, \ldots, [z]_{n_r})$ (เมื่อ $[z]_t$ แทนเซตสมมูลของ z มอดูโล t สำหรับแต่ละจำนวนเต็มบวก t) เป็นสมสัณฐาน ❑

ขอละการพิสูจน์ว่า $\phi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ ที่นิยามในทฤษฎีบทเศษเหลือของจีนเป็นสมสัณฐานไว้เป็นแบบฝึกหัด อย่างไรก็ตามทฤษฎีบทเศษเหลือของจีนไม่ได้แสดงการหาคำตอบของระบบสมการสมภาค จึงได้มีการพิสูจน์ทฤษฎีบทต่อไปนี้ซึ่งบทพิสูจน์แสดงวิธีการหาคำตอบของระบบสมการสมภาคและเป็นวิธีการเดียวกับที่ท่านแม่ทัพจีนใช้คำนวณหาคำตอบ 14,384 ข้างต้น

2.2.2 **สูตรการผกผัน** (Inversion Formula) ให้ $n_1, n_2, \cdots, n_r$ เป็นจำนวนเต็มบวก r จำนวนโดยที่ $(n_i, n_j) = 1$ ทุกๆ $1 \le i \ne j \le r$ และให้ $n = n_1 \cdot n_2 \cdots n_r$ ถ้า $z_1, \cdots, z_r$ เป็นจำนวนเต็มซึ่ง $0 \le z_i < n_i$ ทุกๆ $1 \le i \le r$ แล้วมีจำนวนเต็ม z ซึ่ง $z \equiv z_i \pmod{n_i}$ ทุกๆ $1 \le i \le r$

บทพิสูจน์ แต่ละ $1 \le i \le r$ นิยาม $a_i = \dfrac{n}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_r$ และ b_i เป็นจำนวนเต็มบวกซึ่ง $a_i b_i \equiv 1 \pmod{n_i}$ และให้ $e_i = a_i b_i$ แล้ว $e_i \equiv 1 \pmod{n_i}$ และ $e_j \equiv 0 \pmod{n_i}$ ถ้า $j \ne i$ นั่นคือ

$$
\begin{array}{llllll}
e_1 \equiv 1 \pmod{n_1}; & e_1 \equiv 0 \pmod{n_2}; & e_1 \equiv 0 \pmod{n_3}; & \ldots & e_1 \equiv 0 \pmod{n_r} \\
e_2 \equiv 0 \pmod{n_1}; & e_2 \equiv 1 \pmod{n_2}; & e_2 \equiv 0 \pmod{n_3}; & \ldots & e_2 \equiv 0 \pmod{n_r} \\
e_3 \equiv 0 \pmod{n_1}; & e_3 \equiv 0 \pmod{n_2}; & e_3 \equiv 1 \pmod{n_3}; & \ldots & e_3 \equiv 0 \pmod{n_r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
e_r \equiv 0 \pmod{n_1}; & e_r \equiv 0 \pmod{n_2}; & e_r \equiv 0 \pmod{n_3}; & \ldots & e_r \equiv 1 \pmod{n_r}
\end{array}
$$

เพราะฉะนั้น

$$
\begin{aligned}
z_1 e_1 + z_2 e_2 + \cdots + z_r e_r &\equiv z_1 \cdot 1 + z_2 \cdot 0 + \cdots + z_r \cdot 0 \equiv z_1 \pmod{n_1}, \\
z_1 e_1 + z_2 e_2 + \cdots + z_r e_r &\equiv z_1 \cdot 0 + z_2 \cdot 1 + \cdots + z_r \cdot 0 \equiv z_2 \pmod{n_2} \\
&\vdots \qquad\qquad\qquad \vdots \\
z_1 e_1 + z_2 e_2 + \cdots + z_r e_r &\equiv z_1 \cdot 0 + z_2 \cdot 0 + \cdots + z_r \cdot 1 \equiv z_r \pmod{n_r}
\end{aligned}
$$

ซึ่งแสดงว่า $z = z_1 e_1 + z_2 e_2 + \cdots + z_r e_r$ คือจำนวนเต็มที่ต้องการ ❑

แม้ว่าทฤษฎีบทเศษเหลือของจีนจะเป็นทฤษฎีบทที่กล่าวเฉพาะกรุปอาบีเลียน แต่ยังมีการขยายผลบางส่วนไปสู่กรณีกรุปนอนอาบีเลียนด้วยซึ่งจะขอกล่าวไว้ในแบบฝึกหัด 2.2 ต่อไป

แบบฝึกหัด 2.2

1. ให้ $n_1, n_2, \cdots, n_r$ เป็นจำนวนเต็มบวก r จำนวนโดยที่ $(n_i, n_j) = 1$ ทุกๆ $1 \le i \ne j \le r$ และให้ G เป็นกรุป (อาจเป็นกรุปนอนอาบีเลียน) ซึ่ง $|G| = n = n_1 n_2 \cdots n_r$ จงพิสูจน์ว่าถ้ามีกรุปย่อยปรกติ $N_1, N_2, \cdots, N_r$ ของ G ซึ่ง $|N_i| = n_i$ ทุกๆ $1 \le i \le r$ แล้ว $G \cong N_1 \times \cdots \times N_r$
   [ข้อแนะนำ: พิสูจน์โดยอุปนัยเชิงคณิตศาสตร์]
2. ให้ G เป็นกรุป (อาจเป็นกรุปนอนอาบีเลียน) ซึ่ง $|G| = n$ โดยที่ $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ เมื่อ $r, k_1, \ldots, k_r$ เป็นจำนวนเต็มบวก $p_1, \ldots, p_r$ เป็นจำนวนเฉพาะที่ต่างกันทั้งหมด จงพิสูจน์ว่าถ้ามีกรุปย่อยปรกติ $P_1, P_2, \cdots, P_r$ ของ G ซึ่ง $|P_i| = p_i^{k_i}$ ทุกๆ $1 \le i \le r$ แล้ว
   $G \cong P_1 \times \cdots \times P_r$
3. จงพิสูจน์ทฤษฎีบทเศษเหลือของจีน
4. ให้ $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ เมื่อ $r, k_1, \ldots, k_r$ เป็นจำนวนเต็มบวก $p_1, \ldots, p_r$ เป็นจำนวนเฉพาะที่ต่างกันทั้งหมดและแต่ละ $1 \le i \le r$ ให้ $m_i = \frac{n}{p_i^{k_i}}$ และ $\overline{m}_i$ เป็นเซตสมมูลมอดูโล n ใน $\mathbb{Z}_n$ จงพิสูจน์ว่า $|\overline{m}_i| = p_i^{k_i}$

2.3 ฐานและการเป็นอิสระเชิงเส้น

ให้ A เป็นกรุปอาบีเลียนและ $\phi \ne X \subseteq A$ ขอทบทวนว่ากรุปย่อย $< X >$ ของ A ก่อกำเนิดโดย X คือกรุปที่ประกอบด้วยสมาชิกของ A ที่เขียนได้ในรูป *ผลบวกเชิงเส้น (linear combination)* ของสมาชิกใน X นั่นคือ $a \in < X >$ ก็ต่อเมื่อมีจำนวนเต็มบวก n มี $a_1, a_2, \cdots, a_n \in X$ และ $z_1, z_2, \cdots, z_n \in \mathbb{Z}$ ซึ่ง $a = z_1 a_1 + z_2 a_2 + \cdots + z_n a_n$ โดยเฉพาะกรุปวัฏจักร $< x >$ คือ $\{zx | z \in \mathbb{Z}\}$

2.3.1 บทนิยาม ให้ A เป็นกรุปและ $\phi \ne X \subseteq A$ เรากล่าวว่า X เป็น *ฐาน (basis)* ของ A ถ้า (i) $A = < X >$ และ (ii) ทุกๆ จำนวนเต็มบวก n ทุกๆ $a_1, a_2, \cdots, a_n \in X$ ที่ต่างกันทั้งหมดและทุกๆ $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ ถ้า $z_1 a_1 + z_2 a_2 + \cdots + z_n a_n = 0$ แล้ว $z_1 = z_2 = \cdots = z_n = 0$

เรานิยามฐานของกรุปอาบีเลียนในลักษณะเป็นฐานของปริภูมิเวกเตอร์ (vector space) และโดยความเป็นจริง กรุปอาบีเลียนคือปริภูมิเวกเตอร์เหนือ $\mathbb{Z}$ จึงกล่าวได้ว่าขนาด (cardinality) ของฐานของกรุปอาบีเลียน A คือ *ลำดับที่ (rank)* ของ A ซึ่งแทนด้วยสัญลักษณ์ rank A

ในกรณี rank A คือจำนวนจำกัด n แล้ว n เป็นจำนวนเต็มบวกมากสุดซึ่ง $a_1, a_2, \cdots, a_n \in A$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น นั่นคือ A เป็นกรุปที่มีลำดับที่ n ก็ต่อเมื่อ (i) มี $\{a_1, a_2, \cdots, a_n\} \subseteq A$ เป็นเซตย่อย $\mathbb{Z}-$อิสระเชิงเส้น และ (ii) สำหรับ $b_1, \cdots, b_n, b_{n+1} \in A$ และ $z_1, \cdots, z_n, z_{n+1} \in \mathbb{Z}$ ถ้า $z_1b_1 + z_2b_2 + \cdots + z_{n+1}b_{n+1} = 0$ แล้วมี $b_i \in \{b_1, \cdots, b_n, b_{n+1}\}$ ซึ่ง $b_i \neq 0$

2.3.2 **ตัวอย่าง** ถ้า $0 \neq a \in \mathbb{Z}$ แล้ว $za \neq 0$ ทุกๆ จำนวนเต็ม $z \neq 0$ ดังนั้น rank $\mathbb{Z} \geq 1$ นอกจากนี้ $a_2a_1 + (-a_1)a_2 = 0$ ทุกๆ $a_1, a_2 \in Z \setminus \{0\}$ ซึ่งแสดงว่า rank $\mathbb{Z} \leq 1$ ทำให้ได้ rank $\mathbb{Z} = 1$ ❍

2.3.3 **ตัวอย่าง** ถ้า $0 \neq a \in \mathbb{Q}$ แล้ว $za \neq 0$ ทุกๆ จำนวนเต็ม $z \neq 0$ ทำให้ได้ $\{a\}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น นอกจากนี้ถ้า $a_1, a_2 \in \mathbb{Q} \setminus \{0\}$ แล้วมี $r_1, r_2, s_1, s_2 \in \mathbb{Z} \setminus \{0\}$ ซึ่ง $a_1 = \frac{r_1}{s_1}$ และ $a_2 = \frac{r_2}{s_2}$ ถ้าเลือก $z_1 = r_2s_1$ และ $z_2 = -r_1s_2$ แล้ว $z_1, z_2 \in \mathbb{Z} \setminus \{0\}$ และ $z_1a_1 + z_2a_2 = r_2s_1\frac{r_1}{s_1} - r_1s_2\frac{r_2}{s_2} = 0$ เพราะฉะนั้น rank $\mathbb{Q} = 1$ ❍

2.3.4 **ตัวอย่าง** rank $\mathbb{Z}_n = 0$ เพราะว่า $na = 0$ ทุกๆ $a \in \mathbb{Z}_n$ ดังนั้นทุกๆ เซตย่อยของ $\mathbb{Z}_n$ ไม่เป็น $\mathbb{Z}-$อิสระเชิงเส้น

เราสามารถประยุกต์การพิสูจน์นี้ในกรณีทั่วไป จะได้ว่าลำดับที่ของทุกๆ กรุปอาบีเลียนขนาดจำกัดเป็นศูนย์ เพราะว่าถ้า A เป็นกรุปอาบีเลียนขนาดจำกัดแล้วมีจำนวนเต็มบวก n ซึ่ง $|A| = n$ ดังนั้น $na = 0$ ทุกๆ $a \in A$ ❍

2.3.5 **ตัวอย่าง** ให้ n เป็นจำนวนเต็มบวก เนื่องจาก $\mathbb{Z}^n$ เป็นกรุปเสรีบนตัวก่อกำเนิด n ตัวคือ $a_1 = (1,0,0,\ldots,0), \ldots, a_n = (0,0,\ldots,0,1)$ และเห็นชัดว่าตัวก่อกำเนิด n ตัวนี้เป็น $\mathbb{Z}-$อิสระเชิงเส้น ดังนั้น rank $\mathbb{Z}^n = n$ ❍

แบบฝึกหัด 2.3

1. จงพิสูจน์ว่ากรุป $\mathbb{R}$ ของจำนวนจริงทั้งหมดกับการบวกแบบปกติเป็นกรุปที่มีลำดับที่อนันต์ [**ข้อแนะนำ** : แสดงว่าทุกๆ เซตจำกัดของ $\mathbb{R}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น แต่ไม่ก่อกำเนิด $\mathbb{R}$]
2. ให้ A เป็นกรุปอาบีเลียนและ $\phi \neq X \subseteq A$ จงพิสูจน์ว่า X เป็น $\mathbb{Z}-$อิสระเชิงเส้น ก็ต่อเมื่อแต่ละ $0 \neq x \in X$ มี $0 \notin \{z_1, \ldots, z_k\} \subseteq \mathbb{Z}$ และ $\{a_1, \ldots, a_k\}$ ของสมาชิกที่ต่างกันทั้งหมดใน X อย่างละเพียงชุดเดียวที่ทำให้ $x = z_1a_1 + \cdots + z_na_n$
3. จงพิสูจน์ว่า ผลบวกตรง $\mathbb{Z}^n := \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n}$ เมื่อ n เป็นจำนวนเต็มบวกเป็นกรุปอาบีเลียนที่มีฐานคือ $\{a_1 = (1,0,0,\ldots,0), \ldots, a_n = (0,0,\ldots,0,1)\}$ พร้อมกับสรุปว่า rank $\mathbb{Z}^n = n$

4. จงพิสูจน์ว่าถ้า A เป็นกรุปอาบีเลียนแล้ว $\operatorname{rank}(\mathbb{Z}^n \oplus A) = n + \operatorname{rank} A$
5. จงหา $\operatorname{rank}(\mathbb{Z}^5 \oplus \mathbb{Z}^{16} \oplus \mathbb{Z}^7)$ และจงแสดงว่า $\mathbb{Z}^5 \oplus \mathbb{Z}^3 \cong \mathbb{Z}^8$

2.4 กรุปอาบีเลียนเสรี

หัวข้อนี้ เราประยุกต์แนวคิดเรื่องผลบวกตรงของกรุปเพื่อให้นิยามกรุปอาบีเลียนเสรีและด้วยแนวคิดนี้ยังทำให้เราสามารถอธิบายว่า ทุกๆ กรุปอาบีเลียนก่อกำเนิดแบบจำกัดสร้างจากกรุปวัฏจักรได้อย่างไร นอกจากนี้ยังเป็นการวางนัยทฤษฎีบท 2.1.4 และบทแทรก 2.1.5

2.4.1 **บทนิยาม** เรากล่าวว่ากรุป F เป็น *กรุปอาบีเลียนเสรี (free abelian group)* ถ้า F เป็นผลบวกตรงของกรุปวัฏจักรอันดับอนันต์

2.4.2 **เกณฑ์การเป็นกรุปอาบีเลียนเสรี** (Free Abelian Group Criterion)

ให้ F เป็นกรุปอาบีเลียน แล้วข้อความต่อไปนี้สมมูลกัน

1. F มีฐานที่ไม่ใช่เซตว่าง
2. F เป็นกรุปอาบีเลียนเสรี
3. F สมสัณฐานกับผลบวกตรงของกรุป $\mathbb{Z}$
4. มีเซต X ที่ไม่ใช่เซตว่างและฟังก์ชัน $\iota : X \to F$ ซึ่งสอดคล้องข้อความ : สำหรับทุกๆ กรุปอาบีเลียน A และฟังก์ชัน $f : X \to A$ มีสาทิสสัณฐาน $\bar{f} : F \to A$ เพียงหนึ่งเดียวที่ทำให้ $\bar{f} \circ \iota = f$ [**หมายเหตุ** : เราเรียกสมบัติข้อ 4 นี้ว่า *สมบัติการส่งเอกภาพ (universal mapping property)* ของ F และกล่าวว่า f *ชักนำ (induce)* สาทิสสัณฐาน $\bar{f}$]

บทพิสูจน์ $(1) \Rightarrow (2)$ ให้ $X \neq \phi$ เป็นฐานของ F แล้ว $nx = 0$ ก็ต่อเมื่อ $n = 0$ ทุกๆ $x \in X$ และทุกๆ จำนวนเต็ม n ดังนั้น $< x >$ เป็นกรุปวัฏจักรอันดับอนันต์ทุกๆ $x \in X$ และเป็นกรุปย่อยปรกติของ F (เพราะ F เป็นกรุปอาบีเลียน) เนื่องจาก $F = < X >$ จึงได้ $F = < \bigcup_{x \in X} < x >>$ สมมติว่ามี $z \in X$ ซึ่ง $< z > \cap < \bigcup_{x \in X \setminus \{z\}} < x >> \neq \phi$ แล้วมีจำนวนเต็ม $k, n, n_1, \ldots, n_k$ และ $a_1, \ldots, a_k \in X$ ที่ต่างกันทั้งหมดซึ่ง $nz = n_1 a_1 + n_2 a_2 + \cdots + n_k a_k$ จะขัดแย้งกับสมบัติของฐาน ดังนั้น $< z > \cap < \bigcup_{x \in X \setminus \{z\}} < x >> = \phi$ เพราะฉะนั้น F เป็นผลบวกตรงของ $\{< x > | x \in X\}$ ซึ่งแสดงว่า F เป็นกรุปอาบีเลียนเสรี

$(2) \Rightarrow (3)$ เนื่องจากทุกๆ กรุปวัฏจักรอันดับอนันต์สมสัณฐานกับ $\mathbb{Z}$

$(3) \Rightarrow (1)$ ให้ F สมสัณฐานกับผลบวกตรงของกรุป $\mathbb{Z}$ โดยให้ X เป็นเซตดรรชนีจำนวนของ $\mathbb{Z}$ ในผลบวกตรงและแต่ละ $x \in X$ ให้ θ_x แทนสมาชิก $(u_i)_{i \in X}$ ในผลบวกตรงของ $\mathbb{Z}$ ซึ่ง $u_i = 0$ ถ้า $i \neq x$ และ $u_i = 1$ ถ้า $i = x$ แล้วเห็นชัดว่า $\{\theta_x | x \in X\}$ เป็นฐานของผลบวกตรงของ $\mathbb{Z}$ นอกจากนี้เห็นได้ชัดว่าสมสัณฐานส่ง $\{\theta_x | x \in X\}$ ไปเป็นฐานของ F

$(1) \Rightarrow (4)$ ให้ $X \neq \phi$ เป็นฐานของ F และให้ $\iota : X \to F$ เป็นฟังก์ชันกำกัดลงบน X ของฟังก์ชันเอกลักษณ์บน F สมมติ A เป็นกรุปอาบีเลียนและ $f : X \to A$ แล้วนิยาม $\bar{f} : F \to A$ โดย $\bar{f}(u) = n_1 f(x_1) + n_2 f(x_2) + \cdots + n_k f(x_k)$ สำหรับแต่ละ $u \in F$ ซึ่งมี $x_1, \ldots, x_k \in X$ และจำนวนเต็ม $n_1, \ldots, n_k$ ที่ทำให้ $u = n_1 x_1 + \cdots + n_k x_k$ แล้ว $\bar{f}$ เป็นฟังก์ชัน เพราะ X เป็นฐานของ F ทำให้แต่ละสมาชิกของ F เขียนได้วิธีเดียวในรูปผลบวกเชิงเส้น ดังนั้น $x_1, \ldots, x_k \in X$ และจำนวนเต็ม $n_1, \ldots, n_k$ มีเพียงชุดเดียวสำหรับแต่ละ $u \in F$ และเพราะ F เป็นกรุปอาบีเลียน จึงเห็นชัดว่า $\bar{f}$ เป็นสาทิสสัณฐานและ $\bar{f} \circ \iota = f$

ให้ $g : F \to A$ เป็นฟังชันซึ่งสอดคล้องข้อ 4 แล้วจะแสดงว่า $g = \bar{f}$ ให้ $u \in F$ เพราะ X ก่อกำเนิด F ดังนั้นมี $x_1, \ldots, x_k \in X$ และจำนวนเต็ม $n_1, \ldots, n_k$ ซึ่ง $u = n_1 x_1 + \cdots + \ + n_k x_k$ ทำให้ได้

$$g(u) = g(n_1 x_1 + \cdots + n_k x_k) = n_1 g(x_1) + \cdots + n_k g(x_k) \text{ (เพราะ } g \text{ เป็นสาทิสสัณฐาน)}$$

$$= n_1 (g \circ \iota)(x_1) + \cdots + n_k (g \circ \iota)(x_k) \quad \text{(เพราะว่า } \iota \text{ เป็นฟังก์ชัน เอกลักษณ์)}$$

แต่ $g \circ \iota = f$ จะได้ $g(u) = n_1 f(x_1) + \cdots + n_k f(x_k) = \bar{f}(u)$ ซึ่งเป็นอันจบการพิสูจน์

$(4) \Rightarrow (3)$ ให้ $\iota : X \to F$ แล้วสร้างผลบวกตรงของ $\mathbb{Z}$ จำนวนเท่ากับ $|X|$ (นั่นคือให้จำนวนของ $\mathbb{Z}$ ในผลบวกตรงดรรชนีโดย X) แล้วการพิสูจน์ใน $(3) \Rightarrow (1)$ แสดงว่า $\{\theta_x | x \in X\}$ เป็นฐานของผลบวกตรงของ $\mathbb{Z}$ แล้วจาก $(3) \Rightarrow (4)$ และ $|X| = |Y|$ จะได้ F สมสัณฐานกับผลบวกตรงของ $\mathbb{Z}$ ❑

2.4.3 หมายเหตุ ให้ X และ Y เป็นเซตซึ่ง $X \subseteq Y$ จะเรียก $\iota : X \to F$ ซึ่งเป็นฟังก์ชันกำกัดลงบน X ของฟังก์ชันเอกลักษณ์บน Y ว่า *การส่งเซตย่อย (inclusion maping)*

เกณฑ์การเป็นกรุปอาบีเลียนเสรี แสดงการสร้างกรุปอาบีเลียนเสรีซึ่งมีเซตที่กำหนดให้เป็นฐาน โดยกล่าวว่าวิธีง่ายที่สุดคือให้ F เป็นผลบวกตรงของ $\mathbb{Z}$ ซึ่งดรรชนีโดย X สำหรับแต่ละเซต X นอกจากนี้การพิสูจน์ของ $(3) \Rightarrow (1)$ ยังแสดงว่า $\{\theta_x | x \in X\}$ เป็นฐานของผลบวกตรงของ $\mathbb{Z}$ ซึ่งดรรชนีโดย X จึงเป็นฐานของ F เนื่องจากฟังก์ชัน $\iota : X \to F$ ซึ่งส่ง $x \to \theta_x$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง จึงอาจพิจารณาว่า $X \subseteq F$ ซึ่งจะได้โดยข้อ 4 ว่า X เป็นฐานของ F และกรุปวัฏจักร

$<\theta_x> = \{n\theta_x | n \in \mathbb{Z}\} = \mathbb{Z}\theta_x$ อาจเขียนเป็น $<x> = \mathbb{Z}x$ ดังนั้น $F = \sum_{x \in X} \mathbb{Z}x$ เป็นผลบวกตรงของกรุปวัฏจักรอันดับอนันต์ โดยที่แต่ละสมาชิกของ F เขียนได้ในรูปผลบวกเชิงเส้น $n_1x_1 + \cdots + n_kx_k$

ถ้า F เป็นกรุปอาบีเลียนเสรีที่มีเซต X เป็นฐานของ F จะกล่าวอย่างสั้นๆ ว่า "F เป็นกรุปเสรีบนเซต X (F is free on X)"

เราทราบกันมาก่อนแล้วว่า ลำดับที่คือจำนวนสมาชิกของฐานใดๆ ในปริภูมิเวกเตอร์จะมีขนาดเท่ากันเสมอ เราจึงจะแสดงในทฤษฎีบทต่อไปว่าฐานใดๆ ของกรุปอาบีเลียนเสรีมีขนาดเท่ากัน นอกจากนี้ยังจะพิสูจน์ว่าฐานใดๆ ของกรุปอาบีเลียนเสรีซึ่งสมสัณฐานกัน มีขนาดเท่ากัน

2.4.4 **ทฤษฎีบท** ถ้า X และ Y ต่างเป็นฐานของกรุปอาบีเลียนเสรี F แล้ว $|X| = |Y|$

บทพิสูจน์ (i) จะพิสูจน์ก่อนว่า "ถ้า F มีฐานขนาดจำกัด แล้วทุกๆ ฐานของ F มีขนาดจำกัด"

ให้ X เป็นฐานของกรุปอาบีเลียนเสรี F ซึ่ง $|X| = n$ เป็นจำนวนจำกัด แล้วมีสมสัณฐาน $\alpha : F \to \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$ ซึ่งเห็นชัดว่า $2F = \{2u | u \in F\}$ เป็นกรุปย่อยของ F นอกจากนี้ $\beta : 2u \to 2\alpha(u)$ สำหรับแต่ละ $u \in F$ เป็นสมสัณฐานจาก $2F$ ไปยัง $\underbrace{2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}}_{n}$ ทำให้ได้ $F/2F \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n} \Big/ \underbrace{2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}}_{n} \cong \underbrace{(\mathbb{Z}/2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})}_{n} \cong \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{n}$ และเพราะ $|\mathbb{Z}_2| = 2$ ดังนั้น $|F/2F| = 2^n$

ให้ Y เป็นฐานของ F แล้วจะพิสูจน์ว่า "$|Y| \le n$ ถ้า $|Y| \ge r$ ไม่ว่า r จะเป็นจำนวนเต็มบวกใดๆ" โดยให้ r เป็นจำนวนเต็มบวกซึ่ง $|Y| \ge r$ แล้ว $F \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{|Y|}$ และโดยการพิสูจน์ของย่อหน้าก่อน จะได้ $|F/2F| \ge 2^r$ ซึ่งทำให้ได้ $2^n \ge 2^r$ ดังนั้น $n \ge r$ ต่อไปสมมติว่า $|Y| > n$ แล้ว $|Y| \ge n+1$ และจะได้โดยการพิสูจน์ก่อนหน้านี้ว่า $n \ge n+1$ ซึ่งเป็นไปไม่ได้ เพราะฉะนั้น $|Y| \le n$ ซึ่งแสดงว่า $|Y|$ เป็นจำนวนจำกัด

ให้ $|Y| = m \le n$ แล้วโดยผลการพิสูจน์ในย่อแรกของบทพิสูจน์ (i) จะได้ $|F/2F| = 2^m$ ดังนั้น $2^m = 2^n$ ซึ่งทำให้ได้ $m = n$ เพราะฉะนั้นถ้า F มีฐานขนาดจำกัดแล้วทุกๆ ฐานของ F มีขนาดจำกัดและเท่ากัน

(ii) ให้ F มีฐานขนาดอนันต์ แล้วโดย (i) ทุกๆ ฐานของ F มีขนาดอนันต์ เราจะพิสูจน์ว่า "ถ้า X เป็นฐานของ F แล้ว $|X| = |F|$" ซึ่งทำให้ได้ว่าทุกๆ ฐานของ F ในกรณีนี้มีขนาดเท่ากันและเท่ากับ $|F|$

ให้ X เป็นฐานของ F และ $S := \bigcup_{n \in \mathbb{Z}^+} X^n = \bigcup_{n \in \mathbb{Z}^+} \underbrace{X \times \cdots \times X}_{n}$ แล้วแต่ละ $s \in S$ มี $n \in \mathbb{Z}^+$ และ $x_1, \ldots, x_n \in X$ ซึ่ง $s = (x_1, \ldots, x_n)$ จึงนิยาม $G_s := <x_1, \ldots, x_n>$ สำหรับ $s \in S$ ซึ่ง

$s=(x_1,\ldots,x_n)$ แล้ว G_s เป็นกรุปย่อยของ F ทุกๆ $s\in S$ ให้ $\{y_1,\ldots,y_t\}=\{x_1,\ldots,x_n\}$ โดยที่ $y_1,\ldots,y_t$ ต่างกันทั้งหมดแล้ว $y_1,\ldots,y_t$ เป็น $\mathbb{Z}-$อิสระเชิงเส้นและ $G_s=<y_1,\ldots,y_t>$ จึงเห็นชัดว่า $G_s\cong\mathbb{Z}y_1\oplus\cdots\oplus\mathbb{Z}y_t$ ดังนั้น $|G_s|=|\mathbb{Z}|^t=|\mathbb{Z}|$ แต่ $F=\bigcup_{s\in}G_s$ และ $|S|=|X|\geq|\mathbb{Z}|$ (เพราะว่า X เป็นเซตอนันต์) จะได้ $|F|=\left|\bigcup_{s\in S}G_s\right|\leq|S||\mathbb{Z}|=|X||\mathbb{Z}|=|X|$ ดังนั้น $|F|=|X|$ ❑

2.4.5 **ทฤษฎีบท** ให้ F_1 และ F_2 เป็นกรุปเสรีบนเซต X_1 และ X_2 ตามลำดับแล้ว $F_1\cong F_2$ ก็ต่อเมื่อ $|X_1|=|X_2|$

บทพิสูจน์ ($\Rightarrow$) ให้ $\alpha:F_1\to F_2$ เป็นสมสัณฐานแล้ว $\alpha(X_1)\subseteq F_2$ ซึ่ง $|X_1|=|\alpha(X_1)|$ จะแสดงว่า $\alpha(X_1)$ เป็นฐานของ F_2 (ซึ่งจะทำให้ได้ว่า $|X_2|=|\alpha(X_1)|=|X_1|$)

ให้ $u\in F_2$ แล้วมี $v\in F_1$ ซึ่ง $u=\alpha(v)$ และมี $r,n_1,\ldots,n_r\in\mathbb{Z}$ และ $x_1,\ldots,x_r\in X_1$ ซึ่ง $v=n_1x_1+\cdots+n_rx_r$ จะได้ $u=\alpha(v)=\alpha(n_1x_1+\cdots+n_rx_r)=n_1\alpha(x_1)+\cdots+n_r\alpha(x_r)$ ซึ่งแสดงว่าทุกๆ สมาชิกของ F_2 เขียนได้ในรูปผลบวกเชิงเส้นของสมาชิกใน $\alpha(X_1)$ ต่อไปให้ $n,r_1,\ldots,r_n\in\mathbb{Z}$ และ $y_1,\ldots,y_n\in\alpha(X_1)$ ซึ่ง $r_1y_1+\cdots+r_ny_n=0$ แล้วมี $x_1,\ldots,x_n\in X_1$ ซึ่ง $y_i=\alpha(x_i)$ ทุกๆ $1\leq i\leq n$ ดังนั้น $0=r_1y_1+\cdots+r_ny_n=r_1\alpha(x_1)+\cdots+r_n\alpha(x_n))=\alpha(r_1x_1+\cdots+r_nx_n)$ ซึ่งแสดงว่า $r_1x_1+\cdots+r_nx_n\in\ker\alpha=\{0\}$ ทำให้ได้ $r_1x_1+\cdots+r_nx_n=0$ และเพราะ $x_1,\ldots,x_n$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น ดังนั้น $r_1=\ldots=r_n=0$ จึงได้ว่า $y_1,\ldots,y_n$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น

($\Leftarrow$) ให้ $\alpha:X_1\to X_2$ เป็นฟังก์ชันสมนัยหนึ่งต่อหนึ่ง ให้ $\iota_1:X_1\to F_1$ และ $\iota_2:X_2\to F_2$ ต่างเป็นการส่งเซตย่อยแล้ว $\iota_2\circ\alpha:X_1\to F_2$ และโดยสมบัติการส่งเอกภาพของ F_2 โดยที่ F_1 เป็นกรุปอาบีเลียนและ $\iota_1:X_1\to F_1$ จะมีสาทิสสัณฐาน $\overline{\iota_1}:F_1\to F_2$ ซึ่ง $\overline{\iota_1}\circ\iota_1=\iota_2\circ\alpha$ เพราะว่า ι_1,ι_2 และ α ต่างเป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้น $\overline{\iota_1}$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ในการแสดงว่า $\overline{\iota_1}$ เป็นสมสัณฐาน เหลือเพียงแสดงว่า $\overline{\iota_1}$ เป็นฟังก์ชันทั่วถึง ให้ $u\in F_2$ แล้วเพราะ F_2 เป็นกรุปเสรีบน X_2 จะมี $r,n_1,\ldots,n_r\in\mathbb{Z}$ และ $y_1,\ldots,y_r\in X_2$ ซึ่ง $u=n_1y_1+\cdots+n_ry_r$ และเพราะ $\alpha:X_1\to X_2$ เป็นฟังก์ชันทั่วถึง ดังนั้นแต่ละ $1\leq i\leq n$ มี $x_i\in X_1$ ซึ่ง $y_i=\alpha(x_i)$ จึงได้

$$\begin{aligned}
u&=n_1y_1+\cdots+n_ry_r=n_1\alpha(x_1)+\cdots+n_r\alpha(x_r)=n_1(\iota_2\circ\alpha)(x_1)+\cdots+n_r(\iota_2\circ\alpha)(x_r)\\
&=n_1(\overline{\iota_1}\circ\iota_1)(x_1)+\cdots+n_r(\overline{\iota_1}\circ\iota_1)(x_r)\qquad=n_1\overline{\iota_1}(\iota_1(x_1))+\cdots+n_r\overline{\iota_1}(\iota_1(x_r))\\
&=n_1\overline{\iota_1}(x_1)+\cdots+n_r\overline{\iota_1}(x_r)\qquad=\overline{\iota_1}(n_1x_1+\cdots+n_rx_r)
\end{aligned}$$

โดยที่ $n_1x_1+\cdots+n_rx_r\in F_1$ ❑

สังเกตว่าถ้า F เป็นกรุปเสรีบนเซต X แล้ว $|X|$ สอดคล้องนิยามของลำดับที่ของ F จึงกล่าวได้ว่า F เป็น *กรุปอาบีเลียนเสรีของลำดับที่* $|X|$ *(free abelian group of rank* $|X|$*)*

นอกจากนี้ สังเกตว่าทุกๆ กรุป จะมีเซตย่อยของกรุปที่เป็นตัวก่อกำเนิดของกรุปนั้น (อาจเป็นเอกภพของกรุปนั้นเอง) และด้วยสมบัติการส่งเอกภาพของกรุปเสรี จะได้ทฤษฎีบทต่อไปนี้

2.4.6 **ทฤษฎีบท** ทุกๆ กรุปอาบีเลียนเป็นภาพของกรุปอาบีเลียนเสรีของลำดับที่ $|X|$ เมื่อ X เป็นตัวก่อกำเนิดของกรุปนั้น

บทพิสูจน์ ให้ A เป็นกรุปอาบีเลียนและ $X \subseteq A$ ซึ่ง $A = < X >$ และให้ F เป็นกรุปเสรีบนเซต X นั่นคือ $F = \sum_{x \in X} \mathbb{Z}x$ และลำดับที่ของ F คือ $|X|$ แล้วโดยสมบัติการส่งเอกภาพของ F การส่งเซตย่อย $\iota : X \to A$ จะชักนำสาทิสสัณฐาน $\bar{\iota} : F \to A$ โดยที่ $\bar{\iota}(x) = \iota(x) \in \operatorname{Im}\bar{\iota}$ ทุกๆ $x \in X$ ดังนั้น $X \subseteq \operatorname{Im}\bar{\iota}$ และเนื่องจาก $A = < X >$ ดังนั้น $\operatorname{Im}\bar{\iota} = A$ ❑

ขอจบหัวข้อนี้ด้วยการพิสูจน์ทฤษฎีบทที่จะเป็นประโยชน์ต่อการวิเคราะห์โครงสร้างของกรุปอาบีเลียนเสรีก่อกำเนิดแบบจำกัดซึ่งจะกล่าวในหัวข้อต่อไป

2.4.7 **ทฤษฎีบท** ถ้า n เป็นจำนวนเต็มบวก $\{x_1, \ldots, x_n\}$ เป็นฐานของกรุปอาบีเลียนเสรีและ $a \in \mathbb{Z}$ แล้ว $\{x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\}$ เป็นฐานของ F ทุกๆ $i \neq j$

บทพิสูจน์ เนื่องจาก $x_j = -ax_i + (x_j + ax_i)$ ดังนั้น $F = < x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n >$ และถ้า $k_1, \ldots, k_n \in \mathbb{Z}$ ซึ่ง $k_1x_1 + \ldots + k_{j-1}x_{j-1} + k_j(x_j + ax_i) + k_{j+1}x_{j+1} + \ldots k_nx_n = 0$ แล้ว $k_1x_1 + \ldots + (k_i + k_ja)x_i + \ldots + k_jx_j + \ldots k_nx_n = 0$ ซึ่งทำให้ได้ $k_1 = \ldots = k_n = 0$ ❑

2.4.8 **ทฤษฎีบท** ให้ F เป็นกรุปอาบีเลียนเสรีที่มีฐานขนาดจำกัด n ตัว ถ้า H เป็นกรุปย่อยของ F แล้ว H เป็นกรุปเสรีมีฐานขนาดจำกัด m ตัวโดยที่ $m \leq n$

บทพิสูจน์ ให้ F เป็นกรุปเสรีบนตัวก่อกำเนิด n ตัว ถ้า $n = 1$ แล้ว F เป็นกรุปวัฏจักรอันดับอนันต์ซึ่งเสรีบนตัวก่อกำเนิดหนึ่งตัว ดังนั้นทุกๆ กรุปย่อยของ F เป็นกรุปวัฏจักรอันดับอนันต์ จึงเป็นกรุปเสรีบนตัวก่อกำเนิดหนึ่งตัว ทำให้ได้ทฤษฎีบทเป็นจริง

ต่อไปสมมติให้ทฤษฎีบทเป็นจริงสำหรับกรุปเสรีบนตัวก่อกำเนิดจำนวนน้อยกว่า n ตัว แล้วจะแสดงว่าทฤษฎีบทเป็นจริงสำหรับกรุปเสรีบนตัวก่อกำเนิด n ตัวซึ่งจะทำให้เราสรุปได้โดยอุปนัยเชิงคณิตศาสตร์ว่าทฤษฎีบทเป็นจริงสำหรับทุกๆ กรุปเสรีก่อกำเนิดแบบจำกัด

ให้ $F = < u_1, \ldots, u_n >$ เป็นกรุปเสรีบนตัวก่อกำเนิด n ตัวและให้ H เป็นกรุปย่อยของ F แล้วเพราะว่าแต่ละ $h \in H$ เป็นสมาชิกของ F จึงเขียนได้ในรูป $h = \alpha_1u_1 + \cdots + \alpha_nu_n$ ถ้า α_n ของผลบวกเชิงเส้นของทุกๆ $h \in H$ เป็นศูนย์ จะได้ว่า H ก่อกำเนิดโดย $u_1, \ldots, u_{n-1}$ แล้วเพราะ $\{u_1, \ldots, u_{n-1}\}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น ดังนั้น H เสรีบนตัวก่อกำเนิด $n-1$ ตัว จึงพิจารณากรณีที่มี $h \in H$ ซึ่ง α_n ในผลบวกเชิงเส้นของ h ไม่เป็นศูนย์ แล้ว

$S=\{\alpha_n \in \mathbb{Z}\setminus\{0\} | \alpha_1 u_1+\cdots+\alpha_n u_n \in H\} \neq \phi$

สังเกตว่าถ้า $h \in H$ แล้ว $-h \in H$ จะได้ว่าเซตย่อยที่ประกอบด้วยจำนวนบวกของ S ไม่เป็นเซตว่าง ดังนั้นโดยหลักการเป็นอันดับอย่างดีจะมี $\mu_n > 0$ เป็นจำนวนเต็มน้อยสุดของ S จึงมี $h \in H$ ซึ่ง $h=\mu_1 u_1+\cdots+\mu_n u_n$ ให้ $\alpha_n \in S$ แล้วมี $k \in H$ ซึ่ง $k=\alpha_1 u_1+\cdots+\alpha_n u_n$ และโดยขั้นตอนการหาร จะมี $q,r \in \mathbb{Z}$ ซึ่ง $\alpha_n = q\mu_n + r$ โดยที่ $0 \le r < \mu_n$ ทำให้ได้ $k-qh=(\alpha_1-q\mu_1)u_1+\cdots+(\alpha_n-q\mu_n)u_n \in H$ ซึ่งแสดงว่า $r=\alpha_n-q\mu_n \in S$ ถ้า $r>0$ จะขัดแย้งกับการเลือก μ_n เป็นจำนวนบวกน้อยสุดใน S ดังนั้น $r=0$ ทำให้ได้ $\alpha_n = q\mu_n$ และได้ $k-qh=(\alpha_1-q\mu_1)u_1+\cdots+(\alpha_{n-1}-q\mu_{n-1})u_{n-1} \in H$

ให้ $N=\{k-qh | k \in H\}$ แล้วเห็นได้ชัดว่า N เป็นกรุปย่อยของ H ที่ก่อกำเนิดโดยตัวก่อกำเนิดจำนวนน้อยกว่าหรือเท่ากับ $n-1$ ตัว ดังนั้น N เป็นกรุปย่อยของกรุปเสรีบนตัวก่อกำเนิดจำนวนน้อยกว่าหรือเท่ากับ $n-1$ ตัว (เพราะ $\{u_1,\ldots,u_{n-1}\}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น) โดยสมมติฐานของอุปนัยเชิงคณิตศาสตร์ จะได้ N เป็นกรุปเสรีบนตัวก่อกำเนิด t ตัวซึ่ง $t \le n-1$ สมมติให้ $N=<k_1,\ldots,k_t>$ แล้วจาก $k-qh \in N$ ทุกๆ $k \in H$ จะได้ H เป็นกรุปย่อยของ $N+<h>$ แต่เพราะ N เป็นกรุปย่อยของ H และ $h \in H$ ดังนั้น $N+<h>$ เป็นกรุปย่อยของ H ทำให้ได้ $H=N+<h>=<k_1,\ldots,k_t,h>$

ต่อไปจะแสดงว่า $k_1,\ldots,k_t,h$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น ให้ $\beta_1,\ldots,\beta_t,\beta_{t+1} \in Z$ ซึ่ง $\beta_1 k_1+\cdots+\beta_t k_t+\beta_{t+1}h=0$ แล้วเพราะ $k_1,\ldots,k_t$ เขียนได้ในรูปผลบวกของ $u_1,\ldots,u_{n-1}$ และ $h=\mu_1 u_1+\cdots+\mu_n u_n$ จะได้ $\beta_1 k_1+\ldots+\beta_t k_t+\beta_{t+1}h$ เขียนได้ในรูปผลบวกของ $u_1,\ldots,u_n$ โดยมีพจน์ของ u_n คือ $\beta_{t+1}\mu_n u_n$ และเพราะ $u_1,\ldots,u_n$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น จะได้ $\beta_{t+1}\mu_n=0$ โดยที่ $\mu_n \neq 0$ ดังนั้น $\beta_{t+1}=0$ ทำให้ได้ $\beta_1 k_1+\ldots+\beta_t k_t=0$ แต่ N เสรีบน $\{k_1,\ldots,k_t\}$ จึงทำให้ $\{k_1,\ldots,k_t\}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น ดังนั้น $\beta_1=\ldots=\beta_t=0$ ซึ่งเป็นอันจบการพิสูจน์

ดังนั้น H เป็นกรุปเสรีบนเซต $\{k_1,\ldots,k_t,h\}$ ซึ่งมีขนาด $t+1 \le (n-1)+1=n$ ❑

โดยทฤษฎีบท 2.4.8 ทุกๆ กรุปย่อยของกรุปอาบีเลียนซึ่งเสรีบนตัวก่อกำเนิด n ตัวจะเป็นกรุปเสรีบนตัวก่อกำเนิดไม่เกิน n ตัว ทฤษฎีบทต่อไปแสดงการสร้างฐานของกรุปย่อยของกรุปอาบีเลียนเสรีจากฐานของกรุปอาบีเลียนเสรี

2.4.9 **ทฤษฎีบท** ให้ F เป็นกรุปอาบีเลียนเสรีบนฐานขนาดจำกัด n และ H เป็นกรุปย่อยของ F ซึ่ง $H \neq \{0\}$ แล้วมีฐาน $\{x_1,\ldots,x_n\}$ ของ F จำนวนเต็ม $1 \le r \le n$ และจำนวนเต็มบวก $d_1,\ldots,d_r$ ซึ่ง $d_1|d_2|\ldots|d_r$ (โดยที่ $d_1|d_2|\ldots|d_r$ หมายถึง $d_1|d_2, d_2|d_3,\ldots,d_{r-1}|d_r$) และ H เป็นกรุปเสรีบนฐานจำกัด $\{d_1x_1,\ldots,d_rx_r\}$

บทพิสูจน์ ถ้า F เป็นกรุปอาบีเลียนเสรีบนฐานขนาดจำกัด $n=1$ แล้วมี $x \in F$ ซึ่ง $F = <x> \cong Z$ ดังนั้นมีจำนวนเต็มบวก d_1 ซึ่ง $H = <dx_1> \cong \mathbb{Z}$ ทำให้ได้ทฤษฎีบทเป็นจริงสำหรับ $n=1$ จึงสมมติให้ทฤษฎีบทเป็นจริงสำหรับทุกๆ กรุปอาบีเลียนเสรีบนฐานขนาดจำกัดที่น้อยกว่า n และให้ F เป็นกรุปอาบีเลียนเสรีบนฐานขนาดจำกัด n และ H เป็นกรุปย่อยของ F

ให้ S เป็นเซตของจำนวนเต็ม s ทั้งหลายซึ่งมีฐาน $\{y_1,\ldots,y_n\}$ ของ F และมี $h \in H$ ซึ่ง $h = sy_1 + k_2y_2 + \ldots + k_ny_n$ สำหรับบางจำนวนเต็ม $k_2,\ldots,k_n$ สังเกตว่าถ้า $\{y_1,\ldots,y_n\}$ เป็นฐานของ F แล้ว $\{y_2,y_1,y_3,\ldots,y_n\}$ เป็นฐานของ F ดังนั้นถ้า $s \in S$ แล้ว $k_2,\ldots,k_n \in S$ และเพราะ $\phi \neq H \neq \{0\}$ จะมีฐาน $\{y_1,\ldots,y_n\}$ ของ F และมี $0 \neq h \in H$ ซึ่ง $h = sy_1 + k_2y_2 + \cdots + k_ny_n$ ทำให้ได้ $S \neq \phi$ และเพราะ $h \in H$ ก็ต่อเมื่อ $-h \in H$ ดังนั้นมีจำนวนเต็มบวกเป็นสมาชิกของ S ให้ d_1 เป็นจำนวนเต็มบวกน้อยสุดที่เป็นสมาชิกของ S แล้วมีฐาน $\{y_1,\ldots,y_n\}$ ของ F มี $v \in H$ และจำนวนเต็ม $k_2,\ldots,k_n$ ซึ่ง $v = d_1y_1 + k_2y_2 + \ldots + k_ny_n$ ดังนั้นโดยขั้นตอนการหาร จะมีจำนวนเต็ม q_i และ $0 \le r_i < d_1$ ซึ่ง $k_i = q_id_1 + r_i$ สำหรับแต่ละ $i = 2,\ldots,n$ ทำให้ได้

$$\begin{aligned} v &= d_1y_1 + (q_2d_1 + r_2)y_2 + \ldots + (q_nd_1 + r_n)y_n \\ &= d_1(y_1 + q_2y_2 + \ldots + q_nr_n) + r_2y_2 + \ldots + r_ny_n \end{aligned}$$

ให้ $x_1 = y_1 + q_2y_2 + \ldots + q_nr_n$ แล้ว $\{x_1,y_2,\ldots,y_n\}$ เป็นฐานของ F โดยทฤษฎีบท 2.3.6 ถ้ามี $k \in \{2,\ldots,n\}$ ซึ่ง $r_k \neq 0$ แล้ว r_k เป็นจำนวนเต็มบวกซึ่งเป็นสมาชิกของ S (เพราะว่า $v = r_ky_k + d_1x + \ldots + r_ny_n$) จะขัดแย้งกับการเลือก d_1 ดังนั้น $r_2 = \ldots = r_n = 0$ ทำให้ได้ $v = d_1x_1 \in H$

ต่อไปให้ G เป็นกรุปอาบีเลียนเสรีที่มี $\{y_2,\ldots,y_n\}$ เป็นฐานแล้ว G เป็นกรุปเสรีบนฐานขนาดน้อยกว่า n ยิ่งไปกว่านั้น $F \cong <x_1> \oplus G$ แล้วจะพิสูจน์ว่า $H \cong <v> \oplus (G \cap H)$

เพราะว่า $\{x_1,y_2,\ldots,y_n\}$ เป็นฐานของ F จะได้ $<v> \cap (G \cap H) = \{0\}$ ถ้า $u \in H$ จะมีจำนวนเต็ม $t_1,t_2,\ldots,t_n$ ซึ่ง $u = t_1x_1 + t_2y_2 + \ldots + t_ny_n$ แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม q' และ $0 \le r' < d_1$ ซึ่ง $t_1 = q'd_1 + r'$ ทำให้ได้ $u - q'v = r'x_1 + t_2y_2 + \ldots + t_ny_n \in H$ ถ้า $0 < r'$ จะได้ $r' \in S$ จะขัดแย้งกับการเลือก d_1 ดังนั้น $r' = 0$ ทำให้ได้ $u = qv + (t_2y_2 + \ldots + t_ny_n)$ โดยที่ $qv \in <v>$ และ $t_2y_2 + \ldots + t_ny_n \in G \cap H$ เพราะฉะนั้น $H = <v> + (G \cap H)$

ถ้า $G \cap H = \{0\}$ แล้ว H เป็นไปตามทฤษฎีบทซึ่งเป็นอันจบการพิสูจน์ จึงพิจารณากรณี $G \cap H \neq \{0\}$ จะได้ G และกรุปย่อย $G \cap H$ ของ G เป็นไปตามสมมติฐานของอุปนัยเชิงคณิตศาสตร์ ดังนั้นมีฐาน $\{x_2,\ldots,x_n\}$ ของ G และจำนวนเต็มบวก $r,d_2,\ldots,d_r$ ซึ่ง $d_2|d_3|\ldots|d_r$ และ $G \cap H$ เป็นกรุปเสรีบนฐานจำกัด $\{d_2x_2,\ldots,d_rx_r\}$

เราจะแสดงว่า $\{x_1,x_2,\ldots,x_n\}$ เป็นฐานของ F อย่างแรกเพราะว่า $F \cong <x_1> \oplus G$ ดังนั้นแต่ละ $h \in F$ มีจำนวนเต็ม k_1 และ $g \in G$ ซึ่ง $h = k_1x_1 + g$ แต่จาก $g \in G$ ทำให้มีจำนวนเต็ม

$k_2,\ldots,k_n$ ซึ่ง $g = k_2x_2 + \ldots + k_nx_n$ ทำให้ได้ $h = k_1x_1 + k_2x_2 + \ldots + k_nx_n$ เพราะฉะนั้น $F = < x_2,\ldots,x_n >$ อย่างที่สองให้ $k_1,\ldots,k_n$ เป็นจำนวนเต็มซึ่ง $k_1x_1 + \ldots + k_nx_n = 0$ แล้ว $-k_1x_1 = k_2x_2 + \ldots + k_nx_n \in < x_1 > \cap G = \{0\}$ (เพราะว่า $F \cong < x_1 > \oplus G$) ดังนั้น $k_1x_1 = 0$ และ $k_2x_2 + \ldots + k_nx_n = 0$ ทำให้ได้ $k_1 = 0$ และ $k_2 = \ldots = k_n = 0$ (เพราะว่า $\{x_2,\ldots,x_n\}$ เป็นฐานของ G)

ให้ $h \in H$ แล้ว $h \in G$ โดยผลของย่อหน้าก่อนจะได้ $h = k_1x_1 + k_2x_2 + \ldots + k_nx_n$ ซึ่งทำให้ได้ $h - k_1x_1 = k_2x_2 + \ldots + k_nx_n \in H \cap G = < d_2x_2,\ldots,d_rx_r >$ ดังนั้น $H = < d_1x_1,\ldots,d_rx_r >$ และเพราะ $\{x_1,x_2,\ldots,x_n\}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้น ดังนั้น $\{d_1x_1,\ldots,d_rx_r\}$ เป็น $\mathbb{Z}-$อิสระเชิงเส้นด้วย เพราะฉะนั้น $\{d_1x_1,\ldots,d_rx_r\}$ เป็นฐานของ H โดยที่ $d_2|d_3|\ldots|d_r$

จึงเหลือเพียงแสดงว่า $d_1|d_2$ โดยขั้นตอนการหาร จะมีจำนวนเต็ม q'' และ $0 \le r'' < d_1$ ซึ่ง $d_2 = q''d_1 + r''$ และเพราะ $\{x_2, x_1 + q''x_2, x_3,\ldots,x_n\}$ เป็นฐานของ F และ $r''x_2 + d_1(x_1 + q''x_2) + 0x_3 + \ldots + 0x_n \in F$ จะได้ $r'' \in S$ ถ้า $r'' > 0$ ทำให้ขัดแย้งกับการเลือก d_1 ดังนั้น $r'' = 0$ ทำให้ได้ $d_2 = q''d_1$ ซึ่งแสดงว่า $d_1|d_2$ ตามต้องการ ❑

แบบฝึกหัด 2.4

1. ให้ n เป็นจำนวนเต็มบวกและ F เป็นกรุปอาบีเลียนเสรีที่มี rank $F = n$ จงพิสูจน์ว่า
   1.1 ไม่ใช่ว่าทุกๆ เซตย่อยขนาด n ของ F ที่เป็นอิสระเชิงเส้นจะเป็นฐานของ F
   [ข้อแนะนำ : พิจารณากรุปเสรี $\mathbb{Z}$]
   1.2 ไม่ใช่ว่าทุกๆ เซตย่อยของ F ที่เป็นอิสระเชิงเส้นจะสามารถขยายเป็นฐานของ F
   1.3 ไม่ใช่ว่าทุกๆ เซตตัวก่อกำเนิดของ F จะมีเซตย่อยที่เป็นฐานของ F
2. ให้ $X = \{a_i | i \in I\}$ เป็นเซตซึ่งดรรชนีโดยเซต I จงพิสูจน์ว่า
   2.1 ทุกๆ กรุปอาบีเลียนเสรีบน X สมสัณฐานกับ $\sum_{x \in X} \mathbb{Z}x$ ซึ่งสมสัณฐานกับกรุป $F = \{X | a_ia_ja_i^{-1}a_j^{-1} = e$ ทุกๆ $i, j \in I\}$ ภายใต้การคูณ
   2.2 ผลบวกตรงของกรุปอาบีเลียนเสรีเป็นกรุปอาบีเลียนเสรี
   2.3 ถ้า $x_0 \in X$ และ G เป็นกรุปย่อยของ F ซึ่งมีฐานคือ $X' = X \setminus \{x_0\}$ แล้ว $(F/G) \cong \mathbb{Z}x_0$
   2.4 จงวางนัยผลของ 2.3 สำหรับเซตย่อย X' ใดๆ ของ X
3. ให้ G เป็นกรุปอาบีเลียนเสรีซึ่งก่อกำเนิดโดย X จงพิสูจน์ว่าถ้าไม่มีสมาชิกตัวใดใน G ซึ่งมีอันดับจำกัดแล้ว G เป็นกรุปอาบีเลียนเสรี

4. ให้ F และ G เป็นกรุปอาบีเลียนเสรีบนเซต X และ Y ตามลำดับ และให้ F' และ G' เป็นกรุปย่อยของ F และ G ซึ่งก่อกำเนิดโดยเซต $\{aba^{-1}b^{-1}|a,b\in F\}$ และเซต $\{aba^{-1}b^{-1}\ |a,b\in F\}$ ตามลำดับ จงพิสูจน์ว่า

4.1 F/F' และ G/G' เป็นกรุปอาบีเลียนเสรีของลำดับที่ $|X|$ และ $|Y|$ ตามลำดับ [ข้อแนะนำ : พิสูจน์ว่า $\{xF'|x\in X\}$ เป็นฐานของ F/F']

4.2 ถ้า $F\cong G$ แล้วแต่ละสมสัณฐานจะชักนำสมสัณฐานระหว่าง F/F' และ G/G'

2.5 กรุปอาบีเลียนก่อกำเนิดแบบจำกัด

ในหัวข้อนี้ เราศึกษาและพิสูจน์ทฤษฎีบทโครงสร้างของกรุปอาบีเลียนก่อกำเนิดแบบจำกัดที่ต่างกันสองทฤษฎีบทซึ่งจะนำไปสู่การจำแนกกรุปอาบีเลียนก่อกำเนิดแบบจำกัดอย่างสมบูรณ์ (ถ้าไม่นับการสมสัณฐาน)

ขอทบทวนว่าถ้า G เป็นกรุปอาบีเลียนก่อกำเนิดโดยเซต X นั่นคือ $G=<X>$ โดยที่ X เป็นเซตจำกัด เรากล่าวว่า G เป็นกรุปอาบีเลียนก่อกำเนิดแบบจำกัด และได้นิยามไว้ในหัวข้อก่อนแล้วว่าทุกๆ กรุปอาบีเลียนเสรีบนเซตจำกัดเป็น (ถ้าไม่นับการสมสัณฐาน) ผลบวกตรงของกรุปวัฏจักรอันดับอนันต์จำนวนจำกัดกรุป เราจึงเริ่มต้นหัวข้อนี้ด้วยการแสดงว่ากรุปอาบีเลียนก่อกำเนิดแบบจำกัดก็เป็นเช่นเดียวกัน

2.5.1 **ทฤษฎีบท** ทุกๆ กรุปอาบีเลียนก่อกำเนิดแบบจำกัดจะสมสัณฐานกับผลบวกตรงของกรุปวัฏจักรเป็นจำนวนจำกัดกรุป และถ้ามีกรุปวัฏจักรอันดับจำกัดในผลบวกตรง แล้วกรุปวัฏจักรเหล่านั้นมีอันดับเป็น $m_1,\ldots,m_t$ โดยที่ $m_1>1$ และ $m_1|m_2|\ldots|m_t$

บทพิสูจน์ เห็นได้ชัดว่าทฤษฎีบทเป็นจริงสำหรับกรุป $G=\{0\}$ จึงให้ $G\neq\{0\}$ เป็นกรุปอาบีเลียนซึ่งก่อกำเนิดโดยเซตที่มีสมาชิก n ตัว แล้วโดยทฤษฎีบท 2.4.6 มีกรุปอาบีเลียนเสรี F ของลำดับที่ n และสาทิสสัณฐาน $\pi:F\to G$ เป็นชนิดทั่วถึง

ถ้า π เป็นชนิดหนึ่งต่อหนึ่งแล้ว π เป็นสมสัณฐาน จะได้ $G\cong F\cong\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{n}$ ซึ่งแสดงว่าทฤษฎีบทเป็นจริง และถ้า π ไม่เป็นชนิดหนึ่งต่อหนึ่งแล้ว $K=\ker\pi$ เป็นกรุปย่อยของ F โดยทฤษฎีบท 2.4.9 จะมีฐาน $\{x_1,\ldots,x_n\}$ ของ F จำนวนเต็ม $1\le r\le n$ และจำนวนเต็มบวก $d_1,\ldots,d_r$ ซึ่ง $d_1|d_2|\ldots|d_r$ และ $\{d_1x_1,\ldots,d_rx_r\}$ เป็นฐานของ K

จาก $F=\sum_{i=1}^{n}<x_i>$ และ $K=\sum_{i=1}^{r}<d_ix_i>$ โดยที่ $<x_i>\cong\mathbb{Z}$ และ $<d_ix_i>\cong d_i\mathbb{Z}=\{d_iu\ |u\in Z\}$ ด้วยสมสัณฐานเดียวกันทุกๆ $1\le i\le r$ และสำหรับ $r+1\le i\le n$ ให้ $d_i=0$ แล้ว

อาจเขียนเป็น $K=\sum_{i=1}^{n}<d_ix_i>$ ซึ่งจะได้โดยทฤษฎีบทหลักมูลของสาทิสสัณฐานว่า $G\cong F/K=\sum_{i=1}^{n}<x_i>\Big/\sum_{i=1}^{n}<d_ix_i>$ ดังนั้นโดยแบบฝึกหัด 2.1 ข้อ 3 จะได้ $G\cong\sum_{i=1}^{n}(<x_i>/<d_ix_i>)\cong\sum_{i=1}^{n}(\mathbb{Z}/d_i\mathbb{Z})$

แต่ละ $1\le i\le n$ ถ้า $d_i=1$ แล้ว $(\mathbb{Z}/d_i\mathbb{Z})=\mathbb{Z}/\mathbb{Z}=\{0\}$ แต่ถ้า $d_i=0$ แล้ว $(\mathbb{Z}/d_i\mathbb{Z})=\mathbb{Z}/\{0\}\cong\mathbb{Z}$ และถ้า $d_i>1$ แล้ว $(\mathbb{Z}/d_i\mathbb{Z})\cong\mathbb{Z}_{d_i}$ จึงให้ s และ t เป็นจำนวนของ d_i ซึ่ง $d_i=0$ และ $d_i>1$ ตามลำดับและสำหรับ $1\le i\le t$ ให้ d_i แทนด้วย m_i แล้ว $G\cong\mathbb{Z}_{m_1}\oplus\cdots\oplus Z_{m_t}\oplus(\mathbb{Z}\oplus\cdots\oplus\mathbb{Z})$ โดยที่ $m_1>1,\ m_1|m_2|\ldots|m_t$ และ $\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ เป็นกรุปเสรีลำดับที่ s ❑

ทฤษฎีบทหลักมูลของกรุปอาบีเลียนก่อกำเนิดแบบจำกัดต่อไปนี้เป็นผลโดยตรงของทฤษฎีบท 2.5.1 และบทแทรก 2.1.5 จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

2.5.2 ทฤษฎีบทหลักมูลของกรุปอาบีเลียนก่อกำเนิดแบบจำกัด

(The Fundamental Theorem of Finitely Generated Abelian Groups)

ทุกๆ กรุปอาบีเลียนก่อกำเนิดแบบจำกัด (ไม่นับการเป็นสมสัณฐาน) เป็นผลบวกตรงของกรุปวัฏจักรซึ่งแต่ละกรุปวัฏจักรในผลบวกมีอันดับอนันต์หรืออันดับเป็นกำลังของจำนวนเฉพาะ ❑

การพิสูจน์ทฤษฎีบทโครงสร้างของกรุปอาบีเลียนก่อกำเนิดแบบจำกัดที่สำคัญทฤษฎีบทต่อไปต้องประยุกต์สมบัติสำคัญซึ่งจะกล่าวไว้ในทฤษฎีบทต่อไปนี้

2.5.3 ทฤษฎีบท ให้ m และ n เป็นจำนวนเต็มบวกซึ่ง $m<n$ และ p เป็นจำนวนเฉพาะ แล้ว

1. $\mathbb{Z}_{p^n}[p]\cong\mathbb{Z}_p$ และ $p^m\mathbb{Z}_{p^n}\cong\mathbb{Z}_{p^{n-m}}$
2. ถ้า G เป็นกรุปอาบีเลียน $\{G_i|i\in I\}$ เป็นหมู่ของกรุปอาบีเลียนและมี $g:G\to\sum_{i\in I}G_i$ เป็นสมสัณฐาน แล้ว $mG\cong\sum_{i\in I}mG_i$ และ $G[m]\cong\sum_{i\in I}G_i[m]$ ด้วยฟังก์ชันกำกัดของ g ลงบน mG และบน $G[m]$ ตามลำดับ
3. ถ้า G และ H เป็นกรุปอาบีเลียนโดยมี $g:G\to H$ เป็นสมสัณฐาน แล้ว $G_t\cong H_t$ และ $G(p)\cong H(p)$ ด้วยฟังก์ชันกำกัดของ g ลงบน G_t และบน $G(p)$ ตามลำดับ

บทพิสูจน์ 1. เพราะสมาชิก p^{n-1} ใน $\mathbb{Z}_{p^n}$ มีอันดับ p ดังนั้น $<p^{n-1}>\cong Z_p$ และเห็นได้ชัดว่า $<p^{n-1}>$ เป็นกรุปย่อยของ $\mathbb{Z}_{p^n}[p]$ ในทางกลับกันถ้า $u\in\mathbb{Z}_{p^n}[p]$ แล้ว $pu=0$ ทำให้ได้

$pu \equiv 0 (\bmod p)$ ใน $\mathbb{Z}$ แต่ถ้า p^n เป็นตัวหารของ pu แล้ว p เป็นตัวหารของ u ดังนั้น $u \in < p^{n-1} >$ ใน $\mathbb{Z}_{p^n}$ ทำให้ได้ $\mathbb{Z}_{p^n}[p]$ เป็นกรุปย่อยของ $< p^{n-1} >$ เพราะฉะนั้น $\mathbb{Z}_{p^n}[p] = < p^{n-1} > \cong \mathbb{Z}_p$

ในทำนองเดียวกัน สังเกตว่า p^m ใน $\mathbb{Z}_{p^n}$ มีอันดับ p^{n-m} ดังนั้น $p^m\mathbb{Z}_{p^n} = < p^m > \cong \mathbb{Z}_{p^{n-m}}$

2. เห็นได้ชัด จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

3. ถ้า $g : G \to H$ เป็นสาทิสสัณฐานและ $x \in G(p)$ มีอันดับ p^n แล้ว $p^n g(x) = g(p^n x) = g(0) = 0$ ดังนั้น $g(x) \in H(p)$ ด้วยฟังก์ชันกำกัดของ $g : G(p) \to H(p)$
ถ้า $g : G \to H$ เป็นสมสัณฐาน แล้วการวิเคราะห์ในทำนองเดียวกันก็จะได้ $g^{-1} : H(p) \to G(p)$ และเนื่องจาก $g \circ g^{-1} = id_{H(p)}$ และ $g^{-1} \circ g = id_{G(p)}$ จะได้ $G(p) \cong H(p)$

สำหรับ $G_t \cong H_t$ พิสูจน์ในทำนองเดียวกัน จึงขอละไว้เป็นแบบฝึกหัด ❑

ทฤษฎีบทลากรองจ์กล่าวว่าอันดับของทุกๆ กรุปย่อยของกรุปอันดับจำกัดเป็นตัวหารของอันดับของกรุปนั้น แต่บทกลับไม่เป็นจริงนั่นคือมีบางกรุปอันดับจำกัดและบางตัวหาร m ของอันดับซึ่งกรุปนั้นไม่มีกรุปย่อยอันดับ m จึงเกิดคำถามว่าบทกลับของทฤษฎีบทลากรองจ์จะเป็นจริงในหมู่ของกรุปใดหรือไม่ ผลของทฤษฎีบทหลักมูลของกรุปอาบีเลียนก่อกำเนิดแบบจำกัดข้างต้นทำให้เราได้คำตอบนี้ในหมู่ของกรุปอาบีเลียนอันดับจำกัด ซึ่งจะขอกล่าวไว้เป็นบทแทรกต่อไปนี้

2.5.4 **บทแทรก** ถ้า G เป็นกรุปอาบีเลียนอันดับจำกัด n แล้ว G มีกรุปย่อยอันดับ m สำหรับทุกๆ จำนวนเต็มบวก m ที่เป็นตัวหารของ n

บทพิสูจน์ โดยทฤษฎีบทหลักมูลของกรุปอาบีเลียนก่อกำเนิดแบบจำกัด จะมีจำนวนเต็มบวก k ซึ่ง $G = \sum_{i=1}^{k} G_i$ เมื่อ G_i เป็นกรุปวัฏจักรอันดับกำลังของจำนวนเฉพาะ นั่นคือมีจำนวนเฉพาะ p_i และจำนวนเต็มบวก r_i ซึ่ง $G_i \cong \mathbb{Z}_{p^{r_i}}$ สำหรับแต่ละ $1 \le i \le k$ ดังนั้น $|G| = n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

แต่ $p^{r-i}\mathbb{Z}_{p^r} \cong \mathbb{Z}_{p^i}$ สำหรับแต่ละ $i < r$ โดยทฤษฎีบท 2.5.3 ซึ่งเป็นกรุปย่อยของ $\mathbb{Z}_{p^r}$ ❑

ทฤษฎีบทต่อไปเป็นทฤษฎีบทโครงสร้างที่แสดงการจำแนกกรุปอาบีเลียนก่อกำเนิดแบบจำกัดอย่างสมบูรณ์ (ถ้าไม่นับการเป็นสมสัณฐาน)

2.5.5 **ทฤษฎีบท** ให้ G เป็นกรุปอาบีเลียนก่อกำเนิดแบบจำกัดและให้ F แทนกรุปอาบีเลียนเสรี

1. ไม่ว่าจะเขียน G ในรูปผลบวกตรงของกรุปวัฏจักรรูปแบบใดๆ ก็ตาม จะมีจำนวนเต็ม $s \ge 0$ เพียงจำนวนเดียวเท่านั้นซึ่งเป็นจำนวนของกรุปวัฏจักรอันดับอนันต์ในผลบวกตรงของ G

2. ถ้า G ไม่เป็นกรุปอาบีเลียนเสรี แล้วมีชุดของจำนวนเต็มบวก $m_1,\ldots,m_t$ (อาจซ้ำกันได้) เพียงชุดเดียวซึ่ง $m_1>1,\ m_1|m_2|\ldots|m_t$ และ $G\cong\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_t}\oplus F$

3. ถ้า G ไม่เป็นกรุปอาบีเลียนเสรี แล้วมีจำนวนเต็มบวก $r,k_1,\ldots,k_r$ (อาจซ้ำกันได้) และจำนวนเฉพาะ $p_1,\ldots,p_r$ (อาจซ้ำกันได้) ที่ทำให้ $\left\{p_1^{k_1},p_2^{k_2},\cdots,p_r^{k_r}\right\}$ เป็นเซตของจำนวนเต็มบวกเพียงเซตเดียวซึ่ง $G\cong Z_{p_1^{k_1}}\oplus\cdots\oplus Z_{p_r^{k_r}}\oplus F$

บทพิสูจน์ โดยทฤษฎีบท 2.5.1 จะมีกรุปอาบีเลียนอันดับจำกัด H ซึ่งเป็นผลบวกตรงของกรุปวัฏจักรอันดับจำกัดและมีจำนวนเต็ม $s\geq 0$ และกรุปอาบีเลียนเสรี F ของลำดับที่ s ซึ่ง $\alpha:G\to H\oplus F$ เป็นสมสัณฐาน

1. ถ้า G เป็นกรุปจำกัดแล้ว $G\cong H$ และ $s=0$ ไม่ว่าจะเขียน H ในรูปแบบใด จึงสมมติ G มีอันดับอนันต์และ H อาจคือ $\{0\}$ ให้ $\iota:H\to H\oplus F$ นิยามโดย $\iota(h)=(h,0)$ ทุกๆ $h\in H$ แล้วเห็นชัดว่า $\iota(H)$ เป็นกรุปย่อยทอร์ชันของ $H\oplus F$ ทำให้ได้โดยทฤษฎีบท 2.5.3 ว่า $G_t\cong\iota(H)$ โดยฟังก์ชันกำกัดของ α และโดยบทแทรก 1.7.17 จะได้ $G/G_t\cong(H\oplus F)/\iota(H)\cong F$ ดังนั้นโดยไม่ขึ้นกับรูปแบบผลบวกตรงใดๆ ของ G จะได้ G/G_t เป็นกรุปอาบีเลียนเสรีของลำดับที่ s เสมอ ทำให้ได้ว่าจำนวนของกรุปวัฏจักรอันดับอนันต์ในผลบวกตรงของ G ไม่แปรเปลี่ยน

3. โดยทฤษฎีบท 2.1.5 มีจำนวนเต็มบวก r และ n_i ทุกๆ $1\leq i\leq r$ ซึ่ง $H\cong\sum_{i=1}^{r}\mathbb{Z}_{n_i}$ โดยที่ $n_i=p_i^{a_i}$ เมื่อแต่ละ a_i เป็นจำนวนเต็มบวกและ p_i เป็นจำนวนเฉพาะทุกๆ $1\leq i\leq r$ ซึ่งทำให้ $G\cong\sum_{i=1}^{r}\mathbb{Z}_{n_i}\oplus F$ ต่อไปสมมติมีจำนวนเต็มบวก d และ k_i ทุกๆ $1\leq i\leq d$ อีกชุดหนึ่งซึ่ง $H\cong\sum_{i=1}^{d}\mathbb{Z}_{k_i}$ โดยที่ $k_i=q_i^{c_i}$ เมื่อแต่ละ c_i เป็นจำนวนเต็มบวกและ q_i เป็นจำนวนเฉพาะทุกๆ $1\leq i\leq d$ ที่ทำให้ $G\cong\sum_{i=1}^{d}\mathbb{Z}_{a_i}\oplus F'$ เมื่อ F' เป็นกรุปอาบีเลียนเสรี จะแสดงว่า $r=d$ และ $\{n_i|1\leq i\leq r\}=\{k_i|1\leq i\leq d\}$

โดยการพิสูจน์เช่นเดียวกับข้อ 1 จะได้ว่ากรุปย่อยทอร์ชันของ $\sum_{i=1}^{d}\mathbb{Z}_{a_i}\oplus F'$ สมสัณฐานกับ $\sum_{i=1}^{r}\mathbb{Z}_{n_i}$ และกรุปย่อยทอร์ชันของ $\sum_{i=1}^{r}\mathbb{Z}_{n_i}\oplus F$ สมสัณฐานกับ $\sum_{i=1}^{d}\mathbb{Z}_{k_i}$ ซึ่งต่างก็สมสัณฐานกับ G_t ดังนั้น $\sum_{i=1}^{r}\mathbb{Z}_{n_i}\cong\sum_{i=1}^{d}\mathbb{Z}_{k_i}$ นอกจากนี้ยังเห็นชัดว่า $\left(\sum_{i=1}^{r}\mathbb{Z}_{n_i}\right)(p)$ สมสัณฐานกับผลบวกตรงของ $\mathbb{Z}_{n_i}$ ซึ่ง n_i เป็นกำลังของ p ทุกๆ จำนวนเฉพาะ p และเช่นเดียวกับ $\left(\sum_{i=1}^{d}\mathbb{Z}_{k_i}\right)(p)$ แต่โดยทฤษฎีบท

2.5.3 จะได้ $\left(\sum_{i=1}^{r}\mathbb{Z}_{n_i}\right)(p) \cong \left(\sum_{i=1}^{d}\mathbb{Z}_{k_i}\right)(p)$ ทุกๆจำนวนเฉพาะ p จึงพิจารณาเฉพาะ G_t และสมมติว่าแต่ละ n_i และ k_i เป็นกำลังของจำนวนเฉพาะ p ทำให้ได้ $\sum_{i=1}^{r}\mathbb{Z}_{p^{a_i}} \cong \sum_{i=1}^{d}\mathbb{Z}_{p^{c_i}}$ โดยที่ $1 \le a_1 \le a_2 \le \cdots \le a_r$ และ $1 \le c_1 \le c_2 \le \cdots \le c_d$ แล้วโดยทฤษฎีบท 2.5.3 จะได้ $\sum_{i=1}^{r}\mathbb{Z}_{p^{a_i}}[p] \cong \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{r\ times}$ และ $\sum_{i=1}^{d}\mathbb{Z}_{p^{c_i}}[p] \cong \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{\mathrm{d}\ times}$ จึงได้ $p^r = \left|\sum_{i=1}^{r}\mathbb{Z}_{p^{a_i}}[p]\right| = \left|\sum_{i=1}^{d}\mathbb{Z}_{p^{c_i}}[p]\right| = p^d$ ดังนั้น $r = d$ ต่อไปสมมติมี $1 \le i \le d$ ซึ่ง $a_i \ne c_i$ และให้ $1 \le \nu \le d$ เป็นตัวน้อยสุดซึ่ง $a_\nu \ne c_\nu$ แล้ว $a_i = c_i$ ทุกๆ $i < \nu$ และอาจสมมติว่า $a_\nu < c_\nu$ แต่จาก $1 \le a_1 \le a_2 \le \cdots \le a_r$ จะได้ $p^{a_\nu}\mathbb{Z}_{p^{a_i}} = \{0\}$ สำหรับ $a_i < a_\nu$ โดยทฤษฎีบท 2.5.3 จะได้ $p^{a_\nu}G_t \cong \sum_{i=1}^{r}p^{a_\nu}\mathbb{Z}_{p^{a_i}} \cong \sum_{i=\nu+1}^{r}\mathbb{Z}_{p^{a_i-a_\nu}}$ โดยที่ $a_{\nu+1} - a_\nu \le a_{\nu+2} - a_\nu \le \cdots \le\ a_r - a_\nu$ ทำให้ได้จำนวนของ $\mathbb{Z}_{p^{a_i-a_\nu}} \ne \{0\}$ ในผลบวกตรงของ $p^{a_\nu}G_t$ ไม่เกิน $r-(\nu+1)+1 =\ r-\nu$ และเช่นเดียวกันจาก $a_i = c_i$ ทุกๆ $i < \nu$ และ $a_\nu < c_\nu$ จะได้ $p^{a_\nu}G_t \cong \sum_{i=\nu}^{r}\mathbb{Z}_{p^{c_i-a_\nu}}$ โดยที่ $1 \le c_\nu - a_\nu \le c_{\nu+1} - a_\nu\ \ \le \cdots \le c_r - a_\nu$ ทำให้ได้จำนวนของ $Z_{p^{c_i-a_\nu}} \ne \{0\}$ ในผลบวกตรงของ $p^{a_\nu}G_t$ อย่างน้อยเท่ากับ $r-\nu+1$ จึงได้ $r-\nu+1 = r-\nu$ ซึ่งเป็นไปไม่ได้ ดังนั้น $a_i = c_i$ ทุกๆ i

2. เช่นเดียวกับการพิสูจน์ข้อ 3 เราอาจสมมติว่า

$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F$ และ $G \cong \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_d} \oplus F'$

โดยที่ $m_1 > 1,\ m_1|m_2|\ldots|m_t,\ k_1 > 1,\ k_1|k_2|\ldots|k_d$ และ F, F' เป็นกรุปอาบีเลียนเสรี เนื่องจาก $m_1,\ldots,m_t,k_1,\ldots,k_d$ แต่ละจำนวนเขียนได้ในรูปผลคูณของกำลังของจำนวนเฉพาะ และถ้าจำนวนจำนวนเฉพาะ p ใดที่ไม่ปรากฏในผลคูณของจำนวนใด เราก็อาจเขียน $p^0 = 1$ เป็นตัวประกอบหนึ่งในผลคูณของจำนวนนั้น ดังนั้นจึงสมมติได้ว่า $p_1,\ldots,p_r$ เป็นจำนวนเฉพาะที่ต่างกันทั้งหมดซึ่งปรากฏในทุกๆ การแยกตัวประกอบในรูปผลคูณของกำลังของจำนวนเฉพาะของ $m_1,\ldots,m_t$, $k_1,\ldots,k_d$ และสมมติการเขียนในรูปผลคูณของกำลังของจำนวนเฉพาะทั้งหมดเป็นดังนี้

$$
\begin{aligned}
m_1 &= p_1^{a_{11}}p_2^{a_{12}}\cdots p_r^{a_{1r}}, & k_1 &= p_1^{c_{11}}p_2^{c_{12}}\cdots p_r^{c_{1r}},\\
m_2 &= p_1^{a_{21}}p_2^{a_{22}}\cdots p_r^{a_{2r}}, & k_2 &= p_1^{c_{21}}p_2^{c_{22}}\cdots p_r^{c_{2r}},\\
&\vdots & &\vdots\\
m_t &= p_1^{a_{t1}}p_2^{a_{t2}}\cdots p_r^{a_{tr}}, & k_d &= p_1^{c_{d1}}p_2^{c_{d2}}\cdots p_r^{c_{dr}}
\end{aligned}
$$

เนื่องจาก $m_1|m_2|\ldots|m_t$ และ $k_1|k_2|\ldots|k_d$ ทำให้ได้ $0 \le a_{1j} \le a_{2j} \le \cdots \le a_{tj}$ และ $0 \le c_{1j} \le c_{2j} \le \cdots \le c_{tj}$ สำหรับแต่ละ j แล้วโดยบทแทรก 2.1.5 และทฤษฎีบท 2.5.3 จะได้

$$\sum_{i,j} \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i=1}^{t} \mathbb{Z}_{m_i} \cong G_t \cong \sum_{i=1}^{d} \mathbb{Z}_{k_i} \cong \sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}}$$

โดยอาจมี $\mathbb{Z}_{p_j^{a_{ij}}}$ หรือ $\mathbb{Z}_{p_j^{c_{ij}}}$ บางตัวคือ $\{0\}$ ดังนั้นสำหรับแต่ละ $j = 1,2,\ldots,r$ จะได้

$$\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}} \cong G(p_j) \cong \sum_{i=1}^{d} \mathbb{Z}_{p_j^{c_{ij}}}$$

เนื่องจาก $m_1 > 1$ จะมีบาง p_j ซึ่ง $1 \le a_{1j} \le a_{2j} \le \cdots \le a_{tj}$ จะได้ $\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}}$ ประกอบด้วย $\mathbb{Z}_{p_j^{a_{ij}}} \ne \{0\}$ จำนวน t พจน์ แล้วโดยข้อ 3 ในผลบวก $\sum_{i=1}^{d} \mathbb{Z}_{p_j^{c_{ij}}}$ จะมี $\mathbb{Z}_{p_j^{c_{ij}}} \ne \{0\}$ เป็นจำนวน t พจน์เช่นเดียวกันซึ่งแสดงว่า $t \le d$ ในทำนองเดียวกันจาก $k_1 > 1$ จะได้ $d \le t$ ซึ่งทำให้ได้ $t = d$ และโดยข้อ 3 อีกครั้งที่ทำให้ได้ $a_{ij} = c_{ij}$ ทุกๆ i, j ซึ่งทำให้ได้ $m_i = k_i$ ทุกๆ $1 \le i \le t$ ❑

ถ้า G เป็นกรุปอาบีเลียนก่อกำเนิดแบบจำกัด จะเรียกชุดของจำนวนเต็มบวก $m_1,\ldots,m_t$ ของ G ดังกล่าวในทฤษฎีบท 2.5.5 ข้อ 2 ซึ่งมีเพียงชุดเดียวว่า *ตัวประกอบไม่แปรเปลี่ยน (invariant factor)* ของ G ส่วนสมาชิกในเซตของกำลังของจำนวนเฉพาะที่กล่าวไว้ในทฤษฎีบท 2.5.5 ข้อ 3 ซึ่งมีเพียงเซตเดียวถูกเรียกว่า *ตัวหารมูลฐาน (elementary divisors)* ของ G

2.5.6 **บทแทรก** กรุปอาบีเลียนก่อกำเนิดแบบจำกัด G และ H สมสัณฐานกัน ก็ต่อเมื่อ G/G_t และ H/H_t เป็นกรุปอาบีเลียนเสรีของลำดับที่เดียวกัน และตัวประกอบไม่แปรเปลี่ยนของ G และ H เป็นชุดเดียวกัน (และตัวหารมูลฐานของ G และ H เป็นชุดเดียวกัน) ❑

จากทฤษฎีบท 2.5.5 บทแทรก 2.5.6 และเพราะผลคูณของตัวหารมูลฐานของกรุปอาบีเลียนอันดับจำกัดเท่ากับอันดับของกรุป ทำให้ปัญหาของการหากรุปอาบีเลียนอันดับจำกัด n ทั้งหมดสมมูลกับการหาตัวหารมูลฐานทั้งหมดของ n หรือนั่นคือการหารูปแบบทั้งหมดที่จะเขียน n ในรูปกำลังของจำนวนเฉพาะที่เป็นตัวประกอบของ n ดังจะแสดงให้เห็นเป็นตัวอย่างต่อไปนี้

2.5.7 **ตัวอย่าง** เมื่อต้องการหากรุปอาบีเลียนอันดับ 1500 ทั้งหมด (ไม่นับการเป็นสมสัณฐาน) เราจะหาเซตของตัวหารมูลฐานของ $1500 = 2^2 \cdot 3 \cdot 5^3$ ที่เป็นไปได้ทั้งหมดซึ่งได้แก่เซตต่อไปนี้

$\{2,2,3,5^3\}$, $\{2,2,3,5,5^2\}$, $\{2,2,3,5,5,5\}$, $\{2^2,3,5^3\}$, $\{2^2,3,5,5^2\}$ และ $\{2^2,3,5,5,5\}$

และแต่ละเซตจะกำหนดกรุปอาบีเลียนอันดับ 1500 ซึ่งสมมูลกับผลบวกตรงของกรุปวัฏจักรที่มีอันดับเป็นสมาชิกของแต่ละเซต ตัวอย่างเช่นกรุปที่มีตัวหารมูลฐานเป็น $2,2,3,5^3$ คือกรุปซึ่งสม

สัณฐานกับกรุปผลบวกตรง $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125}$ เป็นต้น

❍

ถ้าเราทราบว่าตัวประกอบไม่แปรเปลี่ยนของกรุปอาบีเลียนก่อกำเนิดแบบจำกัด G คือ $m_1,\ldots,m_t$ แล้วการพิสูจน์ของทฤษฎีบท 2.5.5 แสดงให้ทราบว่าตัวหารมูลฐานของ G คือกำลังของจำนวนเฉพาะ $p^n (n>0)$ ที่ปรากฏในการเขียน $m_1,\ldots,m_t$ ในรูปผลคูณของกำลังของจำนวนเฉพาะ

ในทางกลับกันถ้าตัวหารมูลฐานของ G ถูกกำหนดและต้องการทราบตัวประกอบไม่แปรเปลี่ยนของ G เราจะจัดวางจำนวนเฉพาะทั้งหมดที่ปรากฏในตัวหารมูลฐานโดยเรียงลำดับกำลังของจำนวนเฉพาะดังต่อไปนี้

$$\begin{array}{l} p_1^{n_{11}}, p_2^{12}, \ldots, p_r^{n_{1r}} \\ p_1^{n_{21}}, p_2^{22}, \ldots, p_r^{n_{2r}} \\ \vdots \qquad\qquad \vdots \\ p_1^{n_{t1}}, p_2^{t2}, \ldots, p_r^{n_{tr}} \end{array}$$

โดยที่ $p_1,\ldots,p_r$ เป็นจำนวนเฉพาะที่ต่างกันทั้งหมดและ $0 \le n_{1j} \le n_{2j} \le \cdots \le n_{tj}$ โดยมีบาง $n_{ij} \ne 0$ สำหรับแต่ละ $j = 1,2,\ldots,r$ และมี j ซึ่ง $n_{1j} \ne 0$ แล้วโดยทฤษฎีบท 2.5.5 ข้อ 3 จะได้

$$G \cong \sum_{i=1}^{t} \sum_{j=1}^{r} \mathbb{Z}_{p_j^{n_{ij}}} \oplus F$$

โดยที่ F เป็นกรุปอาบีเลียนเสรี (โดยอาจมีบาง $\mathbb{Z}_{p_j^{n_{ij}}} = \{0\}$ นั่นคือ $p_j^{n_{ij}} = p_j^0 = 1$)

สำหรับแต่ละ $1 \le i \le t$ ให้ $m_i = p_1^{n_{i1}} p_2^{i2} \ldots p_r^{n_{ir}}$ (นั่นคือ m_i เป็นผลคูณของกำลังของจำนวนเฉพาะในแถวที่ i ของการจัดวางจำนวนเฉพาะทั้งหมดข้างต้น) เนื่องจากมีบาง $n_{1j} \ne 0$ ดังนั้น $m_1 > 1$ และ $m_1 | m_2 | \ldots | m_t$ โดยการสร้างและโดยทฤษฎีบท 2.1.5 และทฤษฎีบท 2.5.5 จะได้ $m_1,\ldots,m_t$ เป็นตัวประกอบไม่แปรเปลี่ยนของ G

2.5.8 **ตัวอย่าง** ให้ $G = \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54}$ แล้วโดยทฤษฎีบท 2.1.5 จะได้ $G = \mathbb{Z}_5 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus \mathbb{Z}_{5^2} \oplus (\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2}) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_{3^3})$ ดังนั้นตัวหารมูลฐานของ G คือ $2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2$ ซึ่งนำมาจัดวางจำนวนเฉพาะทั้งหมดดังข้างต้นได้ดังนี้

$$\begin{array}{l} 2^0,\ 3,\ 5 \\ 2,\ 3^2,\ 5 \\ 2^2,\ 3^3,\ 5^2 \end{array}$$

แล้วจะได้ $m_1 = 1 \cdot 3 \cdot 5 = 15$, $m_2 = 2 \cdot 3^2 \cdot 5 = 90$ และ $m_3 = 2^2 \cdot 3^3 \cdot 5^2 = 2700$ ดังนั้น $G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{2700}$ ❍

โดยทฤษฎีบท 2.5.5 สรุปได้ว่าทุกๆ กรุปอาบีเลียนก่อกำเนิดแบบจำกัดเป็นผลบวกตรงของกรุปวัฏจักรจำนวนจำกัดซึ่งอันดับของแต่ละกรุปเป็นกำลังของจำนวนเฉพาะที่ต่างกันหรืออันดับอนันต์ จึงอาจมีคำถามว่า จะสามารถแสดงต่อไปอีกว่ากรุปวัฏจักรแต่ละกรุปในผลบวกตรงดังกล่าวเป็นผลบวกตรงของกรุปที่ย่อยเล็กลงกว่าเดิมได้หรือไม่ ทฤษฎีบทต่อไปจะตอบคำถามเหล่านี้

2.5.9 **บทนิยาม** จะกล่าวว่ากรุป G *แยกตัวประกอบต่อไม่ได้ (indecomposable)* ถ้า $H \cong G$ และ $K \cong \{e\}$ เมื่อใดก็ตามที่ $G \cong H \times K$ สำหรับทุกๆ กรุป H และ K และกล่าวว่ากรุป G *แยกตัวประกอบต่อได้ (decomposable)* ถ้ามีกรุป H และ K ซึ่ง $1 < |H| < |G|, 1 < |K| < |G|$ และ $G \cong H \times K$

2.5.10 **ทฤษฎีบท** กรุปวัฏจักรอันดับอนันต์และกรุปวัฏจักรอันดับกำลังของจำนวนเฉพาะแยกตัวประกอบต่อไม่ได้

บทพิสูจน์ 1. ให้ $<a>$ เป็นกรุปวัฏจักรอันดับอนันต์และให้ A และ B เป็นกรุปย่อยใดๆ ของ $<a>$ ที่ต่างกันซึ่งไม่ใช่ $\{0\}$ แล้ว A และ B เป็นเซตในรูปแบบดังนี้

$$A = \{0, \pm ma, \pm 2ma, \pm 3ma, \ldots\} \text{ และ } B = \{0, \pm ta, \pm 2ta, \pm 3ta, \ldots\}$$

โดยที่ $m \neq 0 \neq t$ ทำให้ได้ $0 \neq tma \in A \cap B$ ดังนั้น $A \cap B \neq \{0\}$ เพราะฉะนั้น $<a> \neq A \oplus B$

2. ให้ $<a>$ เป็นกรุปวัฏจักรอันดับ p^r เมื่อ p เป็นจำนวนเฉพาะและ r เป็นจำนวนเต็มบวก แล้วกรุปย่อยทั้งหมดของ $<a>$ ได้แก่ $\{0\}, <a>, <pa>, <p^2a>, \ldots, <p^{r-1}a>$ ยิ่งไปกว่านั้น $<a> \supset <pa> \supset <p^2a> \supset \ldots \supset <p^{r-1}a> \supset \{0\}$ ดังนั้นถ้า A และ B เป็นกรุปย่อยใดๆ ของ $<a>$ ที่ต่างกันซึ่งไม่ใช่ $\{0\}$ แล้ว $A \cap B \neq \{0\}$ เพราะฉะนั้น $<a> \neq A \oplus B$ ❑

แบบฝึกหัด 2.5

1. จงพิสูจน์ว่าถ้า G เป็นกรุปอาบีเลียนอันดับจำกัดที่ไม่ใช่กรุปวัฏจักร แล้วมีจำนวนเฉพาะ p ซึ่งเป็นตัวหารของ $|G|$ และ $\mathbb{Z}_p \oplus \mathbb{Z}_p$ สมสัณฐานกับบางกรุปย่อยของ G
2. ให้ G เป็นกรุปอาบีเลียนก่อกำเนิดแบบจำกัดซึ่ง G/G_t เป็นลำดับที่ n และ H เป็นกรุปย่อยของ G ซึ่ง H/H_t เป็นลำดับที่ m จงพิสูจน์ว่า $m \leq n$ และ $(G/H)/(G/H)_t$ เป็นลำดับที่ $n-m$
3. จงพิสูจน์ว่าทุกๆ กรุปอาบีเลียนอันดับจำกัดที่เป็น กรุป - p สำหรับบางจำนวนเฉพาะ p ก่อกำเนิดโดยสมาชิกที่มีอันดับมากสุดเฉพาะกลุ่ม (maximal order)

4. ให้ p เป็นจำนวนเฉพาะ จงแสดงว่ากรุป $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$ ประกอบด้วยกรุปย่อยอันดับ p^2 ทั้งหมดจำนวนกี่กรุปย่อย

5. ให้ G, H และ K เป็นกรุปอาบีเลียนก่อกำเนิดแบบจำกัด จงพิสูจน์ว่า

   5.1 ถ้า $G \oplus G \cong H \oplus H$ แล้ว $G \cong H$ 5.2 ถ้า $G \oplus H \cong G \oplus K$ แล้ว $H \cong K$

   5.3 ถ้า G เป็นกรุปอาบีเลียนเสรีอันดับ N แล้ว $G \oplus \mathbb{Z} \oplus \mathbb{Z} \cong G \oplus \mathbb{Z}$ ในขณะที่ $\mathbb{Z} \oplus \mathbb{Z}$ และ $\mathbb{Z}$ ไม่สมสัณฐานกัน

6. จงหาตัวหารมูลฐานและตัวประกอบไม่แปรเปลี่ยนของ $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$ และของ $\mathbb{Z}_{26} \oplus \mathbb{Z}_{42} \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_{200} \oplus \mathbb{Z}_{1000}$

7. จงหากรุปอาบีเลียนทั้งหมด (ไม่นับการเป็นสมสัณฐาน) ที่มีอันดับ 64 และ 96 พร้อมทั้งหากรุปอาบีเลียนทั้งหมดที่มีอันดับน้อยกว่าหรือเท่ากับ 20

8. จงแสดงว่าตัวประกอบไม่แปรเปลี่ยนของ $\mathbb{Z}_m \oplus \mathbb{Z}_n$ คือตัวหารร่วมมาก (m,n) และตัวคูณร่วมน้อย $[m,n]$ ถ้า $(m,n) > 1$ และคือ mn ถ้า $(m,n) = 1$

9. จงแสดงว่าถ้า H เป็นกรุปย่อยของกรุปอาบีเลียนอันดับจำกัด G แล้วมีกรุปย่อยของ G ซึ่งสมสัณฐานกับ G/H

10. ให้ G เป็นกรุปอาบีเลียนก่อกำเนิดแบบจำกัดของลำดับที่ n ถ้า $\{u_1, \ldots, u_n\}$ เป็นฐานของ G และ H เป็นกรุปย่อย G ที่มี $\{v_1, \ldots, v_m\}$ เป็นฐาน เราอาจเขียน $v_i = \sum_{i=1}^{n} \alpha_{ij} u_j$ เมื่อ $\alpha_{ij} \in \mathbb{Z}$ สำหรับ $1 \le i \le m$ ทำให้ได้ $A\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}$ เมื่อ $A = \left(\alpha_{ij}\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ เป็นเมทริกซ์ขนาด $m \times n$ ซึ่งจะเรียกว่าเมทริกซ์ของการเปลี่ยนจากฐานของ G เป็นฐานของ H

    ให้ $G = \langle x, y, z \mid x+y = y+x, x+z = z+x, z+y = y+z, x+y+4z = x+4y+z = 4x+y+z = 0 \rangle$

เป็นกรุปอาบีเลียนและให้ F เป็นกรุปอาบีเลียนเสรีบน $\{x, y, z\}$ และ H เป็นกรุปย่อยของ F ซึ่งก่อกำเนิดโดย $B = \{u = x+y+4z, v = x+4y+z, w = 4x+y+z\}$ จงพิสูจน์ว่า

   10.1 B เป็นฐานของ H

   10.2 $A = \begin{pmatrix} 1 & 1 & 4 \\ 1 & 4 & 1 \\ 4 & 1 & 1 \end{pmatrix}$ เป็นเมทริกซ์ของการเปลี่ยนจากฐานของ G เป็นฐานของ H

   10.3 $G \cong F/H$

10.4 ถ้า $\begin{pmatrix} 1 & 1 & 4 \\ 1 & 4 & 1 \\ 4 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & -3 \\ 1 & -3 & -15 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -3 \\ 0 & -3 & -15 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & -3 & -18 \end{pmatrix} \to$

$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -18 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 18 \end{pmatrix}$ แล้ว

$G \cong \mathbb{Z}_1 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$ เมื่อ $\mathbb{Z}_1 = \{0\}$

11. ให้ F เป็นกรุปอาบีเลียนเสรีบนเซต $\{x_1, x_2, x_3\}$ และ H เป็นกรุปย่อยของ F ซึ่งก่อกำเนิดโดย $\{x_1 + x_2 + 10x_3, x_1 + 10x_2 + x_3, 10x_1 + x_2 + x_3\}$ จงเขียน F/H ในรูปผลบวกตรงของกรุปวัฏจักรซึ่งแยกตัวประกอบต่อไม่ได้
12. ให้ G เป็นกรุปอาบีเลียนก่อกำเนิดโดย $\{a, b, c, d\}$ ภายใต้ความสัมพันธ์ $11a - 10b - -4c - 7d = 0$, $3a - 4b + 2c + 5d = 0$, $3a - 4b - 4c - 7d = 0$ จงเขียน G ในรูปผลบวกตรงของกรุปวัฏจักรซึ่งแยกตัวประกอบต่อไม่ได้

บทที่ 3
รากฐานการนับ

ทฤษฎีกรุปกำเนิดขึ้นด้วยนัยแห่งการสมมาตร แต่การประยุกต์สำคัญอย่างหนึ่งของทฤษฎีกรุปกลับเป็นรากฐานของการนับ ในบทนี้เราจะศึกษาเรื่องราวของการนับผ่านทางทฤษฎีกรุป และตลอดบทนี้หากไม่มีการกล่าวเป็นอย่างอื่น G จะแทนกรุปที่มี e เป็นเอกลักษณ์

3.1 การกระทำของกรุปบนเซตและการประยุกต์

ให้ G เป็นกรุปและ X เป็นเซตที่ไม่ใช่เซตว่าง ในหัวข้อนี้เราสนใจศึกษาฟังก์ชันจากเซต $G\times X$ ไปยัง X ซึ่งเป็นเครื่องมือสำคัญสำหรับการพิสูจน์ทฤษฎีบทของโคชีและทฤษฎีบทของเบิร์นไซด์ อันเป็นรากฐานสำคัญของการพัฒนาวิชาคอมบินาทอริกส์ซึ่งเป็นวิชาที่ว่าด้วยเรื่องราวของการนับล้วนๆ ในกาลต่อมา

3.1.1 **บทนิยาม** *การกระทำของกรุป G บนเซต X ที่ไม่ใช่เซตว่าง (action of G on X)* คือ ฟังก์ ชัน $*: G\times X \to X$ ซึ่งสอดคล้องเงื่อนไขต่อไปนี้

1. $*(e,x)=x$ สำหรับทุกๆ $x\in X$

และ 2. $*(g_1g_2,x)=*(g_1,*(g_2,x))$ สำหรับทุกๆ $x\in X$ และ $g_1,g_2\in G$

เราเรียก X ว่า *$G-$เซต ($G-set$)*

3.1.2 **ตัวอย่าง** แต่ละจำนวนเต็มบวก n ให้ $I_n := \{1,2,\ldots,n\}$ แทนเซตที่ประกอบด้วยสมาชิก n ตัว แล้วพิสูจน์ได้ไม่ยากว่าฟังก์ชัน $*: S_n\times I_n \to I_n$ ซึ่งนิยามสำหรับแต่ละ $\sigma\in S_n$ และ $x\in I_n$ โดย $*(\sigma,x)=\sigma(x)$ เป็นการกระทำของกรุปสมมาตร S_n บน I_n ❍

3.1.3 **ตัวอย่าง** ให้ H เป็นกรุปย่อยของกรุป G และ $*: H\times G\to G$ นิยามสำหรับทุกๆ $g\in G$ และ $h\in H$ โดย $*(h,g)=hg$ แล้ว $*(e,g)=eg=g$ ทุกๆ $g\in G$ นอกจากนี้ $*(h_1h_2,g)=(h_1h_2)g=h_1(h_2g)=*(h_1,*(h_2,g))$ สำหรับแต่ละ $g\in G$ และ $h_1,h_2\in H$ จึงเห็นชัดว่า $*$ เป็นการกระทำของ H บน G ซึ่งจะเรียกว่า *การเลื่อนไปทางซ้ายทั้งหมด (left translation)* ❍

3.1.4 **ตัวอย่าง** ให้ H และ K เป็นกรุปย่อยของกรุป G และให้ A แทนเซตของโคเซตซ้ายทั้งหมดของ K ใน G และ $*: H\times \mathrm{A}\to \mathrm{A}$ นิยามโดย $*(h,gK)=hgK$ ทุกๆ $h\in H$ และ $g\in G$ แล้วสำหรับ $h_1,h_2\in H$ และ $g_1,g_2\in G$ โดยที่ $(h_1,g_1K)=(h_2,g_2)K$ จะได้ $h_1=h_2$ และ $g_1K=g_2K$ ทำให้ได้ $h_1^{-1}h_2=e$ และ $g_1^{-1}g_2\in K$ ดังนั้น $(h_1g_1)^{-1}(h_2g_2)=g_1^{-1}(h_1^{-1}h_2)g_2=g_1^{-1}g_2\in$

K ซึ่งแสดงว่า $h_1g_1K = h_2g_2K$ นั่นคือ $*$ เป็นฟังก์ชัน นอกจากนี้ $*(e,gK) = gK$ ทุกๆ $g \in G$ และ $*(h_1h_2,gK) = (h_1h_2)gK = h_1(h_2g)K = *(h_1,*(h_2,gK))$ ทุกๆ $g \in G$ และ $h_1,h_2 \in H$ เพราะฉะนั้น $*$ เป็นการกระทำของ H บน A ซึ่งจะเรียกว่า *การเลื่อนไปทางซ้ายทั้งหมด (left translation)* เช่นเดียวกัน ❍

ข้อตกลง ถ้า $*$ เป็นการกระทำของกรุป G บนเซต X แล้วสำหรับแต่ละ $g \in G$ และ $x \in X$ จะแทน $*(g,x)$ ด้วย gx ในกรณีที่จะไม่ทำให้เกิดการสับสน

3.1.5 **ทฤษฎีบท** ให้ G เป็นกรุปและ X เป็น $G-$เซต แล้วความสัมพันธ์ $\sim$ บน X ซึ่งนิยามโดย "$x_1 \sim x_2 \Leftrightarrow$ มี $g \in G$ ซึ่ง $gx_1 = x_2$" ทุกๆ $x_1,x_2 \in X$ เป็นความสัมพันธ์สมมูล

บทพิสูจน์ เนื่องจาก X เป็น $G-$เซต ดังนั้น $ex = x$ ทุกๆ $x \in X$ ทำให้ได้ $x \sim x$ ทุกๆ $x \in X$ ต่อไปให้ $x_1,x_2 \in X$ โดยที่ $x_1 \sim x_2$ แล้วมี $g \in G$ ซึ่ง $gx_1 = x_2$ ทำให้ได้ $x_1 = g^{-1}x_2$ โดยที่ $g^{-1} \in G$ ดังนั้น $x_2 \sim x_1$ สุดท้ายให้ $x_1,x_2,x_3 \in X$ โดยที่ $x_1 \sim x_2$ และ $x_2 \sim x_3$ แล้วมี $g_1,g_2 \in G$ ซึ่ง $g_1x_1 = x_2$ และ $g_2x_2 = x_3$ ทำให้ได้ $x_3 = g_2x_2 = g_2(g_1x_1) = (g_2g_1)x_1$

เพราะฉะนั้น $\sim$ เป็นความสัมพันธ์สมมูลบน X ❐

ถ้า $\sim$ เป็นความสัมพันธ์ในทฤษฎีบท 3.1.5 แล้วแต่ละ $a \in X$ เซตสมมูลสัมพัทธ์กับ $\sim$ คือ $\bar{a} = \{x \in X | x \sim a\} = \{ga | g \in G\}$ และในกรณีนี้จะใช้สัญลักษณ์ $G(a)$ แทนเซตสมมูล $\bar{a}$ และเรียกว่า *ออร์บิทของ a ใน X ภายใต้ G (orbit of a in X under G)*

ตัวอย่างเช่นกรุป $G = \{(1),(12)(3456),(35)(46),(12)(3654)\}$ ซึ่งเป็นกรุปย่อยของ S_6 กระทำบนเซต $I_6 := \{1,2,3,4,5,6\}$ ดังนิยามในตัวอย่าง 3.1.2 แล้วความสัมพันธ์ที่นิยามดังในทฤษฎีบท 3.1.5 คือ "$a \sim b \Leftrightarrow$ มี $\sigma \in G$ ซึ่ง $\sigma(a) = b$" ซึ่งเขียน $\sim$ ในรูปแจกแจงสมาชิกได้ดังนี้

$$\sim = \Delta_{I_6} \cup \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(1,2),(2,1),(3,4),(4,3),(3,5),$$
$$(5,3),(3,6),(6,3),(4,5),(5,4),(4,6),(6,4),(5,6),(6,5)\}$$

ทำให้ได้ $G(1) = \{1,2\} = G(2)$ และ $G(3) = \{3,4,5,6\} = G(4) = G(5) = G(6)$ เพราะฉะนั้น $I_6/\sim = \{\{1,2\},\{3,4,5,6\}\}$ เป็นผลแบ่งกั้นที่กำหนดโดย $\sim$ เป็นต้น

3.1.6 **ทฤษฎีบท** ให้ G เป็นกรุป X เป็น $G-$เซตและ $a \in X$ แล้ว

1. $G_a := \{g \in G | ga = a\}$ เป็นกรุปย่อยของ G

2. ขนาด (cardinal number) ของแต่ละออร์บิทของ $a \in X$ เท่ากับดรรชนีของกรุปย่อย G_a ใน G นั่นคือ $|G(a)| = [G : G_a]$

บทพิสูจน์ ให้ $a \in X$ แล้วเห็นชัดว่า $e \in G_a$

1. ให้ $g_1, g_2 \in G_a$ แล้ว $g_1 a = a = g_2 a$ ทำให้ได้ $a = ea = (g_1^{-1} g_1)a = g_1^{-1}(g_1 a) = g_1^{-1}(g_2 a) = (g_1^{-1} g_2)a$ ซึ่งแสดงว่า $g_1^{-1} g_2 \in G_a$ เพราะฉะนั้น G_a เป็นกรุปย่อยของ G

2. ให้ $H = \{gG_a | g \in G\}$ เป็นเซตของโคเซตซ้ายทั้งหมดของ G_a ใน G และสังเกตว่าถ้า $x \in G(a)$ แล้วมี $g \in G$ ซึ่ง $x = ga$ จึงนิยาม $\varphi := \{(x, gG_a) \in G(a) \times H | x = ga\}$ แล้วสำหรับ $g_1 a = g_2 a \in G(a)$ จะได้ $a = ea = (g_1^{-1} g_1)a = g_1^{-1}(g_1 a) = g_1^{-1}(g_2 a) = (g_1^{-1} g_2)a$ ซึ่งทำให้ได้ $g_1^{-1} g_2 \in G_a$ และได้ว่า $\varphi(g_1 a) = g_1 G_a = g_2 G_a = \varphi(g_2 a)$ ดังนั้น φ เป็นฟังก์ชัน ต่อไปให้ $g_1, g_2 \in G$ ซึ่ง $g_1 G_a = g_2 G_a$ แล้ว $g_1^{-1} g_2 \in G_a$ ทำให้ได้ $a = (g_1^{-1} g_2)a = g_1^{-1}(g_2 a)$ ดังนั้น $g_1 a = g_2 a$ ซึ่งแสดงว่า φ เป็นฟังก์ชันหนึ่งต่อหนึ่ง สุดท้ายให้ $gG_a \in H$ แล้วมี $ga \in G(a)$ ที่ทำให้ $\varphi(ga) = gG_a$ ดังนั้น φ เป็นฟังก์ชันทั่วถึง เพราะฉะนั้น $|G(a)| = |H| = [G : G_a]$ ❐

3.1.7 **หมายเหตุ** เรียก G_a ของ G ว่า *กรุปย่อยตรึง (fixed)* $a \in X$ หรือ *กรุปย่อยสเตบิไลเซอร์ (stabilizer subgroup)* ของ a

3.1.8 **บทแทรก** ถ้า X เป็น $G-$เซต แล้ว $b \in G(a)$ ก็ต่อเมื่อ $G(b) = G(a)$ ทุกๆ $a, b \in X$ ❐

3.1.9 **บทแทรก** ถ้า X เป็น $G-$เซต และ $\sim$ เป็นความสัมพันธ์สมมูลบน X ดังนิยามในทฤษฎีบท 3.1.5 แล้ว $G_a \cong G_b$ เมื่อใดก็ตามที่ $a \sim b$ สำหรับทุกๆ $a, b \in X$

บทพิสูจน์ ให้ $a \sim b$ ใน X แล้วมี $g \in G$ ซึ่ง $ga = b$ นั่นคือ $g^{-1} b = a$ และสังเกตว่าถ้า $x \in G_a$ แล้ว $xa = a$ จึงได้ $(gxg^{-1})b = (gx)(g^{-1} b) = (gx)a = g(xa) = ga = b$ ซึ่งแสดงว่า $gxg^{-1} \in G_b$ เราจึงนิยาม $\varphi : G_a \to G_b$ โดย $\varphi(x) = gxg^{-1}$ ทุกๆ $x \in G_a$

เห็นชัดว่า $x_1 = x_2 \in G_a$ ก็ต่อเมื่อ $gx_1 g^{-1} = gx_2 g^{-1} \in G_b$ ดังนั้น φ เป็นฟังก์ชันหนึ่งต่อหนึ่ง และการพิสูจน์เช่นเดียวกับย่อหน้าแรก จะแสดงว่าถ้า $y \in G_b$ แล้ว $g^{-1} yg \in G_a$ โดยเฉพาะ $\varphi(g^{-1} yg) = g(g^{-1} yg) = y$ ทำให้ได้ φ เป็นฟังก์ชันทั่วถึง และสุดท้ายถ้า $x_1, x_2 \in G_a$ แล้ว $\varphi(x_1 x_2) = \varphi(x_1 x_2) = g(x_1 x_2)g^{-1} = (gx_1 g^{-1})(gx_2 g^{-1}) = \varphi(x_1)\varphi(x_2)$ ดังนั้น φ เป็นสมสัณฐาน จึงสรุปได้ว่า $G_a \cong G_b$ ❐

สังเกตว่า บทแทรก 3.1.9 แสดงด้วยว่า $|G_a| = |G_b|$ ถ้า $a \sim b$ ทุกๆ $a, b \in X$

3.1.10 **บทนิยาม** ให้ X เป็น $G-$เซต และ $g \in G$ เรียกเซต $X_g := \{a \in X | ga = a\}$ ว่า *เซตจุดตรึง (fixed point set)* โดย g

3.1.11 ทฤษฎีบท ถ้า G เป็นกรุปและ X เป็น $G-$เซต แล้วการกระทำของ G บน X ชักนำสาทิสสัณฐานจาก G ไปยังกรุปสมมาตร $A(X)$

บทพิสูจน์ แต่ละ $g \in G$ เรานิยาม $\tau_g : X \to X$ โดย $\tau_g(x) = gx$ ทุกๆ $x \in X$ แล้วเพราะ $x = g(g^{-1}x)$ ทุกๆ $x \in X$ ซึ่งแสดงว่า $\tau_g(g^{-1}x) = x$ สำหรับแต่ละ $x \in X$ ดังนั้น τ_g เป็นฟังก์ชันทั่วถึง และในทำนองคล้ายกันถ้า $gx = gy$ แล้ว $x = g^{-1}(gx) = g^{-1}(gy) = y$ ทุกๆ $x, y \in X$ ทำให้ได้ τ_g เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น τ_g เป็นวิธีเรียงสับเปลี่ยนบน X สุดท้ายเพราะ $\tau_{gg'} = \tau_g \tau_{g'}$ ทุกๆ $g, g' \in G$ ดังนั้น $\tau : G \to A(X)$ ซึ่งนิยามโดย $\tau(g) = \tau_g$ ทุกๆ $g \in G$ เป็นสาทิสสัณฐาน ❐

ผลของทฤษฎีบท 3.1.11 ทำให้เราพิสูจน์ทฤษฎีบทของเคย์เลย์ได้อย่างสั้นๆ อีกแบบหนึ่ง ดังแสดงในบทแทรกต่อไปนี้

3.1.12 บทแทรก ถ้า G เป็นกรุป แล้วมีสาทิสสัณฐานชนิดหนึ่งต่อหนึ่งจาก G ไปยัง $A(G)$ ซึ่งทำให้ได้ว่า ทุกๆ กรุปจะสมสัณฐานกับกรุปของวิธีเรียงสับเปลี่ยน และกรุปจำกัดจะสมสัณฐานกับกรุปย่อยของกรุปสมมาตร S_n เมื่อ $n = |G|$

บทพิสูจน์ ให้ G กระทำบน G แบบการเลื่อนไปทางซ้ายทั้งหมด (ตัวอย่าง 3.1.3) แล้วโดยทฤษฎีบท 3.1.11 ให้ $\tau : G \to A(G)$ เป็นสาทิสสัณฐานซึ่งชักนำโดยการเลื่อนไปทางซ้ายทั้งหมดบน G จะเห็นว่าถ้า $\tau(g) = \tau_g = \iota_G$ สำหรับ $g \in G$ แล้ว $gx = \tau_g(x) = x$ ทุกๆ $x \in G$ และในกรณีเฉพาะจะได้ $g = ge = e$ ซึ่งแสดงว่า $\ker \tau = \{e\}$ เพราะฉะนั้น τ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง

ข้อความสุดท้าย ได้จากการสังเกตว่าถ้า $|G| = n$ แล้ว $A(G) \cong S_n$ ❐

เบิร์นไซด์ (Burnside) นักคณิตศาสตร์ชาวอังกฤษซึ่งมีชีวิตในช่วงปีคริสตศักราช 1853 – 1927 สนใจศึกษาทฤษฎีโครงสร้างของกรุปจำกัดโดยเฉพาะ *กรุปเชิงเดียว (simple group)* ซึ่งคือกรุปที่มีเฉพาะกรุปนั้นกับ $\{e\}$ เท่านั้นที่เป็นกรุปย่อยปรกติ และได้ตั้งข้อคาดการณ์ (Conjecture) ไว้ว่า "*กรุปเชิงเดียวที่เป็นกรุปนอนอาบีเลียนมีอันดับเป็นจำนวนคู่*" ซึ่งข้อคาดการณ์นี้ได้รับการพิสูจน์โดยซิโลว์ (P.L. Sylow นักคณิตศาสตร์ชาวนอร์เวย์ที่มีชีวิตในช่วงปี 1832 – 1918) และต่อมา J. Thomson และ W. Feit นักคณิตศาสตร์ชาวอเมริกันได้พัฒนาการพิสูจน์อีกครั้งในปี ค.ศ.1964 และภายหลังเมื่อซิโลว์ได้พิสูจน์ทฤษฎีบทของซิโลว์แล้ว ท่านได้ประยุกต์ผลงานในการวิเคราะห์ว่ากรุปใดบ้างเป็นกรุปเชิงเดียวซึ่งเราจะศึกษาเรื่องราวเหล่านี้ในหัวข้อ 3.4 แต่เราจะปิดท้ายหัวข้อนี้ด้วยการประยุกต์การนับจำนวนออร์บิทใน $G-$เซตที่เป็นเซตจำกัดในการพิสูจน์ทฤษฎีบทที่มีชื่อเสียง

เกี่ยวกับเรื่องการนับ และอาจถือได้ว่าเป็นทฤษฎีบทที่เป็นรากฐานของวิชาคอมบินาทอริกส์ในยุคต่อมา นั่นคือทฤษฎีบทของเบิร์นไซด์

3.1.13 ทฤษฎีบทของเบิร์นไซด์ (Burnside's Theorem)

ให้ X เป็น $G-$เซตที่เป็นเซตจำกัดของกรุปจำกัด G ถ้า r เป็นจำนวนออร์บิททั้งหมดใน X ภายใต้ G แล้ว $r|G| = \sum_{g\in G}|X_g|$

บทพิสูจน์ ให้ $\mathrm{P} := \{(g,a) \in G\times X \,|\, ga = a\}$ แล้วเพราะ $ga = a$ ก็ต่อเมื่อ $a \in X_g$ ทุกๆ $g \in G$ และ $a \in X$ ดังนั้นแต่ละ $g \in G$ จำนวนคู่อันดับ (g,a) ใน P เท่ากับ $|X_g|$ จึงได้ $|\mathrm{P}| = \sum_{g\in G}|X_g|$ และในทำนองเดียวกันแต่ละ $a \in X$ จำนวนคู่อันดับ (g,a) ใน P เท่ากับ $|G_a|$ ดังนั้น $|\mathrm{P}| = \sum_{a\in X}|G_a|$ ทำให้ได้ $\sum_{g\in G}|X_g| = \sum_{a\in X}|G_a|$ และเพราะ $a \sim b$ ทุกๆ $a \in X$ และ $b \in G(a)$ จะได้ $|G_a| = |G_b|$ ดังนั้น $\sum_{b\in G(a)}|G_b| = |G(a)||G_a| = |G|$

เมื่อหาผลรวมของจำนวนออร์บิททั้งหมดที่ต่างกันใน X จำนวน r เซต จะได้ $|X| = \sum_{a\in X}|G_a| = r|G|$ ดังนั้น $\sum_{g\in G}|X_g| = \sum_{a\in X}|G_a| = r|G|$ ❐

3.1.14 ตัวอย่าง

เราต้องการหาจำนวนวิธีระบายสีแผ่นไม้กระดานรูปสี่เหลี่ยมจัตุรัสซึ่งแบ่งออกเป็นตารางสี่ช่อง ตามหมายเลขดังนี้

1	2
4	3

(ก)

โดยใช้สี m สี โดยที่แต่ละช่องจะระบายสีได้เพียงสีเดียวเท่านั้น และจะระบายสีแผ่นไม้กระดานนี้เพียงหน้าเดียว

เนื่องจากแผ่นไม้กระดานเป็นวัตถุแข็งเกร็งในระนาบซึ่งสามารถหมุนได้ ทำให้การระบายสีในบางแบบเป็นการระบายสีแบบเดียวกัน ตัวอย่างเช่นการระบายสีตามรูปข้างล่างนี้

ถือว่าเป็นการระบายสีวิธีเดียวกัน เพราะหากเราหมุนรูปใดรูปหนึ่งใน 4 รูปข้างต้นตามเข็มนาฬิกาหรือทวนเข็มนาฬิกาเป็นมุม $2n\pi$ เรเดียน (เมื่อ n เป็นจำนวนเต็ม) จะได้รูปที่เป็นรูปใดรูปหนึ่งในสี่รูปข้างต้น

ให้ X แทนเซตของภาพทั้งหมดที่เกิดจากการระบายสีลงในช่องหมายเลข 1–4 ช่องละสีจากสีที่มีอยู่ทั้งหมด m สี เราจะหากรุป G และนิยามการกระทำของ G บน X เพื่อให้ได้ความสัมพันธ์สมมูลบน X ที่กำหนดผลแบ่งกั้นของ X ซึ่งเป็นจำนวนวิธีระบายสีที่ทำให้ได้ภาพที่ต่างกันทั้งหมด นั่นคือจำนวนออร์บิทต่างกันทั้งหมดใน X และดังได้กล่าวแล้วว่าการหมุนภาพทำให้บางภาพซ้ำกัน เราจึงเลือกกรุป $G = <(1234)>$ และนิยามการกระทำของ G บน X เพื่อให้ X เป็น $G-$เซต และเพื่อความสะดวกขอกำหนดสัญลักษณ์แทนภาพต่างๆ ดังนี้

4	1
3	2

(ข)

3	4
2	1

(ค)

4	3
1	2

(ง)

ภาพ (ข), (ค) และ (ง) คือภาพที่ได้จากการหมุนภาพ (ก) ตามเข็มนาฬิกาเป็นมุม $\frac{\pi}{2}$, π และ $\frac{3\pi}{2}$ เรเดียน ตามลำดับ แล้วภาพ (ก) – (ง) เป็นสมาชิกของเซต X จึงกำหนด $\varphi : G \times X \to X$ โดยให้ $\varphi((1), f)$, $\varphi((1234), f)$, $\varphi((13)(24), f)$ และ $\varphi((1432), f)$ แทนภาพที่ได้จากการหมุน f ตามเข็มนาฬิกาเป็นมุม $0, \frac{\pi}{2}$, π และ $\frac{3\pi}{2}$ เรเดียนตามลำดับ แล้วเห็นได้ชัดว่า φ สอดคล้องเงื่อนไขข้อ 1 ของบทนิยาม 3.1.1 นอกจากนี้โดยวิธีหมุนภาพ จะได้

$$\varphi((1)(1234), f) = \varphi((1234), f) = \varphi((1), \varphi((1234), f)),$$
$$\varphi((1)(13)(24), f) = \varphi((13)(24), f) = \varphi((1), \varphi((13)(24), f)),$$
$$\varphi((1)(1432), f) = \varphi((1432), f) = \varphi((1), \varphi((1432), f)),$$
$$\varphi((1234)(1234), f) = \varphi((13)(24), f) = \varphi((1234), \varphi((1234), f)),$$
$$\varphi((1234)(13)(24), f) = \varphi((1432), f) = \varphi((1234), \varphi((13)(24), f)),$$
$$\varphi((1234)(1432), f) = \varphi((1), f) = \varphi((1234), \varphi((1432), f)),$$
$$\varphi((13)(24)(1234), f) = \varphi((1432), f) = \varphi((13)(24), \varphi((1234), f)),$$
$$\varphi((13)(24)(13)(24), f) = \varphi((1), f) = \varphi((13)(24), \varphi((13)(24), f)),$$
$$\varphi((13)(24)(1432), f) = \varphi((1234), f) = \varphi((13)(24), \varphi((1432), f)),$$

และ $$\varphi((1432)(1432), f) = \varphi((1), f) = \varphi((1432), \varphi((1432), f))$$

ทำให้ได้ว่า φ สอดคล้องเงื่อนไขข้อ 2 ของบทนิยาม 3.1.1 ดังนั้น X เป็น $G-$เซตที่ต้องการ ❍

แบบฝึกหัด 3.1

1. ให้ G เป็นกรุปและ X เป็น $G-$เซต โดยที่ $|X| \geq 2$ และสอดคล้องเงื่อนไขว่า สำหรับแต่ละ $a, b \in X$ จะมี $g \in G$ ซึ่ง $ga = b$ จงพิสูจน์ว่า

1.1 ออร์บิท $\bar{a}$ ของแต่ละ a ใน X ภายใต้ G คือ X

1.2 $G_a = gG_ag^{-1}$ สำหรับทุกๆ $a \in X$ และ $g \in G$

1.3 ถ้า $\{g \in G | (\forall a \in X)(ga = a)\} = \{e\}$ และ N เป็นกรุปย่อยปรกติของ G ที่มี $a \in X$ ซึ่ง N เป็นกรุปย่อยของ G_a แล้ว $N = \{e\}$

1.4 $|X| = [G : G_a]$ สำหรับทุกๆ $a \in X$ (ทำให้ได้ว่า $|X|$ เป็นตัวหารของ $|G|$)

2. จงประยุกต์ทฤษฎีบทของเบิร์นไซด์เพื่อหาจำนวนวิธีที่ต่างกันทั้งหมดสำหรับการจัดวางสิ่งกลมสีดำ 2 อันและสีขาว 2 อันบนขดลวดวงกลม โดยมีข้อตกลงว่าการจัดวาง 2 วิธีถือว่าเป็นวิธีเดียวกันถ้าสามารถเปลี่ยนการจัดวางวิธีหนึ่งเป็นอีกวิธีหนึ่งได้ด้วยการเลื่อนสิ่งทั้งสี่ไปตามกันเป็นวงกลม หรือหมุนขดลวดในอากาศแล้วทำให้สิ่ง 2 สิ่งที่เคยอยู่ประชิดกันยังคงอยู่ประชิดกัน

3.2 ทฤษฎีบทของโคชี

ทฤษฎีบทของลากรองจ์กล่าวว่า "*อันดับของสมาชิกในกรุปจำกัดเป็นตัวหารของอันดับของกรุปนั้น*" แต่เป็นที่ทราบกันดีว่ากรุปสมมาตร S_4 ที่มีอันดับ 24 ไม่มีกรุปย่อยอันดับ 6 ซึ่งแสดงว่าบทกลับของทฤษฎีบทของลากรองจ์ไม่เป็นจริง กล่าวคือถ้า n เป็นจำนวนเต็มบวกซึ่งเป็นตัวหารของอันดับของกรุปจำกัดแล้วกรุปจำกัดนั้น**อาจไม่มี**กรุปย่อยอันดับ n อย่างไรก็ตามในหัวข้อนี้ เราจะประยุกต์การกระทำของกรุปบนเซตในการพิสูจน์ทฤษฎีบทของโคชี (Arthur Cauchy 1789 – 1857) ซึ่งเป็นทฤษฎีบทที่มีความสำคัญในการแสดงว่า แม้บทกลับของทฤษฎีบทของลากรองจ์ไม่เป็นจริงโดยทั่วไป แต่ก็เป็นจริงในกรณีของจำนวนเฉพาะซึ่งทำให้เราสามารถจำแนกกรุปอันดับ 6

ถ้า G เป็นกรุปจำกัดและ X เป็น $G-$เซต ออร์บิทของ $a \in X$ คือ $G(a) = \{ga | g \in G\}$ และแต่ละสมาชิกของ X เป็นสมาชิกของออร์บิทใดออร์บิทหนึ่งเพียงออร์บิทเดียว ดังนั้นถ้ามีออร์บิทใน X ภายใต้ G เป็นจำนวน r เซตและสำหรับแต่ละ $1 \le i \le r$ เลือก a_i เพียงหนึ่งเดียวจาก $G(a_i)$ แล้ว $|X| = \sum_{i=1}^{r} |G(a_i)|$

ถ้า $X_G := \{a \in X | ga = a$ ทุกๆ $g \in G\}$ แล้ว X_G เป็นส่วนรวมของออร์บิทใน X ที่ประกอบด้วยสมาชิกเพียงหนึ่งตัว ถ้าสมมติมีออร์บิทใน X ที่ประกอบด้วยสมาชิกเพียงตัวเดียวจำนวน s ออร์บิทโดยที่ $0 \le s \le r$ และ $G(a_{s+1}), G(a_{s+2}), \ldots, G(a_r)$ เป็นออร์บิทใน X ที่ประกอบด้วยสมาชิกมากกว่าหนึ่งตัวแล้ว $|X_G| = s$ ซึ่งทำให้ได้

$$|X| = \sum_{i=1}^{r} |G(a_i)| = |X_G| + \sum_{i=s+1}^{r} |G(a_i)|$$

3.2.1 **ทฤษฎีบท** ให้ p เป็นจำนวนเฉพาะและ n เป็นจำนวนเต็มที่ไม่ใช่จำนวนลบ ถ้า G เป็นกรุปอันดับ p^n และ X เป็น $G-$เซตที่เป็นเซตจำกัดแล้ว $|X| \equiv |X_G| (\text{mod}\, p)$

บทพิสูจน์ ให้ X เป็น $G-$เซตที่เป็นเซตจำกัดแล้ว $|X| = |X_G| + \sum_{i=s+1}^{r} |G(a_i)|$ และเพราะ $|G(a)| = [G:G_a]$ เป็นตัวหารของ $|G| = p^n$ ทุกๆ $a \in X$ ดังนั้น p เป็นตัวหารของ $|G(a)|$ ทำให้ได้ว่า p เป็นตัวหารของ $\sum_{i=s+1}^{r} |G(a_i)|$ จึงได้ p เป็นตัวหารของ $|X| - |X_G|$ นั่นคือ $|X| \equiv |X_G| (\text{mod}\, p)$ ❐

3.2.2 **ทฤษฎีบทของโคชี** (Cauchy's Theorem) ให้ G เป็นกรุปจำกัด ถ้า p เป็นจำนวนเฉพาะซึ่งเป็นตัวหารของ $|G|$ แล้วมี $a \in G$ ซึ่ง $|a| = p$

บทพิสูจน์ ให้ $X := \{(g_1, \cdots, g_p) \in G^p \,|\, g_1 g_2 \cdots g_p = e\}$ จะพิสูจน์ก่อนว่า p เป็นตัวหารของ $|X|$

ให้ $(g_1, g_2, \cdots, g_p) \in X$ แล้ว $g_1 g_2 \cdots g_p = e$ ดังนั้น $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$ และในทางกลับกันแต่ละ $g_1, \ldots, g_{p-1} \in G$ จะมี $g_p = (g_1 g_2 \cdots g_{p-1})^{-1} \in G$ ซึ่ง $(g_1, g_2, \cdots, g_p) \in X$ ดังนั้น $|X|$ เท่ากับจำนวนวิธีเลือกสมาชิกใน G เพื่อใส่ลงในกล่อง $p-1$ กล่อง ทำให้ได้ $|X| = |G|^{p-1}$ และเพราะ p เป็นตัวหารของ $|G|$ ดังนั้น p เป็นตัวหารของ $|X|$ ต่อไปนิยามการกระทำของ S_p บน X โดย $\sigma(g_1, g_2, \cdots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)})$ ทุกๆ $\sigma \in S_p$ และทุกๆ $(g_1, g_2, \cdots, g_p) \in X$ แล้ว

1. $(1)(g_1, g_2, \cdots, g_p) = (g_1, g_2, \cdots, g_p)$ สำหรับทุกๆ $(g_1, g_2, \cdots, g_p) \in X$

และ 2. ให้ $\sigma_1, \sigma_2 \in S_p$ และ $(g_1, g_2, \cdots, g_p) \in X$ แล้ว

$$\begin{aligned}\sigma_1\sigma_2(g_1, g_2, \cdots, g_p) &= (g_{\sigma_1\sigma_2(1)}, g_{\sigma_1\sigma_2(2)}, \cdots, g_{\sigma_1\sigma_2(p)}) = (g_{\sigma_1(\sigma_2(1))}, g_{\sigma_1(\sigma_2(2))}, \cdots, g_{\sigma_1(\sigma_2(p))}) \\ &= \sigma_1(g_{\sigma_2(1)}, g_{\sigma_2(2)}, \cdots, g_{\sigma_2(p)}) \quad = \sigma_1(\sigma_2(g_1, g_2, \cdots, g_p))\end{aligned}$$

ให้ $\sigma = (12 \cdots p) \in S_p$ แล้ว $|\sigma| = p$ และ X เป็น $<\sigma>-$เซต และพิจารณาออร์บิท

$$X_{<\sigma>} = \{(g_1, g_2, \ldots, g_p) \in X \,|\, \sigma(g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p)\}$$

โดยทฤษฎีบท 3.2.1 จะได้ $|X| \equiv |X_{<\sigma>}| (\text{mod}\, p)$ แต่ p เป็นตัวหารของ $|X|$ ดังนั้น p เป็นตัวหารของ $|X_{<\sigma>}|$ ซึ่งแสดงว่า $|X_{<\sigma>}| \geq p$ ดังนั้น $X_{<\sigma>} \neq \phi$

ให้ $(g_1, g_2, \cdots, g_p) \in X_{<\sigma>}$ แล้ว $\sigma(g_1, g_2, \cdots, g_p) = (g_1, g_2, \cdots, g_p)$ และ $\sigma(g_1, \cdots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)}) = (g_2, g_3, \ldots g_p, g_1)$ ดังนั้น $(g_1, g_2, \cdots, g_p) = (g_2, g_3, \ldots g_p, g_1)$ ทำให้ได้ว่า $g_1 = g_2 = g_3 = \cdots = g_p$

ให้ $a := g_1 = g_2 = g_3 = \cdots = g_p$ แล้ว $e = g_1 g_2 \cdots g_p = a^p$ เพราะฉะนั้น $|a| = p$ ❐

3.2.3 **บทนิยาม** ให้ p เป็นจำนวนเฉพาะ เรากล่าวว่ากรุป G เป็น *$p-$กรุป ($p-$group)* ถ้าอันดับของแต่ละสมาชิกที่ไม่ใช่เอกลักษณ์ใน G เป็นจำนวนในรูปกำลังของ p นั่นคือสำหรับแต่ละ

$e \neq g \in G$ มีจำนวนเต็มบวก n ซึ่ง $|g| = p^n$

เรากล่าวว่ากรุปย่อย H ของกรุป G เป็น *$p-$กรุปย่อย ($p-$subgroup)* ของ G ถ้า H เป็น $p-$กรุป

3.2.4 **ทฤษฎีบท** ให้ p เป็นจำนวนเฉพาะแล้วกรุปจำกัด G เป็น $p-$กรุป ก็ต่อเมื่อ มีจำนวนเต็มบวก n ซึ่ง $|G| = p^n$

บทพิสูจน์ ให้ G เป็นกรุปจำกัดซึ่งเป็น $p-$กรุปและให้ q เป็นจำนวนเฉพาะซึ่งเป็นตัวหารของ $|G|$ แล้วโดยทฤษฎีบทของโคชีจะมี $a \in G$ ซึ่ง $|a| = q$ แต่ G เป็น $p-$กรุป ดังนั้นมีจำนวนเต็มบวก k ซึ่ง $|a| = p^k$ ทำให้ได้ $q = p^k$ ซึ่งแสดงว่า p เป็นตัวหารของ q โดยที่ q เป็นจำนวนเฉพาะ จึงได้ $q = p$ นั่นคือมีจำนวนเฉพาะ p เพียงหนึ่งเดียวที่เป็นตัวหารของ $|G|$ ดังนั้นมีจำนวนเต็มบวก n ซึ่ง $|G| = p^n$ ในทางกลับกันสมมติว่ามีจำนวนเต็มบวก n ซึ่ง $|G| = p^n$ และให้ $g \in G$ แล้วโดยผลของทฤษฎีบทของลากรองจ์ ได้ว่า $|g|$ เป็นตัวหารของ $|G| = p^n$ ดังนั้นมีจำนวนเต็ม $0 \leq k \leq n$ ซึ่ง $|g| = p^k$ เพราะฉะนั้น G เป็น $p-$กรุป ❐

ตัวอย่างต่อไปแสดงการประยุกต์ทฤษฎีบทของโคชี วิเคราะห์หากรุปที่มีอันดับ 6 ทั้งหมด

3.2.5 **ตัวอย่าง** ให้ G เป็นกรุปซึ่ง $|G| = 6 = (2)(3)$ แล้วโดยทฤษฎีบทของโคชี มี $a, b \in G \setminus \{e\}$ ซึ่ง $|a| = 2$ และ $|b| = 3$ ทำให้ได้ e, a, b, b^2, ab, ab^2 เป็นสมาชิกของ G ที่ต่างกันทั้งหมด ดังนั้น $G = \{e, a, b, b^2, ab, ab^2\}$ แต่ $ba \in G$ จึงได้ว่า

ถ้า $ba = e$ หรือ $ba = b^2$ แล้ว $b = a^{-1}$ หรือ $b = a$ ตามลำดับ ทำให้ได้ $2 = |a| = |a^{-1}| = |b| = 3$ ซึ่งเป็นไปไม่ได้ และถ้า $ba = a$ หรือ $ba = b$ แล้ว $b = e$ หรือ $a = e$ จะเกิดข้อขัดแย้งกันเองเช่นกัน เพราะฉะนั้น $ba = ab$ หรือ $ba = ab^2$

กรณี $ba = ab$ จะได้ G เป็นกรุปอาบีเลียน และเพราะ $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ เป็นกรุปอาบีเลียนอันดับ 6 ซึ่งก่อกำเนิดโดย $\overline{2}$ และ $\overline{3}$ โดยที่ $|\overline{2}| = 3$ และ $|\overline{3}| = 2$ ตามลำดับ และสมสัณฐานจะส่งตัวก่อกำเนิดไปเป็นตัวก่อกำเนิดอันดับเดียวกัน เราจึงนิยาม $f : G \to \mathbb{Z}_6$ ดังแสดงในตารางข้างล่างนี้

x	e	a	b	b^2	ab	ab^2
$f(x)$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{1}$

แล้วเห็นชัดว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ส่วนการเป็นสาทิสสัณฐานของ f พิจารณาด้วยการเปรียบเทียบตารางการคูณของ G และ $\mathbb{Z}_6$ ในตารางต่อไปนี้ซึ่งจะทำให้ได้ $G \cong \mathbb{Z}_6$

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab	b^2	e	ab^2	a
b^2	b^2	ab^2	e	b	a	ab
ab	ab	b	ab^2	a	b^2	e
ab^2	ab^2	b^2	a	ab	e	b

ตารางการคูณของกรุป G

	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{5}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{3}$
$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{3}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{2}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{4}$	$\overline{3}$	$\overline{5}$	$\overline{0}$	$\overline{2}$

ตารางการคูณของกรุป $\mathbb{Z}_6$

กรณี $ba = ab^2$ แล้ว G เป็นกรุปนอนอาบีเลียน และเพราะกรุปสมมาตร $S_3 = \{(1),(12),(13),(23),(123),(132)\}$ เป็นกรุปนอนอาบีเลียนอันดับ 6 ซึ่งก่อกำเนิดโดย (12) และ (123) โดยที่ $|(123)| = 3$ และ $|(12)| = 2$ ตามลำดับ เราจึงนิยาม $g : G \to S_3$ ดังแสดงในตารางข้างล่างนี้

x	e	a	b	b^2	ab	ab^2
$g(x)$	(1)	(12)	(123)	(132)	(23)	(13)

ตารางการส่งของสมสัณฐาน

เห็นได้ชัดว่า g เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ส่วนการเป็นสาทิสสัณฐานของ g พิจารณาด้วยการเปรียบเทียบตารางการคูณของ G และ S_3 ซึ่งทำให้ได้ $G \cong S_3$

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab	b^2	e	ab^2	a
b^2	b^2	ab^2	e	b	a	ab
ab	ab	b	ab^2	a	b^2	e
ab^2	ab^2	b^2	a	ab	e	b

ตารางการคูณของกรุป G

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

ตารางการคูณของกรุป S_3

เพราะฉะนั้นภายใต้กรุปสมสัณฐาน มีเพียง $\mathbb{Z}_6$ และ S_3 เท่านั้นที่เป็นกรุปอันดับ 6 ซึ่งแตกต่างกัน ❐

เราจะจบหัวข้อนี้ด้วยตัวอย่างการประยุกต์ทฤษฎีบทของโคชีในการแสดงว่ากรุปสลับ A_4 ไม่มีกรุปย่อยอันดับ 6

3.2.6 **ตัวอย่าง** กรุปสลับ A_4 เป็นกรุปอันดับ 12 โดยสมาชิกทั้ง 12 ตัวของ A_4 ได้แก่

สมาชิกอันดับ 1 คือ $\sigma_0 = (1)$

สมาชิกอันดับ 2 ได้แก่ $\sigma_1 = (12)(34),\ \sigma_2 = (13)(24),\ \sigma_3 = (14)(23),$

สมาชิกอันดับ 3 ได้แก่ $\sigma_4 = (123), \sigma_5 = (124), \sigma_6 = (132), \sigma_7 = (134), \sigma_8 = (142),$

$$\sigma_9 = (143), \sigma_{10} = (234),\ \sigma_{11} = (243)$$

สมมติมีกรุปย่อย H ของ A_4 ซึ่งมีอันดับ $6 = 2\times 3$ โดยทฤษฎีบทของโคชี H มีสมาชิกอันดับ 2 และอันดับ 3 ซึ่งต่างก่อกำเนิดกรุปย่อยวัฏจักร ถ้า σ_1 และ σ_4 เป็นสมาชิกของ H แล้ว $\{(1),\sigma_1\}$ และ $\{(1),\sigma_4,\sigma_6\}$ เป็นกรุปย่อยของ H ทำให้สมาชิกของ A_4 ต่อไปนี้เป็นสมาชิกของ H

$$\sigma_1\sigma_4 = (12)(34)(123) = (243) = \sigma_{11},\ \sigma_4\sigma_1 = (123)(12)(34) = (134) = \sigma_7,$$

$$\sigma_1\sigma_6 = (12)(34)(132) = (143) = \sigma_9,\ \ \sigma_6\sigma_1 = (132)(12)(34) = (234) = \sigma_{10}$$

ซึ่งทำให้ H ประกอบด้วยสมาชิกที่ต่างกันอย่างน้อย 8 ตัว จะขัดแย้งกับอันดับของ H และจะเกิดข้อขัดแย้งลักษณะเดียวกัน ถ้าสมาชิกอันดับ 2 และอันดับ 3 คู่อื่นๆ ใน A_4 เป็นสมาชิกของ H เพราะฉะนั้น A_4 ไม่มีกรุปย่อยอันดับ 6 ❍

แบบฝึกหัด 3.2

1. จงพิสูจน์ว่าถ้า p เป็นจำนวนเฉพาะซึ่งเป็นตัวหารของอันดับของกรุปจำกัด G แล้วมีกรุปวัฏจักรอันดับ p เป็นกรุปย่อยของ G

2. ให้ p เป็นจำนวนเฉพาะและ H เป็นกรุปย่อยปรกติของกรุป G จงพิสูจน์ว่าถ้า H และ G/H ทั้งคู่ต่างเป็น $p-$กรุป แล้ว G เป็น $p-$กรุป
3. จงพิสูจน์ว่าทุกๆ กรุปอันดับ p^2 เป็นกรุปอาบีเลียน ทุกๆ จำนวนเฉพาะ p
4. ให้ p เป็นจำนวนเฉพาะและ G เป็น $p-$กรุปจำกัด จงพิสูจน์ว่าถ้า H เป็นกรุปย่อยปรกติของ G และ $H \neq \{e\}$ แล้ว $H \cap Z(G) \neq \{e\}$

3.3 การกระทำของกรุปบนกรุป

ในหัวข้อ 3.1 เราได้แนะนำการกระทำของกรุปบนเซต และได้ให้ตัวอย่างหนึ่งของ $G-$เซตบนกรุป G ซึ่งเรียกว่า "การเลื่อนไปทางซ้ายทั้งหมด" และแสดงการประยุกต์การกระทำดังกล่าวในการพิสูจน์ทฤษฎีบทของเคย์เลย์อีกวิธีหนึ่งซึ่งง่ายขึ้นและสั้นลง ในหัวข้อนี้เราจึงสนใจหาการกระทำของกรุปบนกรุปอื่นๆ และแสดงประโยชน์ของการกระทำเหล่านั้น

3.3.1 **ตัวอย่าง** ให้ H เป็นกรุปย่อยของกรุป G และนิยามการกระทำสำหรับแต่ละ $x \in G$ และ $h \in H$ โดย $(h,x) \to hxh^{-1}$ และเพื่อหลีกเลี่ยงความสับสนของสัญลักษณ์ hx ซึ่งแทนการกระทำของ h ที่ x กับผลของการกระทำ hxh^{-1} จึงนิยมใช้ hxh^{-1} แทนการกระทำ hx ในกรณีนี้ จึงได้ $exe^{-1} = x$ ทุกๆ $x \in G$ และ $(h_1h_2)x(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1}$ ทุกๆ $g \in G$ และ $h_1, h_2 \in H$ จึงได้ว่า $(h,x) \to hxh^{-1}$ เป็นการกระทำของ H บน G ซึ่งเรียกว่า *การสังยุค (conjugation)* และเรียก hxh^{-1} ว่า *คู่สังยุค (conjugate)* ของ x ○

3.3.2 **ทฤษฎีบท** ให้ H เป็นกรุปย่อยของกรุป G และให้ H กระทำบน G โดยการสังยุค แล้ว

1. ทุกๆ สมาชิกในแต่ละเซตสังยุคมีอันดับเดียวกัน
2. H เป็นกรุปย่อยปรกติของ G ก็ต่อเมื่อ $H = \bigcup_{h \in H} C(h)$

บทพิสูจน์ 1. ให้ $x \in G$ แล้วแต่ละจำนวนเต็มที่ไม่ใช่จำนวนลบ n เห็นชัดว่า $(gxg^{-1})^n = (gxg^{-1})(gxg^{-1})\cdots(gxg^{-1})(gxg^{-1}) = gx^ng^{-1}$ ทุกๆ $g \in G$ ดังนั้นถ้า $x, y \in G$ เป็นสมาชิกในเซตสังยุคเดียวกันแล้วมี $g \in G$ ซึ่ง $y = gxg^{-1}$ จะได้ว่าถ้า $|y| = n$ แล้ว $e = y^n = (gxg^{-1})^n = gx^ng^{-1}$ นั่นคือ $x^n = e$ ซึ่งแสดงว่า $|x|$ เป็นจำนวนจำกัดและ $|y|$ เป็นตัวหารของ $|x|$ และในทำนองเดียวกันถ้า $|x| = m$ แล้ว $y^m = (gxg^{-1})^m = gx^mg^{-1} = e$ ทำให้ได้ $|y|$ เป็นจำนวนจำกัดและ $|x|$ เป็นตัวหารของ $|y|$ เพราะฉะนั้นอันดับของสมาชิกทั้งสองเป็นจำนวนจำกัดหรือจำนวนอนันต์พร้อมๆ กันและในกรณีอันดับจำกัด จะได้ $|x| = |y|$

2. ให้ H เป็นกรุปย่อยปรกติของ G และ $h \in H$ เห็นชัดว่าถ้า $x \in C(h)$ จะมี $g \in G$ ซึ่ง $x = ghg^{-1} \in H$ ดังนั้น $\bigcup_{h \in H} C(h) \subseteq H$ แต่เพราะ $h \in C(h)$ ทุกๆ $h \in H$ ดังนั้น $H \subseteq \bigcup_{h \in H} C(h)$ ❐

3.3.3 **ทฤษฎีบท** ให้ H เป็นเซตย่อยของกรุป G และ $g \in G$ แล้ว

1. $|H| = |gHg^{-1}|$
2. gHg^{-1} เป็นกรุปย่อยของ G ก็ต่อเมื่อ H เป็นกรุปย่อยของ G
3. ถ้า H เป็นกรุปย่อยของ G แล้ว $H \cong gHg^{-1}$

บทพิสูจน์ 1. ให้ $f : H \to gHg^{-1}$ นิยามโดย $f(h) = ghg^{-1}$ ทุกๆ $h \in H$ แล้ว $gh_1g^{-1} = gh_2g^{-1}$ $\Leftrightarrow g^{-1}(gh_1g^{-1})g = g^{-1}(gh_2g^{-1}) \Leftrightarrow h_1 = h_2$ ทุกๆ $h_1, h_2 \in H$ ดังนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่ง และเห็นได้ชัดว่า f เป็นฟังก์ชันทั่วถึง

2. ให้ H เป็นกรุปย่อยของ G ให้ $x = gh_1g^{-1}$ และ $y = gh_2g^{-1}$ เป็นสมาชิกของ gHg^{-1} แล้ว $h_1h_2^{-1} \in H$ ดังนั้น $xy^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = gh_1h_2^{-1}g^{-1} \in gHg^{-1}$ ซึ่งแสดงว่า gHg^{-1} เป็นกรุปย่อยของ G ในการพิสูจน์บทกลับให้ gHg^{-1} เป็นกรุปย่อยของ G แล้ว โดยการพิสูจน์ทำนองเดียวกันจะได้ $H = g^{-1}(gHg^{-1})(g^{-1})^{-1}$ เป็นกรุปย่อยของ G

3. เหลือเพียงแสดงว่า f ในข้อ 1 เป็นสาทิสสัณฐานซึ่งเห็นชัดว่า $f(h_1h_2) = g(h_1h_2)g^{-1} = gh_1(g^{-1}g)h_2g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = f(h_1)f(h_2)$ ทุกๆ $h_1, h_2 \in H$ ❐

3.3.4 **ตัวอย่าง** ให้ X เป็นเซตของกรุปย่อยทั้งหมดของ G และนิยามการกระทำสำหรับทุกๆ $K \in X$ และ $h \in H$ โดย $(h, K) \to hKh^{-1}$ แล้ว X เป็น $H-$เซตโดยการพิสูจน์ในทำนองเดียวกับตัวอย่าง 3.3.1 ซึ่งจะเรียก hKh^{-1} ว่าคู่สังยุคของ K เช่นเดียวกัน ❍

ถ้ากรุป G กระทำบน G โดยการสังยุค จะเรียกออร์บิท $C(x) = \{gxg^{-1} | g \in G\}$ ของ $x \in G$ ว่า *ชั้นสังยุค (conjugacy class)* ของ x และ $G_a = \{g \in G | gag^{-1} = a\}$ เป็นกรุปย่อยของ G ทุกๆ $a \in G$ ในทำนองเดียวกันถ้ากรุป G กระทำบนเซต X ของกรุปย่อยทั้งหมดของ G โดยการสังยุคแล้ว $G_H = \{g \in G | gHg^{-1} = H\}$ เป็นกรุปย่อยของ G ทุกๆ กรุปย่อย H ของ G ดังนั้น H เป็นกรุปย่อยปรกติของ G_H ยิ่งไปกว่านั้นถ้า K เป็นกรุปย่อยของ G ซึ่ง H เป็นกรุปย่อยปรกติของ K แล้ว $gHg^{-1} = H$ ทุกๆ $g \in K$ ทำให้ได้ว่า $g \in G_H$ ทุกๆ $g \in K$ นั่นคือ K เป็นกรุปย่อยของ G_H ซึ่งแสดงว่า G_H เป็น *กรุปย่อยใหญ่สุดเฉพาะกลุ่ม (maximal subgroup)* ของ G ที่มี H เป็นกรุปย่อยปรกติ

3.3.5 **บทนิยาม** เรียกกรุปย่อย $\{g \in G | ga = ag\}$ ของกรุป G ว่า *เซตเชิงศูนย์กลาง (centralizer)* ของ a ใน G และแทนด้วยสัญลักษณ์ $C_G(a)$

สำหรับกรุปย่อย H ของกรุป G เราเรียกกรุปย่อยใหญ่สุดเฉพาะกลุ่มของ G ที่มี H เป็นกรุปย่อยปรกติว่า *นอร์มัลไลเซอร์ (normalizer)* ของ H ใน G และแทนด้วยสัญลักษณ์ $N_G(H)$

โดยทฤษฎีบท 3.1.5 จะได้บทแทรกต่อไปนี้

3.3.6 **บทแทรก** $[G : C_G(a)] = |C(a)|$ ทุกๆ กรุปจำกัด G และทุกๆ $a \in G$

บทพิสูจน์ ให้ A แทนเซตของโคเซตซ้ายทั้งหมดของ $C_G(a)$ ใน G และนิยาม $f : \mathrm{A} \to C(a)$ โดย $f(gC_G(a)) = gag^{-1}$ ทุกๆ $gC_G(a) \in \mathrm{A}$ แล้ว $g_1C_G(a) = g_2C_G(a) \Leftrightarrow g_1^{-1}g_2 \in C_G(a)$ $\Leftrightarrow (g_1^{-1}g_2)a(g_1^{-1}g_2)^{-1} = a \Leftrightarrow g_1^{-1}(g_2ag_2^{-1})g_1 = a \Leftrightarrow g_2ag_2^{-1} = g_1ag_1^{-1}$ ทุกๆ $g_1, g_2 \in G$ และถ้า $x \in C(a)$ จะมี $g \in G$ ซึ่ง $x = gag^{-1}$ ดังนั้นมี $gC_G(a) \in \mathrm{A}$ ซึ่ง $f(gC_G(a)) = gag^{-1}$ $= x$ เพราะฉะนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ❐

สังเกตว่ากรุปย่อย H ของกรุป G เป็นกรุปย่อยปรกติ ก็ต่อเมื่อ H เท่านั้นที่เป็นคู่สังยุคของตัวเอง นั่นคือมีคู่สังยุคของ H ใน G เพียงเซตเดียวคือ H จึงอาจมีคำถามโดยทั่วไปว่า สำหรับกรุปย่อย H ของ G จะมีคู่สังยุคของ H ใน G ที่ต่างกันทั้งหมดกี่เซต แต่ทฤษฎีบท 3.1.5 แสดงแล้วว่าจำนวนคู่สังยุคของ H ใน G ที่ต่างกันทั้งหมดเท่ากับดรรชนีของ $N_G(H)$ ใน G จึงขอสรุปเป็นบทแทรกต่อไปนี้

3.3.7 **บทแทรก** จำนวนคู่สังยุคทั้งหมดของกรุปย่อย H ของกรุป G เท่ากับ $[G : N_G(H)]$ ❐

ถ้า G เป็นกรุปและ X เป็น $G-$เซต การพิสูจน์ทฤษฎีบทของโคชีได้กำหนดเซต $X_G := \{a \in X | ga = a$ ทุกๆ $g \in G\}$ ซึ่งเป็นส่วนรวมของออร์บิทใน X ที่ประกอบด้วยสมาชิกเพียงหนึ่งตัวและสำหรับกรุป G ซึ่งกระทำบน G โดยการสังยุค สมาชิก $x \in G$ ที่เป็นเพียงหนึ่งเดียวในเซตของคู่สังยุค จะเป็นสมาชิกของกรุปที่มีคุณลักษณะพิเศษซึ่งสมบัติของสมาชิกเหล่านี้ทำให้เกิดผลการศึกษาที่น่าสนใจต่อมา เราจึงเรียกเซตของ $x \in G$ ทั้งหลายที่มีคุณลักษณะซึ่ง $x = gxg^{-1}$ ทุกๆ $g \in G$ ว่า *ศูนย์กลาง (center)* ของ G และแทนด้วย $Z(G)$ ดังนั้น

$$Z(G) := \{x \in G | xg = gx \text{ ทุกๆ } g \in G\}$$

ทฤษฎีบทต่อไป กล่าวรวบรวมสมบัติที่มีประโยชน์ของศูนย์กลางของกรุป

3.3.8 **ทฤษฎีบท** ให้ G เป็นกรุป

1. การกระทำของ G บนเซต S ชักนำสาทิสสัณฐานจาก G ไปยังกรุป $A(S)$

2. ถ้า H เป็นกรุปย่อยของ G และ S เป็นเซตของโคเซตซ้ายทั้งหมดของ H ใน G แล้ว ส่วนกลางของสาทิสสัณฐานในข้อ 1 โดยการเลื่อนไปทางซ้ายทั้งหมดเป็นเซตย่อยของ H

บทพิสูจน์ 1. แต่ละ $g \in G$ นิยาม $\tau_g : S \to S$ โดย $x \to gx$ แล้ว $\tau_g \in A(S)$ โดยบทพิสูจน์ของทฤษฎีบทของเคย์เลย์ และเห็นชัดว่าการส่ง $\tau : g \to \tau_g$ เป็นสาทิสสัณฐาน

2. กรณีนี้ $\tau_g : S \to S$ ของข้อ 1 ทุกๆ $g \in G$ นิยามโดย $\tau_g(xH) = gxH$ ดังนั้นถ้า $g \in \ker\tau$ แล้ว $\tau_g = id_S$ ทำให้ได้ $gxH = xH$ ทุกๆ $x \in G$ โดยเฉพาะเมื่อ $x = e$ จะได้ $gH = H$ ซึ่งสมมูลกับ $g \in H$ ดังนั้น $\ker\tau \subseteq H$ ❐

ถ้า G เป็นกรุป เราเรียกสมสัณฐานจาก G ไปบน G ว่า *อัตสัณฐาน (automorphism)* และสัญลักษณ์ $Aut(G)$ หมายถึงเซตของอัตสัณฐานทั้งหมดบน G

3.3.9 **ทฤษฎีบท** ให้ G เป็นกรุป

1. แต่ละ $g \in G$ การส่ง τ_g ซึ่งส่งแต่ละ $x \in G$ ไปยังคู่สังยุค gxg^{-1} (นิยามดังในทฤษฎีบท 3.1.12) เป็นอัตสัณฐานบน G ซึ่งเรียกว่า *อัตสัณฐานภายใน (inner automorphism)*

2. มีสาทิสสัณฐาน $\tau : G \to Aut(G)$ ซึ่ง $\ker\tau = Z(G)$

บทพิสูจน์ ข้อ 1 เห็นได้ชัด จึงขอละการพิสูจน์เป็นแบบฝึกหัด ส่วนการพิสูจน์ข้อ 2 เห็นได้ชัดว่าภาพของสาทิสสัณฐาน $\tau : G \to A(G)$ ในบทแทรก 3.1.13 เป็นกรุปย่อยของ $Aut(G)$ ยิ่งไปกว่านั้น

$$g \in \ker\tau \;\Leftrightarrow\; \tau_g = id_G \;\Leftrightarrow\; gxg^{-1} = \tau_g(x) = x \text{ ทุกๆ } x \in G$$

แต่ $gxg^{-1} = x$ ก็ต่อเมื่อ $gx = xg$ ทุกๆ $g, x \in G$ ดังนั้น $\ker\tau = Z(G)$ ❐

3.3.10 **ทฤษฎีบท** ให้ G เป็นกรุป

1. $Z(G)$ เป็นกรุปอาบีเลียนซึ่งเป็นกรุปย่อยปรกติของ G

2. ถ้า G เป็นกรุปจำกัด แล้วมีจำนวนเต็ม $r \geq 0$ ซึ่ง $|G| = |Z(G)| + \sum_{i=1}^{r}[G : C_G(a_i)]$ เมื่อ a_i เป็นสมาชิกในเซตของคู่สังยุคลำดับที่ $i \leq r$ และเรียกสมการนี้ว่า *สมการชั้นสมมูล (class equation)* ของ G

3. ถ้า p เป็นจำนวนเฉพาะและ G เป็น $p-$กรุปจำกัด แล้วมีจำนวนเต็มบวก s ซึ่ง $|Z(G)| = p^s > 1$ [กล่าวโดยเฉพาะว่า $Z(G) \neq \{e\}$]

บทพิสูจน์ ข้อ 1 เป็นผลโดยตรงของทฤษฎีบท 3.3.8 ส่วนข้อ 2 พิสูจน์ได้โดยใช้สมการ $|X| = |X_G| + \sum_{i=s+1}^{r}|G(a_i)|$ ของทฤษฎีบท 3.2.1 ในการพิสูจน์ข้อ 3 ให้ p เป็นจำนวนเฉพาะและ r เป็น

จำนวนเต็มบวกซึ่ง $|G| = p^r$ ให้สมการชั้นสมมูลของ G คือ $p^r = |Z(G)| + h_1 + h_2 + \cdots + h_t$ โดยที่ $h_i > 1$ ทุกๆ $1 \le i \le t$ แต่ $h_i = [G : C_G(a_i)]$ เป็นตัวหารของ $|G| = p^r$ ทุกๆ $1 \le i \le t$ ทำให้ได้

$$|Z(G)| = p^r - p^{l_1} - p^{l_2} - \cdots - p^{l_t}$$

ดังนั้น p เป็นตัวหารของ $|Z(G)|$ และโดยทฤษฎีบทของลากรองจ์ $|Z(G)|$ เป็นตัวหารของ $|G| = p^r$ จากทั้งสองเหตุผลนี้ทำให้ได้ว่ามีจำนวนเต็มบวก s ซึ่ง $|Z(G)| = p^s > 1$ ดังนั้นทุกๆ $p-$กรุปจำกัด มีศูนย์กลางที่ไม่ใช่ $\{e\}$ ❐

3.3.11 **บทแทรก** กรุป G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $G = Z(G)$ ❐

3.2.12 **บทแทรก** ให้ p เป็นจำนวนเฉพาะซึ่งเป็นตัวหารของอันดับของกรุปจำกัด G

1. ถ้า H เป็น $p-$กรุปย่อยของ G แล้ว $[N_G(H) : H] \equiv [G : H] \pmod p$
2. ถ้า p เป็นตัวหารของ $[G : H]$ แล้ว $N_G(H) \ne H$

บทพิสูจน์ 1. ให้ A แทนเซตของโคเซตซ้ายทั้งหมดของ H ใน G แล้ว A เป็น $H-$เซตโดยการกระทำที่นิยามในตัวอย่าง 3.1.4 และขอละการพิสูจน์ว่า $|\mathrm{A}_H| = |B|$ ไว้เป็นแบบฝึกหัดเมื่อ $\mathrm{A}_H = \{gH \mid gH = hgH$ ทุกๆ $h \in H\}$ และ $B = \{gH \mid g \in N_G(H)\}$

2. จาก $[N_G(H) : H] \ge 1$ ถ้า p เป็นตัวหารของ $[G : H]$ แล้ว $[G : H] \equiv 0 \pmod p$ และโดยข้อ 1 จะได้ $[N_G(H) : H] \equiv 0 \pmod p$ นั่นคือ p เป็นตัวหารของ $[N_G(H) : H]$ ดังนั้น $[N_G(H) : H] > 1$ ❐

3.3.13 **ทฤษฎีบท** ถ้า H เป็นกรุปย่อยของกรุปจำกัด G ซึ่ง $[G : H] = p$ โดยที่ p เป็นจำนวนเฉพาะเล็กสุดซึ่งเป็นตัวหารของ G แล้ว H เป็นกรุปย่อยปรกติของ G

บทพิสูจน์ ให้ S เป็นเซตของโคเซตซ้ายทั้งหมดของ H ใน G แล้วเพราะ $[G : H] = p = |S|$ ดังนั้น $A(S) \cong S_p$ นอกจากนี้การส่ง $\tau : G \to A(S)$ ซึ่งนิยามโดย $\tau(g) = \tau_g$ ทุกๆ $g \in G$ เมื่อ $\tau_g : S \to S$ นิยามโดย $\tau_g(xH) = gxH$ ทุกๆ $x \in G$ เป็นสาทิสสัณฐานโดยที่ $K = \ker\tau \subseteq H$ และ G/K สมสัณฐานกับกรุปย่อยของ $A(S) \cong S_p$ ดังนั้น $|G/K|$ เป็นตัวหารของ $|S_p| = p!$ แต่ทุกๆ ตัวหารของ $|G/K| = [G : K]$ เป็นตัวหารของ $|G| = |K|[G : K]$ และไม่มีจำนวนนับใดที่เล็กกว่า p ซึ่งเป็นตัวหารของ $|G|$ ยกเว้น 1 ทำให้ได้ว่า $|G/K| = p$ หรือ $|G/K| = 1$

แต่ $|G/K| = [G : K] = [G : H][H : K] = p[H : K] \ge p$ ดังนั้น $|G/K| = p$ และ $[H : K] = 1$ ทำให้ได้ $H = K$ โดยที่ K เป็นกรุปย่อยปรกติของ G ❐

3.3.14 **ตัวอย่าง** พิจารณากรุป $S_3 = \{(1),(12),(13),(23),(123),(132)\}$ ซึ่งเป็นกรุปนอนอาบีเลียนเล็กสุด เราทราบว่า $(1) \in Z(S_3)$ ดังนั้นเซตสังยุคของ (1) จะมี (1) เป็นสมาชิกเพียงตัวเดียวและ

$$(12)(13)=(132),\ (13)(12)=(123),\ (12)(23)=(123),\ (23)(12)=(132)$$

ดังนั้น (12),(13) และ (23) ต่างไม่ใช่สมาชิกของ $Z(S_3)$ จึงไม่ใช่สมาชิกเพียงตัวเดียวในเซตสังยุคของแต่ละตัว และเพราะสมาชิกในเซตสังยุคจะมีอันดับเดียวกัน ดังนั้นในเซตสังยุคของทั้งสามตัวนี้จึงไม่มี (123) และ (132) เป็นสมาชิก ทำให้ได้ว่าเซตสังยุคเซตหนึ่งคือ

$$C(12)=C(13)=C(23)=\{(12),(13),(23)\}$$

ในทำนองเดียวกัน $(123)(12)=(13)$ และ $(12)(123)=(23)$ ดังนั้น $(123)\notin Z(S_3)$ และโดยการวิเคราะห์เช่นเดียวกัน จะได้เซตสังยุคอีกเซตหนึ่งคือ

$$C(123)=C(132)=\{(123),(132)\}$$

เพราะฉะนั้นเซตของเซตสังยุคทั้งหมดของ S_3 คือ $\{\{(1)\},\{(12),(13),(23)\},\{(123),(132)\}\}$ ทำให้ได้สมการชั้นสมมูลของ S_3 คือ $|S_3|=|Z(S_3)|+h_1+h_2$ โดยที่ h_1 และ h_2 เป็นจำนวนสมาชิกในเซตสังยุค $\{(12),(13),(23)\}$ และ $\{(123),(132)\}$ ตามลำดับ ซึ่งอาจคำนวณตามทฤษฎีบทดังนี้

$$h_1=[S_3:C_{S_3}((12))]=\frac{|S_3|}{|C_{S_3}((12))|}$$

และ $x\in C_{S_3}((12))\Leftrightarrow x(12)=(12)x\Leftrightarrow x=(1)$ หรือ $x=(12)$ ดังนั้น $C_{S_3}((12))=\{(1),(12)\}$ ทำให้ได้ $h_1=\dfrac{|S_3|}{|C_{S_3}((12))|}=\dfrac{6}{2}=3$ และเช่นเดียวกัน $h_2=[S_3:C_{S_3}((123))]=\dfrac{|S_3|}{|\{(1),(123),(132)\}|}$ $=\dfrac{6}{3}=2$ เพราะฉะนั้นสมการชั้นสมมูลของ S_3 คือ $6=1+3+2$ ❍

แบบฝึกหัด 3.3

1. ให้ G เป็นกรุป จงพิสูจน์ว่า $Aut(G)$ กับการประกอบของฟังก์ชันเป็นกรุป และถ้า H เป็นกรุปย่อยอาบีเลียนของ G แล้วการกระทำของ G/H บน H โดยการสังยุคจะชักนำสาทิสสัณฐานจาก G/H ไปยัง $Aut(G)$
2. จงแสดงว่าถ้ามีสมาชิกของกรุป G ซึ่งมีคู่สังยุคเท่ากับสองตัว แล้วมีกรุปย่อยปรกติของ G ซึ่งไม่ใช่ทั้ง G และ $\{e\}$
3. ให้ H และ K เป็นกรุปย่อยของกรุป G จงพิสูจน์ว่า
   3.1 ถ้า H เป็นกรุปย่อยปรกติของ K แล้ว K เป็นกรุปย่อยของ $N_G(H)$
   3.2 เซตศูนย์กลางของ H ใน G (นั่นคือ $C_G(H):=\{g\in G|gh=hg$ ทุกๆ $h\in H\}$) เป็นกรุปย่อยของ $N_G(H)$ และ $N_G(H)/C_G(H)$ จะสมสัณฐานกับกรุปย่อยของ $Aut(H)$
4. จงพิสูจน์ว่าถ้า $G/Z(G)$ เป็นกรุปวัฏจักรแล้ว G เป็นกรุปอาบีเลียน

5. ให้ G เป็นกรุปและสัญลักษณ์ $In(G)$ แทนเซตของอัตสัณฐานภายในทั้งหมดของ G จงพิสูจน์ว่า $In(G)$ เป็นกรุปย่อยปรกติของ $Aut(G)$ พร้อมทั้งหาอัตสัณฐานของ $\mathbb{Z}_6$ ที่ไม่ใช่อัตสัณฐานภายใน
6. จงพิสูจน์ว่าศูนย์กลางของ S_4 คือ $\{e\}$ เพื่อสรุปว่า S_6 เป็นสมสัณฐานกับ $In(S_4)$
7. ให้ H เป็นกรุปย่อยของกรุป G ซึ่ง $[G:H]=n$ เมื่อ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่าถ้าไม่มีกรุปย่อยปรกติ N ที่ไม่ใช่ทั้ง G และ $\{e\}$ ซึ่ง $N \subseteq H$ แล้ว G สมสัณฐานกับกรุปย่อยของ S_n
8. ให้ p เป็นจำนวนเฉพาะ n เป็นจำนวนเต็มบวกและ G เป็นกรุป จงพิสูจน์ว่า
   8.1 ถ้า $|G| = pn$ โดยที่ $p > n$ และ H เป็นกรุปย่อยอันดับ p ของ G แล้ว H เป็นกรุปย่อยปรกติ
   8.2 ถ้า $|G| = p^n$ และ H เป็นกรุปย่อยอันดับ p ของ G แล้ว $H = Z(G)$

3.4 ทฤษฎีบทของซิโลว์

ทฤษฎีบทของลากรองจ์กล่าวว่า "อันดับของสมาชิกในกรุปจำกัดเป็นตัวหารของอันดับของกรุปนั้น" และเรามีตัวอย่างว่า "กรุปสลับ A_4 ไม่มีกรุปย่อยอันดับ 6 " ซึ่งแสดงว่าบทกลับของทฤษฎีบทของลากรองจ์ไม่เป็นจริง อย่างไรก็ตามในบทที่ 2 ได้แสดงการจำแนกกรุปอาบีเลียนก่อกำเนิดแบบจำกัดซึ่งทำให้เกิดผลพลอยได้ว่า บทกลับของทฤษฎีบทของลากรองจ์เป็นจริงในหมู่ของกรุปอาบีเลียนอันดับจำกัด และแม้หมู่ของกรุปนอนอาบีเลียนจะมีขนาดใหญ่และซับซ้อนมากก็ตาม ในหัวข้อ 3.2 ทฤษฎีบทของโคชีได้แสดงว่าบทกลับของทฤษฎีบทของลากรองจ์เป็นจริงในกรณีของจำนวนเฉพาะและทำให้สามารถจำแนกกรุปอันดับ 6 ได้ทั้งหมด (ไม่นับการเป็นสมสัณฐาน) ในหัวข้อนี้ เราจะศึกษาและพิสูจน์ทฤษฎีบทของซิโลว์ซึ่งเป็นกลุ่มของทฤษฎีบทที่แสดงความพยายามหาลักษณะเฉพาะของจำนวนเต็มบวกที่เป็นตัวหารของอันดับของกรุปจำกัดและกรุปนั้นมีกรุปย่อยที่มีอันดับเท่ากับจำนวนเต็มบวกเหล่านั้น

ทฤษฎีบทที่หนึ่งของซิโลว์แสดงการขยายผลของทฤษฎีบทของโคชี นั่นคือการพิสูจน์ว่าบทกลับของทฤษฎีบทของลากรองจ์เป็นจริงเมื่อจำนวนเต็มบวกที่เป็นตัวหารของอันดับของกรุปจำกัดเป็นกำลังของจำนวนเฉพาะ ทำให้เกิดการขยายผลต่อมาเป็นทฤษฎีบทที่สองและที่สามของซิโลว์ซึ่งศึกษาเรื่องราวของกรุปที่มีอันดับเป็นกำลังสูงสุดของจำนวนเฉพาะที่เป็นตัวหารของอันดับของกรุป

จำกัด ทำให้เรามีเครื่องมือมากพอที่จะจำแนกกรุปจำกัดอันดับไม่เกิน 30 และสามารถหากรุปย่อยของกรุปจำกัดได้

3.4.1 **ทฤษฎีบทที่หนึ่งของซีโลว์** (First Sylow Theorem)

ให้ G เป็นกรุปจำกัดซึ่ง $|G| = p^n m$ เมื่อ p เป็นจำนวนเฉพาะ m และ n เป็นจำนวนเต็มบวกซึ่ง $(p,m)=1$ แล้วมีกรุปย่อยของ G อันดับ p^k ทุกๆ $1 \le k \le n$ และแต่ละกรุปย่อยอันดับ p^k ของ G เป็นกรุปย่อยของกรุปย่อยอันดับ p^{k+1} ของ G ทุกๆ $1 \le k < n$

บทพิสูจน์ โดยทฤษฎีบทของโคชี G มีกรุปย่อยวัฏจักรอันดับ p ให้ $1 \le k < n$ และ H เป็นกรุปย่อยของ G ซึ่ง $|H| = p^k$ แล้ว H เป็น $p-$กรุปย่อยของ G ซึ่ง p เป็นตัวหารของ $[G:H]$ จึงได้โดยบทแทรก 3.3.11 ว่า H เป็นกรุปย่อยปรกติของ $N_G(H)$ แต่ $1 < |N_G(H)/H| = [N_G(H):H] \equiv 0 \pmod p$ ดังนั้น p เป็นตัวหารของ $|N_G(H)/H|$ ทำให้ได้โดยทฤษฎีบทของโคชีว่า $N_G(H)/H$ มีกรุปย่อยวัฏจักรอันดับ p และกรุปย่อยนี้เขียนได้ในรูปแบบ K/H สำหรับบางกรุปย่อย K ของ $N_G(H)$ ดังนั้น H เป็นกรุปย่อยปรกติของ K ด้วย และสุดท้าย $|K| = |H||K/H| = p^k p = p^{k+1}$

โดยอุปนัยเชิงคณิตศาสตร์ มีกรุปย่อยของ G อันดับ p^k ทุกๆ $1 \le k \le n$ และแต่ละกรุปย่อยอันดับ p^k ของ G เป็นกรุปย่อยของกรุปย่อยของ G ที่มีอันดับ p^{k+1} ❐

3.4.2 **บทนิยาม** ให้ p เป็นจำนวนเฉพาะและ H เป็นกรุปย่อยของกรุปจำกัด G จะกล่าวว่า H เป็น *ซีโลว์ $p-$กรุปย่อย (Sylow $p-$subgroup)* ถ้า H เป็น *$p-$กรุปย่อยใหญ่สุดเฉพาะกลุ่ม (maximal $p-$subgroup)* ของ G นั่นคือถ้า H เป็น $p-$กรุปย่อยและสำหรับ $p-$กรุปย่อย K ของ G ซึ่ง $H \subseteq K \subset G$ แล้ว $H = K$

ทฤษฎีบทที่หนึ่งของซีโลว์กล่าวว่า ถ้าจำนวนเฉพาะ p เป็นตัวหารของอันดับของ G แล้วจะมีซีโลว์ $p-$กรุปย่อยของกรุปจำกัด G ซึ่งไม่ใช่ $\{e\}$ และทุกๆ $p-$กรุปย่อยของ G เป็นกรุปย่อยของซีโลว์ $p-$กรุปย่อยกรุปหนึ่งเสมอ ทฤษฎีบทต่อไปแสดงสมบัติและการจำแนกของซีโลว์ $p-$กรุปย่อย

3.4.3 **บทแทรก** ให้ G เป็นกรุปจำกัดซึ่ง $|G| = p^n m$ เมื่อ p เป็นจำนวนเฉพาะ m และ n เป็นจำนวนเต็มบวกซึ่ง $(p,m)=1$ และ H เป็น $p-$กรุปย่อยของ G แล้ว

1. H เป็นซีโลว์ $p-$กรุปย่อย ก็ต่อเมื่อ $|H| = p^n$
2. ทุกๆ สังยุคของซีโลว์ $p-$กรุปย่อยเป็นซีโลว์ $p-$กรุปย่อย
3. ถ้า H เป็นซีโลว์ $p-$กรุปย่อยเพียงหนึ่งเดียวของ G แล้ว H เป็นกรุปย่อยปรกติของ G

บทพิสูจน์ 1. ให้ H เป็น $p-$กรุปย่อยของ G และ $|H|=p^k$ ถ้า $k<n$ แล้วโดยทฤษฎีบทที่หนึ่งของซีโลว์ H เป็นกรุปย่อยของบาง $p-$กรุปย่อย G ที่มีอันดับ p^{k+1} ดังนั้น H ไม่เป็นซีโลว์ $p-$กรุปย่อย ในการพิสูจน์บทกลับให้ H เป็น $p-$กรุปย่อยของ G ซึ่ง $|H|=p^n$ และให้ K เป็น $p-$กรุปย่อยของ G ซึ่ง $H\subseteq K\subset G$ แล้ว $|K|\geq|H|$ และ $|K|$ อยู่ในรูปกำลังของ p ที่เป็นตัวหารของ $|G|$ แต่ p^n เป็นจำนวนมากสุดในรูปกำลังของ p ที่เป็นตัวหารของ $|G|$ จึงทำให้ $|K|=p^n$ ดังนั้น $H=K$ นั่นคือ H เป็นซีโลว์ $p-$กรุปย่อย

2. โดยทฤษฎีบท 3.3.3 ทุกๆ สังยุคของซีโลว์ $p-$กรุปย่อยมีอันดับเท่ากันและเท่ากับอันดับของซีโลว์ $p-$กรุปย่อยและโดยข้อ 1 อันดับของสังยุคของซีโลว์ $p-$กรุปย่อยเท่ากับ p^n ทำให้ได้โดยข้อ 1 อีกครั้งว่า สังยุคของซีโลว์ $p-$กรุปย่อยปีนซีโลว์ $p-$กรุปย่อย

3. ให้ H เป็นซีโลว์ $p-$กรุปย่อยเพียงหนึ่งเดียวของ G และให้ $a\in G$ แล้วโดยข้อ 2 สังยุค aHa^{-1} ของ H เป็นซีโลว์ $p-$กรุปย่อยของ G แต่ H เป็นซีโลว์ $p-$กรุปย่อยเพียงหนึ่งเดียวของ G ดังนั้น $aHa^{-1}=H$ เพราะฉะนั้น $aHa^{-1}=H$ ทุกๆ $a\in G$ นั่นคือ H เป็นกรุปย่อยปรกติของ G ❐

ทฤษฎีบทที่สองของซีโลว์จะแสดงให้เห็นว่าบทกลับของบทแทรก 3.4.3 ข้อ 2 เป็นจริงด้วย ซึ่งจะเป็นวิธีการหาซีโลว์ $p-$กรุปย่อยอีกวิธีหนึ่ง

3.4.4 ทฤษฎีบทที่สองของซีโลว์ (Second Sylow Theorem)

ให้ G เป็นกรุปจำกัดซึ่ง $|G|=p^n m$ เมื่อ p เป็นจำนวนเฉพาะ m และ n เป็นจำนวนเต็มบวกซึ่ง $(p,m)=1$ แล้ว

1. แต่ละ $p-$กรุปย่อย H และซีโลว์ $p-$กรุปย่อย P ของ G จะมี $a\in G$ ซึ่ง H เป็นกรุปย่อยของ aPa^{-1}

2. ซีโลว์ $p-$กรุปย่อยของ G เป็นสังยุคของกันและกัน

บทพิสูจน์ 1. ให้ X เป็นเซตของโคเซตซ้ายทั้งหมดของ P ใน G และให้ H กระทำบน X แบบการเลื่อนไปทางซ้ายทั้งหมด โดยทฤษฎีบท 3.2.1 จะได้ $[G:P]=|X|\equiv|X_G|(\text{mod}\,p)$ แต่ $|G|=|P|[G:P]=p^n m$ โดยที่ $|P|=p^n$ และ $(p,m)=1$ ดังนั้น p ไม่เป็นตัวหารของ $[G:P]$ ทำให้ได้ $|X_G|\neq 0$ ดังนั้นมี $xP\in X_G$ และเพราะว่า

$$xP\in X_G \;\Leftrightarrow\; hxP=xP \text{ ทุกๆ } h\in H \;\Leftrightarrow\; x^{-1}hxP=P \text{ ทุกๆ } h\in H$$
$$\Leftrightarrow\; x^{-1}Hx \text{ เป็นกรุปย่อยของ } P \;\Leftrightarrow\; H \text{ เป็นกรุปย่อยของ } xPx^{-1}$$

ดังนั้น H เป็นกรุปย่อยของ xPx^{-1}

2. ให้ H และ P เป็นซีโลว์ $p-$กรุปย่อยของ G โดยข้อ 1 จะมี $a \in G$ ซึ่ง H เป็นกรุปย่อยของซีโลว์ $p-$กรุปย่อย aPa^{-1} โดยที่ $|H| = |P| = |aPa^{-1}|$ ดังนั้น $H = aPa^{-1}$ เป็นสังยุคของ P ❐

ทฤษฎีบทที่สามของซีโลว์แสดงข้อมูลของจำนวนซีโลว์ $p-$กรุปย่อยทั้งหมดของกรุปจำกัด

3.4.5 ทฤษฎีบทที่สามของซีโลว์ (Third Sylow Theorem)

ให้ G เป็นกรุปจำกัดซึ่ง $|G| = p^n m$ เมื่อ p เป็นจำนวนเฉพาะ m และ n เป็นจำนวนเต็มบวกซึ่ง $(p,m)=1$ และให้ N_p เป็นจำนวนซีโลว์ $p-$กรุปย่อยที่ต่างกันทั้งหมดของ G แล้ว N_p เป็นตัวหารของ $|G|$ และ $N_p \equiv 1 \pmod p$ [นั่นคือ N_p เขียนได้ในรูป $kp+1$ สำหรับบางจำนวนเต็ม ที่ไม่เป็นลบ k]

บทพิสูจน์ โดยทฤษฎีบทที่สองของซีโลว์ ซีโลว์ $p-$กรุปย่อยทั้งหมดของ G เป็นสังยุคของกันและกัน ให้ P เป็นซีโลว์ $p-$กรุปย่อยของ G แล้วจำนวนซีโลว์ $p-$กรุปย่อยทั้งหมดของ G เท่ากับจำนวนสังยุคทั้งหมดของ P และโดยบทแทรก 3.3.7 จำนวนสังยุคของ P ที่ต่างกันทั้งหมดเท่ากับ $N_p = [G : N_G(H)]$ ซึ่งเป็นตัวหารของ $|G|$

ให้ X เป็นเซตของซีโลว์ $p-$กรุปย่อยทั้งหมดของ G ให้ P กระทำบน X โดยการสังยุค โดยทฤษฎีบท 3.2.1 จะได้ $|X| \equiv |X_G| \pmod p$ แต่

$$Q \in X_G \quad \Leftrightarrow \quad xQx^{-1} = Q \text{ ทุกๆ } x \in P \quad \Leftrightarrow \quad P \text{ เป็นกรุปย่อยของ } N_G(Q)$$

ให้ $Q \in X_G$ แล้ว P เป็นกรุปย่อยของ $N_G(Q)$ และเพราะ $N_G(Q)$ เป็นกรุปย่อยของ G และ P และ Q เป็นซีโลว์ $p-$กรุปย่อยของ G ดังนั้น P และ Q เป็นซีโลว์ $p-$กรุปย่อยของ $N_G(Q)$ จึงเป็นคู่สังยุคกันใน $N_G(Q)$ แต่ Q เป็นกรุปย่อยปรกติของ $N_G(Q)$ ดังนั้น Q เป็นซีโลว์ $p-$กรุปย่อยเพียงหนึ่งเดียวของ $N_G(Q)$ ทำให้ได้ $P = Q$ เพราะฉะนั้น $X_G = \{P\}$ นั่นคือ $|X_G| = 1$ ทำให้ได้ $N_p = |X| \equiv |X_G| = 1 \pmod p$ ❐

3.4.6 ทฤษฎีบท ถ้า P เป็นซีโลว์ $p-$กรุปย่อยของกรุปจำกัด G แล้ว $N_G(N_G(P)) = N_G(P)$

บทพิสูจน์ การพิสูจน์ทฤษฎีบทที่สามของซิโลว์แสดงว่า ทุกๆ คู่สังยุคของ P เป็นซีโลว์ $p-$กรุปย่อยของ G และของทุกๆ กรุปย่อยของ G ที่มีคู่สังยุคของ P เป็นกรุปย่อย และเพราะ P เป็นกรุปย่อยปรกติของ $T = N_G(P)$ ดังนั้น P เป็นซีโลว์ $p-$กรุปย่อยเพียงหนึ่งเดียวของ T ทำให้ได้

$$x \in N_G(T) \Rightarrow \quad xTx^{-1} = T \quad \Rightarrow \quad xPx^{-1} \text{ เป็นกรุปย่อยของ } T$$

$$\Rightarrow \quad xPx^{-1} = P \quad \Rightarrow \quad x \in T$$

ดังนั้น $N_G(N_G(P)) \subseteq T$ แต่โดยทั่วไป $T \subseteq N_G(N_G(P))$ จึงได้ $N_G(P) = T = N_G(N_G(P))$ ❐

ขอปิดท้ายหัวข้อนี้ด้วยตัวอย่างการประยุกต์ทฤษฎีบทของซีโลว์ในการแสดงว่ากรุปใดไม่เป็นกรุปเชิงเดียว

3.4.7 **ตัวอย่าง** ให้ G เป็นกรุปอันดับ $12 = 2^2 \cdot 3$ โดยทฤษฎีบทที่หนึ่งของซีโลว์ G ประกอบด้วยซีโลว์ $2-$กรุปย่อย อันดับ 4 และซีโลว์ $3-$กรุปย่อย อันดับ 3 แต่โดยทฤษฎีบทที่สามของซีโลว์จะได้

$N_2 \equiv 1 \pmod 2$ และ N_2 เป็นตัวหารของ 12 ซึ่งทำให้ได้ $N_2 \in \{1,3\}$

และ $N_3 \equiv 1 \pmod 3$ และ N_3 เป็นตัวหารของ 12 ซึ่งทำให้ได้ $N_3 \in \{1,4\}$

สมมติ $N_2 = 3$ และ $N_3 = 4$ ให้ H_1, H_2, H_3 และ H_4 เป็นซีโลว์ $3-$กรุปย่อยที่ต่างกันทั้งหมดและ K_1, K_2 และ K_3 เป็นซีโลว์ $2-$กรุปย่อยที่ต่างกันทั้งหมดของ G แล้ว $H_i \cap H_j = \{e\}$ ทุกๆ $1 \le i \ne j \le 4$ และ $K_i \cap K_j = \{e\}$ ทุกๆ $1 \le i \ne j \le 3$ โดยที่ $|K_i| = 4$ ทุกๆ $1 \le i \le 3$ จึงได้ว่าซีโลว์ $3-$กรุปย่อยทั้งสี่กรุปย่อยมีสมาชิกที่ต่างกันรวมทั้งสิ้น $(2)(4)+1 = 9$ ตัวและซีโลว์ $2-$กรุปย่อยทั้งสี่กรุปย่อย มีสมาชิกที่ต่างกันรวมทั้งสิ้น $(3)(3)+1 = 10$ ตัว ดังนั้น G ประกอบด้วยสมาชิกที่ต่างกันอย่างน้อย $8+9+1 = 18 > 12$ ซึ่งเป็นไปไม่ได้ แสดงว่า G ประกอบด้วยซีโลว์ $2-$กรุปย่อยจำนวน 1 กรุปย่อย หรือซีโลว์ $3-$กรุปย่อยจำนวน1 กรุปย่อย ซึ่งไม่ว่ากรณีใดกรุปย่อยซีโลว์นั้นจะเป็นกรุปย่อยปรกติของ G ที่ไม่ใช่ G และไม่ใช่ $\{e\}$ ทำให้ได้ว่า G ไม่เป็นกรุปเชิงเดียว ❍

3.4.8 **ตัวอย่าง** ให้ G เป็นกรุปอันดับ $18 = 2 \cdot 3^2$ โดยทฤษฎีบทที่หนึ่งของซีโลว์ G ประกอบด้วยซีโลว์ $2-$กรุปย่อยอันดับ 2 และซีโลว์ $3-$กรุปย่อยอันดับ 9 แต่โดยทฤษฎีบทที่สามของซีโลว์จะได้

$N_2 \equiv 1 \pmod 2$ และ N_2 เป็นตัวหารของ 18 ซึ่งทำให้ได้ $N_2 \in \{1,3,9\}$

และ $N_3 \equiv 1 \pmod 3$ และ N_3 เป็นตัวหารของ 18 ซึ่งทำให้ได้ $N_3 = 1$

ดังนั้นซีโลว์ $3-$กรุปย่อยซึ่งมีเพียงหนึ่งเดียวจะเป็นกรุปย่อยปรกติของ G ที่ไม่ใช่ G และไม่ใช่ $\{e\}$ ทำให้ได้ว่า G ไม่เป็นกรุปเชิงเดียว ❍

3.4.9 **ตัวอย่าง** ให้ G เป็นกรุปอันดับ $30 = 2 \cdot 3 \cdot 5$ โดยทฤษฎีบทที่หนึ่งของซีโลว์ G ประกอบด้วยซีโลว์ $2-$กรุปย่อยอันดับ 2 ซีโลว์ $3-$กรุปย่อยอันดับ 3 และซีโลว์ $5-$กรุปย่อยอันดับ 5 และโดยทฤษฎีบทที่สามของซีโลว์ จะได้

$N_2 \equiv 1 \pmod 2$ และ N_2 เป็นตัวหารของ 30 ซึ่งทำให้ได้ $N_2 \in \{1,3,5,15\}$

$N_3 \equiv 1 \pmod 3$ และ N_3 เป็นตัวหารของ 30 ซึ่งทำให้ได้ $N_3 \in \{1,10\}$

และ $N_5 \equiv 1 \pmod 5$ และ N_5 เป็นตัวหารของ 30 ซึ่งทำให้ได้ $N_5 \in \{1,6\}$

สมมติ $N_2 = 3$, $N_3 = 10$ และ $N_5 = 6$ แล้วแต่ละ $p \in \{2,3,5\}$ ส่วนร่วมของแต่ละคู่ของซีโลว์ $p-$กรุปย่อยที่ต่างกันคือ $\{e\}$ ทำให้ G ประกอบด้วยสมาชิกที่มีอันดับ 2 อย่างน้อย $(2-1)(3)$

$=3$ ตัว ที่มีอันดับ 3 อย่างน้อย $(3-1)(10)=20$ ตัวและที่มีอันดับ 5 อย่างน้อย $(5-1)(6)=24$ ตัว ทำให้ G ประกอบด้วยสมาชิกที่ต่างกันอย่างน้อย $3+20+24=47>30$ ซึ่งเป็นไปไม่ได้ ดังนั้น $N_2=1$ หรือ $N_3=1$ หรือ $N_5=1$ ซึ่งไม่ว่ากรณีใดกรุปย่อยซีโลว์นั้นจะเป็นกรุปย่อยปรกติของ G ที่ไม่ใช่ G และไม่ใช่ $\{e\}$ ทำให้ได้ว่า G ไม่เป็นกรุปเชิงเดียว ❍

แบบฝึกหัด 3.4

1. ให้ p เป็นจำนวนเฉพาะซึ่งเป็นตัวหารของอันดับของกรุปจำกัด G จงพิสูจน์ว่า
   1.1 ถ้า G เป็น $p-$กรุปอนันต์ แล้วมีกรุปย่อยอันดับ p^n ของ G ทุกๆจำนวนเต็มบวก n หรือมีจำนวนเต็มบวก m ซึ่งทุกๆ กรุปย่อยจำกัดของ G มีอันดับไม่เกิน p^m
   1.2 ถ้า G เป็นกรุปนอนอาบีเลียนอันดับ p^3 ซึ่ง $|Z(G)|=p$ แล้ว $G/Z(G)$ เป็นกรุปอาบีเลียน
   1.3 ถ้า $f:G\to G$ เป็นสาทิสสัณฐาน P เป็นกรุปย่อยปรกติและซีโลว์ $p-$กรุปย่อยของ G แล้ว $f(P)$ เป็นกรุปย่อยของ P
   1.4 ถ้า H เป็นกรุปย่อยปรกติของ G ซึ่ง $|H|=p^k$ เมื่อ k เป็นจำนวนเต็มที่ไม่ใช่จำนวนลบแล้ว H เป็นกรุปย่อยของทุกๆ ซีโลว์ $p-$กรุปย่อยของ G
   1.5 ถ้า H เป็นกรุปย่อยปรกติของ G และ P เป็นซีโลว์ $p-$กรุปย่อยของ H แล้ว $G=N_G(P)\cdot H$
2. ถ้า P เป็นซีโลว์ $p-$กรุปย่อยของ G และ U เป็นกรุปย่อยของ G ซึ่ง $N_G(P)\subseteq U\subseteq G$ แล้ว $N_G(U)=U$
3. จงหาซีโลว์ $2-$กรุปย่อย และซีโลว์ $3-$กรุปย่อย ของกรุป S_3, S_4, S_5 และ A_4
4. ให้ G เป็นกรุปจำกัด จงพิสูจน์ว่าถ้าทุกๆ ซีโลว์ $p-$กรุปย่อยของ G เป็นกรุปย่อยปรกติของ G ทุกๆ จำนวนเฉพาะ p ที่เป็นตัวหารของอันดับของ G แล้ว G เป็นผลคูณตรงของทุกๆ ซีโลว์ $p-$กรุปย่อยเหล่านั้น (เราเรียกกรุปเช่นนี้ว่า finite nilpotent group)
5. จงแสดงว่าทุกๆ กรุปอันดับ 255 เป็นกรุปวัฏจักร
6. ให้ G เป็นกรุปจำกัดซึ่ง $|G|=p^nq$ เมื่อ p และ q เป็นจำนวนเฉพาะต่างกันและ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่าถ้า $p>q$ แล้วมีกรุปย่อยปรกติ H ของ G เพียงหนึ่งเดียว ซึ่ง $[G:H]=q$
7. จงแสดงว่าทุกๆ กรุปอันดับ 20,28,36,48,56 และ 200 มีซิโลว์กรุปย่อยซึ่งเป็นกรุปย่อยปรกติ (เพราะฉะนั้นกรุปเหล่านี้จึงไม่เป็นกรุปเชิงเดียว)
8. จงแสดงว่า $\mathbb{Z}_2\oplus\mathbb{Z}_{84}$ และ $\mathbb{Z}_7\oplus\mathbb{Z}_7$ เป็นกรุปเชิงเดียวหรือไม่

9. จงแสดงว่าทุกๆ กรุปอันดับ 21 และ 35 เป็นกรุปเชิงเดียว

10. จงพิสูจน์ทฤษฎีบทของอาเบล (Abel's Theorem) ซึ่งกล่าวว่า A_n เป็นกรุปเชิงเดียวทุกๆ จำนวนเต็มบวก $n \neq 4$

11. ให้ p เป็นจำนวนเฉพาะและ n เป็นจำนวนเต็มบวกซึ่ง $p > n$ จงพิสูจน์ว่าถ้า G เป็นกรุปอันดับ pn แล้วทุกๆ กรุปย่อยของ G ที่มีอันดับ p เป็นกรุปย่อยปรกติ

12. ให้ G เป็นกรุปอันดับ $2p$ เมื่อ p เป็นจำนวนเฉพาะคี่ จงพิสูจน์ว่า G ประกอบด้วยกรุปย่อยอันดับ p เพียงหนึ่งกรุปย่อย หรือกรุปย่อยอันดับ 2 จำนวน p กรุปย่อย หรือกรุปย่อยอันดับ 2 เพียงหนึ่งกรุปย่อย และถ้าข้อความสุดท้ายเกิดขึ้นแล้ว G เป็นกรุปวัฏจักร

13. จงพิสูจน์ว่าทุกๆ อัตสัณฐานของ S_4 เป็นอัตสัณฐานภายในและ $S_4 \cong Aut(S_4)$
[ข้อแนะนำ: ประยุกต์แบบฝึกหัด 3.3 ข้อ 9 และพิสูจน์ว่าทุกๆ อัตสัณฐานของ S_4 ชักนำวิธีเรียงสับเปลี่ยนบนเซต $\{P_1, P_2, P_3, P_4\}$ ของกรุปย่อย $3-$ซีโลว์ของ S_4 และถ้า f เป็นอัตสัณฐานของ S_4 ซึ่ง $f(P_i) = P_i$ สำหรับทุกๆ $1 \leq i \leq 4$ แล้ว $f = id_{S_4}$]

3.5 การจำแนกกรุปจำกัด

ในหัวข้อนี้ เราแสดงการประยุกต์ทฤษฎีบทของซีโลว์ เพื่อจำแนกกรุปจำกัดอันดับ pq เมื่อ p และ q เป็นจำนวนเฉพาะที่ต่างกันและจำแนกกรุปอันดับไม่เกิน 15

3.5.1 ทฤษฎีบท ให้ p และ q เป็นจำนวนเฉพาะซึ่ง $p > q$

1. ถ้า q ไม่เป็นตัวหารของ $p-1$ แล้วทุกๆ กรุปอันดับ pq สมสัณฐานกับกรุป $\mathbb{Z}_{pq}$

2. ถ้า q เป็นตัวหารของ $p-1$ แล้วมีกรุปอันดับ pq เพียง 2 กรุปที่ต่างกัน (เมื่อไม่นับการเป็นสมสัณฐาน) คือกรุปวัฏจักร $\mathbb{Z}_{pq}$ และกรุปนอนอาบีเลียนซึ่งก่อกำเนิดโดย c และ d ซึ่ง $|c| = p$ และ $|d| = q$ และมีจำนวนเต็ม s ที่ทำให้ $dc = c^s d$ โดยที่ s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่ $s^q \equiv 1 \pmod{p}$

บทพิสูจน์ ให้ G เป็นกรุปอันดับ pq โดยที่ p และ q เป็นจำนวนเฉพาะซึ่ง $p > q$ โดยทฤษฎีบทของโคชี จะมี $c, d \in G$ ซึ่ง $|c| = p$ และ $|d| = q$ และโดยทฤษฎีบทของซิโลว์ จะได้ N_p และ N_q เป็นจำนวนในรูปแบบ $1+kp$ และ $1+mq$ สำหรับบางจำนวนเต็มไม่เป็นลบ k และ m ที่ทำให้ N_p และ N_q เป็นตัวหารของ pq แต่ถ้า $k \geq 1$ แล้ว $1+kp > p > q$ ทำให้ $1+kp$ ไม่เป็นตัวหาร

ของ p และของ q ทำให้ $1+kp$ ไม่เป็นตัวหารของ pq ดังนั้น $N_p=1$ และเช่นเดียวกันถ้า $m\geq 1$ แล้ว $1+mq>q$ ดังนั้น $1+mq$ เป็นตัวหารของ pq ทำให้ได้ว่า $1+mq=p$ จึงสรุปได้ว่า $N_q=1$ หรือ $N_q=p$ และจาก $S=<c>$ เป็นซีโลว์ $p-$ กรุปย่อยเพียงหนึ่งเดียวของ G จะได้ S เป็นกรุปย่อยปรกติโดยที่ $[G:S]=|G/S|=\frac{|G|}{|S|}=q$ แต่ $d\notin S$ และ $|dS|=q$ ดังนั้น $G/S=<dS>$ เป็นกรุปวัฏจักรอันดับ q นอกจากนี้เพราะ G/S เป็นผลแบ่งกั้นของ G จึงได้ $G=\bigcup_{x\in<d>} xS$ ดังนั้น ถ้า $g\in G$ จะมี $0\leq i<q$ และ $0\leq j<p$ ซึ่ง $x=d^i\in<d>$ และ $s=c^j\in S$ และ $g=xs=d^ic^j$ แสดงว่าทุกๆ สมาชิกของ G เขียนได้ในรูป d^ic^j สำหรับ $0\leq i<q$ และ $0\leq j<p$ นั่นคือ G ก่อ กำเนิดโดย c และ d

1. ถ้า q ไม่เป็นตัวหารของ $p-1$ แล้วไม่มีจำนวนเต็มบวก m ซึ่ง $p=1+mq$ ทำให้กรณีนี้ $N_q=1$ จะได้ว่า $T=<d>$ เป็นซีโลว์ $p-$ กรุปย่อยเพียงหนึ่งเดียวของ G จึงเป็นกรุปย่อยปรกติ ดังนั้น G สมสัณฐานกับผลคูณตรง $S\times T$ โดยแบบฝึกหัด 3.4 ข้อ 6 และโดยทฤษฎีบท 2.1.4 ข้อ 1 จะได้ $S\times T\cong\mathbb{Z}_{pq}$

2. ถ้า q เป็นตัวหารของ $p-1$ แล้ว $N_q=p$ และเพราะ $S=<c>$ เป็นกรุปย่อยปรกติของ G และ $d\in G$ ดังนั้น $dcd^{-1}\in S$ ทำให้มีจำนวนเต็ม $0\leq s<p$ ซึ่ง $dcd^{-1}=c^s$ นั่นคือ $dc=c^sd$

ถ้า $s\equiv 1 \pmod p$ จะมีจำนวนเต็มบวก k ซึ่ง $s=1+kp$ ทำให้ได้ $dcd^{-1}=c^s=c^{1+kp}=c(c^p)^k=ce=c$ และได้ $dc=cd$ ดังนั้น G เป็นกรุปอาบีเลียน และได้ $T=<d>$ เป็นกรุปย่อยปรกติ จึงได้ $N_q=1$ ซึ่งขัดแย้งกับ q เป็นตัวหารของ $p-1$ เพราะฉะนั้น s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่จาก $dcd^{-1}=c^s$ โดยการพิสูจน์แบบอุปนัยเชิงคณิตศาสตร์ จะได้ว่า $d^jcd^{-j}=c^{s^j}$ ทุกๆ จำนวนเต็มบวก j โดยเฉพาะ $j=q$ จะได้ $c=d^qcd^{-q}=c^{s^q}$ ซึ่งทำให้ได้ $s^q\equiv 1 \pmod p$

เพราะฉะนั้นถ้า G เป็นกรุปอันดับ pq โดยที่จำนวนเฉพาะ $p>q$ และ q เป็นตัวหารของ $p-1$ แล้ว G เป็นกรุปนอนอาบีเลียนซึ่งก่อกำเนิดโดย c และ d ซึ่ง $|c|=p$ และ $|d|=q$ และมีจำนวนเต็ม s ที่ทำให้ $dc=c^sd$ โดยที่ s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่ $s^q\equiv 1 \pmod p$

เพื่อให้การพิสูจน์สมบูรณ์ ต้องแสดงว่ามีกรุปนอนอาบีเลียนที่ก่อกำเนิดโดย c และ d ซึ่ง $|c|=p$, $|d|=q$ และมีจำนวนเต็ม s ซึ่ง $dc=c^sd$ โดยที่ s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่ $s^q\equiv 1 \pmod p$ และกรุปที่มีนี้จะสมสัณฐานกับ G ซึ่งขอละการพิสูจน์ดังกล่าวไว้เป็นแบบฝึกหัด ❐

3.5.2 **บทแทรก** ถ้า p เป็นจำนวนเฉพาะคี่ แล้วทุกๆ กรุปอันดับ $2p$ สมสัณฐานกับกรุปวัฏจักร $\mathbb{Z}_{2p}$ หรือกรุปไดฮิดรัล D_p

บทพิสูจน์ ประยุกต์ทฤษฎีบท 3.5.1 ด้วย $q=2$ แล้ว $p>q$ และ q เป็นตัวหารของ $p-1$ จึงสอดคล้องเงื่อนไขข้อ 2 ของทฤษฎีบท 3.5.1 ดังนั้นถ้า G เป็นกรุปอันดับ $2p$ ซึ่งไม่สมสัณฐานกับกรุปวัฏจักร $\mathbb{Z}_{2p}$ แล้ว G เป็นกรุปนอนอาบีเลียนที่ก่อกำเนิดโดย c และ d ซึ่ง $|c|=p,\ |d|=2$ และมีจำนวนเต็ม s ซึ่ง $dc=c^s d$ โดยที่ s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่ $s^2\equiv 1 \pmod p$ นั่นคือ p เป็นตัวหารของ $s^2-1=(s-1)(s+1)$ แต่ p ไม่เป็นตัวหารของ $s-1$ ดังนั้น p เป็นตัวหารของ $s+1$ ซึ่งสมมูลกับ $s\equiv -1 \pmod p$ ทำให้ได้ $c^s=c^{-1}$ เพราะฉะนั้น $dc=c^{-1}d$ ดังนั้น $G=<c,d\,|\,c^p=e=d^2, dc=c^{-1}d>\cong D_p$ ❐

3.5.3 **ทฤษฎีบท** มีกรุปนอนอาบีเลียนอันดับ 8 เพียงสองกรุปที่ต่างกัน (ไม่นับการเป็นสมสัณฐาน)คือกรุป $Q_8=<a,b\,|\,a^4=e, a^2=b^2, ba=a^3b>$ ซึ่งเรียกว่า *กรุปควอเทอร์เนียน (quaternion group)* และกรุปไดฮิดรัล D_4

บทพิสูจน์ ขอละการพิสูจน์ว่า Q_8 และ D_4 ไม่สมสัณฐานกันไว้เป็นแบบฝึกหัด

ให้ G เป็นกรุปนอนอาบีเลียนอันดับ 8 แล้วไม่มีสมาชิกใน G ที่มีอันดับ 8 (ถ้ามี $a\in G$ ซึ่ง $|a|=8$ แล้ว $G=<a>$ เป็นกรุปวัฏจักร) แต่มีสมาชิกใน G ซึ่งมีอันดับไม่เท่ากับ 2 (เพราะถ้า $a^2=e$ ทุกๆ $a\in G$ แล้ว G เป็นกรุปอาบีเลียน) และถ้า $a\in G$ แล้ว $|a|\in\{1,2,4,8\}$ ดังนั้นมี $a\in G$ ซึ่ง $|a|=4$ ทำให้ $S=<a>$ เป็นกรุปย่อยของ G ซึ่ง $[G:S]=2$ นั่นคือ S เป็นกรุปย่อยปรกติ

เลือก $b\notin S$ (เพราะว่า $G\neq S$) แล้วเพราะ $|G/S|=2$ ดังนั้น $b^2\in S=\{e,a,a^2,a^3\}$ ถ้า $b^2\in\{a,a^3\}$ แล้ว $b^8=(b^2)^4=a^4=e$ หรือ $b^8=(b^2)^4=(a^3)^4=(a^4)^3=e$ ซึ่งไม่ว่ากรณีใด b เป็นสมาชิกของ G ที่มีอันดับ 8 จะขัดแย้งกับเงื่อนไขในย่อหน้าแรก ดังนั้น $b^2=e$ หรือ $b^2=a^2$

เพราะ S เป็นกรุปย่อยปรกติของ G ดังนั้น $bab^{-1}\in S$ และโดยการวิเคราะห์ในลักษณะเดียวกับย่อหน้าก่อน จะได้ $bab^{-1}=a^3=a^{-1}$ ทำให้แสดงต่อได้ว่าแต่ละสมาชิกของ G เขียนได้ในรูป $b^i a^j$ ดังนั้น G ก่อกำเนิดโดย a และ b

ถ้า $b^2=e$ แล้ว $G=<a,b\,|\,a^4=e=b^2, ba=a^{-1}b>\cong D_4$

ถ้า $b^2=a^2$ แล้ว $G=<a,b\,|\,a^4=e, a^2=b^2, ba=a^3b>\cong Q_8$ ❐

3.5.4 **ทฤษฎีบท** มีกรุปนอนอาบีเลียนอันดับ 12 เพียง 3 กรุปที่ต่างกัน (ไม่นับการเป็นสมสัณฐาน) คือกรุปไดฮิดรัล D_6 กรุปสลับ A_4 และกรุป $T=<a,b\,|\,a^6=e, b^2=a^3, ba=a^{-1}b>$

บทพิสูจน์ แบบฝึกหัด 3.5 แสดงว่ามีกรุปนอนอาบีเลียน T นอกจากนี้ D_6, A_4 และ T ไม่มีกรุปคู่ใดสมสัณฐานกัน

ให้ G เป็นกรุปอันดับ $12=2^2\cdot 3$ และให้ P เป็นซีโลว์ $3-$ กรุปย่อยของ G แล้ว $|P|=3$ และ $[G:P]=4$ โดยทฤษฎีบท 3.3.8 ข้อ 2 มีสาทิสสัณฐาน $f:G\to S_4$ ซึ่ง $K=\ker f\subseteq P$

ดังนั้น $K=\{e\}$ หรือ $K=P$ ถ้า $K=\{e\}$ แล้ว f เป็นฟังก์ชันหนึ่งต่อหนึ่งซึ่งแสดงว่า G สมสัณฐานกับกรุปย่อยอันดับ 12 ของ S_4 ซึ่งคือกรุปสลับ A_4

ถ้า $K=P$ แล้ว P เป็นกรุปย่อยปรกติของ G จะได้ว่า P เป็นซีโลว์ 3 – กรุปย่อยเพียงหนึ่งเดียวของ G จึงมีสมาชิกอันดับ 3 ของ G เพียง 2 ตัว ให้ $c\in G$ ซึ่ง $|c|=3$ เพราะ $[G:C_G(c)]$ คือจำนวนคู่สังยุคของ c และอันดับของคู่สังยุคของ c เท่ากับ 3 ดังนั้น $[G:C_G(c)]=1$ หรือ $[G:C_G(c)]=2$ ทำให้ได้ $C_G(c)=G$ หรือ $C_G(c)$ เป็นกรุปย่อยอันดับ 6 ของ G แต่ไม่ว่ากรณีใด (โดยทฤษฎีบทของโคชี) จะมี $d\in C_G(c)$ ซึ่ง $|d|=2$ ทำให้ได้ $|cd|=6$

ให้ $a=cd$ แล้ว $<a>$ เป็นกรุปย่อยปรกติของ G เพราะว่า $[G:<a>]=2$ และดังนั้นมี $e\neq b\in G\backslash <a>$ ซึ่ง $b^2\in <a>$ และ $bab^{-1}\in <a>$ แต่ G เป็นกรุปนอนอาบีเลียนและ $|a|=6$ ทำให้แสดงได้ไม่ยากว่า $bab^{-1}=a^5=a^{-1}$ ซึ่งสมมูลกับ $ba=a^{-1}b$

ถ้า ($b^2=a^2$ หรือ $b^2=a^4$) จะนำไปสู่ข้อขัดแย้ง และถ้า ($b^2=a$ หรือ $b^2=a^5$) ทำให้ได้ G เป็นกรุปอาบีเลียน ดังนั้นจาก $b^2\in <a>$ จะได้ $b^2=e$ หรือ $b^2=a^3$ จะได้กรณีที่เป็นไปได้ทั้งหมดคือ $|a|=6$, $b^2=e$ และ $ba=a^{-1}b$ นั่นคือ $G=<a,b|a^6=e=b^2, ba=a^{-1}b>\cong D_6$ หรือ $|a|=6$, $b^2=a^3$ และ $ba=a^{-1}b$ นั่นคือ $G=<a,b|a^6=e, b^2=a^3, ba=a^{-1}b>\cong T$ ❐

ตารางแสดงการจำแนกกรุปอันดับ 1–15

อันดับของกรุป	กรุปที่แตกต่างกัน
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2\oplus\mathbb{Z}_2$ หรือ $\mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$ หรือ $D_3\,(\cong S_3)$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$, $\mathbb{Z}_2\oplus\mathbb{Z}_4$, $\mathbb{Z}_8$, D_4, Q_8
9	$\mathbb{Z}_3\oplus\mathbb{Z}_3$ หรือ $\mathbb{Z}_9$
10	$\mathbb{Z}_{10}$ หรือ D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2\oplus\mathbb{Z}_6$, $\mathbb{Z}_{12}$, A_4, D_6, T
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$ หรือ D_7
15	$\mathbb{Z}_{15}$

แบบฝึกหัด 3.5

1. ให้ p และ q เป็นจำนวนเฉพาะซึ่ง $p > q$ และ q เป็นตัวหารของ $p-1$ จงพิสูจน์ว่า
   1.1 ถ้า s ไม่เป็นสมภาคกับ 1 มอดูโล p และ k เป็นจำนวนเต็มบวกน้อยสุดซึ่ง $s^q \equiv 1 \pmod{p}$ แล้ว k เป็นตัวหารของ q (ทำให้ได้ $k = q$)
   1.2 สมการสมภาค $x^q \equiv 1 \pmod{p}$ มีคำตอบต่างกัน q คำตอบคือ $1, s, s^2, \ldots, s^{q-1}$
2. ให้ $C_p = <a>$ และ $C_q = <b>$ เป็นกรุปวัฏจักร (ภายใต้การคูณ) อันดับเป็นจำนวนเฉพาะ p และ q ตามลำดับโดยที่ $p > q$ และ q เป็นตัวหารของ $p-1$ แล้วความรู้ในทฤษฎีจำนวนซึ่งกล่าวว่ามีจำนวนเต็ม s ซึ่ง s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่ $s^q \equiv 1 \pmod{p}$ จะทำให้ s ไม่เป็นสมภาคกับ 0 มอดูโล p จงพิสูจน์ว่า
   2.1 $\alpha : C_p \to C_p$ นิยามโดย $a^i \to a^{si}$ เป็นอัตสัณฐาน
   2.2 $\theta : C_q \to Aut(C_p)$ นิยามโดย $\theta(b^i) = \alpha^i$ (เมื่อ α เป็นดังใน 2.1 และ $\alpha^0 = id_{C_p}$) เป็นสาทิสสัณฐาน
3. ให้ p และ q เป็นจำนวนเฉพาะซึ่ง $p > q$ และ q เป็นตัวหารของ $p-1$ จงพิสูจน์ว่ามีกรุปนอนอาบีเลียนซึ่งก่อกำเนิดโดย c และ d ซึ่ง $|c| = p$ และ $|d| = q$ และมีจำนวนเต็ม s ซึ่ง $dc = c^s d$ โดยที่ s ไม่เป็นสมภาคกับ 1 มอดูโล p แต่ $s^q \equiv 1 \pmod{p}$
4. จงหา $Z(Q_8)$ พร้อมทั้งแสดงว่า $Q_8/Z(Q_8)$ เป็นกรุปไคลน์ -4
5. จงแสดงว่ามีกรุปย่อยนอนอาบีเลียน T ของ $S_3 \times \mathbb{Z}_4$ ซึ่ง $|T| = 12$ และก่อกำเนิดโดย a และ b ที่สอดคล้องกับ $|a| = 6$, $b^2 = a^3$ และ $ba = a^{-1}b$ นอกจากนี้สำหรับกรุปอันดับ 12 ซึ่งก่อกำเนิดโดย a และ b และสอดคล้องกับ $|a| = 6$, $b^2 = a^3$ และ $ba = a^{-1}b$ จะสมสัณฐานกับกรุป T
6. จงแสดงว่าไม่มีกรุปคู่ใดๆ ใน $\{D_6, A_4, T\}$ สมสัณฐานกัน เมื่อ T คือกรุปในข้อ 5
7. จงพิสูจน์ว่าถ้า G เป็นกรุปนอนอาบีเลียนอันดับ p^3 เมื่อ p เป็นจำนวนเฉพาะแล้ว $Z(G)$ เป็นกรุปย่อยซึ่งก่อกำเนิดโดยเซต $\{aba^{-1}b^{-1} | a, b \in G\}$
8. ให้ p เป็นจำนวนเฉพาะคี่ จงพิสูจน์ว่ามีกรุปนอนอาบีเลียนอันดับ p^3 อย่างมากเพียงสองกรุปเท่านั้นคือกรุปที่เป็นสมสัณฐานกับกรุปสองกรุปต่อไปนี้

   $$<a, b \| a| = p^2, |b| = p, b^{-1}ab = a^{1+p}>$$

   หรือ $$<a, b, c \| a| = |b| = |c| = p, c = a^{-1}b^{-1}ab, ca = ac, cb = bc>$$
9. จงจำแนกกรุปทั้งหมด (ไม่นับการเป็นสมสัณฐาน) ที่มีอันดับ 18, 20 และ 30
10. จงแสดงว่า D_4 ไม่เป็นสมสัณฐานกับ Q_8 [ข้อแนะนำ : นับจำนวนสมาชิกอันดับ 2]

บทที่ 4
สาระของทฤษฎีริง

ในบทที่ 1 เราได้แนะนำระบบคณิตศาสตร์ที่เรียกว่า "กรุป" ซึ่งประกอบด้วยเซตที่ไม่เป็นเซตว่างเซตหนึ่งกับการดำเนินการทวิภาคหนึ่งตัวที่นิยามบนเซตนั้นและสอดคล้องสมบัติของกรุป สังเกตว่าบทนิยามของกรุปเป็นแนวคิดเชิงนามธรรมซึ่งขยายโครงสร้างของระบบจำนวนเต็มกับการบวก อย่างไรก็ตามในระบบจำนวนเต็มยังประกอบด้วยโครงสร้างที่เกี่ยวกับการคูณอีกด้วย จึงได้มีการศึกษาระบบคณิตศาสตร์ซึ่งขยายโครงสร้างของระบบจำนวนเต็มอย่างเต็มรูปแบบและเรียกระบบนี้ว่า "ริง" แต่เพราะเรื่องราวของทฤษฎีริงเบื้องต้นได้มีการศึกษารายละเอียดกันมาบ้างแล้วในวิชาพีชคณิตนามธรรม ระดับปริญญาตรี ในบทนี้เราจึงจะศึกษาเนื้อหาดังกล่าวในลักษณะทบทวนและลงรายละเอียดเพื่อเป็นพื้นฐานของการศึกษาเรื่องริงขั้นกลางและขั้นสูงในบทต่อๆ ไป

4.1 บทนิยามและสมบัติเบื้องต้น

ให้ R เป็นเซต $*$ และ $\circ$ เป็นการดำเนินการทวิภาค 2 ตัวบน R เรียกโครงสร้าง $(R;*,\circ)$ ว่า *ริง (ring)* ถ้าเงื่อนไขต่อไปนี้เป็นจริง

1. โครงสร้าง $(R;*)$ เป็นกรุปอาบีเลียน
2. $\circ$ สอดคล้องกฎการเปลี่ยนหมู่
3. $\circ$ สอดคล้องกฎการกระจายเหนือ $*$ นั่นคือ $a\circ(b*c)=(a\circ b)*(a\circ c)$ และ $(b*c)\circ a=(b\circ a)*(c\circ a)$ สำหรับทุกๆ $a,b,c\in R$

โดยทั่วไป นิยมแทนการดำเนินการ $*$ และ $\circ$ ของริงด้วย $+$ และ $\cdot$ และเรียกว่า "การบวก" และ "การคูณ" ตามลำดับ โดยเฉพาะ "การคูณ $\cdot$" จะเขียนแทน $a\cdot b$ โดยละสัญลักษณ์การคูณไว้เป็น ab และเรียกว่า "ผลคูณของ a และ b" ทั้งนี้เพื่อให้สอดคล้องกับระบบของจำนวนเต็มที่เราคุ้นเคยกันเป็นอย่างดี และในกรณีที่จะไม่ทำให้เกิดการสับสน อาจกล่าวถึง "ริง R" โดยละการดำเนินการไว้

เนื่องจาก $(R;+)$ เป็นกรุปการบวก ดังนั้นการกล่าวถึง R เมื่อหมายความถึงกรุป R เราจึงใช้สัญลักษณ์ที่เกี่ยวกับ เอกลักษณ์ ตัวผกผันและสมาชิกในรูปยกกำลังของกรุปด้วยสัญลักษณ์ของกรุปการบวกเป็น $0,-a$ และ na (a บวกกัน n ครั้ง) ตามลำดับ สำหรับเอกลักษณ์ 0 ของกรุปการบวกซึ่งมีเพียงตัวเดียวใน R จะเรียกว่า "*ศูนย์ (zero)* ของริง R" หรือเรียกสั้นๆ ว่า "ศูนย์" และเรียกตัวผกผันการบวก $-a$ ของ $a\in R$ ว่า "*สมาชิกลบ (negative)* ของ a"

ด้วยข้อตกลงดังกล่าว จะกล่าวว่าโครงสร้าง $(R;+,\cdot)$ เป็นริงก็ต่อเมื่อเงื่อนไขต่อไปนี้เป็นจริง

1. $a+b=b+a$ สำหรับทุกๆ $a,b\in R$
2. $a+(b+c)=(a+b)+c$ สำหรับทุกๆ $a,b,c\in R$
3. มี $0\in R$ เพียงหนึ่งเดียวซึ่ง $a+0=a$ สำหรับทุกๆ $a\in R$
4. สำหรับแต่ละ $a\in R$ มี $-a\in R$ เพียงหนึ่งเดียวซึ่ง $a+(-a)=0$
5. $a(bc)=(ab)c$ สำหรับทุกๆ $a,b,c\in R$
6. $a(b+c)=ab+ac$ และ $(b+c)a=ba+ca$ สำหรับทุกๆ $a,b,c\in R$

โดยสมบัติข้อ 4 ของริง เราสามารถนิยามการดำเนินการผกผันของการบวกซึ่งเรียกว่า "การลบ" โดย $a-b=a+(-b)$ ทุกๆ $a,b\in R$ แล้วเห็นชัดว่า $a(b-c)=0=ab-ac$ และ $(a-b)c=ac-bc$ ทุกๆ $a,b,c\in R$

ถ้าริง R สอดคล้องกฎการสลับที่เพิ่มเติมดังนี้ "$ab=ba$ *ทุกๆ* $a,b\in R$" จะเรียก R ว่า *ริงสลับที่ (commutative ring)* และถ้ามี $1\in R$ ซึ่งสอดคล้องสมบัติดังนี้ "$a1=a=1a$ ทุกๆ $a\in R$" จะเรียก R ว่า *ริงมีเอกลักษณ์ (ring with identity)*

ในทำนองเดียวกับกรณีของกรุป ถ้าขนาดของ R เป็นจำนวนจำกัด จะเรียก R ว่า *ริงจำกัด (finite ring)* แต่ถ้า R ไม่ใช่ริงจำกัด จะเรียก R ว่า *ริงอนันต์ (infinite ring)*

ทฤษฎีบทต่อไป กล่าวถึงเลขคณิตในริง R โดยจะแสดงเพียงแนวคิดของการพิสูจน์เท่านั้น

4.1.1 **ทฤษฎีบท** ให้ R เป็นริง แล้ว

1. $0a=0=a0$ สำหรับทุกๆ $a\in R$
2. $(-a)b=a(-b)=-(ab)$ สำหรับทุกๆ $a,b\in R$
3. $(-a)(-b)=ab$ สำหรับทุกๆ $a,b\in R$
4. $(na)b=a(nb)=n(ab)$ สำหรับทุกๆ $a,b\in R$ และทุกๆ $n\in\mathbb{Z}$
5. $\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$ สำหรับทุกๆ $a_i,b_j\in R$ และทุกๆ $m,n\in\mathbb{Z}^+$

บทพิสูจน์ 1. ให้ $a\in R$ แล้ว $0+0a=0a=(0+0)a=0a+0a$ และโดยกฎการตัดออกในกรุปการบวก R จะได้ $0a=0$ และโดยการพิสูจน์ในทำนองคู่กันจะได้ $0=a0$

2. ให้ $a,b\in R$ แล้ว $ab+(-a)b=[a+(-a)]b=0b=0$ จะได้ $(-a)b$ เป็นตัวผกผันการบวกของ ab ในกรุป R ซึ่งมีเพียงตัวเดียว ดังนั้น $(-a)b=-(ab)$ และโดยการพิสูจน์ในทำนองคู่กัน จะได้ $a(-b)=-(ab)$

3. ให้ $a,b \in R$ แล้วโดยการประยุกต์ข้อ 2 จะได้ $(-a)(-b) = -a(-b) = -(-ab) = ab$

เราสามารถพิสูจน์ข้อ 5 โดยอุปนัยเชิงคณิตศาสตร์ และข้อ 4 เป็นกรณีเฉพาะของข้อ 5 เมื่อ $a_i = a$ ทุก ๆ $1 \le i \le n$ และ $b_1 = b$ หรือเมื่อ $b_j = b$ ทุกๆ $1 \le j \le n$ และ $a_1 = a$ ❑

สังเกตว่าถ้า R เป็นริงมีเอกลักษณ์ที่ไม่ใช่ *ริงศูนย์ (zero ring)* นั่นคือ $R \ne \{0\}$ แล้ว $0 \ne 1$ เพราะมี $0 \ne a \in R$ ดังนั้นถ้า $0 = 1$ แล้ว $a = a1 = a0 = 0$ จะเกิดข้อขัดแย้งกันเอง

ก่อนให้ตัวอย่างของริง ขอแนะนำสมาชิกในริงที่เป็นประโยชน์ในการศึกษาสมบัติของริงต่อไป ดังนี้

4.1.2 **บทนิยาม** ให้ R เป็นริงและ $0 \ne a \in R$ เราเรียก a ว่า *ตัวหารของศูนย์ทางซ้าย (left zero divisor)* [หรือ *ตัวหารของศูนย์ทางขวา (right zero divisor)*] ถ้ามี $0 \ne b \in R$ ซึ่ง $ab = 0$ [หรือ $ba = 0$] และเรียก $0 \ne a \in R$ ว่า *ตัวหารของศูนย์ (zero divisor)* ถ้า a เป็นทั้งตัวหารของศูนย์ทางซ้ายและตัวหารของศูนย์ทางขวา

สังเกตว่าถ้า R เป็นริงแล้วมี $0 \ne a \in R$ เป็นตัวหารของศูนย์ทางซ้าย ก็ต่อเมื่อ มี $0 \ne b \in R$ ซึ่ง $ab = 0$ นั่นคือก็ต่อเมื่อมี $0 \ne b \in R$ เป็นตัวหารของศูนย์ทางขวา

ให้ R เป็นริงที่ไม่มีตัวหารของศูนย์ (นั่นคือทุกๆ $a \in R$ ถ้า $a \ne 0$ แล้ว $ab = 0$ เฉพาะเมื่อ $b = 0$) แล้วสำหรับ $a,b,c \in R$ ซึ่ง $a \ne 0$ และ $ab = ac$ จะได้ $0 = a(b-c)$ ทำให้ได้ $0 = b - c$ ซึ่งสมมูลกับ $b = c$ นั่นคือ R สอดคล้องกฎการตัดออกภายใต้การคูณ ในทำนองกลับกันถ้า R เป็นริงที่สอดคล้องกฎการตัดออกภายใต้การคูณ แล้วสำหรับ $0 \ne a \in R$ จะได้ $ab = 0 = a0$ และได้ $b = 0$ ซึ่งแสดงว่า R ไม่มีตัวหารของศูนย์ จึงสรุปได้ทฤษฎีบทต่อไปนี้

4.1.3 **ทฤษฎีบท** R เป็นริงไม่มีตัวหารของศูนย์ ก็ต่อเมื่อ กฎการตัดออกภายใต้การคูณเป็นจริงใน R ❑

4.1.4 **บทนิยาม** ให้ R เป็นริงมีเอกลักษณ์ 1 จะกล่าวว่า $a \in R$ *ผกผันได้ทางซ้าย(left invertible)* [หรือ *ผกผันได้ทางขวา (right invertible)*] ถ้ามี $c \in R$ ซึ่ง $ca = 1$ [หรือ $ac = 1$] และเรียก c ว่า *ตัวผกผันทางซ้าย (left inverse)* [หรือ *ตัวผกผันทางขวา (right inverse)*] ของ a

เรากล่าวว่า a เป็น *สมาชิกผกผันได้ (invertible element)* หรือ *หน่วย (unit)* ถ้า a ผกผันได้ทางซ้ายและผกผันได้ทางขวา

4.1.5 **ข้อสังเกต** ให้ R เป็นริงมีเอกลักษณ์ 1

1. ถ้า $a \in R$ เป็นหน่วยแล้วตัวผกผันทางซ้ายและตัวผกผันทางขวาของ a เป็นตัวเดียวกัน เพราะถ้า $b,c \in R$ เป็นตัวผกผันทางซ้ายและทางขวาของ a ตามลำดับแล้ว $b = b1 = b(ac) = (ba)c = 1c = c$ และในกรณีเช่นนี้ จะเรียกตัวผกผันทางซ้ายซึ่งก็คือตัวผกผันทางขวาของ a ว่า *ตัวผกผัน (inverse)* ของ a และเขียนแทนด้วย a^{-1}

2. ถ้า U เป็นเซตของหน่วยทั้งหมดใน R แล้ว $1 \in U$ และ $(U;\cdot)$ เป็นกรุป

เห็นได้ชัดว่าระบบจำนวนเต็ม $\mathbb{Z}$ ระบบจำนวนตรรกยะ $\mathbb{Q}$ ระบบจำนวนจริง $\mathbb{R}$ และระบบจำนวนเชิงซ้อน $\mathbb{C}$ ภายใต้การบวกและการคูณแบบปกติเป็นริงสลับที่มีเอกลักษณ์

4.1.6 **ตัวอย่าง** แต่ละจำนวนเต็ม $n \geq 2$ เซตของเมทริกซ์ขนาด $n \times n$ ทั้งหมดเหนือ $\mathbb{Q}$ (หรือ $\mathbb{R}$ หรือ $\mathbb{C}$) ภายใต้การบวกและการคูณแบบปกติของเมทริกซ์เป็นริงมีเอกลักษณ์ที่ไม่ใช่ริงสลับที่ ❍

4.1.7 **ตัวอย่าง** สำหรับจำนวนเต็มบวก n เซต $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ ของจำนวนเต็มมอดูโล n ภายใต้การบวกและการคูณมอดูโล n เป็นริงสลับที่มีเอกลักษณ์ $\overline{1}$

ถ้า n เป็นจำนวนประกอบ นั่นคือมีจำนวนเต็ม $1 < k,r < n$ ซึ่ง $n = kr$ แล้ว $\overline{k} \neq \overline{0}$ และ $\overline{r} \neq \overline{0}$ แต่ $\overline{k}\overline{r} = \overline{kr} = \overline{n} = \overline{0}$ ซึ่งแสดงว่า $\overline{k}$ และ $\overline{r}$ ต่างเป็นตัวหารของศูนย์ใน $\mathbb{Z}_n$

ถ้า n เป็นจำนวนเฉพาะแล้ว n เป็นตัวหารของ kr สำหรับทุกๆ จำนวนเต็ม k และ r ซึ่ง $\overline{k}\overline{r} = \overline{0}$ ดังนั้น n เป็นตัวหารของ k หรือ n เป็นตัวหารของ r ซึ่งสมมูลกับ $\overline{k} = \overline{0}$ หรือ $\overline{r} = \overline{0}$ แสดงว่า $\mathbb{Z}_n$ ไม่มีตัวหารของศูนย์ ❍

4.1.8 **ตัวอย่าง** ให้ A เป็นกรุปอาบีเลียนและ $End\ A$ แทนเซตของสาทิสสัณฐานทั้งหมดบน A ถ้านิยามการบวก + บน $End\ A$ โดย $(f+g)(a) = f(a) + g(a)$ ทุกๆ $f,g \in End\ A$ และทุกๆ $a \in A$ แล้วเห็นชัดว่า $f+g \in End\ A$ ทุกๆ $f,g \in End\ A$ ยิ่งไปกว่านั้น $(End\ A;+)$ เป็นกรุปอาบีเลียนและถ้าให้ "ฟังก์ชันประกอบ" เป็นการคูณบน $End\ A$ แล้ว $End\ A$ เป็นริงมีเอกลักษณ์คือฟังก์ชันเอกลักษณ์ 1_A ❍

4.1.9 **ตัวอย่าง** ให้ $\Im(\mathbb{R})$ แทนเซตของฟังก์ชันค่าจริงทั้งหมดและนิยาม "การบวก" และ "การคูณ" บน $\Im(\mathbb{R})$ โดย $(f+g)(x) = f(x) + g(x)$ และ $(fg)(x) = f(x)g(x)$ ทุกๆ $x \in \mathbb{R}$ และ $f,g \in \Im(\mathbb{R})$ แล้วขอให้แสดงเป็นแบบฝึกหัดว่า $\Im(\mathbb{R})$ เป็นริง

ถ้านิยาม "การคูณ" บน $\Im(\mathbb{R})$ ด้วย "ฟังก์ชันประกอบ $\circ$" (ขอให้เปรียบเทียบกับตัวอย่าง 4.1.8) สังเกตว่าถ้า $f,g,h \in \Im(\mathbb{R})$ โดยที่ h ไม่ใช่สาทิสสัณฐานแล้ว $h \circ (f+g)(x) = h((f+g)(x)) = h(f(x) + g(x))$ ซึ่งอาจไม่ใช่ $h(f(x)) + h(g(x)) = (h \circ f)(x) + (h \circ g)(x)$

สำหรับบาง $x \in R$ ดังนั้น $\Im(\mathbb{R})$ ไม่เป็นริง ตัวอย่างเช่น $f,g,h \in \Im(\mathbb{R})$ ที่นิยามตามลำดับโดย $f(x)=1$ และ $g(x)=-1$ ทุกๆ $x \in R$ แต่ $h(x)=1$ ถ้า $x \neq 0$ และ $h(x)=0$ ถ้า $x=0$ จะได้ว่า $h \circ (f+g)(0) = h(f(0)+g(0)) = h(1-1) = h(0) = 0 \neq 2 = 1+1 = h(1)+h(-1) = h(f(0))+h(g(0)) = ((h \circ f)+(h \circ g))(0)$ ดังนั้น $\circ$ ไม่สอดคล้องกฎการกระจายเหนือ $+$ ❍

4.1.10 **ตัวอย่าง** ให้ R และ S เป็นริงและนิยามการดำเนินการ "การบวก" และ "การคูณ" บนผลคูณคาร์ทีเซียน $R \times S$ แบบตามองค์ประกอบแล้วการพิสูจน์ในบทที่ 1 แสดงว่า $R \times S$ เป็นกรุปอาบีเลียน และการคำนวณโดยตรง จะแสดงว่า "การคูณ" สอดคล้องกฎการเปลี่ยนหมู่และกฎการกระจายเหนือ "การบวก" ดังนั้น $R \times S$ เป็นริงซึ่งเรียกว่า *ริงผลคูณตรง (direct product)* นอกจากนี้ถ้า R และ S ต่างเป็นริงสลับที่ แล้วเห็นชัดว่า $R \times S$ เป็นริงสลับที่ และถ้า R และ S มีเอกลักษณ์ 1 และ $1'$ ตามลำดับแล้ว $(1,1')$ เป็นเอกลักษณ์ใน $R \times S$

อย่างไรก็ตามถ้า $|R|>1$ และ $|S|>1$ โดยที่ $0 \neq a \in R$ และ $0 \neq b \in S$ แล้วมี $(0,0) \neq (a,0) \in R \times S$ และ $(0,0) \neq (0,b) \in R \times S$ เป็นตัวหารของศูนย์ใน $R \times S$ แม้ R และ S จะไม่มีตัวหารของศูนย์ก็ตาม ❍

ให้ R เป็นริง เช่นเดียวกับข้อสังเกตในบทที่ 1 เราจะกำหนดสัญลักษณ์เกี่ยวกับการคูณสมาชิกตัวหนึ่งจำนวนจำกัดครั้งในรูป "ยกกำลัง" ใน R แบบอุปนัย นั่นคือถ้า $a \in R$ และ n เป็นจำนวนเต็มบวก จะแทนผลคูณ $aa\cdots a$ (n ครั้ง) ด้วยสัญลักษณ์ a^n และอ่านว่า "กำลัง n ของ a" หรือ "a ยกกำลัง n" เพราะฉะนั้น

$$a^1 = a,\ a^2 = aa,\ a^3 = (aa)a = aaa, \ldots,\ a^n = a^{n-1}a$$

และถ้า R เป็นริงมีเอกลักษณ์ จะนิยามให้ $a^0 = 1$ ดังนั้นสำหรับจำนวนเต็มบวก m และ n จะได้

$$a^m a^n = a^{m+n} \quad \text{และ} \quad (a^m)^n = a^{mn}$$

ทฤษฎีบทต่อไป มีประโยชน์สำหรับการคำนวณในริง แต่การกล่าวทฤษฎีบทนี้ ต้องขอทบทวนสัญลักษณ์ $\binom{n}{k}$ สำหรับจำนวนเต็ม k และ n ซึ่ง $0 \le k \le n$ ที่เรียกว่า *สัมประสิทธิ์ทวินาม (binomial coefficient)* ซึ่งแทนจำนวนเต็ม $\frac{n!}{k!(n-k)!}$ โดยที่ $0! = 1$ และ $k! = k(k-1)\cdots 2 \cdot 1$

4.1.11 **ทฤษฎีบททวินาม** (Binomial Theorem) ให้ R เป็นริงมีเอกลักษณ์ n และ s เป็นจำนวนเต็มบวกและ $a,b,a_1,\ldots,a_s \in R$

1. ถ้า $ab = ba$ แล้ว $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

2. $(a_1+\cdots+a_s)^n = \sum \frac{n!}{(i_1!)\cdots(i_s!)} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$ ถ้า $a_i a_j = a_j a_i$ ทุกๆ $1 \le i, j \le s$ โดยที่ $i_1+i_2+\cdots+i_s = n$

บทพิสูจน์ 1. โดยประยุกต์อุปนัยเชิงคณิตศาสตร์บน n กับเอกลักษณ์ $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$ ทุกๆ $0 \le k < n$

2. ด้วยการประยุกต์อุปนัยเชิงคณิตศาสตร์บน $s \ge 2$ โดยที่ข้อ 1 คือกรณี $s=2$ เพราะว่า $(a_1+a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k} = \sum_{k+j=n} \frac{n!}{k!\,j!} a_1^k a_2^j$ และถ้าทฤษฎีบทเป็นจริงที่ $s \ge 2$ แล้วโดยประยุกต์ข้อ 1 อีกครั้งจะได้

$$(a_1+\cdots+a_s+a_{s+1})^n = [(a_1+\cdots+a_s)+a_{s+1}]^n = \sum_{k=0}^{n} \binom{n}{k} (a_1+\cdots+a_s)^k a_{s+1}^{n-k}$$

$$= \sum_{k+j=n} \frac{n!}{k!\,j!} (a_1+\cdots+a_s)^k a_{s+1}^j$$

และประยุกต์สมมติฐานกับผลบวกสุดท้าย ❑

แบบฝึกหัด 4.1

1. ให้ R เป็นริง จงคำนวณ $(a+b)(c+d)$ เมื่อ $a,b,c,d \in R$ และจงพิสูจน์ว่า
   1.1 $(a+b)^2 = a^2+ab+ba+b^2$ ทุกๆ $a,b \in R$
   1.2 $(na)(mb) = (nm)(ab)$ ทุกๆ $a,b \in R$ และทุกๆ จำนวนเต็ม m และ n
2. จงพิสูจน์ว่าริง R เป็นริงสลับที่ ก็ต่อเมื่อ $a^2-b^2 = (a+b)(a-b)$ ทุกๆ $a,b \in R$
3. จงแสดงว่าแต่ละกรุปอาบีเลียน $(A;+)$ ที่มี 0 เป็นเอกลักษณ์ จะเป็นริงภายใต้ "การคูณ" ซึ่งนิยามโดย $ab=0$ ทุกๆ $a,b \in A$
4. ให้ R เป็นริงมีเอกลักษณ์ จงพิสูจน์ว่า
   4.1 เอกลักษณ์ของ R มีเพียงหนึ่งเดียว
   4.2 ถ้า $a \in R$ มีตัวผกผันแล้วตัวผกผันของ a มีเพียงหนึ่งเดียว
   4.3 ถ้า $a \in R$ เป็นตัวหารของศูนย์ แล้ว a ไม่มีตัวผกผัน
5. ให้ S แทนเซตของเซตย่อยทั้งหมดของเซต X นิยาม "การบวก" และ "การคูณ" บน S โดย $A+B = (A-B)\cup(B-A)$ และ $AB = A\cap B$ ทุกๆ $A,B \in S$ จงแสดงว่า S เป็นริง เป็นริงสลับที่และมีเอกลักษณ์
6. เราเรียกริง R ว่า *บูลีนริง (Boolean ring)* ถ้า R สอดคล้อง $a^2=a$ ทุกๆ $a \in R$ จงพิสูจน์ว่า ทุกๆ บูลีนริง R เป็นริงสลับที่และ $a+a=0$ ทุกๆ $a \in R$

7. ให้ $I \neq \phi$ และ $\{R_i \mid i \in I\}$ เป็นหมู่ของริงที่มีเอกลักษณ์และนิยาม "การบวก" และ "การคูณ" บนผลคูณคาร์ทีเซียน $\sum_{i \in I} R_i$ แบบตามองค์ประกอบ จงแสดงว่า $\sum_{i \in I} R_i$ เป็นริงซึ่งเรียกว่า *ริงผลบวกตรง (direct sum)* ของ $\{R_i \mid i \in I\}$ และจงแสดงว่า $\sum_{i \in I} R_i$ เป็นริงที่มีเอกลักษณ์หรือไม่

8. จงแสดงว่า $End\ (\mathbb{Z} \times \mathbb{Z})$ เป็นริงที่ไม่ใช่ริงสลับที่

9. ให้ R เป็นริงมีเอกลักษณ์ที่ไม่ใช่ริงศูนย์ จงพิสูจน์ว่า

   9.1 ถ้า $a \in R$ ซึ่ง $a^2 = 0$ แล้ว $a-1$ และ $a+1$ เป็นหน่วย

   9.2 ถ้า $a,b \in R$ ซึ่ง ab เป็นหน่วยแล้ว a และ b เป็นหน่วย

   9.3 ถ้า R เป็นริงสลับที่และ $a,b \in R$ ต่างเป็นหน่วยแล้วผลคูณ ab เป็นหน่วย

   9.4 ถ้า $a \in R$ ซึ่ง $a \neq \pm 1$ และ $a^2 = 1$ แล้ว $a-1$ และ $a+1$ เป็นตัวหารของศูนย์

   9.5 ถ้า $a,b \in R$ ซึ่ง ab เป็นตัวหารของศูนย์แล้ว a หรือ b เป็นตัวหารของศูนย์

   9.6 ถ้า R เป็นริงสลับที่และ $a,b \in R$ ซึ่ง a หรือ b เป็นตัวหารของศูนย์โดยที่ $ab \neq 0$ แล้ว ab เป็นตัวหารของศูนย์

   9.7 ถ้า R ไม่มีตัวหารของศูนย์แล้ว $ab = 1$ ก็ต่อเมื่อ $ba = 1$ ทุกๆ $a,b \in R$ และสำหรับ $a \in R$ ซึ่ง $a^2 = 1$ จะได้ $a = 1$ หรือ $a = -1$

10. ให้ k และ n เป็นจำนวนเต็มซึ่ง $0 \leq k \leq n$ จงแสดงว่า

    10.1 $\binom{n}{k} = \binom{n}{k-1}$ เป็นจำนวนเต็ม [ข้อแนะนำ : พิจารณา $\binom{m}{0} = \binom{m}{m} = 1$]

    10.2 ถ้า p เป็นจำนวนเฉพาะและ $1 \leq k \leq p^n - 1$ แล้ว p เป็นตัวหารของ $\binom{p^n}{k}$

    10.3 $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ ถ้า $k < n$

11. ให้ R เป็นริงมีเอกลักษณ์ที่ไม่ใช่ริงศูนย์และไม่มีตัวหารของศูนย์ จงพิสูจน์ว่าถ้า R สอดคล้องเงื่อนไข "ถ้า $0 \neq a \in R$ แล้วมี $b \in R$ เพียงหนึ่งเดียวซึ่ง $aba = a$" แล้ว $bab = b$ สำหรับทุกๆ $a,b \in R$ ซึ่ง $aba = a$

12. ให้ R เป็นริง จะกล่าวว่า $a \in R$ เป็น *นิรพล (nilpotent)* ถ้ามีจำนวนเต็ม n ซึ่ง $a^n = 0$ จงพิสูจน์ว่าในริงสลับที่ R ถ้า $a,b \in R$ เป็นนิรพลแล้ว $a+b$ เป็นนิรพล แต่ข้อความนี้ไม่เป็นจริงในริงที่ไม่ใช่ริงสลับที่ นอกจากนี้ข้อความต่อไปนี้สมมูลกันริง R ใดๆ

    (ก) R มี 0 เท่านั้นที่เป็นนิรพล (นั่นคือ R ไม่มีสมาชิกนิรพลที่ไม่ใช่ศูนย์)

    (ข) ถ้า $a \in R$ และ $a^2 = 0$ แล้ว $a = 0$

4.2 ริงชนิดสำคัญและค่าลักษณะเฉพาะของริง

ในหัวข้อ 4.1 เราได้แนะนำสมาชิกที่นอกเหนือจากศูนย์และเอกลักษณ์ของริงซึ่งมีประโยชน์ต่อการศึกษามโนคติเรื่องริง ในหัวข้อนี้ จะศึกษาการกำหนดชนิดของริงด้วยสมบัติของสมาชิกเหล่านี้

4.2.1 **บทนิยาม** ให้ R เป็นริงมีเอกลักษณ์ $1 \neq 0$ จะกล่าวว่า R เป็น *อินทิกรัลโดเมน (integral domain)* ถ้า R เป็นริงสลับที่ซึ่งไม่มีตัวหารของศูนย์ และกล่าวว่า R เป็น *ริงการหาร (division ring)* ถ้าทุกๆ สมาชิกใน $R \setminus \{0\}$ เป็นหน่วยของ R และเรียก R ว่า *ฟีลด์ (field)* ถ้า R เป็นริงสลับที่และเป็นริงการหาร

4.2.2 **ข้อสังเกต**

1. ทุกๆ อินทิกรัลโดเมนและทุกๆ ริงการหารประกอบด้วยสมาชิกอย่างน้อยสองตัวคือศูนย์ 0 และเอกลักษณ์ 1 ซึ่งจะไม่ใช่สมาชิกตัวเดียวกัน
2. ริง R มีเอกลักษณ์ 1 เป็นริงการหาร ก็ต่อเมื่อ $U = R \setminus \{0\}$ เป็นเซตของหน่วยใน R
3. ทุกๆ ฟีลด์ F เป็นอินทิกรัลโดเมน เพราะแต่ละ $a,b \in F$ ถ้า $ab = ac$ และ $a \neq 0$ แล้ว $a, a^{-1} \in U = F \setminus \{0\}$ จึงได้ $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = 1c = c$ ซึ่งแสดงว่ากฎการตัดออกภายใต้การคูณเป็นจริงใน F

4.2.3 **ตัวอย่าง** ริง $\mathbb{Z}$ เป็นอินทิกรัลโดเมนที่มีเพียง 1 และ -1 ที่ผกผันได้ $\mathbb{Z}$ จึงไม่เป็นฟีลด์ แต่ริง E ของจำนวนเต็มคู่ทั้งหมดเป็นริงสลับที่ซึ่งไม่มีเอกลักษณ์จึงไม่ใช่อินทิกรัลโดเมน ส่วนแต่ละริง $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ ต่างเป็นฟีลด์ ❍

4.2.4 **ตัวอย่าง** นิยาม "การบวก $\oplus$" และ "การคูณ $\odot$" บน $\mathbb{Q}$ ในรูปของการบวกและการคูณแบบปกติในริงของจำนวนตรรกยะ $\mathbb{Q}$ โดย $a \oplus b = a + b + 1$ และ $a \odot b = a \cdot b + a + b$ ทุกๆ $a,b \in \mathbb{Q}$ จะแสดงว่า $(\mathbb{Q}; \oplus, \odot)$ เป็นฟิลด์ ดังต่อไปนี้

1. $\oplus$ และ $\odot$ สอดคล้องกฎการเปลี่ยนหมู่และกฎการสลับที่ : ให้ $a,b,c \in \mathbb{Q}$ แล้ว

$$a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + (b + c + 1) + 1 = (a + b + 1) + c + 1$$
$$= (a + b + 1) \oplus c = (a \oplus b) \oplus c,$$
$$a \oplus b = a + b + 1 = b + a + 1 = b \oplus a,$$
$$a \odot (b \odot c) = a \odot (b \cdot c + b + c) = a \cdot (b \cdot c + b + c) + a + b \cdot c + b + c$$
$$= a \cdot b \cdot c + a \cdot b + a \cdot c + b \cdot c + a + b + c$$
$$= (a \cdot b + a + b) \cdot c + (a \cdot b + a + b) + c = (a \cdot b + a + b) \odot c = (a \odot b) \odot c$$

และ $$a \odot b = a \cdot b + a + b = b \cdot a + b + a = b \odot a$$

2. $\odot$ สอดคล้องกฎการกระจายเหนือ $\oplus$: ให้ $a,b,c \in \mathbb{Q}$ แล้ว

$$a\odot(b\oplus c)=a\odot(b+c+1)=a\cdot(b+c+1)+a+b+c+1$$
$$=a\cdot b+a\cdot c+a+a+b+c+1=(a\cdot b+a+b)+(a\cdot c+a+c)+1$$
$$=(a\odot b)+(a\odot c)+1 \qquad =(a\odot b)\oplus(a\odot c)$$

3. หาเอกลักษณ์สำหรับ $\oplus$ (นั่นคือศูนย์ของ $(\mathbb{Q};\oplus,\odot)$): ให้ $a,b\in\mathbb{Q}$ ซึ่ง $a\oplus b=b$ แล้ว $b=a+b+1$ ทำให้ได้ $a=-1$ ต่อไปให้ $x\in\mathbb{Q}$ แล้ว $x\oplus -1=x+(-1)+1=x$ ซึ่งแสดงว่า -1 เป็นเอกลักษณ์สำหรับ $\oplus$

4. หาตัวผกผันภายใต้ $\oplus$ สำหรับแต่ละ $a\in\mathbb{Q}$: ให้ $a,b\in\mathbb{Q}$ ซึ่ง $a\oplus b=-1$ แล้ว $-1=a+b+1$ ซึ่งสมมูลกับ $b=-2-a$ แต่เพราะ $a\oplus(-a-2)=a+(-a-2)+1=-1$ ดังนั้น $-2-a$ เป็นตัวผกผันของ a สำหรับ $\oplus$

จากข้อ 1, 3 และ 4 จะได้ว่า $(\mathbb{Q};\oplus)$ เป็นกรุปอาบีเลียน

5. หาเอกลักษณ์สำหรับ $\odot$: ให้ $a,b\in\mathbb{Q}$ ซึ่ง $a\odot b=b$ แล้ว $a\cdot b+a+b=b$ โดยเฉพาะเมื่อ $b=0$ จะได้ $a=0$ ต่อไปให้ $x\in\mathbb{Q}$ แล้ว $x\odot 0=x\cdot 0+x+0=x$ ซึ่งแสดงว่า 0 เป็นเอกลักษณ์สำหรับ $\odot$

เพราะฉะนั้น $(\mathbb{Q};\oplus,\odot)$ เป็นริงสลับที่ มี 0 เป็นเอกลักษณ์และ -1 เป็นศูนย์ของริง

6. จะแสดงว่า $(\mathbb{Q};\oplus,\odot)$ ไม่มีตัวหารของศูนย์: ให้ $a,b\in\mathbb{Q}$ ซึ่ง $a\odot b=-1$ แล้ว $-1=a\cdot b+a+b$ ซึ่งสมมูลกับ $0=a\cdot b+a+b+1=a\cdot(b+1)+(b+1)=(a+1)(b+1)$ และสมมูลกับ $a=-1$ หรือ $b=-1$

เพราะฉะนั้น $(\mathbb{Q};\oplus,\odot)$ เป็นอินทิกรัลโดเมน

7. หาตัวผกผันภายใต้ $\odot$ สำหรับแต่ละ $-1\neq a\in\mathbb{Q}$: ให้ $-1\neq a\in\mathbb{Q}$ และ $b\in\mathbb{Q}$ ซึ่ง $a\odot b=0$ แล้ว $0=a\cdot b+a+b$ ทำให้ได้ $b=-\frac{a}{a+1}$ และเพราะ

$$a\odot -\frac{a}{a+1}=a\cdot\left(-\frac{a}{a+1}\right)+a-\frac{a}{a+1}=\frac{-a^2+a\cdot(a+1)-a}{a+1}=\frac{-a^2+a^2+a-a}{a+1}=0$$

ดังนั้น $-\frac{a}{a+1}$ เป็นตัวผกผันของ a สำหรับ $\odot$

เพราะฉะนั้น $(\mathbb{Q};\oplus,\odot)$ เป็นฟิลด์ ❍

4.2.5 **ตัวอย่าง** ให้ K แทนผลคูณคาร์ทีเซียน $\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}$ ให้ $S=\{1,i,j,k\}$ และแทนแต่ละ $(a_0,a_1,a_2,a_3)\in K$ ในรูป $a_0 1+a_1 i+a_2 j+a_3 k$ แล้ว $a_0 1+a_1 i+a_2 j+a_3 k=b_0 1+b_1 i+b_2 j+b_3 k$ ก็ต่อเมื่อ $a_t=b_t$ ทุกๆ $a_t,b_t\in\mathbb{R}$ และทุกๆ $0\le t<4$ นอกจากนี้ $a_0 1\in K$ อาจแทนด้วย

$a_0 \in \mathbb{R}$ และจะละเทอมที่มีสัมประสิทธิ์เป็นศูนย์ (ตัวอย่างเช่น $4+2j = 4\cdot 1+0i+4j+0k$ และ $i = 0+1i+0j+0k$ เป็นต้น) แล้วให้การบวกนิยามตามองค์ประกอบดังนี้

$$\begin{aligned}&(a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k)\\&\qquad = (a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k\end{aligned}$$

จะได้ว่า K เป็นกรุปอาบีเลียนผลบวกตรงและนิยามการคูณบน K ดังนี้

$$\begin{aligned}&(a_0+a_1i+a_2j+a_3k)(b_0+b_1i+b_2j+b_3k)\\&\qquad = (a_0b_0-a_1b_1-a_2b_2-a_3b_3)+(a_0b_1+a_1b_0+a_2b_3-a_3b_2)i\\&\qquad\qquad +(a_0b_2+a_2b_0+a_3b_1-a_1b_3)j+(a_0b_3+a_3b_0+a_1b_2-a_2b_1)k\end{aligned}$$

ซึ่งผลคูณได้จากเลขคณิตของฟีลด์ $\mathbb{R}$ และกฎการคูณบน $S=\{1,i,j,k\}$ ซึ่งกำหนดโดย

(i) $ir = ri,\ rj = jr, rk = kr$ ทุกๆ $r \in \mathbb{R}$

และ (ii) $i^2 = j^2 = k^2 = ijk = -1;\ ij = -ji = k;\ jk = -kj = i;\ ki = -ik = j$

การพิสูจน์โดยการคำนวณด้วยการบวกและการคูณดังนิยามข้างต้น แสดงให้เห็นว่า K ไม่เป็นริงสลับที่ ซึ่งจะเรียกว่าริงการหารของ *จำนวนจริงควอเทอร์เนียน (real quaternions)* โดยมีตัวผกผันการคูณของ $a_0+a_1i+a_2j+a_3k$ เมื่อ $0 \neq d = a_0^2+a_1^2+a_2^2+a_3^2$ คือ

$$(a_0+a_1i+a_2j+a_3k)^{-1} = \frac{a_0}{d}-\frac{a_1}{d}i-\frac{a_2}{d}j-\frac{a_3}{d}k = \frac{a_0-a_1i-a_2j-a_3k}{d} \quad \bigcirc$$

ข้อสังเกต 4.2.2 ข้อ 3 แสดงให้เห็นว่าทุกๆ ฟีลด์เป็นอินทิกรัลโดเมน แต่ตัวอย่าง 4.2.3 แสดงว่ามีอินทิกรัลโดเมน $\mathbb{Z}$ ที่ไม่ใช่ฟีลด์ เราจึงได้ความสัมพันธ์ของหมู่ริงชนิดต่างๆ ดังนี้

ฟีลด์ $\subset$ อินทิกรัลโดเมน $\subset$ ริงสลับที่ $\subset$ ริง

โดยทั่วไปหมู่ของริงเหล่านี้ไม่เป็นหมู่เดียวกัน แต่ในกรณีริงจำกัด อินทิกรัลโดเมนและฟีลด์เป็นหมู่เดียวกัน ดังจะแสดงการพิสูจน์ในทฤษฎีบทต่อไปนี้

4.2.6 **ทฤษฎีบท** ถ้า R เป็นอินทิกรัลโดเมนขนาดจำกัดแล้ว R เป็นฟีลด์

บทพิสูจน์ ให้ R เป็นอินทิกรัลโดเมนขนาดจำกัดแล้ว R เป็นริงสลับที่มีเอกลักษณ์ 1 ในการพิสูจน์ว่า R เป็นฟีลด์ จึงเหลือเพียงแสดงว่าแต่ละ $0 \neq a \in R$ เป็นหน่วยซึ่งจะทำให้ได้ R เป็นริงการหารที่เป็นริงสลับที่

เพราะว่า R เป็นเซตจำกัด จึงอาจกำหนดให้ $R=\{x_0,x_1,\ldots,x_n\}$ และให้ $0 \neq a \in R$ แล้ว $ax_0, ax_1, \ldots, ax_n$ ทั้งหมดเป็นสมาชิกของ R แล้วจะแสดงว่าสมาชิกเหล่านี้ก็ต่างกันทั้งหมด โดยสมมติว่ามี $1 \le i \neq j \le n$ ซึ่ง $ax_i = ax_j$ แล้ว $a(x_i-x_j)=0$ แต่ $a \neq 0$ และ R ไม่มีตัวหารของศูนย์ดังนั้น $x_i - x_j = 0$ ซึ่งสมมูลกับ $x_i = x_j$ จึงขัดแย้งกับ $x_0,x_1,\ldots,x_n$ เป็นสมาชิกต่างกันทั้งหมดใน R ทำให้ได้ $\{x_0,x_1,\ldots,x_n\} = R = \{ax_0,ax_1,\ldots,ax_n\}$ แต่เพราะ $1 \in R = \{ax_0,ax_1,\ldots,ax_n\}$ จึง

มี $1 \le k \le n$ ซึ่ง $1 = ax_k = x_k a$ นั่นคือ a ผกผันได้ใน R เพราะฉะนั้น $U = R \setminus \{0\}$ ❑

4.2.7 **ตัวอย่าง** ในตัวอย่าง 4.1.7 ได้แสดงให้เห็นว่า $\mathbb{Z}_n$ ของจำนวนเต็มมอดูโล n เมื่อ n เป็นจำนวนเต็มบวกจะเป็นอินทิกรัลโดเมนถ้า n เป็นจำนวนเฉพาะและเพราะ $\mathbb{Z}_n$ เป็นริงจำกัด จึงได้โดยทฤษฎีบท 4.2.4 ว่า $\mathbb{Z}_n$ เป็นฟีลด์เมื่อ n เป็นจำนวนเฉพาะ ○

เพราะฟีลด์เป็นอินทิกรัลโดเมน ดังนั้นแต่ละฟีลด์จึงประกอบด้วยสมาชิกอย่างน้อย 2 ตัวคือ ศูนย์ 0 และเอกลักษณ์ $1 \ne 0$ และตัวอย่าง 4.2.7 แสดงให้เห็นว่ามีฟีลด์เล็กสุดที่ประกอบด้วยสมาชิก 2 ตัวนั่นคือฟีลด์ $\mathbb{Z}_2$

สังเกตจากตัวอย่าง 4.1.10 ถ้า R และ S เป็นอินทิกรัลโดเมน (หรือฟีลด์) แล้ว $R \times S$ ไม่เป็นอินทิกรัลโดเมนและดังนั้นไม่เป็นฟีลด์

ให้ R เป็นริง ถ้าพิจารณา R กับการดำเนินการ + แล้ว R เป็นกรุปอาบีเลียนและขอทบทวนว่า "อันดับ" ของแต่ละสมาชิก a ในกรุป R คือจำนวนเต็มบวก n น้อยสุดซึ่ง $na = 0$ และถ้าไม่มีจำนวนเต็มบวกน้อยสุดดังกล่าวแล้ว a มีอันดับอนันต์ และสำหรับในริง R เราเรียกจำนวนเต็มบวก n น้อยสุดดังกล่าวของ a ว่า "*อันดับการบวก (additive order)*" ของ a

ในริง R ที่มีเอกลักษณ์ ถ้าเอกลักษณ์ $1 \in R$ มีอันดับการบวกเป็น n นั่นคือ $\underbrace{1+1+\cdots+1}_{n\ times} = 0$ แล้วแต่ละ $0 \ne a \in R$ จะได้ $na = \underbrace{a+\cdots+a}_{n\ times} = \underbrace{1a+\cdots+1a}_{n\ times} = (\underbrace{1+\cdots+1}_{n\ times})a = 0a = 0$ ดังนั้นอันดับการบวกของ a จะน้อยกว่าหรือเท่ากับ n ในทางกลับกันถ้า $0 \ne a \in R$ มีอันดับการบวกเป็น m แล้ว $0 = ma = \underbrace{a+\cdots+a}_{m\ times} = \underbrace{1a+\cdots+1a}_{m\ times} = (\underbrace{1+\cdots+1}_{m\ times})a = (m1)a$ จึงสังเกตได้ว่าถ้า R เป็นอินทิกรัลโดเมนแล้ว $m1 = 0$ ดังนั้นอันดับการบวกของ 1 จะน้อยกว่าหรือเท่ากับ m เราจึงสรุปได้ทฤษฎีบทต่อไปนี้

4.2.8 **ทฤษฎีบท** ทุกๆ สมาชิกที่ไม่ใช่ศูนย์ในอินทิกรัลโดเมนมีอันดับการบวกเท่ากันและเท่ากับอันดับการบวกของเอกลักษณ์ของอินทิกรัลโดเมน ❑

4.2.9 **บทนิยาม** ให้ R เป็นริงมีเอกลักษณ์ 1 เรียกจำนวนเต็มบวก n น้อยสุดซึ่ง $\underbrace{1+1+\cdots+1}_{n\ times} = n1 = 0$ ว่า *ค่าลักษณะเฉพาะ (characteristic)* ของ R และแทนด้วยสัญลักษณ์ $char(R)$ แต่ถ้าไม่มีจำนวนเต็มบวกดังกล่าว จะกล่าวว่า R มีค่าลักษณะเฉพาะเป็นศูนย์ นั่นคือ $char(R) = 0$

ริงของจำนวนเต็ม ริงของจำนวนตรรกยะ และริงของจำนวนจริง เป็นตัวอย่างของริงที่มีค่าลักษณะเฉพาะเป็นศูนย์ ในขณะที่ริงของเซตย่อยทั้งหมดของเซต X (แบบฝึกหัด 4.1 ข้อ 5) มีค่าลักษณะเฉพาะเป็น 2 เพราะว่า $2A = A + A = (A - A) \cup (A - A) = \phi$ ทุกๆ เซตย่อย A ของ X

4.2.10 **ทฤษฎีบท** $char(R) = 0$ หรือ $char(R)$ เป็นจำนวนเฉพาะ ทุกๆ อินทิกรัลโดเมน R

บทพิสูจน์ ให้ R เป็นอินทิกรัลโดเมนซึ่ง $char(R) \neq 0$ แล้วมีจำนวนเต็มบวกน้อยสุด n ซึ่ง $n1 = 0$ สมมติ n เป็นจำนวนประกอบ นั่นคือมีจำนวนเต็มบวก $1 < r, s < n$ ซึ่ง $n = rs$ ดังนั้น $r1 \neq 0$ และ $s1 \neq 0$ แต่ $(r1)(s1) = \left(\underbrace{1+1+\cdots+1}_{r\ times}\right)\left(\underbrace{1+1+\cdots+1}_{s\ times}\right) = \underbrace{1+1+\cdots+1}_{rs\ times} = (rs)1 = n1 = 0$ ทำให้ $r1$ และ $s1$ เป็นตัวหารของศูนย์ซึ่งจะขัดแย้งกับ R เป็นอินทิกรัลโดเมน ❑

สังเกตว่าถ้า R เป็นอินทิกรัลโดเมนที่มีค่าลักษณะเฉพาะไม่ใช่ศูนย์ แล้วมีจำนวนเฉพาะ p ซึ่ง $char(R) = p$ และสำหรับ $a, b \in R$ โดยทฤษฎีบททวินามจะได้

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$$

โดยที่ p เป็นตัวหารของสัมประสิทธิ์ทวินาม $\binom{p}{k}$ ทุกๆ $0 < k < p$ ดังนั้น $\binom{p}{k}a^{p-k}b^k = 0$ ทุกๆ $0 < k < p$ จึงได้ $(a+b)^p = a^p + b^p$

แบบฝึกหัด 4.2

1. ให้ S เป็นเซต + และ · เป็นการดำเนินการบน S ที่ทำให้
   (ก) $(S;+)$ เป็นกรุป
   (ข) $(S^*;\cdot)$ เป็นกรุปเมื่อ S^* คือเซตของสมาชิกใน S ทั้งหมดยกเว้นเอกลักษณ์การบวก +
   (ค) $a(b+c) = ab + ac$ และ $(b+c)a = ba + ca$ สำหรับทุกๆ $a, b, c \in S$
   จงพิสูจน์ว่า $(S;+,\cdot)$ เป็นริงการหาร
   [ข้อแนะนำ : ประยุกต์ (ข) กับ $(1+1)(a+b)$ เพื่อพิสูจน์ว่า $(S;+)$ เป็นกรุปอาบีเลียน]
2. นิยาม "การบวก $\oplus$" และ "การคูณ $\odot$" บน $\mathbb{Z}$ ในรูปของการบวกและการคูณแบบปกติในริงของจำนวนเต็ม $\mathbb{Z}$ โดย $a \oplus b = a + b - 1$ และ $a \odot b = a \cdot b - (a+b) + 2$ ทุกๆ $a, b \in \mathbb{Z}$ จงแสดงว่า $(\mathbb{Z};\oplus,\odot)$ เป็นริง หรือเป็นอินทิกรัลโดเมน หรือเป็นฟิลด์
3. ในริง $\mathbb{Z}_n$ ของจำนวนเต็มมอดูโล n เมื่อ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่า
   3.1 ถ้า $0 \neq a \in \mathbb{Z}_n$ แล้ว a ผกผันได้ก็ต่อเมื่อ n และ a เป็นจำนวนเฉพาะสัมพัทธ์
   3.2 ถ้า n เป็นจำนวนประกอบแล้ว $\mathbb{Z}_n$ มีตัวหารของศูนย์ที่ไม่ใช่ศูนย์และผกผันไม่ได้

4. ให้ R เป็นอินทิกรัลโดเมน จงพิสูจน์ว่า

4.1 สำหรับ $0 \neq a \in R$ มีจำนวนเต็มบวก n ซึ่ง $na = 0$ โดยเฉพาะ $char(R) \neq 0$

4.2 ถ้า $0 \neq a \in R$ และ $n \neq 0$ เป็นจำนวนเต็มซึ่ง $na = 0$ แล้ว n เป็นพหุคูณของ $char(R)$

4.3 ถ้า $char(R) = 0$ และ $n \neq 0$ เป็นจำนวนเต็มซึ่ง $na = 0$ แล้ว $a = 0$

4.4 ถ้า $char(R) = 3$ และ $a \in R$ ซึ่ง $5a = 0$ แล้ว $a = 0$

4.5 ถ้ามี $a,b \in R$ ซึ่ง $a \neq b$ และ $125a = 125b$ แล้ว $char(R) = 5$

4.6 ถ้ามี $a,b \in R \setminus \{0\}$ ซึ่ง $10a = 0$ และ $14b = 0$ แล้ว $char(R) = 2$

4.7 ถ้า $char(R) = q$ แล้ว q เป็นตัวหารของ $|R|$

4.8 ถ้า $|R| = p^m$ เมื่อ p เป็นจำนวนเฉพาะและ m เป็นจำนวนเต็มบวกแล้ว $char(R) = p$

4.9 ถ้า $(R;+)$ เป็นกรุปวัฏจักรขนาดจำกัด แล้ว $|R|$ เป็นจำนวนเฉพาะ

5. ให้ R เป็นริงสลับที่ขนาดจำกัดและมีเอกลักษณ์ จงพิสูจน์ว่า

5.1 ถ้า $0 \neq a \in R$ แล้ว a เป็นตัวหารของศูนย์หรือ a ผกผันได้ [ข้อแนะนำ : ประยุกต์การพิสูจน์ทฤษฎีบท 4.2.6]

5.2 ถ้า $R = \{a_1, \ldots, a_n\}$ และ n_i เป็นอันดับของ a_i สำหรับแต่ละ $i = 1, 2, \ldots, n$ แล้ว $char(R)$ เท่ากับตัวคูณร่วมน้อย (least common multiple) ของ $n_1, \ldots, n_n$

4.3 ริงย่อยและไอดีล

เราได้เห็นตัวอย่างมากมายของริงที่เล็กกว่าบรรจุในริงที่ใหญ่กว่า เช่นริงของจำนวนเต็มบรรจุในริงของจำนวนตรรกยะ และริงของจำนวนตรรกยะก็บรรจุในริงของจำนวนจริง เป็นต้น ลักษณะของริงซึ่งเล็กกว่าบรรจุในริงที่ใหญ่กว่าเช่นนี้ เป็นไปในลักษณะเดียวกับกรุปย่อยบรรจุในกรุปที่ใหญ่กว่า กล่าวคือภายใต้การดำเนินการ "การบวก" ริงที่เล็กกว่าเป็นกรุปย่อยของริงที่ใหญ่กว่าและ "การคูณ" ของริงที่ใหญ่กว่าเมื่อกำกัดลงบนริงที่เล็กกว่ายังคงเป็นการดำเนินการของริงที่เล็กกว่า เราเรียกริงที่เล็กกว่าในลักษณะเช่นนี้ว่า "ริงย่อย" ของริงที่ใหญ่กว่า

เราจะตรวจสอบก่อนว่าถ้า R เป็นริงและ $\phi \neq S \subseteq R$ มีสมบัติปิดภายใต้ "การบวก" "การมีจำนวนลบ" และการคูณ" ของ R แล้ว S เป็นริง ให้ $a,b,c \in S$ แล้ว $a,b,c \in R$ ดังนั้น $a+(b+c) = (a+b)+c$, $a(bc) = (ab)c$, $a(b+c) = ab+ac$ และ $(b+c)a = ba+ca$ นั่นคือ "การบวก" และ "การคูณ" ของ R กำกัดลงบน S สอดคล้องกฎการเปลี่ยนหมู่และกฎการกระจาย ต่อไปเพราะ $S \neq \phi$ ดังนั้นมี $b \in S$ และเพราะ S มีสมบัติปิดภายใต้การมีจำนวนลบ ดังนั้น $-b \in S$ และเพราะ S มีสมบัติปิดภายใต้การบวก ทำให้ $0 = b+(-b) \in S$ เพราะฉะนั้น S เป็นริง

4.3.1 **บทนิยาม** ให้ R เป็นริงและ $\phi \neq S \subseteq R$ เรากล่าวว่า S เป็น *ริงย่อย (subring)* ของ R ถ้า S มีสมบัติปิดภายใต้ "การบวก" "การมีจำนวนลบ" และ "การคูณ" ของ R

โดยเกณฑ์การเป็นกรุปย่อย และบทนิยามของริงย่อย เราได้เกณฑ์การเป็นริงย่อย ต่อไปนี้

4.3.2 **ทฤษฎีบท** ให้ R เป็นริงและ $\phi \neq S \subseteq R$ แล้ว S เป็นริงย่อยของ R ก็ต่อเมื่อ S มีสมบัติปิดภายใต้การลบและการคูณ (นั่นคือ $a-b \in S$ และ $ab \in S$ ทุกๆ $a,b \in S$) ของ R ❑

โดยการวิเคราะห์ข้างต้น ถ้า S เป็นริงย่อยของริง R แล้วศูนย์ของ R เป็นศูนย์ของ S ยิ่งไปกว่านั้น จำนวนลบของแต่ละสมาชิกใน S เป็นจำนวนลบตัวเดียวกับใน R ทำให้สังเกตว่าทุกๆ ริง R มีอย่างน้อยสองริงย่อยคือริงศูนย์ $\{0\}$ และ R จึงเรียกสองริงย่อยนี้ว่า *ริงย่อยขัด (trivial subring)* และเรียกริงย่อยซึ่งไม่เท่ากับ R ว่า *ริงย่อยแท้ (proper subring)* ตัวอย่างเช่นเซตของจำนวนเต็มคู่เป็นริงย่อยแท้ของริงของจำนวนเต็ม เป็นต้น

สังเกตต่อได้อีกว่า ริงของจำนวนเต็มมีเอกลักษณ์ แต่ริงของจำนวนเต็มคู่ไม่มีเอกลักษณ์ นอกจากนี้ $\mathbb{Z}\times\{0\}$ เป็นริงย่อยแท้ของริงผลคูณ $\mathbb{Z}\times\mathbb{Z}$ โดยที่ $(1,0)$ และ $(1,1)$ เป็นเอกลักษณ์ของ $\mathbb{Z}\times\{0\}$ และ $\mathbb{Z}\times\mathbb{Z}$ ตามลำดับ จึงขอสรุปเป็นข้อสังเกตดังนี้

4.3.3 **ข้อสังเกต**

1. ถ้า R เป็นริงมีเอกลักษณ์แล้วไม่จำเป็นที่ริงย่อยของ R ต้องมีเอกลักษณ์
2. ถ้า R เป็นริงมีเอกลักษณ์และริงย่อย S ของ R ก็มีเอกลักษณ์ แล้วเอกลักษณ์ของ R และของ S ไม่จำเป็นต้องเป็นตัวเดียวกัน
3. ถ้าเอกลักษณ์ของริงย่อย S และของริง R ต่างกัน แล้ว R มีตัวหารของศูนย์ เพราะว่า ถ้า 1 และ $1'$ เป็นเอกลักษณ์ของ R และของ S ตามลำดับโดยที่ $1 \neq 1'$ แล้ว $1-1' \neq 0$, $1' \neq 0$, $1' \cdot 1 = 1'$ และ $1' \cdot 1' = 1'$ ทำให้ได้ $1'(1-1') = 1' \cdot 1 - 1' \cdot 1' = 1' - 1' = 0$ ซึ่งแสดงว่า $1'$ และ $1-1'$ เป็นตัวหารของศูนย์ใน R

   จากข้อสังเกตนี้ เอกลักษณ์ $(1,0)$ ของ $\mathbb{Z}\times\{0\}$ เป็นตัวหารของศูนย์ใน $\mathbb{Z}\times\mathbb{Z}$ และ โดยความเป็นจริง $(1,0)(0,1) = (0,0)$

4.3.4 **บทนิยาม** ให้ R เป็นริง เรียกเซตย่อย $C(R) := \{a \in R \mid ar = ra \text{ ทุกๆ } r \in R\}$ ว่า *ศูนย์กลาง (center)* ของ R (และพิสูจน์ได้ไม่ยากว่าศูนย์กลางของริงเป็นริงย่อย)

ถ้า R เป็นริงและ S เป็นริงย่อยของ R แล้ว S เป็นกรุปย่อยของกรุปอาบีเลียน R ดังนั้น S เป็นกรุปย่อยปรกติของ R ทำให้ R/S เป็นกรุปผลหารซึ่งเป็นกรุปอาบีเลียน จึงเกิดคำถามว่าเรา

จะสร้างริงผลหารได้จากกรุปผลหาร R/S ทุกๆ ริงย่อย S ของ R หรือไม่ และการตอบคำถามดังกล่าวคือการแสดงว่าการคูณบนเซต R/S ของโคเซตทั้งหมดของ S ใน R นั่นคือ

$$(a+S)(b+S)=ab+S$$

ทุกๆ $a,b\in R$ เป็นการดำเนินการบน R/S ซึ่งสอดคล้องกฎการเปลี่ยนหมู่ หรือไม่

ให้ $a,b,c,d\in R$ ซึ่ง $a+S=b+S$ และ $c+S=d+S$ แล้ว $a-b\in S$ และ $c-d\in S$ และเราต้องการ $ac+S=(a+S)(c+S)=(b+S)(d+S)=bd+S$ ซึ่งสมมูลกับ $ac-bd\in S$ แต่ $ac-bd=a(c-d)+d(a-b)$ ดังนั้น $ac-bd\in S$ ถ้าแต่ละริงย่อย S สอดคล้องเงื่อนไข "ถ้า $s\in S$ และ $r\in R$ แล้ว $rs,sr\in S$"

พิจารณาริงย่อย S ของเมทริกซ์ขนาด 2×2 ในรูปแบบ $\begin{pmatrix}0 & 0\\ 0 & x\end{pmatrix}$ เมื่อ $x\in\mathbb{R}$ ของริง R ของเมทริกซ์ขนาด 2×2 เหนือ $\mathbb{R}$ ทั้งหมด จะเห็นว่า $\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}\notin S$ ซึ่งแสดงว่ามีบางริงย่อยที่จะไม่สอดคล้องเงื่อนไขที่ต้องการ

ในการสร้างริงผลหาร เราจึงต้องการเซตย่อยของริงซึ่งเป็นกรุปย่อยของกรุปอาบีเลียนในโครงสร้างของริงและสอดคล้องเงื่อนไข "ถ้า $s\in S$ และ $r\in R$ แล้ว $rs,sr\in S$"

4.3.5 **บทนิยาม** ให้ R เป็นริงและ $\phi\neq S\subseteq R$ เรากล่าวว่า S เป็น *ไอดีลซ้าย (left ideal)* [หรือ *ไอดีลขวา (right ideal)* ของ R ถ้า S เป็นกรุปย่อยการบวกของ R (นั่นคือมีสมบัติปิด "การบวก" และ "การมีจำนวนลบ") และ *สมบัติดูดกลืนการคูณทางซ้าย (left absorb product)* นั่นคือ $rs\in S$ ทุกๆ $s\in S$ และ $r\in R$ [หรือ *สมบัติดูดกลืนการคูณทางขวา (right absorb product)* นั่นคือ $sr\in S$ ทุกๆ $s\in S$ และ $r\in R$]

เรากล่าวว่า S เป็น *ไอดีล (ideal)* ของ R ถ้า S เป็นไอดีลซ้ายและไอดีลขวาของ R

หมายเหตุ: จะกล่าวว่า S มี *สมบัติดูดกลืนการคูณ (absorb product)* ถ้า S มีสมบัติดูดกลืนการคูณทางซ้ายและสมบัติดูดกลืนการคูณทางขวา

สังเกตว่าริงของจำนวนเต็มเป็นริงย่อยของริงของจำนวนตรรกยะ แต่ไม่เป็นไอดีล (เพราะว่า $(\frac{1}{2})(3)=\frac{3}{2}$ ไม่เป็นจำนวนเต็ม) หรือริงของจำนวนตรรกยะเป็นริงย่อยของริงของจำนวนจริง แต่ไม่เป็นไอดีล (เพราะว่า $(\frac{1}{2})(\sqrt{2})=\frac{\sqrt{2}}{2}$ ไม่เป็นจำนวนตรรกยะ) แต่ริงของจำนวนเต็มคู่เป็นไอดีลของริงของจำนวนเต็ม เป็นต้น

เมื่อได้เห็นตัวอย่างของริงย่อยที่ไม่เป็นไอดีล จึงอาจมีคำถามว่า ไอดีลเป็นริงย่อยหรือไม่และจากบทนิยามของไอดีล เห็นได้ชัดว่าสมบัติดูดกลืนการคูณทำให้ได้ว่าไอดีลมีสมบัติปิดการคูณ (เพราะถ้า R เป็นริงและ S เป็นไอดีลของ R และ $a,b \in S$ แล้ว $a \in S$ และ $b \in R$ ทำให้ได้ ab, $ba \in S$)

4.3.6 **ทฤษฎีบท** ทุกๆ ริงย่อยของริง $\mathbb{Z}$ ของจำนวนเต็มเป็นไอดีล

บทพิสูจน์ ให้ S เป็นริงย่อยของริง $\mathbb{Z}$ แล้ว $(S;+)$ เป็นกรุปย่อยของ $(\mathbb{Z};+)$ จึงเป็นกรุปย่อยวัฏจักร ดังนั้นมีจำนวนเต็มบวก n ซึ่ง $S = <n> = \{mn | m \in \mathbb{Z}\}$ ต่อไปให้ $mn \in S$ สำหรับแต่ละ $m \in \mathbb{Z}$ และ $k \in \mathbb{Z}$ แล้ว $(mn)k = k(mn) = (km)n \in S$ ❍

โดยประยุกต์การพิสูจน์ทฤษฎีบท 4.3.6 จะได้ด้วยว่าในริง R ซึ่งเป็นริงสลับที่มีเอกลักษณ์ ถ้า $a \in R$ แล้ว $S = \{xa | x \in R\}$ เป็นไอดีลของ R ซึ่งเรียกว่า *ไอดีลมุขสำคัญ (principal ideal)* ก่อกำเนิดโดย a และแทนด้วยสัญลักษณ์ $<a>$

4.3.7 **ตัวอย่าง** ให้ X เป็นเซตที่ไม่ใช่เซตว่างและ $\mathbb{R}^X$ แทนเซตของฟังก์ชันทั้งหมดจาก X ไปยัง $\mathbb{R}$ และนิยาม "การบวก" และ "การคูณ" บน $\mathbb{R}^X$ โดย

$$(f+g)(x) = f(x) + g(x) \text{ และ } (fg)(x) = f(x)g(x)$$

ทุกๆ $x \in R$ และทุกๆ $f, g \in \mathbb{R}^X$ แล้วการแสดงเช่นเดียวกับตัวอย่าง 4.1.9 จะได้ว่า $\mathbb{R}^X$ เป็นริง

แต่ละ $x \in X$ นิยาม $R_x := \{f \in \mathbb{R}^X | f(x) = 0\}$ แล้วสำหรับ $f, g \in R_x$ และ $h \in \mathbb{R}^X$ จะได้ $(f-g)(x) = f(x) - g(x) = 0$, $(fh)(x) = f(x)h(x) = 0h(x) = 0$ และ $(hf)(x) = h(x)f(x) = h(x)0 = 0$ ซึ่งแสดงว่า $f-g, fh, hf \in R_x$ นั่นคือ R_x เป็นไอดีลของ $\mathbb{R}^X$ ทุกๆ $x \in X$ ❍

สังเกตจากตัวอย่าง 4.3.7 ต่อไปว่า $f \in \bigcap_{x \in X} R_x$ ก็ต่อเมื่อ $f(x) = 0$ ทุกๆ $x \in X$ ซึ่งแสดงว่า $\bigcap_{x \in X} R_x = \{0\}$ เป็นไอดีลของ $\mathbb{R}^X$ และความจริงดังกล่าวนี้เป็นกรณีเฉพาะของความจริงที่ว่าส่วนร่วมของไอดีลเป็นไอดีล แต่ก่อนอื่นขอกล่าวถึงทฤษฎีบทซึ่งจะเป็นประโยชน์ต่อการศึกษาไอดีลต่อๆ ไป

4.3.8 **ทฤษฎีบท** ถ้า S เป็นไอดีลของริง R ซึ่ง $S \neq R$ แล้ว $S \cap U = \phi$ เมื่อ U คือเซตของหน่วยทั้งหมดของ R

บทพิสูจน์ เห็นได้ชัดว่าทฤษฎีบทเป็นจริงถ้า $S = \{0\}$ หรือ R ไม่มีเอกลักษณ์ จึงพิจารณากรณีที่ $S \neq \{0\}$ และ R มีเอกลักษณ์ 1 ให้ $0 \neq a \in S$ และสมมติ $a \in U$ แล้วมี $0 \neq b \in R$ ซึ่ง $ab = 1 = ba$ แต่เพราะ S มีสมบัติดูดกลืนการคูณ จึงได้ $1 = ab \in S$ ดังนั้นถ้า $r \in R$ แล้วโดยสมบัติดูด

กลืนการคูณของ S และ $1 \in S$ ทำให้ได้ $r = r1 \in S$ ซึ่งแสดงว่า $S = R$ จะขัดแย้งกับสมมติฐานซึ่งกำหนดว่า $S \neq R$ เพราะฉะนั้น $S \cap U = \phi$ ❑

การพิสูจน์ทฤษฎีบท 4.3.8 ทำให้ได้บทแทรก 4.3.9 ต่อไปนี้

4.3.9 **บทแทรก** ถ้า R เป็นริงมีเอกลักษณ์ 1 และ S เป็นไอดีลของ R ซึ่ง $1 \in S$ แล้ว $S = R$ ❑

4.3.10 **บทแทรก** ให้ R เป็นริงสลับที่มีเอกลักษณ์แล้ว R เป็นฟีลด์ก็ต่อเมื่อมีเพียงริงย่อยชัดเท่านั้นที่เป็นไอดีลของ R

บทพิสูจน์ ให้ R เป็นฟีลด์และ $S \neq \{0\}$ เป็นไอดีลของ R แล้วมี $0 \neq a \in S$ โดยที่ a เป็นหน่วย ดังนั้น $S \cap U \neq \phi$ เมื่อ U คือเซตของหน่วยทั้งหมดของ R เพราะฉะนั้น $S = R$

ในการพิสูจน์บทกลับ เราเหลือเพียงแสดงว่าแต่ละ $0 \neq a \in R$ ผกผันได้ เนื่องจาก aR เป็นไอดีลของ R และ $0 \neq a = a1 \in aR$ ดังนั้น $aR \neq \{0\}$ ทำให้ได้ $aR = R$ แต่ $1 \in R$ จึงมี $0 \neq b \in R$ ซึ่ง $ab = 1$ ❑

4.3.11 **ทฤษฎีบท** ให้ $\{S_i | i \in I\}$ เป็นหมู่ของไอดีลของริง R แล้ว $\bigcap_{i \in I} S_i$ เป็นไอดีลของ R

บทพิสูจน์ เพราะ $0 \in S_i$ ทุกๆ $i \in I$ ดังนั้น $0 \in \bigcap_{i \in I} S_i$ ทำให้ได้ $\bigcap_{i \in I} S_i \neq \phi$ ต่อไปให้ $a, b \in \bigcap_{i \in I} S_i$ และ $r \in R$ แล้ว $a, b \in S_i$ ทุกๆ $i \in I$ ดังนั้น $a - b, ra, ar \in S_i$ ทุกๆ $i \in I$ ทำให้ได้ $\bigcap_{i \in I} S_i$ เป็นไอดีลของ R ❑

ให้ X เป็นเซตย่อยที่ไม่ใช่เซตว่างของริง R และ $\{S_i | i \in I\}$ เป็นหมู่ของไอดีลของริง R ซึ่งบรรจุ X ทฤษฎีบท 4.3.11 แสดงว่า $\bigcap_{i \in I} S_i$ เป็นไอดีลของ R และเห็นชัดว่า $\bigcap_{i \in I} S_i$ บรรจุ X จึงใช้สัญลักษณ์ $< X >$ แทน $\bigcap_{i \in I} S_i$ และเรียกว่า *ไอดีลก่อกำเนิดโดย (ideal generated by)* X โดยเรียกสมาชิกของ X ว่า *ตัวก่อกำเนิด (generators)* ของ $< X >$

สังเกตว่า $X \subseteq < X >$ และถ้า S เป็นไอดีลของ R ซึ่ง $X \subseteq S$ แล้ว $< X > \subseteq S$ ดังนั้น $< X >$ เป็นไอดีลเล็กสุดซึ่งบรรจุ X และถ้า $X = \{x_1, \ldots, x_n\}$ เป็นเซตจำกัด จะแทน $< X >$ ด้วย $< x_1, x_2, \ldots, x_n >$ และกล่าวว่าเป็น *ไอดีลก่อกำเนิดแบบจำกัด (finitely generated ideal)* โดยเฉพาะถ้า $X = \{a\}$ จะเรียก $< a >$ ว่า *ไอดีลมุขสำคัญ (principal ideal)* ก่อกำเนิดโดย a ซึ่งเป็นกรณีทั่วไปของทฤษฎีบท 4.3.6

ให้ R เป็นริงแล้ว ras, ra, as และ na เป็นสมาชิกของ $< a >$ ทุกๆ $r, s \in R$ และ $n \in \mathbb{Z}$ และโดยทั่วไปผลบวกของสมาชิกในรูปแบบ ras เป็นสมาชิกในรูปแบบเดียวกัน จึงได้ว่า

$$< a > = \{na + ra + as + \sum_{i=1}^{m} r_i a s_i \,|\, r, s, r_i, s_i \in R, m \in \mathbb{Z}^+, n \in \mathbb{Z}\}$$

ถ้า R เป็นริงมีเอกลักษณ์แล้วสำหรับ $n \in \mathbb{Z}$ จะได้ $na = (n1)a$ เป็นสมาชิกในรูปแบบ ra เพราะ $n1 \in R$ ทำให้ไอดีล $<a>$ ลดรูปเป็น

$$<a> = \{ra + as + \sum_{i=1}^{m} r_i a s_i \mid r, s, r_i, s_i \in R, m \in \mathbb{Z}^+\}\}$$

ถ้า a เป็นสมาชิกในศูนย์กลางของ R แล้ว ras, ra, as เขียนได้ในรูปแบบเดียวกันเป็น ra ทำให้ไอดีล $<a>$ ลดรูปเป็น

$$<a> = \{na + ra \mid r \in R, n \in \mathbb{Z}\}$$

และถ้า R เป็นริงสลับที่มีเอกลักษณ์แล้ว ras, ra, as เขียนได้ในรูปแบบเดียวกันเป็น ra และสำหรับ $n \in \mathbb{Z}$ จะได้ $na = (n1)a$ เป็นสมาชิกในรูปแบบ ra ทำให้ไอดีล $<a>$ ลดรูปเหลือเพียง

$$<a> = \{ra \mid r \in R\}$$

เห็นได้ชัดว่า $Ra = \{ra \mid r \in R\}$ เป็นไอดีลซ้ายและ $aR = \{ar \mid r \in R\}$ เป็นไอดีลขวาของ R (a เป็นสมาชิกของ Ra หรือ aR หรือไม่ก็ได้) แต่ถ้า R เป็นริงมีเอกลักษณ์แล้ว $a \in Ra$ และ $a \in aR$ โดยเฉพาะอย่างยิ่งถ้า R เป็นริงมีเอกลักษณ์และ a เป็นสมาชิกในศูนย์กลางของ R แล้ว $Ra = <a> = aR$

4.3.12 **บทนิยาม** กล่าวว่า R เป็น *ริงของไอดีลมุขสำคัญ (principal ideal ring)* ถ้าทุกๆ ไอดีลของ R เป็นไอดีลมุขสำคัญและถ้า R เป็นริงของไอดีลมุขสำคัญซึ่งเป็นอินทิกรัลโดเมน จะเรียก R ว่า *โดเมนของไอดีลมุขสำคัญ (principal ideal domain)*

4.3.13 **ทฤษฎีบท** $\mathbb{Z}$ เป็นโดเมนของไอดีลมุขสำคัญและทุกๆ ไอดีลของ $\mathbb{Z}$ อยู่ในรูปแบบ $<n>$ เมื่อ $n \in \mathbb{Z}$

บทพิสูจน์ ให้ A เป็นไอดีลของ $\mathbb{Z}$ ถ้า $A = \{0\} = <0>$ แล้วทฤษฎีบทเป็นจริง จึงให้ $A \neq <0>$ แล้วมี $0 \neq m \in A$ เพราะว่า $-1 \in \mathbb{Z}$ ทำให้ $-m = (-1)m \in A$ นั่นคือมีจำนวนเต็มบวกเป็นสมาชิกของ A ให้ n เป็นจำนวนเต็มบวกน้อยสุดใน A แล้วโดยสมบัติของไอดีลจะได้ $<n> \subseteq A$ ต่อไปให้ $k \in A$ โดยขั้นตอนการหารใน $\mathbb{Z}$ จะมีจำนวนเต็ม q และ r ซึ่ง $k = qn + r$ โดยที่ $0 \leq r < n$ แต่ k และ qn เป็นสมาชิกของ A ทำให้ $r = k - qn \in A$ โดยที่ n เป็นจำนวนเต็มน้อยสุดใน A และ $0 \leq r < n$ จึงได้ $r = 0$ ทำให้ $k = qn$ นอกจากนี้เพราะ $\mathbb{Z}$ เป็นริงสลับที่มีเอกลักษณ์ ดังนั้น $<n> = \{mn \mid m \in \mathbb{Z}\}$ จึงได้ $k = qn \in <n>$ เพราะฉะนั้น $A \subseteq <n>$ และได้ $A = <n>$ ❑

แบบฝึกหัด 4.3

1. ให้ R เป็นริงจำกัด จงแสดงว่าเซตย่อย $S \neq \phi$ ของ R เป็นริงย่อย ก็ต่อเมื่อ S มีสมบัติปิดการคูณและการบวกของ R และถ้า S เป็นริงย่อยของ R แล้ว $|S|$ เป็นตัวหารของ $|R|$
2. ให้ R และ S เป็นริง จงแสดงว่า $R \times \{0\}$ และ $\{0\} \times S$ ต่างเป็นริงย่อยของริง $R \times S$
3. จงแสดงว่าถ้า S เป็นริงย่อยของอินทิกรัลโดเมน R และ $1 \in S$ แล้ว S เป็นอินทิกรัลโดเมน (เรียกว่า *โดเมนย่อย (subdomain)* ของ R)
4. ให้ R เป็นริง จงแสดงว่า $<T> := \cap\{S | T \subseteq S$ และ S เป็นริงย่อยของ $R\}$ เป็นริงย่อยเล็กสุดของ R ที่บรรจุ T ถ้า $\phi \neq T \subseteq R$ [หมายเหตุ : เราเรียก $<T>$ ว่า*ริงย่อยก่อกำเนิดโดย* T *(subring generated by* T*)*
5. ให้ R เป็นริงและ $a \in R$ จงแสดงว่า $C_R(a) = \{r \in R | ra = ar\}$ เป็นริงย่อยของ R และ $C(R) := \{a \in R | ra = ar$ ทุกๆ $r \in R\} = \bigcap_{a \in R} C_R(a)$
6. จงหาริงย่อย A และ B ของ $\mathbb{Z}_{18}$ ที่เป็นไปตามข้อต่อไปนี้
   6.1 A เป็นริงมีเอกลักษณ์ B เป็นริงย่อยของ A ที่ไม่มีเอกลักษณ์
   6.2 A และ B ต่างเป็นริงมีเอกลักษณ์ B เป็นริงย่อยของ A แต่เอกลักษณ์ของ A และ B เป็นสมาชิกแตกต่างกัน
7. จงหาไอดีลทั้งหมดของ $\mathbb{Z}_{12}$ พร้อมทั้งอธิบายว่าเหตุใด ทุกริงย่อยของ $\mathbb{Z}_n$ เป็นไอดีล ทุกๆ จำนวนเต็มบวก n และหาตัวอย่างของริงย่อยของ $\mathbb{Z}_3 \times \mathbb{Z}_3$ ที่ไม่เป็นไอดีล
8. จงพิสูจน์ว่า $\{f \in \Im(\mathbb{R}) | f(x) = 0$ ทุกๆ $x \in \mathbb{Q}\}$ และ $\{f \in \Im(\mathbb{R}) | f(0) = 0\}$ เป็นไอดีลของริง $\Im(\mathbb{R})$ ของฟังก์ชันค่าจริงทั้งหมด
9. ให้ U และ V เป็นไอดีลของริง R จงพิสูจน์ว่า $U \cap V$ เป็นไอดีลของริง R พร้อมพิสูจน์ว่า
   9.1 เซต UV ของสมาชิกในรูปผลบวกจำกัดของผลคูณ uv เมื่อ $u \in U$ และ $v \in V$ เป็นไอดีลของ R ซึ่ง $UV \subseteq U \cap V$
   9.2 $\{x \in R | xu = 0$ ทุกๆ $u \in U\}$ เป็นไอดีลของ R
   9,3 $\{x \in R | rx \in U$ ทุกๆ $r \in R\}$ เป็นไอดีลของ R ซึ่งบรรจุ U
10. ให้ U เป็นไอดีลมุขสำคัญของ $\mathbb{Z}$ ซึ่งก่อกำเนิดโดย 17 จงพิสูจน์ว่าถ้า V เป็นไอดีลของ $\mathbb{Z}$ ซึ่ง $U \subseteq V \subseteq \mathbb{Z}$ แล้ว $V = U$ หรือ $V = \mathbb{Z}$ พร้อมทั้งวางนัยทั่วไป
11. ให้ R เป็นริง จงพิสูจน์ว่า
    11.1 ถ้า $a \in R$ แล้ว $\{x \in R | ax = 0\}$ เป็นไอดีลขวาของ R
    11.2 ถ้า L เป็นไอดีลซ้ายของ R แล้ว $\{x \in R | xa = 0$ ทุกๆ $a \in L\}$ เป็นไอดีล

4.4 ริงผลหาร ไอดีลเฉพาะและไอดีลใหญ่สุดเฉพาะกลุ่ม

การศึกษาสมบัติมูลฐานของริง เราศึกษาแบบคู่ขนานกับสมบัติมูลฐานของกรุปและในทฤษฎีกรุปได้กล่าวถึงการจำแนกภาพสาทิสสัณฐานทั้งหมดด้วยกรุปผลหารของโคเซตของกรุปย่อยปรกติทั้งหมดในกรุป และแม้ริงประกอบด้วยโครงสร้างที่เป็นกรุปอาบีเลียนซึ่งทุกๆ กรุปย่อยเป็นกรุปย่อยปรกติก็ตาม หัวข้อ 4.3 ได้แสดงตัวอย่างของริงย่อยซึ่งไม่สามารถนิยาม "การคูณ" ระหว่างโคเซตเพื่อให้ได้ริงผลหาร อย่างไรก็ตามไอดีลซึ่งเป็นริงย่อยที่มีสมบัติดูดกลืนการคูณสามารถทำหน้าที่เช่นเดียวกับกรุปย่อยปรกติในทฤษฎีกรุป ในหัวข้อนี้เราจะแสดงการสร้างริงผลหาร และจำแนกริงผลหารที่เป็นอินทิกรัลโดเมนและฟีลด์

ให้ J เป็นไอดีลของริง R แล้ว J เป็นริงย่อยของ R ทำให้ $(J;+)$ เป็นกรุปย่อยปรกติของกรุปอาบีเลียน $(R;+)$ ดังนั้นกรุปผลหาร $R/J=\{a+J|a\in R\}$ เป็นกรุปอาบีเลียนภายใต้การบวกซึ่งนิยามโดย $(a+J)+(b+J)=(a+b)+J$ ทุกๆ $a,b\in R$ และนิยามการคูณบนเซต R/J โดย

$$(a+J)(b+J)=ab+J$$

ทุกๆ $a,b\in R$ แล้วจะแสดงว่าการคูณเป็นการดำเนินการบน R/J ดังนี้

ให้ $a,b,c,d\in R$ ซึ่ง $a+J=b+J$ และ $c+J=d+J$ แล้ว $a-b\in J$ และ $c-d\in J$ และเพราะ $ac-bd=a(c-d)+d(a-b)$ โดยที่ J มีสมบัติดูดกลืนการคูณดังนั้น $a(c-d)\in J$ และ $d(a-b)\in J$ แต่โดยสมบัติปิดการบวกของ J จะได้ $ac-bd=a(c-d)+d(a-b)\in J$ ทำให้ $(a+J)(c+J)=ac+J=bd+J=(b+J)(d+J)$ และเห็นชัดว่าการคูณสอดคล้องกฎการเปลี่ยนหมู่ นอกจากนี้

$$\begin{aligned}(a+J)[(b+J)+(c+J)]&=(a+J)[(b+c)+J]=a(b+c)+J=(ab+ac)+J\\&=(ab+J)+(ac+J)=(a+J)(b+J)+(a+J)(c+J)\end{aligned}$$

4.4.1 **ทฤษฎีบท** ถ้า J เป็นไอดีลของริง R แล้ว R/J กับการบวกและการคูณของโคเซตเป็นริงซึ่งเรียกว่า *ริงผลหาร (quotient ring)* ของ J ใน R และถ้า R เป็นริงสลับที่ (หรือมีเอกลักษณ์) แล้ว R/J เป็นริงสลับที่ (หรือมีเอกลักษณ์) ❑

4.4.2 **ตัวอย่าง** เนื่องจากทุกๆ ไอดีลของ $\mathbb{Z}$ เป็นไอดีลมุขสำคัญในรูป $<n>$ เมื่อ n เป็นจำนวนเต็มบวก ดังนั้นริงผลหารอยู่ในรูป $\mathbb{Z}/<n>=\{a+<n>|a\in\mathbb{Z}\}$ ซึ่งได้แสดงในทฤษฎีกรุปแล้วว่าโคเซต $a+<n>$ เมื่อ $a\in\mathbb{Z}$ เป็นเซตสมมูลของคอนกรูเอนซ์มอดูโล n ซึ่ง "การบวก" และ "การคูณ" ระหว่างโคเซตเป็นการดำเนินการเดียวกับ "การบวก" และ "การคูณ" บน $\mathbb{Z}_n$ ของคอนกรูเอนซ์คลาสมอดูโล n เพราะฉะนั้น $\mathbb{Z}_n$ ก็คือริงผลหาร $\mathbb{Z}/<n>$ นั่นเอง ○

สังเกตว่าริง $\mathbb{Z}$ เป็นอินทิกรัลโดเมน แต่ริงผลหาร $\mathbb{Z}_n$ เมื่อ n เป็นจำนวนประกอบมีตัวหารของศูนย์ อย่างไรก็ตามริงผลหาร $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะเป็นฟีลด์ จึงเป็นอินทิกรัลโดเมน เราจึงจะจำแนกริงผลหารที่เป็นอินทิกรัลโดเมนและเป็นฟีลด์ในกรณีทั่วไป

พิจารณาไอดีลมุขสำคัญ $<p>$ เมื่อ p เป็นจำนวนเฉพาะของ $\mathbb{Z}$ ถ้ามีจำนวนเต็ม r และ s ซึ่งผลคูณ $rs \in <p>$ แล้ว p เป็นตัวหารของ rs ทำให้ได้ว่า p เป็นตัวหารของ r หรือ p เป็นตัวหารของ s ซึ่งสมมูลกับ $r \in <p>$ หรือ $s \in <p>$ จึงได้แนวคิดการให้นิยามไอดีลที่มีคุณลักษณะเช่นนี้ในกรณีทั่วไป

4.4.3 **บทนิยาม** ให้ J เป็นไอดีลของริงสลับที่ R เรากล่าวว่า J เป็น *ไอดีลเฉพาะ (prime ideal)* ถ้า $J \neq R$ และสำหรับ $r,s \in R$ ถ้า $rs \in J$ แล้ว $r \in J$ หรือ $s \in J$

จากบทนิยามของไอดีลเฉพาะถ้า R เป็นริงสลับที่มีเอกลักษณ์และ $\{0\}$ เท่านั้นที่เป็นไอดีลเฉพาะของ R แล้วสำหรับ $r,s \in R$ ซึ่ง $rs = 0$ (นั่นคือ $rs \in \{0\}$) จะได้ $r = 0$ หรือ $s = 0$ ซึ่งแสดงว่า R ไม่มีตัวหารของศูนย์ ทำให้ได้ว่า R เป็นอินทิกรัลโดเมน

4.4.4 **ตัวอย่าง** ไอดีล $<n>$ ของริง $\mathbb{Z}$ เป็นไอดีลเฉพาะ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

บทพิสูจน์ ถ้า $n \notin \{0,1\}$ ไม่เป็นจำนวนเฉพาะแล้วมีจำนวนเต็ม $1 < r,s < n$ ซึ่ง $rs = n$ ดังนั้น $rs \in <n>$ โดยที่ $r \notin <n>$ และ $s \notin <n>$ ซึ่งแสดงว่า $<n>$ ไม่เป็นไอดีลเฉพาะ

แต่ถ้า n เป็นจำนวนเฉพาะแล้วแต่ละจำนวนเต็ม r และ s ซึ่ง $rs \in <n>$ จะได้ n เป็นตัวหารของ rs แล้วโดยสมบัติของจำนวนเฉพาะ จะได้ n เป็นตัวหารของ r หรือ n เป็นตัวหารของ s นั่นคือ $r \in <n>$ หรือ $s \in <n>$ ทำให้ได้ $<n>$ เป็นไอดีลเฉพาะ ○

4.4.5 **ทฤษฎีบท** ให้ J เป็นไอดีลของริงสลับที่มีเอกลักษณ์ R แล้ว J เป็นไอดีลเฉพาะ ก็ต่อเมื่อ R/J เป็นอินทิกรัลโดเมน

บทพิสูจน์ ให้ J เป็นไอดีลเฉพาะของ R แล้ว R/J เป็นริงสลับที่มีเอกลักษณ์ จึงเหลือเพียงแสดงว่า R/J ไม่มีตัวหารของศูนย์โดยให้ $a,b \in R$ ซึ่ง $(a+J)(b+J) = J$ แล้ว $ab + J = J$ นั่นคือ $ab \in J$ ดังนั้น $a \in J$ หรือ $b \in J$ นั่นคือ $a + J = J$ หรือ $b + J = J$ สำหรับบทกลับให้ $a,b \in R$ ซึ่ง $ab \in J$ แล้ว $ab + J = J$ แต่ $(a+J)(b+J) = ab + J = J$ แต่โดยสมบัติการไม่มีตัวหารของศูนย์ใน R/J จะได้ $a + J = J$ หรือ $b + J = J$ นั่นคือ $a \in J$ หรือ $b \in J$ ดังนั้น J เป็นไอดีลเฉพาะ ❑

4.4.6 **บทนิยาม** จะกล่าวว่าไอดีล J ของริง R เป็น *ไอดีลใหญ่สุดเฉพาะกลุ่ม (maximal ideal)* ถ้า $J \neq R$ และถ้า K เป็นไอดีลของ R ซึ่ง $J \subseteq K \subseteq R$ แล้ว $K = J$ หรือ $K = R$

หรืออาจกล่าวว่า J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R ก็ต่อเมื่อ $J \neq R$ และไม่มีไอดีลแท้อื่นใดของ R ที่อยู่ระหว่าง J กับ R

ทฤษฎีบทต่อไปเป็นเกณฑ์สำหรับจำแนกไอดีลใหญ่สุดเฉพาะกลุ่มของริง R

4.4.7 **ทฤษฎีบท** ให้ J เป็นไอดีลแท้ของริง R และ $<J,a>$ เป็นไอดีลก่อกำหนดโดย $J \cup \{a\}$ แล้ว J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ก็ต่อเมื่อ $<J,a> = R$ ทุกๆ $a \in R \setminus J$

บทพิสูจน์ ให้ J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R และ $a \in R \setminus J$ แล้ว $J \subset <J,a> \subseteq R$ จึงเห็นชัดว่า $<J,a> = R$ ในทางกลับกันให้ K เป็นไอดีลของ R ซึ่ง $J \subset K \subseteq R$ แล้วมี $a \in K$ ซึ่ง $a \notin J$ ทำให้ได้ $<J,a> = R$ และ $J \subset <J,a> \subseteq K \subseteq R$ ดังนั้น $<J,a> = K = R$ ซึ่งแสดงว่า J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R ❑

แม้เรายังไม่สามารถบอกได้ว่า จะมีไอดีลใหญ่สุดเฉพาะกลุ่มของแต่ละริงหรือไม่ ตัวอย่างต่อไปแสดงว่าไอดีลใหญ่สุดเฉพาะกลุ่มของริงอาจมีได้มากมาย

4.4.8 **ตัวอย่าง** ให้ n เป็นจำนวนเต็มบวก แล้วไอดีล $<n>$ ของริง $\mathbb{Z}$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

บทพิสูจน์ ให้ $<n>$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่มเมื่อ n เป็นจำนวนเต็มบวกและให้ a และ b เป็นจำนวนเต็มบวกซึ่ง $n = ab$ แล้ว $<n> \subseteq <a> \subseteq \mathbb{Z}$ ทำให้ได้ $<n> = <a>$ หรือ $<a> = \mathbb{Z}$ นั่นคือ $a = n$ หรือ $a = 1$ ซึ่งแสดงว่า n เป็นจำนวนเฉพาะ

ในทางกลับกันให้ n เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มซึ่ง $a \notin <n>$ แล้ว a และ n เป็นจำนวนเฉพาะสัมพัทธ์ จึงมีจำนวนเต็ม r และ s ซึ่ง $nr + as = 1$ และเพราะ a และ n เป็นสมาชิกของ $<<n>,a>$ ทำให้ได้ $1 = nr + as \in <<n>,a>$ จึงได้ $<<n>,a> = \mathbb{Z}$ แล้วโดยทฤษฎีบท 4.4.7 จะได้ว่า $<n>$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ❍

4.4.9 **ตัวอย่าง** พิจารณาริงสลับที่ $\Im(\mathbb{R})$ ในตัวอย่าง 4.1.9 ซึ่งมีเอกลักษณ์คือฟังก์ชันคงตัวที่นิยามโดย $1(x) = 1$ ทุกๆ $x \in \mathbb{R}$ แล้วเห็นชัดว่าเซต $J = \{f \in \Im(\mathbb{R}) | f(0) = 0\}$ เป็นไอดีลของ $\Im(\mathbb{R})$

ให้ $1_{\mathbb{R}}$ เป็นฟังก์ชันเอกลักษณ์นั่นคือ $1_{\mathbb{R}}(x) = x$ ทุกๆ $x \in \mathbb{R}$ และให้ $g \in \Im(\mathbb{R}) \setminus J$ แล้ว $g(0) \neq 0$ ทำให้ $(1_{\mathbb{R}}^2 + g^2)(x) \neq 0$ ทุกๆ $x \in \mathbb{R}$ จึงได้ว่า $1_{\mathbb{R}}^2 + g^2$ เป็นสมาชิกที่มีตัวผกผันใน $\Im(\mathbb{R})$ และ $1_{\mathbb{R}}^2 + g^2 \in (J,g) = \{h + fg | h \in J, f \in \Im(\mathbb{R})\}$ ดังนั้นผลคูณของตัวผกผันของ $1_{\mathbb{R}}^2 + g^2$ กับ $1_{\mathbb{R}}^2 + g^2$ คือฟังก์ชันคงตัว 1 จะเป็นสมาชิกของ (J,g) ซึ่งแสดงว่า $(J,g) = \Im(\mathbb{R})$ นั่นคือ J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ❍

4.4.10 **ข้อสังเกต** ให้ R เป็นริงและ $\Re$ แทนเซตของไอดีลแท้ทั้งหมดของ R แล้ว $\Re$ เป็นเซตอันดับโดยความสัมพันธ์ "เซตย่อย" ทำให้ได้ว่า J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R ก็ต่อเมื่อ J เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มของ $\Re$ นอกจากนี้ขอละการพิสูจน์ซึ่งใช้การประยุกต์ "ทฤษฎีบทประกอบของซอร์น (Zorn's Lemma)" ไว้เป็นแบบฝึกหัดว่า

"ริงมีเอกลักษณ์ $R \neq \{0\}$ มีไอดีล M ซึ่งเป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R ยิ่งไปกว่านั้นแต่ละไอดีล J ของ R มีไอดีลใหญ่สุดเฉพาะกลุ่ม M ของ R ซึ่ง J เป็นริงย่อยของ M"

ทฤษฎีบทต่อไปแสดงการจำแนกไอดีลใหญ่สุดเฉพาะกลุ่ม

4.4.11 **ทฤษฎีบท** ให้ J เป็นไอดีลของริงสลับที่มีเอกลักษณ์ R ซึ่ง $J \neq R$ แล้ว J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R ก็ต่อเมื่อ R/J เป็นฟีลด์

บทพิสูจน์ ให้ R เป็นริงสลับที่มีเอกลักษณ์และ $J \neq R$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R แล้ว R/J เป็นริงสลับที่มี $1+J$ เป็นเอกลักษณ์ จึงเหลือเพียงแสดงว่าแต่ละสมาชิกของ R/J ที่ไม่ใช่ J มีตัวผกผัน โดยให้ $a \notin J$ แล้วโดยทฤษฎีบท 4.4.7 จะได้ $R = <J,a> = \{j+ra \mid j \in J, r \in R\}$ แต่ $1 \in R$ จึงมี $j \in J$ และ $r \in R$ ซึ่ง $1 = j+ra$ นั่นคือ $1-ra = j \in J$ ทำให้ได้ $1+J = ra+J$ แต่ $ra+J = (r+J)(a+J)$ ซึ่งแสดงว่า $r+J$ เป็นตัวผกผันของ $a+J$ ใน R/J

ในทางกลับกันเมื่อให้ R/J เป็นฟีลด์และ K เป็นไอดีลของ R ซึ่ง $J \subset K \subseteq R$ แล้ว $1 \notin J$ และมี $a \in K$ ซึ่ง $a \notin J$ ดังนั้น $a+J \neq J$ และเพราะ R/J เป็นฟีลด์ที่มี J เป็นศูนย์จึงมี $r+J \in R/J$ ซึ่ง $(r+J)(a+J) = 1+J$ ดังนั้น $1+J = ra+J$ ซึ่งสมมูลกับ $1-ra \in J$ แต่ $J \subset K$ ทำให้ $1-ra \in K$ โดยที่ $ra \in K$ จึงมี $k \in K$ ซึ่ง $1 = k+ra \in K$ ทำให้ได้ $K = R$ เพราะฉะนั้น J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R ❑

4.4.12 **ตัวอย่าง** สังเกตว่าไอดีลมุขสำคัญ $<4> = 4\mathbb{Z}$ ในริงสลับที่ซึ่งไม่มีเอกลักษณ์ E ของจำนวนเต็มคู่ทั้งหมด เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม เพราะถ้า $n \in E$ โดยที่ $n \notin <4>$ แล้ว n เป็นจำนวนเต็มคู่ซึ่งไม่เป็นจำนวนประกอบของ 4 ดังนั้นโดยขั้นตอนการหารจะมีจำนวนเต็ม m ซึ่ง $n = 4m+2$ ทำให้ได้ $2 = n-4m = n+4(-m) \in <<4>,n>$ และได้ $E = <2> = <<4>,n>$

สังเกตว่า $(2+<4>)(2+<4>) = 4+<4> = <4>$ ซึ่งแสดงว่า $2+<4>$ เป็นตัวหารของศูนย์ในริงผลหาร $E/<4>$ ดังนั้น $E/<4>$ ไม่เป็นฟีลด์ ○

ตัวอย่าง 4.4.12 แสดงให้เห็นว่าเงื่อนไขการมีเอกลักษณ์ของริงในทฤษฎีบท 4.4.11 มีความสำคัญต่อการเป็นฟีลด์ของริงผลหาร R/J หรือ J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม

เราได้รู้จักและจำแนกหมู่ของไอดีลเฉพาะและหมู่ของไอดีลใหญ่สุดเฉพาะกลุ่มของริงสลับที่มีเอกลักษณ์แล้ว จึงอาจมีคำถามว่าหมู่ของไอดีลทั้งสองเป็นหมู่เดียวกันหรือไม่ หรือมีความสัมพันธ์กันเช่นใด เราจะแสดงในตัวอย่างต่อไปว่าหมู่ของไอดีลทั้งสองไม่เป็นหมู่เดียวกัน

4.4.13 **ตัวอย่าง** ในริงผลคูณตรง $\mathbb{Z}\times\mathbb{Z}$ เห็นได้ชัดว่าริงย่อย $\mathbb{Z}\times\{0\}$ เป็นไอดีลเฉพาะของ $\mathbb{Z}\times\mathbb{Z}$ และ $\mathbb{Z}\times E$ ก็เป็นไอดีลของ $\mathbb{Z}\times\mathbb{Z}$ ยิ่งไปกว่านั้น $\mathbb{Z}\times\{0\}\subset\mathbb{Z}\times E\subset\mathbb{Z}\times\mathbb{Z}$ ทำให้เห็นตัวอย่างของริงที่มีริงย่อยเป็นไอดีลเฉพาะแต่ไม่เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ○

ทฤษฎีบทต่อไปแสดงว่าหมู่ของไอดีลใหญ่สุดเฉพาะกลุ่มเป็นเซตย่อยของหมู่ของไอดีลเฉพาะ (จึงไม่มีตัวอย่างของริงที่ประกอบด้วยไอดีลใหญ่สุดเฉพาะกลุ่มที่ไม่เป็นไอดีลเฉพาะ)

4.4.14 **ทฤษฎีบท** ถ้า J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของริงสลับที่มีเอกลักษณ์ R แล้ว J เป็นไอดีลเฉพาะของ R

บทพิสูจน์ ให้ J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R และให้ $a,b\in R$ โดยที่ $ab\in J$ แต่ $a\notin J$ โดยทฤษฎีบท 4.4.7 จะได้ $<J,a>=R$ แต่ $1\in R$ จึงมี $j\in J$ และ $r\in R$ ซึ่ง $1=j+ra$ และเพราะ $j\in J$ และ $ab\in J$ ดังนั้น $b=1b=(j+ra)b=jb+r(ab)\in J$ จึงได้ J เป็นไอดีลเฉพาะ ❑

ทฤษฎีบทต่อไป แสดงว่าในโดเมนของไอดีลมุขสำคัญ หมู่ของไอดีลทั้งสองเป็นหมู่เดียวกัน

4.4.15 **ทฤษฎีบท** ให้ R เป็นโดเมนของไอดีลมุขสำคัญแล้ว $J\neq\{0\}$ เป็นไอดีลเฉพาะของ R ก็ต่อเมื่อ J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R

บทพิสูจน์ เราเหลือเพียงแสดงว่าถ้า $J\neq\{0\}$ เป็นไอดีลเฉพาะของ R แล้ว J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม โดยให้ J เป็นไอดีลเฉพาะของ R และให้ K เป็นไอดีลของ R ซึ่ง $J\subset K\subseteq R$ แต่ R เป็นโดเมนของไอดีลมุขสำคัญ จึงมี $a,b\in R\setminus\{0\}$ ซึ่ง $J=<a>$ และ $K=<b>$ ดังนั้น $a\in<a>\subset<b>$ จะมี $r\in R$ ซึ่ง $a=rb\in J$ แต่ J เป็นไอดีลเฉพาะ จึงได้ $r\in<a>$ หรือ $b\in<a>$

ถ้า $b\in<a>$ แล้ว $J=K$ จะขัดแย้งกับสมมติฐาน ดังนั้น $r\in<a>$ ทำให้มี $s\in R$ ซึ่ง $r=sa$ จึงได้ $a=rb=(sa)b=a(sb)$ แต่จาก R เป็นอินทิกรัลโดเมนและ $a\neq 0$ จะได้ว่า $sb=1$ ซึ่งแสดงว่า b เป็นหน่วย ดังนั้น $K=<b>=R$ ทำให้ได้ J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ❑

4.4.16 **บทแทรก** ไอดีล $<a>$ ของโดเมน $\mathbb{Z}$ เป็นไอดีลเฉพาะ ก็ต่อเมื่อ $<a>$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ซึ่งก็ต่อเมื่อ a เป็นจำนวนเฉพาะ ❑

แบบฝึกหัด 4.4

1. ให้ R เป็นริงสลับที่มีเอกลักษณ์ $a \in R$ และ U เป็นไอดีลของ R จงพิสูจน์ว่า
   1.1 a ผกผันได้ ก็ต่อเมื่อ $a \notin J$ ทุกๆ ไอดีลใหญ่สุดเฉพาะกลุ่ม J ของ R
   1.2 R เป็นฟีลด์ ก็ต่อเมื่อ $\{0\}$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R
   1.3 $<U,a> = \{u + ar \mid u \in U, r \in R\}$ เป็นไอดีลเล็กสุดซึ่งก่อกำเนิดโดยเซต $U \cup \{a\}$
2. จงแสดงว่ามีไอดีลใหญ่สุดเฉพาะกลุ่ม K ของริงของจำนวนเต็มคู่ E ซึ่ง E/K ไม่เป็นฟีลด์
3. ให้ U และ V เป็นไอดีลของริง R จงแสดงว่า $U \cup V$ อาจไม่เป็นไอดีลของ R แต่ $U + V = \{u + v \mid u \in U, v \in V\}$ เป็นไอดีลเล็กสุดของ R ซึ่งบรรจุ $U \cup V$
4. ให้ $\{U_i \mid i = 1,2,\ldots\}$ เป็นหมู่ของไอดีลของริง R ซึ่ง $U_1 \subseteq U_2 \subseteq \cdots \subseteq U_n \subseteq \cdots$ จงแสดงว่า JU_i เป็นไอดีลของ R ทุกๆ ไอดีล J ของ R และทุกๆ $i = 1,2,\ldots$
5. จงพิสูจน์ว่าข้อความต่อไปนี้สมมูลกัน
   (ก) U และ V ต่างเป็นไอดีลขวาของริง R ซึ่ง $UV \subseteq J$ แล้ว $U \subseteq J$ หรือ $V \subseteq J$
   (ข) ถ้า U และ V ต่างเป็นไอดีลซ้ายขอริง R ซึ่ง $UV \subseteq J$ แล้ว $U \subseteq J$ หรือ $V \subseteq J$
6. ให้ R เป็นริง (อาจไม่ใช่ริงสลับที่) และ J เป็นไอดีลของ R ข้อความต่อไปนี้สมมูลกัน
   (ก) J เป็นไอดีลเฉพาะ
   (ข) ถ้า $a,b \in R$ ซึ่ง $aRb \subseteq J$ แล้ว $a \in J$ หรือ $b \in J$ [ข้อแนะนำ : ถ้า (ก) เป็นจริงและ $a,b \in R$ ซึ่ง $aRb \subseteq J$ แล้ว $(RaR)(RbR) \subseteq J$ จงพิสูจน์ว่า $RaR \subseteq J$ หรือ $RbR \subseteq J$ ในกรณี $RaR \subseteq J$ ถ้า $A := <a>$ แล้ว $A^3 \subseteq RaR \subseteq J$ และพิสูจน์ว่า $a \in A \subseteq J$]
   (ค) ถ้า $a,b \in R$ โดยที่ $<a>$ และ $<b>$ เป็นไอดีลมุขสำคัญซึ่ง $<a><b> \subseteq J$ แล้ว $a \in J$ หรือ $b \in J$
7. ให้ R เป็นริงสลับที่มีเอกลักษณ์และ $J \neq R$ เป็นไอดีลของ R ข้อความต่อไปนี้สมมูลกัน
   (ก) J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม
   (ข) สำหรับแต่ละ $r \notin J$ มี $a \in R$ ซึ่ง $1 - ra \in J$
   (ค) $K \subseteq J$ หรือ $J + K = R$ ทุกๆ ไอดีล K ของ R
8. ให้ R เป็นริงของฟังก์ชันค่าจริงซึ่งต่อเนื่องบนช่วงปิดหน่วย $[0,1]$ จงแสดงว่าเซต $\{f \in R \mid f(\frac{1}{2}) = 0\}$ เป็นไอดีลและเป็นไอดีลใหญ่สุดเฉพาะกลุ่มของ R
9. ให้ R เป็นริงสลับที่มีเอกลักษณ์ $1 \neq 0$ และ J เป็นไอดีลของ R จงแสดงว่า
   9.1 ถ้า R/J เป็นริงการหารแล้ว J เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม
   9.2 ถ้า J เป็นไอดีลใหญ่สุดเฉพาะกลุ่มและ R ไม่ใช่ริงสลับที่แล้ว R/J เป็นริงการหาร

4.5 สาทิสสัณฐานและทฤษฎีบทหลักมูล

ดังกล่าวไว้ในเรื่องกรุปว่า เราสนใจการจำแนกกรุปที่มีโครงสร้างเหมือนกันหรือที่เรียกว่าสมสัณฐานกัน และได้เห็นแล้วว่ามโนคติของสาทิสสัณฐานส่งผลดีต่อการศึกษาสมบัติของกรุป ทั้งนี้เพราะสาทิสสัณฐานเป็นฟังก์ชันระหว่างกรุปซึ่งยืนยงการดำเนินการของกรุปทั้งสอง นอกจากนี้การศึกษาสมบัติมูลฐานของริง เราศึกษาแบบคู่ขนานกับสมบัติมูลฐานของกรุป ในเมื่อทฤษฎีกรุปกล่าวถึงการจำแนกภาพสาทิสสัณฐานทั้งหมด ในหัวข้อนี้เราจึงให้นิยามของสาทิสสัณฐานของริงในลักษณะภาคขยายสาทิสสัณฐานของกรุป และพิสูจน์ทฤษฎีบทหลักมูลของริงซึ่งแสดงการจำแนกภาพสาทิสสัณฐานทั้งหมดของริง

4.5.1 **บทนิยาม** ให้ R และ S เป็นริงและ $\theta : R \to S$ เรากล่าวว่า θ เป็น *สาทิสสัณฐาน (homomorphism)* ถ้าทุกๆ $a,b \in R$ (ก) $\theta(a+b) = \theta(a)+\theta(b)$ และ (ข) $\theta(ab) = \theta(a)\theta(b)$

ถ้าสาทิสสัณฐาน θ เป็นชนิดหนึ่งต่อหนึ่งและทั่วถึง จะเรียก θ ว่า *สมสัณฐาน (isomorphism)* และถ้ามีสมสัณฐานจาก R ไปยัง S จะกล่าวว่า R *สมสัณฐานกับ (isomorphic)* S และแทนด้วยสัญลักษณ์ $R \cong S$

ถ้า θ เป็นสมสัณฐานจาก R ไปบน R จะเรียก θ ว่า *อัตสัณฐาน (automorphism)*

เช่นเดียวกับสาทิสสัณฐานของกรุป การดำเนินการ "การบวก" และ "การคูณ" ทางซ้ายมือและทางขวามือของสมการ (ก) และ (ข) ในบทนิยาม 4.5.1 เป็น "การบวก" และ "การคูณ" ในริง R และในริง S ตามลำดับ และเพราะริงประกอบด้วยโครงสร้างที่เป็นกรุปการบวก (อาบีเลียน) ความจริงเกี่ยวกับสาทิสสัณฐานของกรุป จึงเป็นจริงสำหรับกรุปการบวกในริงด้วย โดยเฉพาะการยืนยง "ศูนย์" และ "สมาชิกลบ"

ตัวอย่างเช่นถ้า R และ S เป็นริงและ $\theta : R \to S$ เป็นฟังก์ชันซึ่งส่งทุกๆ สมาชิกใน R ไปที่ศูนย์ของ S เป็นสาทิสสัณฐาน (ซึ่งเรียกว่า *สาทิสสัณฐานศูนย์ (zero homomorphism)*) เพราะ $\theta(a+b) = 0 = 0+0 = \theta(a)+\theta(b)$ และ $\theta(ab) = 0 = 0\cdot 0 = \theta(a)\theta(b)$ ทุกๆ $a,b \in R$ แต่ $\theta : \mathbb{Z} \to 2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ นิยามโดย $\theta(n) = 2n$ ทุกๆ $n \in \mathbb{Z}$ ไม่เป็นสาทิสสัณฐาน เพราะจะมี $m,n \in \mathbb{Z}$ ที่ไม่ใช่ศูนย์ทั้งคู่ ซึ่งทำให้ $\theta(mn) = 2mn \neq 4mn = (2m)(2n) = \theta(m)\theta(n)$ เช่นถ้าให้ $m = n = 1$ แล้ว $\theta(mn) = \theta(1) = 2 \neq 4 = 2(1)2(1)$ เป็นต้น อย่างไรก็ตามถ้า n เป็นจำนวนเต็มบวกแล้ว $\theta : \mathbb{Z} \to \mathbb{Z}_n$ ซึ่งนิยามโดย $\theta(k) = \overline{k}$ เป็นสาทิสสัณฐานชนิดทั่วถึง

4.5.2 **ตัวอย่าง** ให้ $\theta:\mathbb{Z}\to\mathbb{Z}$ เป็นสาทิสสัณฐานและ $n\in\mathbb{Z}$ ถ้า $n>0$ แล้ว $\theta(n)=\theta(\underbrace{1+\cdots+1}_{\text{n times}})$ $=\underbrace{\theta(1)+\cdots+\theta(1)}_{\text{n times}}=n\theta(1)$ ถ้า $n<0$ แล้ว $-n>0$ จะได้โดยกรณีของจำนวนเต็มบวกว่า $\theta(n)=$ $-\theta(-n)=-(-n)\theta(1)=n\theta(1)$ และ $\theta(0)=0=0\theta(1)$ จึงสรุปได้ว่า $\theta(n)=n\theta(1)$ ทุกๆ $n\in\mathbb{Z}$ และเพราะ $\theta(1)=\theta(1\cdot 1)=\theta(1)^2$ ซึ่งสมมูลกับ $\theta(1)(\theta(1)-1)=0$ ดังนั้น $\theta(1)=0$ หรือ $\theta(1)=1$

ถ้า $\theta(1)=0$ แล้ว $\theta(n)=n\theta(1)=n0=0$ ทุกๆ $n\in\mathbb{Z}$ จะได้ θ เป็นฟังก์ชันศูนย์ แต่ถ้า $\theta(1)=1$ แล้ว $\theta(n)=n\theta(1)=n1=n$ ทุกๆ $n\in\mathbb{Z}$ จะได้ $\theta=1_{\mathbb{Z}}$ เป็นฟังก์ชันเอกลักษณ์ ❍

ตัวอย่าง 4.5.2 แสดงว่าถ้า R เป็นริงซึ่งสมสัณฐานกับ $\mathbb{Z}$ แล้วจะมีสมสัณฐานระหว่าง R กับ $\mathbb{Z}$ เพียงหนึ่งเดียวเท่านั้น ทั้งนี้เพราะถ้า f และ g ต่างเป็นสมสัณฐานระหว่าง R กับ $\mathbb{Z}$ แล้ว $f\circ g^{-1}$ จะเป็นสมสัณฐานจาก $\mathbb{Z}$ ไปยัง $\mathbb{Z}$ ซึ่ง $f\circ g^{-1}$ ไม่เป็นฟังก์ชันศูนย์ (เพราะว่าฟังก์ชันศูนย์ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง) ทำให้ได้ $f\circ g^{-1}=1_{\mathbb{Z}}$ ซึ่งสมมูลกับ $f=g$

แม้ R และ S เป็นริงมีเอกลักษณ์ 1 และ $1'$ ตามลำดับและ $\theta:R\to S$ เป็นสาทิสสัณฐานที่ไม่ใช่ศูนย์ ก็ไม่จำเป็นที่ $\theta(1)=1'$ และในกรณี $\theta(1)\neq 1'$ แล้ว $\theta(1)$ อาจเป็นตัวหารของศูนย์ใน S เพราะ $\theta(1)(\theta(1)-1')=\theta(1)\theta(1)-\theta(1)1'=\theta(1\cdot 1)-\theta(1)=\theta(1)-\theta(1)=0$ โดยที่ $\theta(1)-1'$ ไม่ใช่ศูนย์ใน S หรือแม้ $u\in R$ เป็นหน่วยก็ตาม $\theta(1)$ ก็อาจไม่เป็นหน่วย อย่างไรก็ตามถ้า S เป็นอินทิกรัลโดเมนหรือ θ เป็นชนิดทั่วถึง แล้ว $\theta(1)=1'$

4.5.3 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากริง R ไปยังริง S

1. $\theta(0)=0$ และ $\theta(-a)=-\theta(a)$ ทุกๆ $a\in R$
2. ถ้า R และ S เป็นริงมีเอกลักษณ์ 1 และ $1'$ ตามลำดับและ $\theta(R)=S$ แล้ว $\theta(1)=1'$
3. ถ้า R เป็นอินทิกรัลโดเมนที่มีเอกลักษณ์ 1 และ S เป็นริงมีเอกลักษณ์ $1'$ และ $u\in R$ เป็นหน่วยซึ่ง $\theta(u)$ เป็นหน่วยแล้ว $\theta(1)=1'$ และ $\theta(u^{-1})=\theta(u)^{-1}$

บทพิสูจน์ 1. เห็นได้ชัด จึงจะพิสูจน์เฉพาะข้อ 2 และข้อ 3

2. ให้ $v\in S$ แล้วเพราะ $\theta(R)=S$ จะมี $u\in R$ ซึ่ง $\theta(u)=v$ จะได้ $\theta(1)v=\theta(1)\theta(u)=$ $\theta(1u)=\theta(u)=v$ ซึ่งแสดงว่า $\theta(1)$ เป็นเอกลักษณ์ของ S แต่เอกลักษณ์ของ S มีเพียงหนึ่งเดียว จึงได้ $\theta(1)=1'$

3. ให้ $u\in R$ เป็นหน่วยซึ่ง $\theta(u)$ เป็นหน่วย แล้ว $u\neq 0$ และ $\theta(u)\neq 0$ และทั้งคู่ไม่เป็นตัวหารของศูนย์ และเพราะ $\theta(u)(\theta(1)-1')=\theta(u)\theta(1)-\theta(u)1'=\theta(u\cdot 1)-\theta(u)=\theta(u)-\theta(u)$ $=0$ ดังนั้น $\theta(1)-1'=0$ ทำให้ได้ $\theta(1)=1'$ นอกจากนี้ $\theta(u^{-1})\theta(u)=\theta(u^{-1}u)=\theta(1)=1'$ ซึ่งแสดงว่า $\theta(u^{-1})$ เป็นตัวผกผันของ $\theta(u)$ ใน S ดังนั้น $\theta(u^{-1})=\theta(u)^{-1}$ ❑

4.5.4 **ทฤษฎีบท** ให้ θ เป็นสาทิสสัณฐานจากริง R ไปยังริง S

1. ถ้า $\bar{R}$ เป็นริงย่อยของ R แล้ว $\theta(\bar{R})$ เป็นริงย่อยของ S
2. ถ้า $\bar{S}$ เป็นริงย่อยของ S แล้ว $\theta^{-1}(\bar{S})$ เป็นริงย่อยของ R

บทพิสูจน์ โดยทฤษฎีกรุป $\theta(\bar{R})$ และ $\theta^{-1}(\bar{S})$ เป็นกรุปย่อยของกรุป S และ R ตามลำดับ จึงเหลือเพียงแสดงว่า $\theta(\bar{R})$ และ $\theta^{-1}(\bar{S})$ มีสมบัติปิดการคูณของ S และ R ตามลำดับ ซึ่งจะแสดงการพิสูจน์กรณีของ $\theta(\bar{R})$ เท่านั้น ให้ $x, y \in \theta(\bar{R})$ แล้วมี $a, b \in \bar{R}$ ซึ่ง $x = \theta(a)$ และ $y = \theta(b)$ ทำให้ได้ $xy = \theta(a)\theta(b) = \theta(ab)$ และเพราะ $\bar{R}$ เป็นริงย่อยของ R ดังนั้น $ab \in \bar{R}$ จึงได้ $xy \in \theta(\bar{R})$ ❑

ขอละการพิสูจน์ไว้เป็นแบบฝึกหัดว่า ถ้าสาทิสสัณฐานเป็นชนิดทั่วถึงแล้วทฤษฎีบท 4.5.4 จะเป็นจริงสำหรับ $\bar{R}$ เป็นไอดีลของ R และ $\bar{S}$ เป็นไอดีลของ S ด้วย

4.5.5 **บทนิยาม** กล่าวว่าริง R *ถูกฝัง (embedded)* ในริง S ถ้ามีริงย่อย $\bar{S}$ ของ S ซึ่ง $R \cong \bar{S}$ และในกรณีที่ R ถูกฝังใน S จะกล่าวว่า S เป็น *ภาคขยาย (extension)* ของ R

4.5.6 **ทฤษฎีบท** ทุกๆ ริงถูกฝังในริงมีเอกลักษณ์

บทพิสูจน์ ให้ R เป็นริง แล้วกรุปผลบวกตรง $S = R \oplus \mathbb{Z}$ เป็นกรุปอาบีเลียนและนิยาม "การคูณ" บน S โดย $(r_1, k_1)(r_2, k_2) = (r_1r_2 + k_2r_1 + k_1r_2, k_1k_2)$ ทุกๆ $r_1, r_2 \in R$ และ $k_1, k_2 \in \mathbb{Z}$ แล้วการคำนวณโดยตรงแสดงว่า S เป็นริงที่มี $(0,1)$ เป็นเอกลักษณ์ นอกจากนี้เห็นชัดว่า $R \oplus \{0\}$ เป็นริงย่อยของ S และ $\theta : R \to R \oplus \{0\}$ ซึ่งนิยามโดย $\theta(r) = (r, 0)$ ทุกๆ $r \in R$ เป็นสมสัณฐาน ❑

จากบทนิยามของสาทิสสัณฐานของริง ถ้า θ เป็นสาทิสสัณฐานจากริง R ไปยังริง S แล้ว θ เป็นสาทิสสัณฐานระหว่างกรุปอาบีเลียน และในทฤษฎีกรุปเราสนใจส่วนกลางของ θ นั่นคือเซต

$$\ker\theta = \{x \in R \mid \theta(x) = 0\}$$

ซึ่งเป็นกรุปย่อยปรกติของกรุปอาบีเลียน R และเป็นตัวกำหนดกรุปผลหาร จึงนิยาม $\ker\theta$ เป็น *ส่วนกลาง (kernel)* ของริง และสนใจว่า $\ker\theta$ ของริงเป็นไอดีลหรือไม่

4.5.7 **ทฤษฎีบท** ให้ R และ S เป็นริง

1. ถ้า $\theta : R \to S$ เป็นสาทิสสัณฐานแล้ว $\ker\theta$ เป็นไอดีลของ R นอกจากนี้ $\ker\theta = \{0\}$ ก็ต่อเมื่อ θ เป็นชนิดหนึ่งต่อหนึ่ง
2. ถ้า J เป็นไอดีลของ R แล้ว $\pi : R \to R/J$ นิยามโดย $\pi(a) = a + J$ ทุกๆ $a \in R$ เป็นสาทิสสัณฐานชนิดทั่วถึง และเรียก π ว่า *สาทิสสัณฐานธรรมชาติ (natural homomorphism)*

บทพิสูจน์ 1. เพราะ $\ker\theta$ เป็นกรุปย่อยอาบีเลียนของกรุปการบวก R จึงเหลือเพียงแสดงว่า $\ker\theta$ สอดคล้องสมบัติดูดกลืนการคูณ โดยให้ $a \in \ker\theta$ และ $r \in R$ แล้ว $\theta(ar) = \theta(a)\theta(r) = 0\theta(r) = 0$ และ $\theta(ra) = \theta(r)\theta(a) = \theta(r)0 = 0$ ซึ่งแสดงว่า $ar, ra \in \ker\theta$ ส่วน $\ker\theta = \{0\}$ ก็ต่อเมื่อ θ เป็นชนิดหนึ่งต่อหนึ่ง เป็นผลโดยตรงจากทฤษฎีกรุป

2. โดยทฤษฎีกรุปการส่งธรรมชาติ π เป็นสาทิสสัณฐานของกรุปชนิดทั่วถึง จึงเหลือเพียงแสดงว่า π ยืนยงการคูณ โดยให้ $a, b \in R$ จากนิยามของ π และนิยามการคูณของโคเซตจะได้ $\pi(ab) = ab + J = (a+J)(b+J) = \pi(a)\pi(b)$ ❑

4.5.8 **ตัวอย่าง** ให้ R เป็นริงมีเอกลักษณ์และ $\theta : \mathbb{Z} \to R$ นิยามโดย $\theta(n) = n1 = \underbrace{1+\cdots+1}_{n\ times}$ ทุกๆ $n \in \mathbb{Z}$ แล้ว $\theta(n+m) = (n+m)1 = \underbrace{1+\cdots+1}_{n+m\ times} = \underbrace{1+\cdots+1}_{n\ times} + \underbrace{1+\cdots+1}_{m\ times} = n1 + m1 = \theta(n) + \theta(m)$

และ $\theta(nm) = (nm)1 = \underbrace{1+\cdots+1}_{nm\ times} = \underbrace{\underbrace{1+\cdots+1}_{m\ times} + \cdots + \underbrace{1+\cdots+1}_{m\ times}}_{n\ times} = \underbrace{m1+\cdots+m1}_{n\ times} = n(m1) =$

$n(1 \cdot m1) = (n1)(m1) = \theta(n)\theta(m)$ ทุกๆ $n, m \in \mathbb{Z}$ ซึ่งแสดงว่า θ เป็นสาทิสสัณฐานโดยมีส่วนกลางคือ $\ker\theta = \{n \in \mathbb{Z} | n1 = 0\}$ ดังนั้น $\ker\theta = <p>$ เมื่อ $p > 0$ เป็นค่าลักษณะเฉพาะของ R แต่ถ้าค่าลักษณะเฉพาะของ R เป็นศูนย์แล้วเห็นชัดว่า $\mathbb{Z}1 = \{n1 | n \in \mathbb{Z}\}$ เป็นริงย่อยของ R (ที่มีเอกลักษณ์เป็นตัวเดียวกับของ R) ซึ่งสมสัณฐานกับ $\mathbb{Z}$ ❍

ทฤษฎีบทหลักมูลของสาทิสสัณฐาน บทแทรกและทฤษฎีบทที่หนึ่ง ที่สองและที่สามของสมสัณฐานสำหรับริงต่อไปนี้ พิสูจน์ได้ในทำนองเดียวกันกับกรณีของกรุปซึ่งได้แสดงไว้ในบทที่ 1 แล้วจึงขอละการพิสูจน์ทฤษฎีบทและบทแทรกเหล่านี้ไว้เป็นแบบฝึกหัด

4.5.9 **ทฤษฎีบทหลักมูลของสาทิสสัณฐาน** (Fundamental Theorem of Homomorphism)

ให้ $\theta : R \to S$ เป็นสาทิสสัณฐานของริงและ J เป็นไอดีลของริง R ซึ่ง $J \subseteq \ker\theta$ แล้วมีสาทิสสัณฐาน $\overline{\theta} : R/J \to S$ เพียงหนึ่งเดียวซึ่ง $\overline{\theta}(a+J) = \theta(a)$ ทุกๆ $a \in R$, $\operatorname{Im}\overline{\theta} = \operatorname{Im}\theta$ และ $\ker\overline{\theta} = (\ker\theta)/J$ ยิ่งไปกว่านั้น $\overline{\theta}$ เป็นสมสัณฐานก็ต่อเมื่อ θ เป็นชนิดทั่วถึงและ $J = \ker\theta$

❑

4.5.10 **ตัวอย่าง** ให้ $\mathbb{Z}_4$ และ $\mathbb{Z}_2$ เป็นริงของเรซิดิวคลาสมอดูโล 4 และ 2 ตามลำดับและนิยาม $\theta : \mathbb{Z}_4 \to \mathbb{Z}_2$ โดย $\theta(0) = \theta(2) = 0$ และ $\theta(1) = \theta(3) = 1$ แล้วเห็นชัดว่า θ เป็นสาทิสสัณฐานชนิดทั่วถึงโดยที่ $\ker\theta = \{0, 2\}$ ดังนั้น $\mathbb{Z}_4/(\ker\theta) = \{\{0,2\},\{1,3\}\}$ สมสัณฐานกับ $\mathbb{Z}_2$ ❍

4.5.11 **ข้อสังเกต**

1. โดยทฤษฎีบทมูลฐานของสาทิสสัณฐานและผลที่กล่าวไว้ท้ายตัวอย่าง 4.5.2 ทำให้พิสูจน์ได้ไม่ยากว่า แต่ละไอดีล J ของริง R มีสาทิสสัณฐาน θ จาก R ไปบน $\mathbb{Z}$ เพียงหนึ่งเดียวที่ทำให้ $J = \ker\theta$ ซึ่งต่างจากในทฤษฎีของกรุปเพราะ $\iota_{\mathbb{Z}}$ และ $-\iota_{\mathbb{Z}}$ เป็นสาทิสสัณฐานที่ต่างกันจากกรุปการบวก $\mathbb{Z}$ ไปบน $\mathbb{Z}$ โดยที่ $\ker\iota_{\mathbb{Z}} = \ker(-\iota_{\mathbb{Z}}) = \{0\}$

2. ถ้ามีสาทิสสัณฐาน θ จากริง $\mathbb{Z}$ ไปบนฟีลด์ F แล้ว F เป็นฟีลด์จำกัด เพราะทฤษฎีบทหลักมูลของสาทิสสัณฐานทำให้ได้ $\mathbb{Z}/(\ker\theta) \cong F$ โดย $\mathbb{Z}$ ไม่สมสัณฐานกับ F (เพราะ F เป็นฟีลด์ แต่ $\mathbb{Z}$ ไม่เป็นฟีลด์) ดังนั้น $\ker\theta$ ไม่ใช่ไอดีลศูนย์ของ $\mathbb{Z}$ และเพราะ $\mathbb{Z}$ เป็นโดเมนของไอดีลหลัก จะมีจำนวนเต็มบวก n ซึ่ง $\ker\theta = <n>$ เพราะฉะนั้น $F \cong \mathbb{Z}/(\ker\theta) = \mathbb{Z}/<n> \cong \mathbb{Z}_n$ ทำให้ได้ว่า n เป็นจำนวนเฉพาะและ F เป็นฟีลด์จำกัด

3. ถ้าโดเมน F ของสาทิสสัณฐาน θ ระหว่างริง เป็นฟีลด์แล้ว θ เป็นฟังก์ชันศูนย์หรือฟังก์ชันชนิดหนึ่งต่อหนึ่ง เพราะ $\ker\theta$ เป็นไอดีลของฟีลด์ และฟีลด์ประกอบด้วยริงย่อยชัดเท่านั้น ดังนั้น $\ker\theta = \{0\}$ หรือ $\ker\theta = F$ ในกรณี $\ker\theta = \{0\}$ จะได้ θ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง และในกรณี $\ker\theta = F$ จะได้ว่า θ ส่งทุกๆ สมาชิกของ F ไปยังศูนย์ นั่นคือ θ เป็นฟังก์ชันศูนย์

4.5.12 **ทฤษฎีบทที่หนึ่งของสมสัณฐาน** (First Isomorphism Theorem)

ถ้า $\theta : R \to S$ เป็นสาทิสสัณฐานของริงแล้ว θ ชักนำสมสัณฐาน $R/(\ker\theta) \cong \operatorname{Im}\theta$ ❑

4.5.13 **บทแทรก** ถ้า $\theta : R \to S$ เป็นสาทิสสัณฐานของริง J เป็นไอดีลของ R และ K เป็นไอดีลของ S ซึ่ง $\theta(J) \subseteq K$ แล้ว

1. θ ชักนำสาทิสสัณฐาน $\bar{\theta} : R/J \to S/K$ ซึ่งนิยามโดย $\bar{\theta}(a+J) = \theta(a) + K$ ทุกๆ $a \in R$
2. $\bar{\theta}$ เป็นสมสัณฐาน ก็ต่อเมื่อ $\operatorname{Im}\theta + K = S$ และ $\theta^{-1}(K) \subseteq J$
3. ถ้า θ เป็นชนิดทั่วถึงซึ่ง $\theta(J) = K$ และ $\ker\theta \subseteq J$ แล้ว $\bar{\theta}$ เป็นสมสัณฐาน ❑

4.5.14 **ทฤษฎีบทที่สองและที่สามของสมสัณฐาน** (Second and Third Isomorphism Theorem)

ให้ J และ K เป็นไอดีลของริง R แล้ว $J/(J \cap K) \cong (J+K)/K$

ยิ่งไปกว่านั้นถ้า $J \subseteq K$ แล้ว K/J เป็นไอดีลของ R/J และ $\dfrac{R/J}{K/J} \cong R/K$ ❑

4.5.15 **ทฤษฎีบท** ถ้า J เป็นไอดีลของริง R แล้วฟังก์ชันซึ่งส่ง K ไปยัง K/J เป็นชนิดหนึ่งต่อหนึ่งและทั่วถึงระหว่างเซตของไอดีล K ทั้งหมดของ R ซึ่งบรรจุ J กับเซตของไอดีล K/J ทั้งหมดของ R/J โดยเฉพาะทุกๆ ไอดีลของ R/J อยู่ในรูปแบบ K/J เมื่อ K เป็นไอดีลของ R ซึ่งบรรจุ J ❑

แบบฝึกหัด 4.5

1. ให้ θ เป็นสาทิสสัณฐานจากริง R ไปยังริง S จงพิสูจน์ว่า $\theta(C(R)) \subseteq C(\theta(R))$ และถ้า θ เป็นฟังก์ชันทั่วถึงแล้ว $\theta(\bar{R})$ เป็นไอดีลของ S และ $\theta^{-1}(\bar{S})$ เป็นไอดีลของ R ทุกๆ ไอดีล $\bar{R}$ ของ R และไอดีล $\bar{S}$ เป็นของ S
2. ให้ R เป็นริงมีเอกลักษณ์และ $a \in R$ เป็นหน่วย จงแสดงว่า $\lambda_a : R \to R$ ซึ่งนิยามโดย $\lambda_a(x) = axa^{-1}$ เป็นอัตสัณฐาน
3. จงแสดงว่าริง $R \oplus \mathbb{Z}$ ในทฤษฎีบท 4.5.6 มีค่าลักษณะเฉพาะเป็น n ถ้า R เป็นริงที่มีค่าลักษณะเฉพาะเป็น $n > 0$ และแสดงว่า $R \oplus \mathbb{Z}$ มีตัวหารของศูนย์หรือไม่ถ้า R เป็นริงซึ่งไม่มีตัวหารของศูนย์และไม่มีเอกลักษณ์
4. ให้ R เป็นริงและ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่า
   4.1 $J_n = \{na | a \in R\}$ และ $I_n = \{a \in R | na = 0\}$ ต่างเป็นไอดีลของ R
   4.2 ถ้าจำนวนเต็ม m เป็นค่าลักษณะเฉพาะของ R/J_n แล้ว m เป็นตัวประกอบของ n
   4.3 ถ้าค่าลักษณะเฉพาะของ R เป็นจำนวนเต็ม $k \neq 0$ และค่าลักษณะเฉพาะของ R/J_n คือจำนวนเต็ม m แล้ว k เป็นตัวประกอบของ mn
5. ให้ R และ S เป็นริงของไอดีลหลักและ $\theta : R \to S$ เป็นสมสัณฐาน จงพิสูจน์ว่า $\theta(<a>) = <\theta(a)>$ ทุกๆ $a \in R$
6. ให้ S และ J เป็นริงย่อยและไอดีลของริง R ตามลำดับ จงแสดงว่าถ้า $S \cap J = \{0\}$ แล้วมีริงย่อยของ R/J_n ซึ่งสมสัณฐานกับ S
7. ให้ $\theta : R \to S$ เป็นสาทิสสัณฐานของริงและ J เป็นไอดีลของ R และ K เป็นไอดีลของ S จงพิสูจน์ว่า $\theta^{-1}(K)$ เป็นไอดีลของ R ซึ่งบรรจุ $\ker\theta$ และถ้า θ เป็นชนิดทั่วถึงแล้ว $\theta(J)$ เป็นไอดีลของ S แต่ถ้า θ ไม่เป็นชนิดทั่วถึงแล้ว $\theta(J)$ อาจไม่เป็นไอดีลของ S
8. จงพิสูจน์ว่าถ้า f และ g เป็นสาทิสสัณฐานจากฟีลด์ $\mathbb{Q}$ ไปยังริง R โดยที่ $f|_{\mathbb{Z}} = g|_{\mathbb{Z}}$ แล้ว $f = g$ [**ข้อแนะนำ**: จงแสดงว่า $f\left(\frac{1}{n}\right)g(n) = g(1)$ ทุกๆ จำนวนเต็ม $n \neq 0$ แล้วจึงพิสูจน์ว่า $f\left(\frac{1}{n}\right) = g\left(\frac{1}{n}\right)$ ทุกๆ จำนวนเต็ม $n \neq 0$]
9. ให้ θ เป็นสาทิสสัณฐานจากริง R ไปทั่วถึงริง S จงพิสูจน์ความจริงของข้อความต่อไปนี้
   9.1 R เป็นริงสลับที่ ก็ต่อเมื่อ S เป็นริงสลับที่
   9.2 R เป็นริงมีเอกลักษณ์ ก็ต่อเมื่อ S เป็นริงมีเอกลักษณ์
   9.3 u เป็นหน่วยใน R ก็ต่อเมื่อ $\theta(u)$ เป็นหน่วยใน S สำหรับแต่ละ $u \in R$
   9.4 z เป็นตัวหารของศูนย์ใน R ก็ต่อเมื่อ $\theta(z)$ เป็นตัวหารของศูนย์ใน S ทุกๆ $z \in R$

9.5 R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ S เป็นอินทิกรัลโดเมน

10. ให้ θ เป็นสาทิสสัณฐานจากริง R ไปริง S จงพิสูจน์ว่าถ้า R เป็นริงมีเอกลักษณ์ 1 และ S เป็นอินทิกรัลโดเมนแล้ว $\theta(1)=0$ หรือ $\theta(1)=1$ โดยเฉพาะถ้า $\ker\theta \neq R$ แล้ว $\theta(1)=1$

11. ให้ A แทนริง $\mathbb{R}\times\mathbb{R}$ ภายใต้การบวก + แบบปกติและการคูณนิยามโดย $(a,b)(c,d)$ $=(ac,bc)$ ทุกๆ $a,b,c\in\mathbb{R}$ และให้ $\mathrm{M}_2(\mathbb{R})$ แทนริงของเมทริกซ์ขนาด 2×2 ทั้งหมด จงแสดงว่า $\theta:\mathrm{A}\to\mathrm{M}_2(\mathbb{R})$ ซึ่งนิยามโดย $\theta(x,y)=\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$ ทุกๆ $x,y\in\mathbb{R}$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง

4.6 อินทิกรัลโดเมนและฟีลด์

เราทราบกันดีว่าจำนวนตรรกยะคือจำนวนที่เขียนได้ในรูปเศษส่วนของจำนวนเต็มโดยที่ตัวส่วนไม่เป็นศูนย์ ยิ่งไปกว่านั้น $\mathbb{Q}$ เป็นฟีลด์เล็กสุดที่ประกอบด้วยอินทิกรัลโดเมน $\mathbb{Z}$ โดยเฉพาะ $\mathbb{Q}$ เป็นฟีลด์ที่ไม่มีฟีลด์ย่อยอื่นนอกจาก $\mathbb{Q}$ ซึ่งเราเรียกฟีลด์เช่นนี้ว่า "ฟีลด์เฉพาะ" นอกจากนี้ริงสลับที่มีเอกลักษณ์ซึ่งเป็นริงย่อยของฟีลด์เป็นอินทิกรัลโดเมน จึงอาจมีคำถามในกรณีทั่วไปว่า อินทิกรัลโดเมนจะถูกฝังในฟีลด์หรือไม่ และจะมีฟีลด์เฉพาะสำหรับทุกๆ อินทิกรัลโดเมนหรือไม่ สำหรับอินทิกรัลโดเมนขนาดจำกัดซึ่งเราได้พิสูจน์แล้วว่าเป็นฟีลด์ จึงตอบคำถามนี้ในเชิงบวก ในหัวข้อนี้เราจะตอบคำถามนี้โดยการสร้างฟีลด์เล็กสุดที่ประกอบด้วยอินทิกรัลโดเมน ในลักษณะเดียวกันกับการสร้างจำนวนตรรกยะด้วยจำนวนเต็ม

สังเกตว่าถ้า F เป็นฟีลด์ซึ่ง $|F|>2$ แล้ว $\{0,1\}$ ไม่เป็นฟีลด์ย่อยของ F เพราะ $1+1\notin\{0,1\}$ ซึ่งแสดงว่า $\{0,1\}$ ไม่มีสมบัติปิดภายใต้การบวก

4.6.1 บทนิยาม กล่าวว่าฟีลด์ F เป็น*ฟีลด์เฉพาะ (prime field)* ถ้ามีเพียง F เท่านั้นที่เป็นฟีลด์ย่อยของ F

นอกจากฟีลด์ $\mathbb{Q}$ ที่เป็นตัวอย่างของฟีลด์เฉพาะดังกล่าวแล้ว ฟีลด์ $\mathbb{Z}_p$ ของจำนวนเต็มมอดูโลจำนวนเฉพาะ p ก็เป็นฟีลด์เฉพาะ เพราะทฤษฎีบทของลากรองจ์กล่าวว่า กรุปการบวก $\mathbb{Z}_p$ จะมีเพียง $\mathbb{Z}_p$ และ $\{0\}$ ที่เป็นกรุปย่อย อย่างไรก็ตามแต่ละฟีลด์ก็มีฟีลด์เฉพาะเป็นฟีลด์ย่อยเสมอ เพราะถ้า Γ เป็นหมู่ของฟีลด์ย่อยของฟีลด์ F แล้ว $\cap\Gamma$ เป็นฟีลด์ย่อยของ F ที่เล็กสุดและถ้า H เป็นฟีลด์ย่อยของ $\cap\Gamma$ แล้ว H เป็นฟีลด์ย่อยของ F ทำให้ $H\in\Gamma$ จึงได้ $\cap\Gamma\subseteq H$ ดังนั้น $H=\cap\Gamma$ นั่นคือ $\cap\Gamma$ ไม่มีฟีลด์ย่อยอื่นใดนอกจาก $\cap\Gamma$ ยิ่งไปกว่านั้นฟีลด์เฉพาะซึ่งเป็นฟีลด์ย่อยของฟีลด์ F มีได้เพียงหนึ่งเดียวเท่านั้น เพราะถ้า K_1 และ K_2 ต่างเป็นฟีลด์เฉพาะซึ่งเป็นฟีลด์ย่อย

ของ F แล้ว $K_1 \cap K_2$ เป็นฟีลด์ย่อยของฟีลด์ F โดยที่ $K_1 \cap K_2 \subseteq K_1$ และ $K_1 \cap K_2 \subseteq K_2$ แต่โดยสมบัติของฟีลด์เฉพาะ จะได้ $K_1 \subseteq K_1 \cap K_2$ และ $K_2 \subseteq K_1 \cap K_2$ ดังนั้น $K_1 = K_1 \cap K_2 = K_2$

4.6.2 **ทฤษฎีบท** 1. ทุกๆ ฟีลด์มีฟีลด์เฉพาะเป็นฟีลด์ย่อย

2. ฟีลด์เฉพาะซึ่งเป็นฟีลด์ย่อยของฟีลด์ F มีเพียงหนึ่งเดียว ❑

ต่อไปจะพิสูจน์ว่าทุกๆ ฟีลด์เฉพาะสมสัณฐานกับ $\mathbb{Q}$ หรือ $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ แต่จะแสดงก่อนว่าทุกๆ อินทิกรัลโดเมนบรรจุในฟีลด์เฉพาะ ซึ่งจะทำให้แสดงสมาชิกของฟีลด์เฉพาะได้ในรูปเศษส่วนของสมาชิกของอินทิกรัลโดเมนเช่นเดียวกับ $\mathbb{Q}$

4.6.3 **บทนิยาม** ให้ R เป็นริงและ S เป็นเซตย่อยของ R ที่ไม่ใช่เซตว่าง ถ้า S มีสมบัติปิดภายใต้การคูณ จะเรียก S ว่า *เซตการคูณ (multiplicative set)*

สังเกตว่าเซต S ของสมาชิกที่ไม่เป็นตัวหารของศูนย์ทั้งหมด หรือเซตของหน่วยทั้งหมดในริงมีเอกลักษณ์เป็นเซตการคูณ โดยเฉพาะเซตของสมาชิกที่ไม่ใช่ศูนย์ทั้งหมดในอินทิกรัลโดเมนเป็นเซตการคูณ ดังนั้นเซตของจำนวนเต็มที่ไม่ใช่ศูนย์ทั้งหมดเป็นเซตการคูณและถ้า P เป็นไอดีลเฉพาะในริงสลับที่ แล้วทั้ง P และ $R-P$ ต่างเป็นเซตการคูณ

เพื่อให้เห็นแนวทางการสร้างฟีลด์เฉพาะที่บรรจุอินทิกรัลโดเมน ขอทบทวนสมบัติและความสัมพันธ์ของจำนวนตรรกยะที่เขียนในรูปของจำนวนเต็มเมื่อ S แทนเซตของจำนวนเต็มที่ไม่ใช่ศูนย์ทั้งหมดดังนี้

ให้ $a,c \in \mathbb{Z}$ และ $b,d \in S$ แล้ว $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow ad - bc = 0$ ทำให้เห็นว่าจำนวนตรรกยะอาจสร้างโดยนิยามความสัมพันธ์ $\sim$ บนเซต $\mathbb{Z} \times S$ โดย

$$(a,b) \sim (c,d) \Leftrightarrow ad - bc = 0$$

เห็นชัดว่า $\sim$ เป็นความสัมพันธ์สมมูลและจะแทนเซตสมมูลของ (a,b) ด้วย $\frac{a}{b}$ และแทนผลแบ่งกั้นที่กำหนดโดย $\sim$ ด้วย $\mathbb{Q}$ และเมื่อพิจารณา $\mathbb{Q}$ ร่วมกับ "การบวก" และ "การคูณ" แบบปกติแล้ว $\mathbb{Q}$ เป็นฟีลด์ โดยเฉพาะ $\theta : \mathbb{Z} \to \mathbb{Q}$ ซึ่งนิยามโดย $\theta(a) = \frac{a}{1}$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง

เราจะขยายการสร้างสำหรับกรณีทั่วไป โดยการกำหนดให้ S เป็นเซตการคูณที่เป็นเซตย่อยของริงสลับที่ R และนิยามความสัมพันธ์ $\sim$ บนเซต $R \times S$ โดย

$$(a,b) \sim (c,d) \Leftrightarrow (\exists s \in S)[s(ad - bc) = 0]$$

แล้วขอละการพิสูจน์เป็นแบบฝึกหัดว่า $\sim$ เป็นความสัมพันธ์สมมูลบน $R \times S$ โดยเฉพาะถ้า R ไม่มีตัวหารของศูนย์และ $0 \notin S$ แล้ว

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad ad - bc = 0$$

ทุกๆ $(a,b),(c,d) \in R \times S$ และจะแทนเซตสมมูลของ $(a,b) \in R \times S$ ด้วย $\frac{a}{b}$ และแทนเซตของเซตสมมูลทั้งหมดด้วย $S^{-1}R$ แล้วเห็นชัดว่าข้อความต่อไปนี้เป็นจริง

1. $\frac{a}{b} = \frac{c}{d} \quad \Leftrightarrow \quad (\exists s \in S)[s(ad - bc) = 0]$
2. $\frac{ra}{rb} = \frac{a}{b}$ ทุกๆ $a \in R$ และทุกๆ $r, b \in S$
3. ถ้า $0 \in S$ แล้ว $S^{-1}R$ ประกอบด้วยสมาชิกเพียงหนึ่งเดียว

4.6.4 **ทฤษฎีบท** ให้ R, S และ $S^{-1}R$ เป็นดังกล่าวข้างต้น

1. $S^{-1}R$ เป็นริงสลับที่มีเอกลักษณ์ ด้วย "การบวก" และ "การคูณ" ซึ่งนิยามตามลำดับโดย $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ และ $(\frac{a}{b})(\frac{c}{d}) = \frac{ac}{bd}$ ทุกๆ $a, c \in R$ และทุกๆ $b, d \in S$

2. ถ้าริง $R \neq \{0\}$ ไม่มีตัวหารของศูนย์ แล้ว

   2.1 ถ้า $0 \notin S$ แล้ว $S^{-1}R$ เป็นอินทิกรัลโดเมน

   2.2 ถ้า S เป็นเซตของสมาชิกที่ไม่ใช่ศูนย์ทั้งหมดของ R แล้ว $S^{-1}R$ เป็นฟีลด์

บทพิสูจน์ 1. ให้ $\frac{a}{b} = \frac{c}{d} \in S^{-1}R$ และ $\frac{x}{y} = \frac{u}{v} \in S^{-1}R$ แล้ว $a, c, x, u \in R$ และ $b, d, y, v \in S$ แต่ S เป็นเซตการคูณจึงได้ $\frac{ay + bx}{by} \in S^{-1}R$ และ $\frac{cv + du}{dv} \in S^{-1}R$ และมี $s, t \in S$ ซึ่ง $s(ad - bc) = 0$ และ $t(xv - yu) = 0$ เมื่อคูณสมการแรกด้วย tyv และคูณสมการสองด้วย sbd แล้วนำมารวมกัน จะได้ $st[dv(ay + bx) - by(cv + du)] = 0$ ซึ่งสมมูลกับ $\frac{ay + bx}{by} = \frac{cv + du}{dv}$ ดังนั้น "การบวก" เป็นการดำเนินการบน $S^{-1}R$ และสำหรับ "การคูณ" เป็นการดำเนินการบน $S^{-1}R$ พิสูจน์ในทำนองเดียวกัน

เพราะ $\frac{0}{b} = \frac{0}{d}$ ทุกๆ $b, d \in S$ และ $\frac{a}{b} + \frac{0}{d} = \frac{ad}{bd} = \frac{a}{b}$ ดังนั้น $\frac{0}{b}$ เป็นเอกลักษณ์ "การบวก" โดยมี $\frac{-a}{b}$ เป็นสมาชิกลบของ $\frac{a}{b}$ ทุกๆ $a \in R$ และ $b \in S$ และเห็นชัดว่า "การบวก" สอดคล้องกฎการสลับที่ และ "การคูณ" สอดคล้องกฎการเปลี่ยนหมู่

เพราะ $\frac{b}{b} = \frac{d}{d}$ ทุกๆ $b, d \in S$ และ $(\frac{a}{b})(\frac{b}{b}) = \frac{a}{b}$ ทุกๆ $a \in R$ และ $b \in S$ ดังนั้น $\frac{b}{b}$ เป็นเอกลักษณ์ "การคูณ" บน $S^{-1}R$ และสุดท้ายให้ $\frac{a}{b}, \frac{c}{d}, \frac{x}{y} \in S^{-1}R$ แล้ว

$$\frac{x}{y}(\frac{a}{b} + \frac{c}{d}) = \frac{x}{y}(\frac{ad + bc}{bd}) = \frac{x(ad + bc)}{ybd} = \frac{(xa)(yd) + (cx)(yb)}{(yb)(yd)} = (\frac{x}{y})(\frac{a}{b}) + (\frac{x}{y})(\frac{c}{d})$$

ซึ่งแสดงว่า "การคูณ" สอดคล้องกฎการกระจายเหนือ "การบวก"

2. ให้ $R \neq \{0\}$ ไม่มีตัวหารของศูนย์และ $0 \notin S$ แล้ว $\frac{a}{b} = \frac{0}{b}$ ก็ต่อเมื่อ $a = 0$ ดังนั้น $\frac{0}{b} \neq \frac{b}{b}$ ทุกๆ $a \in R$ และ $b \in S$ ทำให้ได้ $(\frac{a}{b})(\frac{c}{d}) = \frac{0}{b}$ ใน $S^{-1}R$ ก็ต่อเมื่อ $ac = 0$ ใน R แต่ R ไม่มีตัวหารของศูนย์ จึงได้ $a = 0$ หรือ $c = 0$ ซึ่งจะได้ $\frac{a}{b} = \frac{0}{b}$ หรือ $\frac{c}{d} = \frac{0}{d}$ ดังนั้น $S^{-1}R$ เป็นอินทิกรัลโดเมน และถ้า $0 \neq a \in R$ ตัวผกผันการคูณของ $\frac{a}{b} \in S^{-1}R$ คือ $\frac{b}{a} \in S^{-1}R$ ดังนั้น $S^{-1}R$ เป็นฟีลด์ ❑

เราเรียกริง $S^{-1}R$ ในทฤษฎีบท 4.6.4 ว่า *ริงของเศษส่วน (ring of fraction) ของ R โดย S* และถ้า S เป็นเซตของสมาชิกที่ไม่ใช่ศูนย์ทั้งหมดในอินทิกรัลโดเมน R ซึ่ง $S^{-1}R$ เป็นฟีลด์ จะเรียกฟีลด์ $S^{-1}R$ ว่า *ฟีลด์ผลหาร (quotient field)* ของอินทิกรัลโดเมน R ตัวอย่างเฉพาะเช่นฟีลด์ผลหารของ $\mathbb{Z}$ คือฟีลด์ของจำนวนตรรกยะ $\mathbb{Q}$

ทฤษฎีบทต่อไป กล่าวกรณีทั่วไปของ $\theta : \mathbb{Z} \to \mathbb{Q}$ ที่นิยามโดย $\theta(a) = \frac{a}{1}$ ซึ่งเป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง ทำให้ได้ว่าว่า $\mathbb{Z}$ ถูกฝังในฟีลด์ผลหาร $\mathbb{Q}$

4.6.5 **ทฤษฎีบท** ให้ S เป็นเซตการคูณซึ่งเป็นเซตย่อยของริงสลับที่ R

1. การส่ง $\theta_S : R \to S^{-1}R$ ซึ่งนิยามโดย $\theta_S(a) = \frac{ab}{b}$ ทุกๆ $a \in R$ และ $b \in S$ เป็นสาทิสสัณฐานระหว่างริง โดยที่ $\theta_S(b)$ เป็นหน่วยใน $S^{-1}R$ ทุกๆ $b \in S$

2. ถ้า R ไม่มีตัวหารของศูนย์และ $0 \notin S$ แล้ว θ_S ในข้อ 1 เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง โดยเฉพาะอินทิกรัลโดเมนถูกฝังในฟีลด์ผลหาร

3. ถ้า R มีเอกลักษณ์และไม่มีตัวหารของศูนย์และ S เป็นเซตของสมาชิกหน่วยใน R แล้ว θ_S ในข้อ 1 เป็นสมสัณฐาน โดยเฉพาะฟีลด์ผลหารของฟีลด์ F สมสัณฐานกับ F

บทพิสูจน์ 1. สังเกตว่า $\frac{ab}{b} = \frac{ad}{d}$ ทุกๆ $a \in R$ และ $b, d \in S$ จึงได้ θ_S ในข้อ 1 กำหนดแจ่มชัด และเห็นชัดว่า θ_S เป็นสาทิสสัณฐานและสุดท้าย $\frac{b}{b^2}$ เป็นตัวผกผันการคูณของ $\frac{b^2}{b} = \theta_S(b)$ ทุกๆ $b \in S$ ซึ่งแสดงว่า $\theta_S(b)$ เป็นหน่วยใน $S^{-1}R$ ทุกๆ $b \in S$

2. ให้ $a \in \ker\theta_S$ แล้ว $\frac{ab}{b} = \theta_S(a) = \frac{0}{b}$ ทุกๆ $b \in S$ จึงมี $d \in S$ ซึ่ง $ab^2d = 0$ แต่ R ไม่มีตัวหารของศูนย์และ $0 \notin S$ ทำให้ได้ $b^2d \neq 0$ และทำให้ได้ $a = 0$ ดังนั้น $\ker\theta_S = \{0\}$ ซึ่งแสดงว่า θ_S เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง

ถ้า R เป็นอินทิกรัลโดเมนที่มีเอกลักษณ์ 1 แล้ว θ_S ซึ่งนิยามโดย $\theta_S(a) = \frac{a}{1}$ ทุกๆ $a \in R$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง

3. θ_S เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่งโดยข้อ 2 จึงเหลือการแสดงว่า θ_S เป็นชนิดทั่วถึง โดยให้ $\frac{a}{b} \in S^{-1}R$ แล้ว $a \in R$ และ b เป็นหน่วยใน R จึงมี $u \in R$ ซึ่ง $ub = 1$ ดังนั้น $au \in R$ และ $(aud)b = a(ub)d = ad$ ทุกๆ $d \in S$ ทำให้ได้ $\theta_S(au) = \frac{aud}{d} = \frac{a}{b}$ ❑

โดยทฤษฎีบท 4.6.5 ข้อ 2 อาจแทนอินทิกรัลโดเมน R ด้วยภาพของ R ภายใต้ θ_S (เพราะ $1 \in S$ ดังนั้นอาจแทนแต่ละ $a \in R$ ด้วย $\frac{a}{1} \in S^{-1}R$) ซึ่งเป็นริงย่อยของฟีลด์ผลหาร F ของ R และนิยมกล่าวสั้นๆ ว่า " R เป็นอินทิกรัลโดเมนซึ่งเป็นริงย่อยของฟีลด์ผลหาร"

ทฤษฎีบทต่อไปแสดงว่า ฟีลด์ผลหารที่บรรจุแต่ละอินทิกรัลโดเมนมีได้เพียงหนึ่งเดียว (ถ้าไม่นับการเป็นสมสัณฐาน)

4.6.6 **ทฤษฎีบท** ให้ S เป็นเซตการคูณในริงสลับที่ R และ T เป็นริงสลับที่ซึ่งมีเอกลักษณ์ ถ้า $\theta : R \to T$ เป็นสาทิสสัณฐานซึ่ง $\theta(s)$ เป็นหน่วยใน T ทุกๆ $s \in S$ แล้วมีสาทิสสัณฐาน $\overline{\theta} : S^{-1}R \to T$ เพียงหนึ่งเดียวซึ่ง $\overline{\theta} \circ \theta_S = \theta$

บทพิสูจน์ เห็นชัดว่า $\overline{\theta} : S^{-1}R \to T$ นิยามโดย $\overline{\theta}(\frac{a}{b}) = \theta(a)\theta(b)^{-1}$ ทุกๆ $a \in R$ และ $b \in S$ เป็นสาทิสสัณฐานซึ่ง $\overline{\theta} \circ \theta_S = \theta$ ส่วนการพิสูจน์มีเพียงหนึ่งเดียว ให้ $\alpha : S^{-1}R \to T$ เป็นสาทิสสัณฐานซึ่ง $\alpha \circ \theta_S = \theta$ แล้วเพราะ $\theta(s)$ เป็นหน่วยใน T ทุกๆ $s \in S$ ดังนั้น $\alpha(\theta_S(s)) = (\alpha \circ \theta_S)(s)$ เป็นหน่วยใน T โดยที่ $\theta_S(s)$ เป็นหน่วยใน $S^{-1}R$ ทุกๆ $s \in S$ โดยทฤษฎีบท 4.6.5 ข้อ 1 และทฤษฎีบท 4.5.3ข้อ 3 จะได้ $\alpha(\theta_S(s)^{-1}) = \alpha(\theta_S(s))^{-1}$ ทุกๆ $s \in S$ แต่ $\theta_S(s) = \frac{s^2}{s}$ ทุกๆ $s \in S$ จึงได้ $\theta_S(s)^{-1} = \frac{s}{s^2}$ ทุกๆ $s \in S$ สุดท้ายให้ $\frac{a}{b} \in S^{-1}R$ แล้ว $a \in R$ และ $b \in S$ ดังนั้น $\theta_S(a) = \frac{ab}{b}$ และ $\theta_S(b) = \frac{b^2}{b}$ ทำให้ได้ $\alpha(\frac{a}{b}) = \alpha(\frac{ab}{b} \cdot \frac{b}{b^2}) = \alpha(\theta_S(a))\alpha(\theta_S(b)^{-1}) = \alpha(\theta_S(a))\alpha(\theta_S(b))^{-1}$

$$= \alpha(\theta_S(a))(\alpha(\theta_S(b)))^{-1} = \theta(a)\theta(b)^{-1} = \overline{\theta}(\frac{a}{b})$$

ดังนั้น $\alpha = \overline{\theta}$ ❑

4.6.7 **บทแทรก** ให้ R เป็นอินทิกรัลโดเมนที่มี F เป็นฟีลด์ผลหารของ R ถ้า E เป็นฟีลด์และ $\theta : R \to E$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง แล้วมีสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง $\overline{\theta} : F \to E$ เพียงหนึ่งเดียวซึ่ง θ คือ $\overline{\theta}$ กำกัดลงบน R

โดยเฉพาะทุกๆ ฟีลด์ E_1 ที่บรรจุ R มีฟีลด์ย่อย F_1 ซึ่ง $R \subseteq F_1 \subseteq E_1$ และ $F_1 \cong F$

บทพิสูจน์ ให้ S เป็นเซตของสมาชิกที่ไม่ใช่ศูนย์ทั้งหมดของ R แล้ว $S^{-1}R = F$ และโดยทฤษฎีบท 4.6.6 มีสาทิสสัณฐาน $\overline{\theta} : S^{-1}R = F \to E$ เพียงหนึ่งเดียวซึ่ง $\overline{\theta} \circ \theta_S = \theta$ และการพิสูจน์โดยตรง

แสดงว่า $\overline{\theta}$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง สุดท้ายเพราะ θ_S เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง โดยทฤษฎีบท 4.6.5 ข้อ 2 จะได้ $R \cong \theta_S(R)$ ซึ่งหมายความว่า $\overline{\theta}$ กำกัดลงบน R คือ θ

สำหรับข้อความสุดท้ายถ้า $R \subseteq E_1$ จะกำหนด $\theta : R \to E_1$ ด้วยฟังก์ชันเอกลักษณ์แล้วมีสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง $\overline{\theta} : F \to E_1$ ซึ่ง $\overline{\theta}$ กำกัดลงบน R คือฟังก์ชันเอกลักษณ์ ดังนั้น $F_1 := \overline{\theta}(F) \cong F$ และ $R = \overline{\theta}(R) \subseteq \overline{\theta}(F) = F_1 \subseteq E_1$ ❑

4.6.8 **ทฤษฎีบท** ทุกๆ ฟีลด์เฉพาะสมสัณฐานกับ $\mathbb{Q}$ หรือ $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ

บทพิสูจน์ ให้ F เป็นฟีลด์เฉพาะและแต่ละจำนวนเต็ม n ขอทบทวนว่า $n1 = \underbrace{1+\cdots+1}_{n \text{ times}}$ ถ้า $n \geq 0$ และ $n1 = -(\underbrace{1+\cdots+1}_{-n \text{ times}})$ ถ้า $n < 0$ ทำให้ $\mathbb{Z}1 = \{n1 | n \in \mathbb{Z}\}$ เป็นริงย่อยของ F และ $\theta : \mathbb{Z} \to F$ ซึ่งนิยามโดย $\theta(n) = n1$ ทุกๆ $n \in \mathbb{Z}$ เป็นสาทิสสัณฐานจาก $\mathbb{Z}$ ไปบน $\mathbb{Z}1$ โดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $\mathbb{Z}/\ker\theta \cong \mathbb{Z}1$ แต่ $\ker\theta$ เป็นไอดีลของ $\mathbb{Z}$ ซึ่งเป็นโดเมนของไอดีลหลัก จึงมีจำนวนเต็มบวก $n \neq 1$ (ถ้า $n = 1$ จะได้ $1 = \theta(1) = 0$ แต่ $1 \neq 0$ ในฟีลด์ F) ซึ่ง $\ker\theta = <n>$

สมมติ n ไม่ใช่จำนวนเฉพาะแล้วเพราะ $n \neq 1$ ดังนั้น $n = 0$ หรือมีจำนวนเต็มบวก a และ b ซึ่ง $1 < a, b < n$ และ $n = ab$ แต่เพราะ $n \in \ker\theta$ จะได้ $(a1)(b1) = \theta(a)\theta(b) = \theta(ab) = \theta(n) = 0$ ทำให้ขัดแย้งกับ $\mathbb{Z}$ ไม่มีตัวหารของศูนย์ จึงสรุปว่า $n = 0$ หรือ n เป็นจำนวนเฉพาะ ซึ่งแสดงว่า $\mathbb{Z}1 \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$ หรือ $\mathbb{Z}1 \cong \mathbb{Z}_p$ สำหรับบางจำนวนเฉพาะ p

ถ้า $\mathbb{Z}1 \cong \mathbb{Z}_p$ แล้ว $\mathbb{Z}1$ เป็นฟีลด์ย่อยของฟีลด์เฉพาะ F ทำให้ได้ $F = \mathbb{Z}1 \cong \mathbb{Z}_p$ และถ้า $\mathbb{Z}1 \cong \mathbb{Z}$ แล้วโดยบทแทรก 4.6.7 ฟีลด์เฉพาะ F ของ $\mathbb{Z}1$ จะสมสัณฐานกับ $\mathbb{Q}$ ❑

แบบฝึกหัด 4.6

1. จงพิสูจน์ว่าเซตของสมาชิกที่ไม่เป็นตัวหารของศูนย์ทั้งหมดในริง หรือเซตของหน่วยทั้งหมดในริงมีเอกลักษณ์ หรือเซตของสมาชิกที่ไม่ใช่ศูนย์ทั้งหมดในอินทิกรัลโดเมนต่างเป็นเซตการคูณ ดังนั้นเซตของจำนวนเต็มที่ไม่ใช่ศูนย์ทั้งหมดเป็นเซตการคูณ
2. จงพิสูจน์ว่าถ้า P เป็นไอดีลเฉพาะของริงสลับที่ R แล้ว P และ $R - P$ ต่างเป็นเซตการคูณ
3. ให้ S เป็นเซตการคูณซึ่งเป็นเซตย่อยของริงสลับที่ R และนิยามความสัมพันธ์ $\sim$ บนเซต $R \times S$ โดย "$(a,b) \sim (c,d) \Leftrightarrow (\exists s \in S)[s(ad - bc) = 0]$" ทุกๆ $a, c \in R$ และ $b, d \in S$ จงพิสูจน์ว่า $\sim$ เป็นความสัมพันธ์สมมูลบน $R \times S$ พร้อมทั้งพิสูจน์ว่า
   3.1 ถ้า R ไม่มีตัวหารของศูนย์และ $0 \notin S$ แล้ว $(a,b) \sim (c,d)$ ก็ต่อเมื่อ $ad - bc = 0$ ทุกๆ $a, c \in R$ และ $b, d \in S$

3.2 ถ้า $0 \in S$ แล้ว $S^{-1}R$ ประกอบด้วยสมาชิกเพียงหนึ่งเดียว

4. จงแสดงว่า "การคูณ" ซึ่งนิยามในทฤษฎีบท 4.6.4 เป็นการดำเนินการบน $S^{-1}R$ และ $\overline{\theta}$ ซึ่งนิยามในบทพิสูจน์ของทฤษฎีบท 4.6.6 กำหนดแจ่มชัดและเป็นสาทิสสัณฐาน

5. ให้ S เป็นเซตการคูณซึ่งเป็นเซตย่อยของริงสลับที่ R และ I และ J เป็นไอดีลของ R จงพิสูจน์ว่า

5.1 $I \subseteq \theta_S^{-1}(S^{-1}I)$ และ $S^{-1}I := \{\frac{a}{s} | a \in I$ และ $s \in S\}$ เป็นไอดีลของ $S^{-1}R$

5.2 $S^{-1}(I+J) = S^{-1}I + S^{-1}J$, $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ และ

$S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$

5.3 $S^{-1}I = S^{-1}R$ ก็ต่อเมื่อ $S \cap I \neq \phi$

5.4 ถ้า T เป็นไอดีลของ $S^{-1}R$ แล้ว $\theta_S^{-1}(T)$ เป็นไอดีลของ R

5.6 ถ้า I เป็นไอดีลเฉพาะของ R และ $S \cap I = \phi$ แล้ว $S^{-1}I$ เป็นไอดีลเฉพาะของ $S^{-1}R$ และ $\theta_S^{-1}(S^{-1}I) = I$

4.7 ริงผลคูณตรง

สำหรับแต่ละจำนวนเต็มบวก n ให้ $S_1,\ldots,S_n$ เป็นไอดีลของริง R และนิยามเซต

$$S_1 + \ldots + S_n = \{s_1 + \cdots + s_n | s_i \in S_i, i = 1,\ldots,n\}$$

แล้วการพิสูจน์แบบตรงไปตรงมาแสดงให้เห็นว่า $S_1 + \ldots + S_n$ เป็นไอดีลเล็กสุดของ R ซึ่งประกอบด้วย S_i ทุกๆ $i = 1,\ldots,n$ นั่นคือ $S_1 + \ldots + S_n$ เป็นไอดีลที่ก่อกำเนิดโดย $S_1 \cup \ldots \cup S_n$

4.7.1 บทนิยาม ให้ $S_1,\ldots,S_n$ เป็นไอดีลของริง R กล่าวว่า R เป็น *ผลบวกตรงภายใน (internal direct sum)* ของ $S_1,\ldots,S_n$ และแทนด้วยสัญลักษณ์ $R = S_1 \oplus \ldots \oplus S_n$ ถ้า

1. $R = S_1 + \ldots + S_n$ และ
2. $S_i \cap (S_1 + \ldots S_{i-1} + S_{i+1} + S_n) = \{0\}$ ทุกๆ $i = 1,\ldots,n$

สังเกตว่าสำหรับ $n = 2$ จะได้ $R = S_1 \oplus S_2$ ก็ต่อเมื่อ $R = S_1 + S_2$ และ $S_1 \cap S_2 = \{0\}$

ทฤษฎีบทต่อไปแสดงเกณฑ์สำหรับการเป็นผลบวกตรงภายในของริง R

4.7.2 ทฤษฎีบท ริง R เป็นผลบวกตรงภายในของไอดีล $S_1,\ldots,S_n$ ของ R ก็ต่อเมื่อ แต่ละ $x \in R$ เขียนได้วิธีเดียวในรูป $x = s_1 + \ldots + s_n$ โดยที่ $s_i \in S_i$ ทุกๆ $i = 1,\ldots,n$

บทพิสูจน์ จะพิสูจน์เฉพาะกรณี $n = 2$ ส่วนกรณีทั่วไปพิสูจน์ได้โดยอุปนัยเชิงคณิตศาสตร์

ให้ S_1 และ S_2 เป็นไอดีลของริง R ซึ่ง $R = S_1 \oplus S_2$ และให้ $x \in R$ แล้วโดยบทนิยามของผลบวกตรงภายในข้อ 1 มี $s_i \in S_i$ สำหรับ $i = 1,2$ ซึ่ง $x = s_1 + s_2$ สมมติ $x = t_1 + t_2$ โดยที่ $t_i \in S_i$ สำหรับ $i \in \{1,2\}$ แล้ว $s_1 + s_2 = t_1 + t_2$ จะได้ $s_1 - t_1 = t_2 - s_2$ โดยที่ $s_1 - t_1 \in S_1$ และ $t_2 - s_2 \in S_2$ ดังนั้นโดยบทนิยามของผลบวกตรงภายในข้อ 2 จะได้ $s_1 - t_1 = t_2 - s_2 = 0$ จึงได้ $s_1 = t_1$ และ $s_2 = t_2$ นั่นคือ x เขียนได้วิธีเดียวในรูปผลบวก $x = s_1 + s_2$ โดยที่ $s_i \in S_i$ $s_i \in S_i$ สำหรับ $i = 1,2$

ในการพิสูจน์บทกลับกำหนดให้แต่ละ $x \in R$ เขียนได้วิธีเดียวในรูปผลบวก $x = s_1 + s_2$ โดยที่ $s_i \in S_i$ สำหรับ $i = 1,2$ ทำให้ได้ข้อ 1 ของบทนิยาม 4.7.1 จึงเหลือเพียงแสดงว่า $S_1 \cap S_2 = \{0\}$ ให้ $x \in S_1 \cap S_2$ แล้วเพราะ $x + 0 = x = 0 + x$ โดยที่ $x, 0 \in S_1$ และ $x, 0 \in S_2$ แต่ x เขียนได้วิธีเดียวดังกล่าวจึงทำให้ $x + 0$ คือรูปแบบ $0 + x$ ดังนั้น $x = 0$ ❑

เช่นเดียวกับเรื่องของกรุป เราอาจนำริง $R_1, R_2, ..., R_n$ จำนวนจำกัด n ริงมาสร้างริงใหม่บนผลคูณคาร์ทีเซียนของ $R_1, R_2, ..., R_n$ ซึ่งคือเซต $R_1 \times ... \times R_n = \{(r_1, ..., r_n) \mid r_i \in R_i \,;\, i = 1,2,...,n\}$ แล้วภายใต้การดำเนินการตามองค์ประกอบของโครงสร้างกรุปการบวกในแต่ละริง จะได้กรุปผลคูณตรงซึ่งเป็นกรุปอาบีเลียน และเมื่อนิยามการดำเนินการ "การคูณ" ตามองค์ประกอบเช่นเดียวกัน แล้วการพิสูจน์โดยอุปนัยเชิงคณิตศาสตร์ ทำให้ได้ $R_1 \times ... \times R_n$ เป็นริง

4.7.3 **บทนิยาม** กล่าวว่าริง R เป็น*ผลบวกตรงภายนอก (external direct sum)* ของริง $R_1, R_2, ..., R_n$ ถ้า R สมสัณฐานกับริง $R_1 \times ... \times R_n$

สังเกตว่าผลบวกตรงภายนอกของริง เป็นริงที่สร้างจากหมู่ของริงที่กำหนด แต่ผลบวกตรงภายในของริง เป็นริงซึ่งสร้างจากไอดีลของริงนั้น และเช่นเดียวกับเรื่องกรุป ความสัมพันธ์ของผลบวกตรงภายนอกและผลบวกตรงภายในของริงเป็นดังนี้

ให้ R เป็นผลบวกตรงภายนอกของหมู่ริง $\{R_i \mid i = 1,2,...,n\}$ และให้ $i = 1,...,n$ แล้วริง R_i ไม่เป็นริงย่อยของ R แต่มีไอดีลของ R ในรูปแบบ $I_i = \{(0,...,0,a_i,0,...,0) \mid a_i \in R_i\}$ ซึ่งสมสัณฐานกับ R_i โดยที่สมสัณฐานส่งแต่ละ $a_i \in R_i$ ไปยัง $(0,...,0,a_i,0,...,0)$ ใน I_i และเพราะ

$$(a_1, a_2, ..., a_n) = (a_1, 0, ..., 0) + (0, a_2, ..., 0) + \cdots + (0, 0, ..., a_n)$$

จึงเห็นชัดว่าแต่ละสมาชิกของ R เขียนได้วิธีเดียวในรูปผลบวกของสมาชิกในแต่ละ I_i ดังนั้น R เป็นผลบวกตรงภายในของ $I_1, \ldots, I_n$ โดยทฤษฎีบท 4.7.2 นั่นคือ

$$R_1 \times R_2 \times ... \times R_n \cong R = I_1 \oplus I_2 \oplus .... \oplus I_n$$

โดยที่ $R_i \cong I_i$ ทุกๆ $i = 1,2,....,n$ จึงนิยมใช้สัญลักษณ์ $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ แทนทั้งผลบวกตรงภายนอกและผลบวกตรงภายในและกล่าวรวมกันว่า $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ คือ *ผลบวกตรง (direct sum)* ของ $R_1, R_2, ..., R_n$

ถ้า $I \neq \phi$ เป็นเซตดรรชนีและนิยามผลคูณคาร์ทีเซียน $\prod_{i \in I} R_i$ ของหมู่ริง $\{R_i | i \in I\}$ ในทำนองเดียวกับบทนิยาม 2.1.1 และนิยามการดำเนินการ "การบวก" และ "การคูณ" ตามองค์ประกอบ

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I} \quad \text{และ} \quad (a_i)_{i \in I}(b_i)_{i \in I} = (a_i b_i)_{i \in I}$$

แล้วการพิสูจน์แบบตรงไปตรงมา แสดงว่า $\prod_{i \in I} R_i$ เป็นริงซึ่งเรียกว่า *ผลบวกตรง (direct sum)* ของ $\{R_i | i \in I\}$ และสอดคล้องสมบัติตามที่กล่าวในทฤษฎีบทต่อไป ซึ่งขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

4.7.4 **ทฤษฎีบท** ให้ $I \neq \phi$ และ $\{R_i | i \in I\}$ เป็นหมู่ของริง

1. ถ้า R_i เป็นริงมีเอกลักษณ์สำหรับแต่ละ $i \in I$ แล้ว $\prod_{i \in I} R_i$ เป็นริงมีเอกลักษณ์
2. ถ้า R_i เป็นริงสลับที่สำหรับแต่ละ $i \in I$ แล้ว $\prod_{i \in I} R_i$ เป็นริงมีสลับที่
3. แต่ละ $k \in I$ การฉาย $\pi_k : \prod_{i \in I} R_i \to R_k$ ซึ่งนิยามโดย $(a_i)_{i \in I} \to a_k$ เป็นสาทิสสัณฐานของริงชนิดทั่วถึง และการส่งเซตย่อย $\iota_k : R_k \to \prod_{i \in I} R_i$ ซึ่งนิยามโดย $a_k \to (a_i)_{i \in I}$ เมื่อ $a_i = 0$ สำหรับ $i \neq k$ เป็นสาทิสสัณฐานของริงชนิดหนึ่งต่อหนึ่ง ❑

4.7.5 **ทฤษฎีบท** ให้ $I \neq \phi$ และ $\{R_i | i \in I\}$ เป็นหมู่ของริง ถ้า S เป็นริงและ $\{\varphi_i : S \to R_i | i \in I\}$ เป็นหมู่ของสาทิสสัณฐาน แล้วมีสาทิสสัณฐาน $\varphi : S \to \prod_{i \in I} R_i$ เพียงหนึ่งเดียวซึ่ง $\pi_i \circ \varphi = \varphi_i$ ทุกๆ $i \in I$ ❑

ต่อไปจะพิสูจน์การวางนัยทฤษฎีบทเศษเหลือของจีนในระบบจำนวนเต็ม โดยสมมติให้ A เป็นไอดีลของริง R และ $a, b \in R$ จะกล่าวว่า a *สมมูล (congruence)* กับ b *มอดูโล (modulo)* A และแทนด้วยสัญลักษณ์ $a \equiv b (\text{mod}\, A)$ ถ้า $a - b \in A$ นั่นคือ

$$a \equiv b (\text{mod}\, A) \quad \Leftrightarrow \quad a + A = b + A$$

และเพราะ R/A เป็นริง จึงได้ว่าถ้า $a \equiv b (\text{mod}\, A)$ และ $c \equiv d (\text{mod}\, A)$ แล้ว

$$a + c \equiv b + d (\text{mod}\, A) \quad \text{และ} \quad ac \equiv bd (\text{mod}\, A)$$

4.7.6 ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)

ให้ $A_1, ..., A_n$ เป็นไอดีลของริง R ซึ่ง $R^2 + A_i = R$ ทุกๆ $i = 1,....,n$ และ $A_i + A_j = R$ ทุกๆ $i \neq j$ ถ้า $b_1, ..., b_n \in R$ แล้วมี $b \in R$ ซึ่ง $b \equiv b_i (\bmod A_i)$ ทุกๆ $i = 1,....,n$ ยิ่งไปกว่านั้น $b \in R$ เป็นรากของระบบสมการสมภาคมีเพียงหนึ่งเดียว (ภายใต้การสมมูลมอดูโลของไอดีล $A_1 \cap ... \cap A_n$)
[**ข้อสังเกต** ถ้า R เป็นริงมีเอกลักษณ์แล้ว $R^2 = R$ ทำให้ได้ $R^2 + A = R$ ทุกๆ ไอดีล A ของ R]

บทพิสูจน์ จาก $A_1 + A_2 = R$ และ $A_1 + A_3 = R$ จะได้ว่า

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1A_3 + A_2A_1 + A_2A_3 \subseteq A_1 + A_2A_3 \subseteq A_1 + (A_2 \cap A_3)$$

และจาก $R^2 + A_1 = R$ เราจะได้

$$R = R^2 + A_1 \subseteq A_1 + (A_1 + (A_2 \cap A_3)) = A_1 + (A_2 \cap A_3) \subseteq R$$

ดังนั้น $R = A_1 + (A_2 \cap A_3)$

ต่อไปสมมติขั้นอุปนัยว่าถ้า k เป็นจำนวนเต็มบวกซึ่ง $R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_{k-1})$ แล้ว $R^2 = (A_1 + (A_2 \cap A_3 \cap \cdots \cap A_{k-1}))(A_1 + A_k) \subseteq A_1 + (A_2 \cap A_3 \cap \cdots \cap A_k)$ ทำให้ได้

$R = R^2 + A_1 \subseteq A_1 + (A_2 \cap A_3 \cap \cdots \cap A_k) \subseteq R$

โดยอุปนัยเชิงคณิตศาสตร์ $R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_n) = A_1 + \bigcap_{i \neq 1} A_i$ ทุกๆ จำนวนเต็มบวก n ดังนั้นมี $a_k \in A_k$ และ $r_k \in \bigcap_{i \neq k} A_i$ ซึ่ง $b_k = a_k + r_k$ ทุกๆ $k = 1,2,....,n$ ทำให้ได้ $r_k \equiv b_k$ $(\bmod A_k)$ และ $r_k \equiv 0 (\bmod A_i)$ เมื่อ $i \neq k$ ทุกๆ $k = 1,2,....,n$ และให้ $b = r_1 + r_2 + \cdots + r_n$ แล้ว $b = r_1 + r_2 + \cdots + r_n \equiv 0 + \cdots + 0 + b_k + 0 + \cdots + 0 = b_k \ (\bmod A_k)$ ทุกๆ $k = 1,....,n$

ถ้า $c \in R$ ซึ่ง $c \equiv b_i (\bmod A_i)$ ทุกๆ $i = 1,....,n$ แล้ว $c \equiv b (\bmod A_i)$ ทุกๆ $i = 1,....,n$ ทำให้ $b - c \in A_i$ ทุกๆ $i = 1,....,n$ ดังนั้น $b - c \in \bigcap_{i=1}^{n} A_i$ นั่นคือ $b \equiv c (\bmod \bigcap_{i=1}^{n} A_i)$ ❑

4.7.7 บทแทรก ให้ $A_1, ..., A_n$ เป็นไอดีลของริง R แล้ว

1. $R/(A_1 \cap \cdots \cap A_n)$ ถูกฝังใน $(R/A_1) \times (R/A_2) \times \cdots \times (R/A_n)$
2. ถ้า $R^2 + A_i = R$ ทุกๆ $i = 1,2,....,n$ และ $A_i + A_j = R$ ทุกๆ $i \neq j$ แล้ว

$$R/(A_1 \cap \cdots \cap A_n) \cong (R/A_1) \times (R/A_2) \times \cdots \times (R/A_n)$$

บทพิสูจน์ โดยทฤษฎีบท 4.7.5 หมู่ของการฉาย $\{\pi_i : R \to R/A_i | i = 1,\ldots,n\}$ ชักนำสาทิสสัณฐานของริง $\theta_1 : R \to (R/A_1) \times (R/A_2) \times \cdots \times (R/A_n)$ โดยที่ $\theta_1(r) = (r + A_1, \ldots, r + A_n)$ ซึ่งเห็นชัดว่า $\ker \theta_1 = A_1 \cap A_2 \cap \cdots \cap A_n$ ดังนั้น θ_1 ชักนำสาทิสสัณฐาน θ ชนิดหนึ่งต่อหนึ่งจาก $R/(A_1 \cap \cdots \cap A_n)$ ไปยัง $(R/A_1) \times (R/A_2) \times \cdots \times (R/A_n)$

ถ้า $(b_1+A_1,\ldots,b_n+A_n)\in(R/A_1)\times(R/A_2)\times\cdots\times(R/A_n)$ ภายใต้เงื่อนไขของทฤษฎีบท จะมี $b\in R$ เพียงหนึ่งเดียวซึ่ง $b\equiv b_i(\operatorname{mod} A_i)$ ทุกๆ $i=1,2,\ldots,n$ และจะได้ $\theta\left(b+\bigcap_{i=1}^{n}A_i\right)=(b+A_1,\ldots,b+A_n)=(b_1+A_1,\ldots,b_n+A_n)$ ซึ่งแสดงว่า θ เป็นชนิดทั่วถึง ❑

แบบฝึกหัด 4.7

1. ให้ $\wp(X)$ แทนเซตของเซตย่อยทั้งหมดของเซต X จงแสดงว่า
   1.1 $\wp(X)$ เป็นริงภายใต้การดำเนินการ "การบวก" และ "การคูณ" ที่นิยามตามลำดับดังนี้
   $$A+B:=(A-B)\cup(B-A) \text{ และ } AB:=A\cap B$$
   สำหรับทุกๆ เซตย่อย A และ B ของ X
   1.2 หมู่ของเซตย่อยขนาดจำกัดทั้งหมดของ X เป็นไอดีลของ $\wp(X)$
   1.3 ถ้า $Y\subseteq X$ แล้ว $\wp(Y)$ และ $\wp(X-Y))$ เป็นไอดีลมุขสำคัญของ $\wp(X)$
   1.4 $\wp(X)=\wp(Y)\oplus\wp(X-Y)$
2. ให้ θ เป็นสาทิสสัณฐานจากริงสลับที่ R ไปบนริงสลับที่ S และ I และ J เป็นไอดีลของ R
   2.1 $\theta(I+J)=\theta(I)+\theta(J)$ และ $\theta(IJ)=\theta(I)\theta(J)$
   2.2 ถ้า $\ker\theta\subseteq I\cap J$ แล้ว $\theta(I\cap J)=\theta(I)\cap\theta(J)$
3. จงแสดงว่าริงของจำนวนเชิงซ้อน $\mathbb{C}$ เป็นผลคูณตรง $\mathbb{R}\oplus\mathbb{R}$ ของริงของจำนวนจริง
4. จงพิสูจน์ว่า $\prod_{i\in I}R_i$ เป็นริง และสำหรับจำนวนเต็มบวก n ถ้า $\{R_1,\ldots,R_n\}$ เป็นเซตของริงของไอดีลมุขสำคัญแล้ว $R_1\times\ldots\times R_n$ เป็นริงของไอดีลมุขสำคัญ
5. จงประยุกต์ทฤษฎีบทเศษเหลือของจีนเพื่อพิสูจน์ว่า ถ้า $m_1,\ldots,m_n$ เป็นจำนวนเต็มบวก n ตัวซึ่ง $(m_i,m_j)=1$ ทุกๆ $i\neq j$ และ $b_1,\ldots,b_n$ เป็นจำนวนเต็ม แล้วระบบสมการสมภาค $x\equiv b_1(\operatorname{mod} m_1),\ x\equiv b_2(\operatorname{mod} m_2),\ \cdots,\ x\equiv b_n(\operatorname{mod} m_n)$ มีคำตอบเป็นจำนวนเต็มเพียงคำตอบเดียวภายใต้ความสัมพันธ์สมภาคมอดูโล $m=m_1\ldots m_n$
6. ให้ I และ J เป็นไอดีลของโดเมนของไอดีลมุขสำคัญ R จงพิสูจน์ว่าถ้า $a,b\in R$ ซึ่ง $I=<a>$ และ $J=<b>$ แล้ว $IJ=<ab>$ โดยเฉพาะ $I^n=<a^n>$ ทุกๆ จำนวนเต็มบวก n และถ้า $I+J=R$ แล้ว $IJ=I\cap J$

บทที่ 5
โดเมนของการแยกตัวประกอบได้แบบเดียว

ดังกล่าวแล้วว่า ทฤษฎีริงเป็นมโนคติการวางนัยทฤษฎีจำนวน และได้พิสูจน์ว่าระบบจำนวนเต็มเป็นอินทิกรัลโดเมนที่บรรจุในฟีลด์เล็กสุด คือฟีลด์ของจำนวนตรรกยะซึ่งบรรจุในฟีลด์ของจำนวนจริงและฟีลด์ของจำนวนเชิงซ้อนตามลำดับ และเพราะอินทิกรัลโดเมนไม่ใช่ฟีลด์ ดังนั้น "การหาร" จึงไม่เป็นการดำเนินการบนอินทิกรัลโดเมน ในบทนี้เราจะศึกษามโนคติการวางนัย "การหารลงตัว" "ตัวหารร่วมมาก" "ตัวคูณร่วมน้อย" "จำนวนเฉพาะ" และ "ขั้นตอนการหาร" ของระบบจำนวนเต็ม โดยเฉพาะการวางนัย "ทฤษฎีบทมูลฐานของเลขคณิต (Fundamental Theorem of Arithmetic)" ซึ่งกล่าวว่า "ทุกๆ จำนวนเต็มที่ไม่ใช่หน่วยและศูนย์เขียนได้วิธีเดียวในรูปผลคูณของจำนวนเฉพาะ (ถ้าไม่นับอันดับของตัวประกอบในผลคูณ)"

5.1 ทฤษฎีการหารในริงสลับที่

ในหัวข้อนี้ จะให้นิยามในลักษณะวางนัยมโนคติของ "ตัวประกอบหรือตัวหาร" "การหารลงตัว" "ตัว หารร่วมมาก" และ "ตัวคูณร่วมน้อย" ในริงสลับที่ พร้อมทั้งแสดงริงที่มี "ตัวหารร่วมมาก" และ "ตัวคูณร่วมน้อย" ของแต่ละหมู่ของสมาชิกในริง

5.1.1 **บทนิยาม** ให้ R เป็นริงสลับที่ $0 \neq a \in R$ และ $b \in R$ จะกล่าวว่า a *หาร (divide)* b (ลงตัว) และแทนด้วยสัญลักษณ์ $a|b$ ถ้ามี $c \in R$ ซึ่ง $b = ac$ แต่ถ้าไม่มี $c \in R$ ดังกล่าว จะกล่าวว่า a *ไม่หาร (does not divide)* b

ถ้า $a|b$ จะเรียก a ว่า *ตัวหาร (divisor)* หรือ *ตัวประกอบ (factor)* ของ b และเรียก b ว่า *ตัวคูณ (multiple)* ของ a นอกจากนี้จะกล่าวว่า a *สมทบ (associate)* กับ b ถ้า $a|b$ และ $b|a$

สังเกตว่าเมื่อใดก็ตามที่เขียนสัญลักษณ์ $a|b$ จะเข้าใจตรงกันว่า $a \neq 0$ แม้ $b = 0$ ก็ตาม (ซึ่งหมายความว่า เราไม่นิยามการหารด้วยศูนย์)

ทฤษฎีบทต่อไป รวบรวมสมบัติเบื้องต้นเกี่ยวกับการหาร เพื่อใช้ในการอ้างอิง สำหรับการพิสูจน์ทำได้ในทำนองเดียวกับการหารของจำนวนเต็ม จึงขอละไว้เป็นแบบฝึกหัด

5.1.2 **ทฤษฎีบท** ให้ R เป็นริงสลับที่ มีเอกลักษณ์ และ $a,b,c \in R$ แล้ว

1. $a|0$, $1|a$ และ $a|a$
2. $a|1$ ก็ต่อเมื่อ a เป็นหน่วย
3. ถ้า $a|b$ แล้ว $ac|bc$ และ $a|bc$

4. ถ้า $a|b$ และ $b|c$ แล้ว $a|c$

5. ถ้า $c|a$ และ $c|b$ แล้ว $c|(ax+by)$ สำหรับทุกๆ $x,y \in R$ ❑

5.1.3 **ข้อสังเกต** ถ้า a สมทบกับ b แล้วมี $c,d \in R$ ซึ่ง $b=ac$ และ $a=bd$ ทำให้ได้ $a=bd=acd$ นั่นคือ $a-acd=0$ ดังนั้นถ้า R เป็นอินทิกรัลโดเมนแล้ว $0=a-acd=a(1-cd)$ โดยที่ $a \neq 0$ จะได้ $cd=1$ นั่นคือ c และ d เป็นหน่วย ทำให้กล่าวได้ว่า

"ถ้า R เป็นอินทิกรัลโดเมนและ $a,b \in R$ แล้ว a สมทบกับ b ก็ต่อเมื่อ มีหน่วย u ใน R ซึ่ง $a=bu$"

เห็นชัดว่าถ้า R เป็นอินทิกรัลโดเมนและนิยามความสัมพันธ์ $\sim$ บน R โดย "$a \sim b$ ก็ต่อเมื่อ a สมทบกับ b ทุกๆ $a,b \in R$" แล้ว $\sim$ เป็นความสัมพันธ์สมมูลใน R ซึ่งสมาชิกในเซตสมมูลเดียวกันกับเอกลักษณ์คือหน่วยทั้งหมดของ R

ทฤษฎีบทต่อไป พิสูจน์ได้โดยตรงจากบทนิยาม จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

5.1.4 **ทฤษฎีบท** ให้ R เป็นริงสลับที่ มีเอกลักษณ์และ $a,b,u \in R$ แล้ว

1. $a|b$ ก็ต่อเมื่อ $<b> \subseteq <a>$
2. a สมทบกับ b ก็ต่อเมื่อ $<a> = <b>$
3. u เป็นหน่วย ก็ต่อเมื่อ $u|r$ ทุกๆ $r \in R$ และก็ต่อเมื่อ $<u> = R$
4. ถ้า $a=bu$ โดยที่ u เป็นหน่วยแล้ว a สมทบกับ b ❑

ตัวอย่างเช่น ในอินทิกรัลโดเมน $\mathbb{Z}$ สมาชิกที่สมทบกับแต่ละจำนวนเต็ม n คือ $\pm n$ ซึ่งแสดงว่าแต่ละเซตสมมูลภายใต้ความสัมพันธ์ "สมทบ" ใน $\mathbb{Z}$ เป็นเซตที่ประกอบด้วยสมาชิกเพียง 2 ตัว คือเซต $\{-n,n\}$

เกาส์ (C.F. Gauss 1777–1855) นักคณิตศาสตร์ชาวเยอรมันได้แนะนำเซต

$$\mathbb{Z}[i] := \{a+bi \mid a,b \in \mathbb{Z}\}$$

ซึ่งเห็นชัดว่าเป็นริงย่อยของริงของจำนวนเชิงซ้อน $\mathbb{C}$ (นั่นคือการดำเนินการทั้งสองของ $\mathbb{Z}[i]$ คือ "การบวก" และ "การคูณ" แบบปกติใน $\mathbb{C}$ กำกัดลงบน $\mathbb{Z}[i]$) จึงเรียกสมาชิกของ $\mathbb{Z}[i]$ ว่า *จำนวนเต็มแบบเกาส์ (Gaussian integers)* และขอละการพิสูจน์ไว้เป็นแบบฝึกหัดว่า $\mathbb{Z}[i]$ คือตัวอย่างของอินทิกรัลโดเมนที่บรรจุ $\mathbb{Z}$ ซึ่งไม่เป็นฟีลด์

ถ้า $a+bi \in \mathbb{Z}[i]$ เป็นหน่วย จะมี $c+di \in \mathbb{Z}[i]$ ซึ่ง $(a+bi)(c+di)=1$ ดังนั้น $(ac-bd)=1$ และ $(bc+ad)=0$ จึงได้ด้วยว่า $(a-bi)(c-di)=(ac-bd)-i(bc+ad)=1$ ทำให้ได้

$$1 = (a+bi)(c+di)(a-bi)(c-di) = (a^2+b^2)(c^2+d^2)$$

แต่เพราะ $a,b,c,d \in \mathbb{Z}$ จึงได้ $a^2+b^2=1=c^2+d^2$ ดังนั้น ($a=c=\pm 1$ ในขณะที่ $b=d=0$) หรือ ($a=c=0$ ในขณะที่ $b=d=\pm 1$) ซึ่งทำให้ได้ $a+bi \in \{\pm 1,\ \pm i\}$ นั่นคือมีเพียง ± 1 และ $\pm i$ เท่านั้นที่เป็นหน่วยใน $\mathbb{Z}[i]$ เพราะฉะนั้นเซตสมมูลของแต่ละ $a+bi \in \mathbb{Z}[i]$ ภายใต้ความสัมพันธ์ "สมทบ" คือเซต $\{a+bi, -a-bi, -b+ai, b-ai\}$

5.1.5 **บทนิยาม** ให้ R เป็นริงสลับที่ มีเอกลักษณ์และ $a_1,a_2,\ldots,a_n \in R$ ซึ่งไม่ใช่ศูนย์พร้อมกัน จะเรียก $d \in R$ ว่า *ตัวหารร่วมมาก (greatest common divisor)* ของ $a_1,a_2,\ldots,a_n$ ถ้า d ไม่ใช่ศูนย์ และสอดคล้องเงื่อนไขต่อไปนี้

1. d เป็น *ตัวหารร่วม (common divisor)* ของ $a_1,\ldots,a_n$ นั่นคือ $d|a_i$ ทุกๆ $i=1,2,\ldots,n$

และ 2. $c|d$ สำหรับทุกๆ $c \in R$ ซึ่งเป็นตัวหารร่วมของ $a_1,a_2,\ldots,a_n$

สังเกตว่าคำว่า "มาก" ของตัวหารร่วมมาก ไม่ได้หมายความว่าตัวหารร่วมมากมีขนาดใหญ่กว่าตัวหารร่วมตัวอื่นๆ ดังเช่นตัวหารร่วมมากของจำนวนเต็ม (เพราะในริงทั่วไป อาจไม่มีการกำหนด "อันดับ") แต่มีความหมายว่า ตัวหารร่วมมากเป็นตัวคูณของตัวหารร่วมตัวอื่นๆ และแต่ละชุดของสมาชิกในริงอาจ "มี" หรือ "ไม่มี" ตัวหารร่วมมากก็ได้ และสำหรับชุดของสมาชิกที่มีตัวหารร่วมมาก ก็อาจมีตัวหารร่วมมากได้มากกว่าหนึ่งตัว อย่างไรก็ตามถ้า d_1 และ d_2 ต่างเป็นตัวหารร่วมมากของ $a_1,a_2,\ldots,a_n$ แล้ว $d_1|d_2$ และ $d_2|d_1$ ทำให้ได้ว่า d_1 และ d_2 สมทบกัน นั่นคืออยู่ในเซตสมมูลเดียวกันภายใต้ความสัมพันธ์ "สมทบ" จึงอาจกล่าวว่า ตัวหารร่วมมากของแต่ละชุดสมาชิกในริง ถ้ามีจะมีเพียงหนึ่งเดียว (ภายใต้ความสัมพันธ์ "สมทบ") และในภาวะเช่นนั้น จะแทนตัวหารร่วมมากของ $a_1,a_2,\ldots,a_n$ ด้วยสัญลักษณ์ $(a_1,a_2,\ldots,a_n)$

เราได้พิสูจน์แล้วว่า $a|b$ ในริงสลับที่ R ก็ต่อเมื่อ $b \in <a>$ ซึ่งก็ต่อเมื่อ $<b> \subseteq <a>$ โดยเฉพาะถ้า d เป็นตัวหารร่วมของ a และ b แล้ว $<a> \subseteq <d>$, $<b> \subseteq <d>$ และ $<a,b> \subseteq <d>$ ทำให้กำหนดนิยามของ $(a_1,a_2,\ldots,a_n)$ ในรูปไอดีลของ R ได้ดังนี้

"ถ้า $a_1,a_2,\ldots,a_n \in R$ และ $J=<a_1,a_2,\ldots,a_n>$ แล้ว $d \in R$ เป็นตัวหารร่วมมากของ $a_1,a_2,\ldots,a_n$ ก็ต่อเมื่อ $J \subseteq <d>$ และ $<d> \subseteq <d'>$ สำหรับทุกๆ $d' \in R$ ซึ่ง $J \subseteq <d'>$"

ทฤษฎีบทต่อไป แสดงว่าในริงของไอดีลมุขสำคัญมีตัวหารร่วมมาก สำหรับทุกๆ ชุดสมาชิก

5.1.6 **ทฤษฎีบท** ให้ R เป็นริงสลับที่มีเอกลักษณ์และ $a_1,a_2,\ldots,a_n \in R$ โดยที่ทุกตัวไม่ใช่ศูนย์ ถ้า R เป็นริงของไอดีลมุขสำคัญแล้วจะมี $d \in R$ ซึ่ง $d=(a_1,a_2,\ldots,a_n)$ และเขียน d ได้ในรูปผลบวกเชิงเส้นของ $a_1,a_2,\ldots,a_n$ นั่นคือมี $r_1,r_2,\ldots,r_n \in R$ ซึ่ง $d=r_1a_1+r_2a_2+\cdots+r_na_n$

บทพิสูจน์ ให้ R เป็นริงของไอดีลมุขสำคัญและ $a_1,a_2,\ldots,a_n \in R$ โดยที่ทุกตัวไม่ใช่ศูนย์ แล้วไอดีล $<a_1,a_2,\ldots,a_n>$ เป็นไอดีลมุขสำคัญของ R จึงมี $d \in R$ ซึ่ง $<d> = <a_1,a_2,\ldots,a_n>$ และเพราะ $a_i \in <d>$ ทุกๆ $i=1,2,\ldots,n$ ดังนั้นแต่ละ $i \in \{1,2,\ldots,n\}$ มี $b_i \in R$ ซึ่ง $a_i = b_i d$ จะได้ว่า $d|a_i$ ทุกๆ $i \in \{1,2,\ldots,n\}$ ซึ่งแสดงว่า d เป็นตัวหารร่วมของ $a_1,a_2,\ldots,a_n$ นอกจากนี้ $d \in <d> = <a_1,a_2,\ldots,a_n>$ จึงมี $r_1,r_2,\ldots,r_n \in R$ ซึ่ง $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ นั่นคือ d เป็นผลบวกเชิงเส้นของ $a_1,a_2,\ldots,a_n$ และสุดท้ายถ้า $c \in R$ โดยที่ $c|a_i$ ทุกๆ $i \in \{1,2,\ldots,n\}$ แล้วแต่ละ $i \in \{1,2,\ldots,n\}$ มี $s_i \in R$ ซึ่ง $a_i = s_i c$ ทำให้ได้ $d = c(r_1s_1 + r_2s_2 + \cdots + r_ns_n)$ นั่นคือ $c|d$ ❑

ในริงมีเอกลักษณ์ R เมื่อใดก็ตามที่ $d = (a_1,a_2,\ldots,a_n)$ และ $<d> = <a_1,a_2,\ldots,a_n> = R$ แล้วเพราะ $1 \in R$ จะมี $c \in R$ ที่ทำให้ $1 = cd$ ซึ่งแสดงว่าตัวหารร่วมมาก d เป็นหน่วยใน R และเพราะทุกๆ หน่วยใน R สมทบกับเอกลักษณ์ ดังนั้นในกรณีเช่นนี้ จะกล่าวว่า $a_1,a_2,\ldots,a_n$ เป็น *สมาชิกเฉพาะสัมพัทธ์(relatively prime)* และแทนด้วยสัญลักษณ์ $(a_1,a_2,\ldots,a_n) = 1$ แต่โดยทฤษฎีบท 5.1.6 อาจกล่าวได้ว่า

"$a_1,a_2,\ldots,a_n$ *เป็นสมาชิกเฉพาะสัมพัทธ์ในอินทิกรัลโดเมน* R *ก็ต่อเมื่อ มี* $r_1,r_2,\ldots,r_n \in R$ ซึ่ง $1 = r_1a_1 + r_2a_2 + \cdots + r_na_n$"

5.1.7 **บทแทรก** ถ้า R เป็นริงสลับที่มีเอกลักษณ์ $a,b,c \in R$ โดยที่ $(a,c) = 1$ และ $c|ab$ แล้ว $c|b$

บทพิสูจน์ เนื่องจาก $(a,c) = 1$ ดังนั้นมี $r,s \in R$ ซึ่ง $1 = ra + sc$ และเพราะ $c|ab$ จะมี $t \in R$ ซึ่ง $ab = tc$ เพราะฉะนั้น $b = b1 = b(ra+sc) = rab + sbc = c(rt+sb)$ ซึ่งแสดงว่า $c|b$ ❑

เมื่อศึกษาการนิยามและสมบัติของตัวหารร่วมมากของชุดของสมาชิกในริง จะต้องศึกษาแบบคู่ขนานกัน สำหรับการนิยามและสมบัติของตัวคูณร่วมน้อยของชุดของสมาชิกในริง

5.1.8 **บทนิยาม** ให้ R เป็นริงสลับที่มีเอกลักษณ์และ $a_1,a_2,\ldots,a_n \in R$ โดยที่ทุกตัวไม่ใช่ศูนย์ จะเรียก $m \in R$ ว่า *ตัวคูณร่วมน้อย (least common multiple)* ของ $a_1,a_2,\ldots,a_n$ ถ้า m เป็น *ตัวคูณร่วม (common multiple)* ของ $a_1,a_2,\ldots,a_n$ นั่นคือ $a_i|m$ ทุกๆ $i=1,2,\ldots,n$ และ $m|c$ สำหรับทุกๆ $c \in R$ ซึ่งเป็นตัวคูณร่วมของ $a_1,a_2,\ldots,a_n$

เช่นเดียวกันคำว่า "น้อย" ของตัวคูณร่วมน้อยใช้ในความหมายว่า ตัวคูณร่วมน้อยเป็นตัวหารของตัวคูณร่วมตัวอื่นๆ และสำหรับชุดของสมาชิกที่มีตัวคูณร่วมน้อย ก็อาจมีตัวคูณร่วมน้อยได้มากกว่าหนึ่งตัว และด้วยเหตุผลเดียวกับกรณีตัวหารร่วมมาก ตัวคูณร่วมน้อยทุกตัวของสมาชิก

ชุดเดียวกันจะสมทบกัน หรือกล่าวได้ว่า ตัวคูณร่วมน้อยของ $a_1, a_2, \ldots, a_n$ ถ้ามีจะมีเพียงหนึ่งเดียว ภายใต้ความสัมพันธ์ "สมทบ" จึงแทนเซตสมมูลของตัวคูณร่วมน้อยด้วยสัญลักษณ์ $[a_1, a_2, \ldots, a_n]$

5.1.9 **ทฤษฎีบท** ให้ R เป็นริงสลับที่มีเอกลักษณ์และ $a_1, a_2, \ldots, a_n \in R$ โดยที่ทุกตัวไม่ใช่ศูนย์

1. ถ้ามี $m \in R$ ซึ่ง $m = [a_1, a_2, \ldots, a_n]$ แล้ว $\bigcap_{i=1}^{n} < a_i >$ เป็นไอดีลมุขสำคัญ
2. ถ้า R เป็นริงของไอดีลมุขสำคัญ แล้วมี $m \in R$ ซึ่ง $m = [a_1, a_2, \ldots, a_n]$

บทพิสูจน์ 1. สมมติมี $m \in R$ ซึ่ง $m = [a_1, a_2, \ldots, a_n]$ แล้ว $a_i | m$ ทุกๆ $i = 1, 2, \ldots, n$ นั่นคือมี $r_1, \ldots, r_n \in R$ ซึ่ง $m = r_i a_i$ นั่นคือ $m \in < a_i >$ ทุกๆ $i = 1, 2, \ldots, n$ ดังนั้น $< m > \subseteq \bigcap_{i=1}^{n} < a_i >$ และในทางกลับกันถ้า $r \in \bigcap_{i=1}^{n} < a_i >$ แล้ว $a_i | r$ ทุกๆ $i = 1, 2, \ldots, n$ นั่นคือ r เป็นตัวคูณร่วมของ $a_1, a_2, \ldots, a_n$ จึงได้ $m | r$ ดังนั้น $r \in < m >$ ซึ่งแสดงว่า $\bigcap_{i=1}^{n} < a_i > \subseteq < m >$ เพราะฉะนั้น $\bigcap_{i=1}^{n} < a_i > = < m >$ เป็นไอดีลมุขสำคัญ

2. ให้ R เป็นริงของไอดีลมุขสำคัญและ $a_1, a_2, \ldots, a_n \in R$ โดยที่ทุกตัวไม่ใช่ศูนย์แล้ว $\bigcap_{i=1}^{n} < a_i >$ เป็นไอดีลมุขสำคัญของ R จึงมี $m \in R$ ซึ่ง $< m > = \bigcap_{i=1}^{n} < a_i >$ ดังนั้น $m \in < a_i >$ นั่นคือ $a_i | m$ ทุกๆ $i = 1, 2, \ldots, n$ หรือกล่าวว่า m เป็นตัวคูณร่วมของ $a_1, a_2, \ldots, a_n$ และถ้า $b \in R$ เป็นตัวคูณร่วมของ $a_1, a_2, \ldots, a_n$ แล้ว $a_i | b$ ทุกๆ $i = 1, 2, \ldots, n$ ทำให้ $< b > \subseteq < a_i >$ ทุกๆ $i = 1, 2, \ldots, n$ ซึ่งแสดงว่า $< b > \subseteq \bigcap_{i=1}^{n} < a_i > = < m >$ ดังนั้น $m | b$ เพราะฉะนั้น m เป็นตัวคูณร่วมน้อยของ $a_1, a_2, \ldots, a_n$ ❑

5.1.10 **ทฤษฎีบท** ให้ R เป็นโดเมนของไอดีลมุขสำคัญและ $a, b \in R - \{0\}$ แล้ว $ab = (a,b)[a,b]$

บทพิสูจน์ ให้ R เป็นโดเมนของไอดีลมุขสำคัญ $a, b \in R - \{0\}$ และ $d = (a,b) \in R$ แล้วโดยทฤษฎีบท 5.1.6 จะมี $s, t, x, y \in R$ ซึ่ง $a = ds$, $b = dt$ และ $d = ax + by$ จึงได้ $d = dsx + dty = d(sx + ty)$ และโดยกฎการตัดออกใน R เมื่อ $d \neq 0$ ทำให้ได้ $sx + ty = 1$

สังเกตว่า $ab = (ds)(dt) = d(dst)$ และเห็นชัดว่า $a | dst$ และ $b | dst$ จึงเหลือเพียงแสดงว่า dst เป็นตัวหารของตัวคูณร่วมของ a และ b ทุกตัวโดยให้ $c \in R$ เป็นตัวคูณร่วมของ a และ b แล้วมี $p, q \in R$ ซึ่ง $c = ap = bq$ และจาก $sx + ty = 1$ จะได้ $c = csx + cty = bqsx + apty = dst(qx + py)$ ซึ่งแสดงว่า dst เป็นตัวหารของ c ซึ่งเป็นอันจบการพิสูจน์ ❑

แบบฝึกหัด 5.1

1. จงพิสูจน์ว่าความสัมพันธ์ $\sim$ เป็นความสัมพันธ์สมมูลในริงมีเอกลักษณ์ 1 ซึ่งเซตสมมูลของ 1 ประกอบด้วยหน่วยทั้งหมดของ R
2. จงพิสูจน์ว่าเซต $\mathbb{Z}[i]$ ของจำนวนเต็มแบบเกาส์เป็นริงย่อยของริงของจำนวนเชิงซ้อน $\mathbb{C}$ และเป็นอินทิกรัลโดเมน พร้อมทั้งพิสูจน์ว่าถ้า $a+bi \in \mathbb{Z}[i]$ ไม่เป็นหน่วยแล้ว $a^2+b^2>0$
3. จงหาตัวหารร่วมมากใน $\mathbb{Z}[i]$ ของคู่สมาชิกในข้อต่อไปนี้

   3.1 $3+4i$ และ $4-3i$ 3.2 $11+7i$ และ $18-i$
4. ให้ R เป็นอินทิกรัลโดเมนที่มีเอกลักษณ์ 1 และ $0 \neq u \in R$ จงพิสูจน์ว่า u สมทบกับ 1 ก็ต่อเมื่อ u เป็นหน่วยใน R ซึ่งก็ต่อเมื่อ $<u>=R$
5. ให้ R เป็นริงสลับที่ มีเอกลักษณ์และ $a_1,a_2,\ldots,a_n \in R$

   5.1 จงพิสูจน์ว่า $d \in R$ เป็นตัวหารร่วมมากของ $a_1,a_2,\ldots,a_n$ ที่มี $r_1,r_2,\ldots,r_n \in R$ ซึ่ง $d = r_1a_1+r_2a_2+\cdots+r_na_n$ ก็ต่อเมื่อ $<d>=<a_1>+<a_2>+\ldots+<a_n>$

   5.2 จงแสดงว่าในกรณีทั่วไปอาจไม่มีตัวหารร่วมมากของ $a_1,a_2,\ldots,a_n$ และถ้ามี $d \in R$ เป็นตัวหารร่วมมากของ $a_1,a_2,\ldots,a_n$ แล้ว d อาจไม่สามารถเขียนในรูปผลบวกเชิงเส้นของ $a_1,a_2,\ldots,a_n$
6. ให้ $a,b \in \mathbb{Z}$ จงพิสูจน์ว่าถ้า a และ b มีภาวะต่างกันแล้ว $(a,b)=(a+b,a-b)$ และถ้า a และ b เป็นจำนวนคี่ทั้งคู่แล้ว $2(a,b) = (a+b,a-b)$ แต่ถ้า a และ b เป็นจำนวนคู่ทั้งคู่ จงอธิบายว่าเหตุใด จึงสรุปข้อความทั้งสองข้างต้นไม่ได้
7. จงพิสูจน์ว่าถ้า $a,b \in \mathbb{Z}$ แล้วเซตของตัวคูณร่วมทั้งหมดของ a และ b เป็นไอดีลของ $\mathbb{Z}$
8. ให้ G เป็นกรุป H เป็นกรุปย่อยของ G และ $a,b \in G$ จงพิสูจน์ว่า $S=\{n \in \mathbb{Z} \mid a^n \in H\}$ และ $T=\{n \in \mathbb{Z} \mid ab^n = b^na\}$ ต่างเป็นไอดีลของ $\mathbb{Z}$
9. ให้ D เป็นโดเมนของไอดีลมุขสำคัญและ $a,b,d \in D$ จงพิสูจน์ว่าถ้า $(a,b)=d$ แล้ว $<a>+<b>=<d>$ [**ข้อแนะนำ**: จงพิสูจน์ว่าถ้า J และ K เป็นไอดีลของริง R แล้ว $J+K=\{x+y \mid x \in J$ และ $y \in K\}$ เป็นไอดีลของริง R]

5.2 การแยกตัวประกอบในริง

ในหัวข้อนี้ จะให้นิยามในลักษณะวางนัยสมาชิกในริงที่ทำหน้าที่เช่นเดียวกับ "จำนวนเฉพาะ" ในระบบจำนวนเต็ม พร้อมทั้งพิสูจน์การวางนัยทฤษฎีบทมูลฐานของเลขคณิตในริงที่มีสมบัติเฉพาะซึ่งเรียกว่า "โดเมนของการแยกตัวประกอบได้แบบเดียว"

5.2.1 **บทนิยาม** ให้ R เป็นริงสลับที่ มีเอกลักษณ์ จะเรียก $0 \neq c \in R$ ว่า *สมาชิกลดทอนไม่ได้ (irreducible element)* ถ้า c ไม่ใช่หน่วยและถ้า $u, v \in R$ ซึ่ง $c = uv$ แล้ว u เป็นหน่วยหรือ v เป็นหน่วย และกล่าวว่า $0 \neq c \in R$ เป็น *สมาชิกลดทอนได้ (reducible element)* ถ้า c ไม่ใช่หน่วยและไม่ใช่สมาชิกลดทอนไม่ได้

จะเรียก $0 \neq p \in R$ ว่า *สมาชิกเฉพาะ (prime element)* ถ้า p ไม่ใช่หน่วยและถ้า $u, v \in R$ ซึ่ง $p|uv$ แล้ว $p|u$ หรือ $p|v$

5.2.2 **ข้อสังเกต** โดยบทนิยาม 5.2.1 ตัวหารของสมาชิกลดทอนไม่ได้ มีเพียงหน่วยกับสมาชิกที่สมทบกับสมาชิกลดทอนไม่ได้นั้น แต่หน่วยไม่ใช่สมาชิกลดทอนไม่ได้ และเพราะสมาชิกทุกตัวของริงการหารและฟิลด์เป็นหน่วย จึงไม่มีสมาชิกลดทอนไม่ได้ในริงดังกล่าว

5.2.3 **ตัวอย่าง** ถ้า p เป็นจำนวนเฉพาะใน $\mathbb{Z}$ แล้ว p และ $-p$ เป็นสมาชิกลดทอนไม่ได้และสมาชิกเฉพาะตามบทนิยาม 5.2.1 อย่างไรก็ตาม $2 \in \mathbb{Z}_6$ เป็นสมาชิกเฉพาะ แต่ไม่เป็นสมาชิกลดทอนไม่ได้ ทั้งนี้เพราะ $2 = (2)(4)$ ใน $\mathbb{Z}_6$ ในขณะที่ทั้ง 2 และ 4 ไม่ใช่หน่วยใน $\mathbb{Z}_6$ (เพราะทั้งคู่เป็นตัวหารของศูนย์ใน $\mathbb{Z}_6$) ○

ตัวอย่าง 5.2.3 แสดงว่าในริงทั่วไป สมาชิกลดทอนไม่ได้กับสมาชิกเฉพาะไม่มีความเชื่อมโยงกัน ทฤษฎีบทต่อไปแสดงการจำแนกและความเชื่อมโยงกันของสมาชิกทั้งสองประเภทในริงแต่ละชนิด

5.2.4 **ทฤษฎีบท** ให้ R เป็นริงสลับที่มีเอกลักษณ์แล้ว $p \in R$ เป็นสมาชิกเฉพาะก็ต่อเมื่อ $<p> \neq \{0\}$ และ $<p>$ เป็นไอดีลเฉพาะ

บทพิสูจน์ ให้ $p \in R$ เป็นสมาชิกเฉพาะแล้ว $p \neq 0$ และ p ไม่ใช่หน่วย จึงได้ $\{0\} \neq <p> \neq R$ ให้ $a, b \in R$ ซึ่ง $ab \in <p>$ แล้ว $p|ab$ แต่ p เป็นสมาชิกเฉพาะทำให้ได้ $p|a$ หรือ $p|b$ นั่นคือ $a \in <p>$ หรือ $b \in <p>$ ในทำนองกลับกันถ้า $p \in R$ ซึ่ง $<p> \neq \{0\}$ และ $<p>$ เป็นไอดีลเฉพาะแล้ว $p \neq 0$ และ $<p> \neq R$ ทำให้ได้ว่า p ไม่ใช่หน่วย ต่อไปให้ $u, v \in R$ ซึ่ง $p|uv$ แล้ว $uv \in <p>$ และจาก $<p>$ เป็นไอดีลเฉพาะ จะได้ $u \in <p>$ หรือ $v \in <p>$ ซึ่งสมมูลกับ $p|u$ หรือ $p|v$ จึงเป็นอันจบการพิสูจน์ □

5.2.5 **ทฤษฎีบท** ให้ R เป็นอินทิกรัลโดเมน

1. $c \in R$ เป็นสมาชิกลดทอนไม่ได้ ก็ต่อเมื่อ $<c>$ เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มในหมู่ของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R

2. ทุกๆ สมาชิกเฉพาะใน R เป็นสมาชิกลดทอนไม่ได้

3. ทุกๆ สมาชิกใน R ซึ่งสมทบกับสมาชิกลดทอนไม่ได้เป็นสมาชิกลดทอนไม่ได้

4. ทุกๆ สมาชิกใน R ซึ่งสมทบกับสมาชิกเฉพาะเป็นสมาชิกเฉพาะ

5. ตัวหารของสมาชิกลดทอนไม่ได้ของ R มีเพียงหน่วยของ R กับสมาชิกใน R ซึ่งสมทบกับสมาชิกลดทอนไม่ได้นั้น

บทพิสูจน์ 1. ให้ $c \in R$ เป็นสมาชิกลดทอนไม่ได้แล้ว $<c>$ เป็นไอดีลมุขสำคัญของ R ที่ไม่ใช่ R (เพราะว่า c ไม่ใช่หน่วย) และให้ $d \in R$ ซึ่ง $<c> \subseteq <d> \subseteq R$ แล้ว $c \in <d>$ นั่นคือมี $x \in R$ ซึ่ง $c = dx$ ทำให้ได้ d หรือ x เป็นหน่วย ในกรณีที่ d เป็นหน่วย จะได้ $<d> = R$ และในกรณีที่ x เป็นหน่วยจะมี $y \in R$ ซึ่ง $xy = 1$ ทำให้ได้ $d = d1 = (dx)y = cy$ ซึ่งแสดงว่า $d \in <c>$ ดังนั้น $<d> \subseteq <c>$ จึงได้ $<d> = <c>$ เพราะฉะนั้น $<c>$ เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มในหมู่ของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R

ในการพิสูจน์บทกลับให้ $c \in R$ ซึ่ง $<c>$ เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มในเซตของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R แล้ว $c \neq 0$ และ c ไม่ใช่หน่วยโดยทฤษฎีบท 5.1.3 ต่อไปให้ $u, v \in R$ ซึ่ง $c = uv$ แล้ว $<c> \subseteq <u>$ ดังนั้น $<c> = <u>$ หรือ $<u> = R$ ถ้า $<u> = R$ แล้ว u เป็นหน่วย หรือถ้า $<c> = <u>$ แล้วจาก $u \in <c>$ จะมี $y \in R$ ซึ่ง $u = cy$ ทำให้ได้ $c = uv = cyv$ แต่ R เป็นอินทิกรัลโดเมน ดังนั้น $yv = 1$ ซึ่งแสดงว่า v เป็นหน่วย เพราะฉะนั้น c เป็นสมาชิกลดทอนไม่ได้

2. ให้ $p \in R$ เป็นสมาชิกเฉพาะใน R และให้ $a, b \in R$ ซึ่ง $p = ab$ แล้ว $p|ab$ ทำให้ได้ $p|a$ หรือ $p|b$ และโดยไม่เสียนัยทั่วไปสมมติว่า $p|a$ แล้วมี $x \in R$ ซึ่ง $a = px$ ดังนั้น $p = ab = pxb$ นั่นคือ $p(1 - xb) = 0$ จึงได้ $xb = 1$ นั่นคือ b เป็นหน่วย ดังนั้น p เป็นสมาชิกลดทอนไม่ได้

3. ให้ $a, b \in R$ โดยที่ a เป็นสมาชิกลดทอนไม่ได้และ b สมทบกับ a แล้วมี $u \in R$ ซึ่ง u เป็นหน่วยและ $a = bu$ ให้ $c, d \in R$ ซึ่ง $b = cd$ แล้ว $a = bu = cdu$ จะได้ว่า c เป็นหน่วยหรือ du เป็นหน่วย และถ้า du เป็นหน่วย แล้ว d เป็นหน่วย ดังนั้น b เป็นสมาชิกลดทอนไม่ได้

4. พิสูจน์ในทำนองเดียวกับข้อ 3

5. ให้ $a, b \in R$ โดยที่ a เป็นสมาชิกลดทอนไม่ได้และ $b|a$ แล้ว $<a> \subseteq <b>$ และโดยข้อ 1 จะได้ $<a> = <b>$ หรือ $<b> = R$ และโดยทฤษฎีบท 5.1.3 จะได้ว่า b สมทบกับ a หรือ b เป็นหน่วย ❐

5.2.6 **ทฤษฎีบท** ถ้า R เป็นโดเมนของไอดีลมุขสำคัญและ $p \in R$ แล้ว p เป็นสมาชิกเฉพาะ ก็ต่อเมื่อ p เป็นสมาชิกลดทอนไม่ได้

บทพิสูจน์ เพราะว่า R เป็นอินทิกรัลโดเมน จึงได้โดยทฤษฎีบท 5.2.5 ข้อ 2 ว่าทุกๆ สมาชิกเฉพาะเป็นสมาชิกลดทอนไม่ได้ ในการพิสูจน์บทกลับให้ $p \in R$ เป็นสมาชิกลดทอนไม่ได้และให้ $a,b \in R$ ซึ่ง $p|ab$ แล้วมี $d \in R$ ซึ่ง $ab = pd$ และเพราะไอดีล $<p,a>$ เป็นไอดีลมุขสำคัญใน R จึงมี $c \in R$ ซึ่ง $<p,a> = <c>$ แต่ $p \in <c>$ ดังนั้นมี $r \in R$ ซึ่ง $p = cr$ แต่ p เป็นสมาชิกลดทอนไม่ได้ ทำให้ได้ c เป็นหน่วยหรือ r เป็นหน่วย ถ้า c เป็นหน่วยแล้ว $<p,a> = <c> = R$ ดังนั้น $1 \in <p,a>$ จึงมี $s,t \in R$ ซึ่ง $1 = ps + at$ และได้ $b = b1 = bps + bat = p(bs + dt)$ ซึ่งแสดงว่า $p|b$ แต่ถ้า r เป็นหน่วยแล้ว $c = pr^{-1} \in <p>$ ทำให้ได้ $<c> \subseteq <p>$ ดังนั้น $a \in <c> \subseteq <p>$ ซึ่งแสดงว่า $p|a$ ดังนั้นไม่ว่ากรณีใด จะได้ $p|a$ หรือ $p|b$ เพราะฉะนั้น p เป็นสมาชิกเฉพาะ $\square$

โดยทฤษฎีบท 5.2.6 สมาชิกเฉพาะและสมาชิกลดทอนไม่ได้เป็นสมาชิกหมู่เดียวกันในโดเมนของไอดีลมุขสำคัญ จึงขอกล่าวถึงสมบัติสำคัญของริงชนิดนี้ซึ่งจะนำไปสู่การแยกตัวประกอบได้แบบเดียวต่อไป

5.2.7 **ทฤษฎีบท** ให้ R เป็นโดเมนของไอดีลมุขสำคัญและ $\{J_k | k = 1,2,\ldots\}$ เป็นหมู่อนันต์ของไอดีลของ R ซึ่งสอดคล้องเงื่อนไขโซ่เพิ่ม $J_1 \subseteq J_2 \subseteq \cdots J_n \subseteq J_{n+1} \subseteq \cdots$ แล้วมีจำนวนเต็มบวก m ซึ่ง $J_n = J_m$ ทุกๆ จำนวนเต็ม $n \geq m$

บทพิสูจน์ เห็นชัดว่า $J := \bigcup_{n \in \mathbb{N}} J_n$ เป็นไอดีลของ R ซึ่งเป็นโดเมนของไอดีลมุขสำคัญ จึงมี $a \in R$ ซึ่ง $J = <a>$ โดยที่ $a \in J$ ดังนั้นมีจำนวนเต็มบวก m ซึ่ง $a \in J_m$ และสำหรับจำนวนเต็ม $n \geq m$ จะได้ $J = <a> \subseteq J_m \subseteq J_n \subseteq \bigcup_{n \in \mathbb{N}} J_n = J$ ซึ่งแสดงว่า $J_n = J_m$ ทุกๆ จำนวนเต็ม $n \geq m$ $\square$

สังเกตโดยทฤษฎีบท 5.2.7 ถ้า R เป็นโดเมนของไอดีลมุขสำคัญ แล้วจะมีไอดีลของ R ที่เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม สำหรับบทแทรกต่อไปจะแสดงว่าทุกๆ สมาชิกซึ่งไม่ใช่ศูนย์และไม่ใช่สมาชิกหน่วยในโดเมนของไอดีลมุขสำคัญเป็นตัวคูณของสมาชิกเฉพาะตัวใดตัวหนึ่ง (สังเกตว่าในระบบจำนวนเต็ม จำนวนประกอบแต่ละตัวจะมีจำนวนเฉพาะซึ่งเป็นตัวหารของจำนวนประกอบนั้น) ซึ่งเป็นเนื้อหาสำคัญที่นำเราไปสู่การแยกตัวประกอบได้แบบเดียวในโดเมนของไอดีลมุขสำคัญ

5.2.8 **บทแทรก** ให้ R เป็นโดเมนของไอดีลมุขสำคัญ ถ้า $0 \neq a \in R$ ไม่ใช่หน่วย แล้วจะมีสมาชิกเฉพาะ $p \in R$ ซึ่ง $p|a$

บทพิสูจน์ เพราะ a ไม่ใช่หน่วยดังนั้น $<a> \neq R$ ถ้า $J := <a>$ ไม่เป็นไอดีลใหญ่สุดเฉพาะกลุ่มในเซตของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R แล้วมี $0 \neq a_1 \in R$ ซึ่ง $J \subseteq J_1 = <a_1>$ และ

สำหรับ $k>0$ สมมติว่า $\{a,a_1,\ldots,a_{k-1}\}\subseteq R-\{0\}$ ซึ่ง $J\subseteq J_1\subseteq\cdots\subseteq J_{k-1}=<a_{k-1}>$ และถ้า $<a_{k-1}>$ ไม่เป็นไอดีลใหญ่สุดเฉพาะกลุ่มในเซตของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R แล้ว มี $0\neq a_k\in R$ ซึ่ง $J\subseteq J_1\subseteq\cdots\subseteq J_{k-1}\subseteq J_k=<a_k>$ ทำให้ได้โดยอุปนัยเชิงคณิตศาสตร์ว่ามีหมู่อนันต์ของไอดีลของ R ซึ่งสอดคล้องเงื่อนไข $J=J_0\subseteq J_1\subseteq J_2\subseteq\cdots J_n\subseteq J_{n+1}\subseteq\cdots$ และโดยทฤษฎีบท 5.2.6 จะมีจำนวนเต็มบวก m ซึ่ง $J_n=J_m$ ทุกๆ จำนวนเต็ม $n\geq m$ นั่นคือมีไอดีลใหญ่สุดเฉพาะกลุ่ม M ในเซตของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R ซึ่ง $<a>\subseteq M$ เพราะฉะนั้นมีสมาชิกลดทอนไม่ได้ และนั่นคือสมาชิกเฉพาะ $p\in R$ ซึ่ง $M=<p>$ และได้ว่า $<a>\subseteq<p>$ นั่นคือ $p|a$ ❐

ขอปิดท้ายหัวข้อนี้ด้วยการศึกษาการวางนัย "ทฤษฎีบทมูลฐานของเลขคณิต" โดยแสดงว่ามีโดเมนซึ่งทุกๆ สมาชิกที่ไม่ใช่หน่วยในโดเมนเขียนได้วิธีเดียวในรูปผลคูณของสมาชิกเฉพาะ ถ้าไม่นับอันดับของตัวหารในผลคูณ

5.2.9 **บทนิยาม** ให้ R เป็นอินทิกรัลโดเมน เราเรียก R ว่า *โดเมนของการแยกตัวประกอบได้แบบเดียว (unique factorization domain)* ถ้าเงื่อนไขสองข้อต่อไปนี้เป็นจริงใน R

1. แต่ละ $0\neq a\in R$ ที่ไม่ใช่หน่วย มีสมาชิกลดทอนไม่ได้ $p_1,\ldots,p_n\in R$ ซึ่ง $a=p_1\cdots p_n$
2. ถ้า $a=p_1p_2\cdots p_n$ และ $a=q_1q_2\cdots q_m$ โดยที่ $p_1,\ldots,p_n,q_1,\ldots,q_m\in R$ เป็นสมาชิกลดทอนไม่ได้ แล้ว $m=n$ และมีวิธีเรียงสับเปลี่ยน σ บน $\{1,2,\ldots,n\}$ ซึ่ง p_i สมทบกับ $q_{\sigma(i)}$ ทุกๆ $i=1,2,\ldots,n$

สังเกตว่าในโดเมนของไอดีลมุขสำคัญ สมาชิกลดทอนไม่ได้ในบทนิยาม 5.2.9 คือสมาชิกเฉพาะ และสำหรับการหาโดเมนที่จะเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว จะแสดงก่อนว่าโดเมนของไอดีลมุขสำคัญสอดคล้องเงื่อนไขข้อ 1 ของบทนิยาม 5.2.9

5.2.10 **ทฤษฎีบท** ให้ R เป็นโดเมนของไอดีลมุขสำคัญ ถ้า $0\neq a\in R$ ไม่ใช่หน่วย แล้วมีจำนวนเต็มบวก n และสมาชิกเฉพาะ $p_1,p_2,\ldots,p_n\in R$ ซึ่ง $a=p_1p_2\cdots p_n$

บทพิสูจน์ ให้ $0\neq a\in R$ และ a ไม่ใช่หน่วยแล้ว $<a>\neq R$ และโดยบทแทรก 5.2.8 จะมีสมาชิกเฉพาะ $p_1\in R$ ซึ่ง $p_1|a$ ดังนั้นมี $a_1\in R$ ซึ่ง $a=p_1a_1$ ทำให้ได้ $<a>\subseteq<a_1>$ ถ้า $<a>=<a_1>$ แล้วเพราะ $a_1\in<a>$ จะมี $r_1\in R$ ซึ่ง $a_1=r_1a$ ทำให้ได้ $a=p_1a_1=p_1r_1a$ และสรุปได้ว่า $p_1r_1=1$ ทำให้สมาชิกเฉพาะ p_1 เป็นสมาชิกหน่วยซึ่งเป็นไปไม่ได้ ดังนั้น $<a>\subset<a_1>$ แล้วโดยอุปนัยวิธีจะสามารถดำเนินกระบวนการดังกล่าวซ้ำต่อไปได้เรื่อยๆ เมื่อเริ่มจาก $a=a_0$ ทำให้ได้โซ่เพิ่มของไอดีลมุขสำคัญดังนี้

$$< a_0 > \subset < a_1 > \subset \cdots \subset < a_n > \subset \cdots$$

โดยที่ $a_{k-1} = p_k a_k$ เมื่อ p_k เป็นสมาชิกเฉพาะทุกๆ $k \in \mathbb{N}$ แต่โดยทฤษฎีบท 5.2.7 จะมีจำนวนเต็มบวก n ที่ทำให้ $< a_0 > \subset < a_1 > \subset \cdots \subset < a_n > = < a_{n+1} >$ แล้วโดยการแทน $a_{k-1} = p_k a_k$ ทุกๆ k จะได้ $a = p_1 a_1 = p_1 p_2 a_2 \ = \cdots = p_1 p_2 \cdots p_n a_n$ ถ้า $< a_n > \subset R$ แล้ว $< a_n >$ เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มในเซตของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R และถ้า $< a_n > = R$ แล้ว a_n เป็นหน่วยและ $< a_{n-1} >$ เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มในเซตของไอดีลมุขสำคัญทั้งหลายของ R ที่ไม่ใช่ R ทำให้ได้โดยทฤษฎีบท 5.2.5 ข้อ 1 ว่า a_n เป็นสมาชิกลดทอนไม่ได้ (และนั่นคือสมาชิกเฉพาะ) หรือ a_n เป็นหน่วยและ a_{n-1} เป็นสมาชิกเฉพาะ เพราะฉะนั้นไม่ว่ากรณีใด a เขียนได้ในรูปผลคูณของสมาชิกเฉพาะ ❐

5.2.11 **บทแทรก** ให้ R เป็นโดเมนของไอดีลมุขสำคัญ ถ้า $0 \neq a \in R$ ซึ่ง $< a > \neq R$ แล้วมีจำนวนเต็มบวก n และไอดีลเฉพาะ $< p_1 >, \ldots, < p_n >$ ของ R ซึ่ง $< a > = < p_1 > < p_2 > \ldots < p_n >$

บทพิสูจน์ เพราะ $< 0 > \neq < a > \neq R$ ดังนั้น a ไม่เป็นหน่วย ทำให้ได้โดยทฤษฎีบท 5.2.10 ว่ามีจำนวนเต็มบวก n และสมาชิกเฉพาะ $p_1, \ldots, p_n \in R$ ซึ่ง $a = p_1 p_2 \ldots p_n$ ทำให้ได้ $< a > = < p_1 p_2 \cdots p_n > = < p_1 > < p_2 > \ldots < p_n >$ โดยที่ $< p_i >$ เป็นไอดีลเฉพาะทุกๆ $i = 1, 2, \ldots, n$ ❐

5.2.12 **ทฤษฎีบท** ให้ R เป็นโดเมนของไอดีลมุขสำคัญ ถ้า $p, p_1, p_2, \ldots, p_n \in R$ เป็นสมาชิกเฉพาะซึ่ง $p | p_1 p_2 \ldots p_n$ แล้วมี $i = 1, 2, \ldots, n$ ซึ่ง p สมทบกับ p_i

บทพิสูจน์ จะพิสูจน์โดยอุปนัยเชิงคณิตศาสตร์ซึ่งเห็นชัดว่าทฤษฎีบทเป็นจริงเมื่อ $n = 1$ จึงให้ k เป็นจำนวนเต็มบวกซึ่งทฤษฎีบทเป็นจริงเมื่อแทน n ด้วย k และให้ $p, p_1, p_2, \ldots, p_{k+1} \in R$ เป็นสมาชิกเฉพาะซึ่ง $p | p_1 p_2 \cdots p_k p_{k+1}$ ถ้า $p | p_{k+1}$ แล้ว p สมทบกับ p_{k+1} และถ้า p ไม่เป็นตัวหารของ p_{k+1} แล้วเพราะ p และ p_{k+1} ต่างเป็นสมาชิกเฉพาะ ดังนั้น $(p, p_{k+1}) = 1$ จึงได้โดยบทแทรก 5.1.6 ว่า $p | p_1 p_2 \ldots p_k$ ทำให้ได้โดยสมมติฐานขั้นอุปนัยว่ามี $i = 1, 2, \ldots, k$ ซึ่ง p สมทบกับ p_i ดังนั้นทฤษฎีบทเป็นจริงเมื่อแทน n ด้วย $k+1$ ❐

ให้ $R := \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ แล้วเห็นชัดว่า R เป็นอินทิกรัลโดเมนซึ่งเป็นริงย่อยของฟีลด์ของจำนวนจริง $\mathbb{R}$ และขอให้พิสูจน์เป็นแบบฝึกหัดว่า $2, 3, 4 + \sqrt{10}$ และ $4 - \sqrt{10}$ เป็นสมาชิกลดทอนไม่ได้ซึ่งไม่ใช่สมาชิกเฉพาะ ดังนั้น R ไม่ใช่โดเมนของไอดีลมุขสำคัญ โดยเฉพาะอย่างยิ่ง $(2)(3) = 6 = (4 + \sqrt{10})\,(4 - \sqrt{10})$ แสดงว่ามีอินทิกรัลโดเมนซึ่งสมาชิกเขียนได้ในรูปผลคูณของสมาชิกลดทอนไม่ได้มากกว่าหนึ่งแบบ อย่างไรก็ตามทฤษฎีบทต่อไปจะแสดงว่าในโดเมนของไอดีลมุขสำคัญ การแยกตัวประกอบจะเกิดขึ้นเพียงแบบเดียวเช่นเดียวกับในโดเมนของจำนวนเต็ม

5.2.13 **ทฤษฎีบท** ทุกๆ โดเมนของไอดีลมุขสำคัญเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว

บทพิสูจน์ ให้ R เป็นโดเมนของไอดีลมุขสำคัญและให้ $0 \neq a \in R$ ไม่ใช่หน่วย แล้วโดยทฤษฎีบท 5.2.10 จะมีจำนวนเต็มบวก n และสมาชิกเฉพาะ $p_1, p_2, \ldots, p_n \in R$ ซึ่ง $a = p_1 p_2 \cdots p_n$ จึงเหลือเพียงแสดงว่า $p_1, p_2, \ldots, p_n$ เป็นสมาชิกเฉพาะเพียงชุดเดียวเท่านั้นที่มีผลคูณเป็น a โดยสมมติให้ m เป็นจำนวนเต็มบวกและ $q_1, \ldots, q_m \in R$ เป็นสมาชิกเฉพาะซึ่ง $a = q_1 q_2 \cdots q_m$ โดยอาจสมมติว่า $n \leq m$ แล้ว $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ ทำให้ได้ $p_1 | q_1 q_2 \cdots q_m$ และโดยทฤษฎีบท 5.2.11 จะมี $i = 1, 2, \ldots, n$ ซึ่ง p_1 สมทบกับ q_i แต่ด้วยสมบัติการสลับที่ของ R และการเปลี่ยนดรรชนีนั่นคือมีการนิยามวิธีเรียงสับเปลี่ยนบน $\{1, 2, \ldots, n\}$ ทำให้สมมติได้ว่า p_1 สมนัยกับ q_1 จึงมีหน่วย $u_1 \in R$ ซึ่ง $q_1 = p_1 u_1$ และโดยกฎการตัดออกใน R จะได้ $p_2 \cdots p_n = u_1 q_2 \cdots q_m$ และเมื่อดำเนินกระบวนการซ้ำไปเรื่อยๆ n ครั้ง จะได้ $1 = u_1 u_2 \cdots u_n q_{n+1} \cdots q_m$ ทำให้เห็นว่าถ้า $n \neq m$ แล้วแต่ละ $q_{n+1}, \ldots, q_m$ เป็นหน่วยซึ่งขัดแย้งกับการเป็นสมาชิกเฉพาะ ทำให้สรุปได้ว่า $n = m$ และ $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_n\}$ ภายใต้การสมทบ เพราะฉะนั้น R เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว ❐

ในหัวข้อ 5.3 เราจะเห็นตัวอย่างมากมายของโดเมนของการแยกตัวประกอบได้แบบเดียว และจะแสดงในบทที่ 6 ว่าริงพหุนาม $\mathbb{Z}[x]$ เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว แต่ $\mathbb{Z}[x]$ ไม่เป็นโดเมนของไอดีลมุขสำคัญซึ่งแสดงว่าบทกลับของทฤษฎีบท 5.1.13 ไม่เป็นจริง

แบบฝึกหัด 5.2

1. จงพิสูจน์ว่าไอดีลที่ไม่ใช่ไอดีลศูนย์ในโดเมนของไอดีลมุขสำคัญเป็นไอดีลใหญ่สุดเฉพาะกลุ่ม ก็ต่อเมื่อเป็นไอดีลเฉพาะ
2. จงพิสูจน์ว่าถ้า J เป็นไอดีลใน $\mathbb{Z}[i]$ แล้วริงผลหาร $\mathbb{Z}[i]/J$ เป็นริงอันดับจำกัด
3. จงพิสูจน์ว่าอินทิกรัลโดเมน R เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว ก็ต่อเมื่อทุกๆ ไอดีลเฉพาะที่ไม่ใช่ไอดีลศูนย์ใน R บรรจุไอดีลมุขสำคัญที่เป็นไอดีลเฉพาะที่ไม่ใช่ไอดีลศูนย์
4. จงพิสูจน์ว่า $R := \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ เป็นอินทิกรัลโดเมนที่เป็นริงย่อยของฟีลด์ $\mathbb{R}$ โดยมี $2, 3, 4 + \sqrt{10}$ และ $4 - \sqrt{10}$ เป็นสมาชิกลดทอนไม่ได้ซึ่งไม่ใช่สมาชิกเฉพาะ
5. ให้ $\mathbb{Z}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ จงพิสูจน์ว่า $\mathbb{Z}(\sqrt{2})$ เป็นอินทิกรัลโดเมนที่มี $<\sqrt{2}>$ เป็นไอดีลใหญ่สุดเฉพาะกลุ่ม และถ้า $u > 0$ เป็นหน่วยใน $\mathbb{Z}(\sqrt{2})$ จะมีจำนวนเต็มบวก n ซึ่ง $u = \pm\,(1+\sqrt{2})^n$ [**ข้อแนะนำ**: มีจำนวนเต็มบวก n ซึ่ง $(1+\sqrt{2})^n \leq u < (1+\sqrt{2})^{n+1}$ ทำให้ $1 \leq u(1+\sqrt{2})^{-n} < 1+\sqrt{2}$ และถ้า $u(1+\sqrt{2})^{-n} = a + b\sqrt{2}$ แล้ว $a = 1$ และ $b = 0$]

5.3 โดเมนแบบยุคลิด

อินทิกรัลโดเมนขาดสมบัติการเป็นฟีลด์ เพราะอาจมีสมาชิกที่ผกผันไม่ได้ ทำให้ "การหาร" ไม่เป็นการดำเนินการในอินทิกรัลโดเมน อย่างไรก็ตามเราพิสูจน์ขั้นตอนการหารได้ในระบบจำนวนเต็มซึ่งเป็นโดเมนของไอดีลมุขสำคัญ ในหัวข้อนี้ จะศึกษาการวางนัยขั้นตอนการหารในโดเมนของไอดีลมุขสำคัญ โดยสังเกตว่าขั้นตอนการหารของจำนวนเต็มกล่าวในรูปค่าสัมบูรณ์ซึ่งเป็นฟังก์ชันจากเซตของจำนวนเต็มไปยังเซตของจำนวนเต็มที่ไม่เป็นลบ ยุคลิด (Euclid of Alexandria ประมาณ 450 – 380 ปีก่อนคริสต์ศักราช) นักคณิตศาสตร์ชาวกรีก ได้สร้างฟังก์ชันชนิดพิเศษขึ้นเพื่อการวางนัยขั้นตอนการหารในโดเมนของไอดีลมุขสำคัญ จึงนิยมเรียกโดเมนเหล่านี้ว่า "โดเมนแบบยุคลิด" นอกจากนี้ยุคลิดยังสร้างกระบวนการเพื่อหาตัวหารร่วมมากของชุดสมาชิกในโดเมนแบบยุคลิดซึ่งรู้จักกันดีในชื่อ "ขั้นตอนยุคลิด"

5.3.1 **บทนิยาม** ให้ $\mathbb{N}^*$ แทนเซตของจำนวนเต็มที่ไม่เป็นจำนวนลบและ R เป็นริงสลับที่ จะเรียก R ว่า *ริงแบบยุคลิด (Euclidean ring)* โดย δ ถ้ามีฟังก์ชัน $\delta : R \to \mathbb{N}^*$ ซึ่งสอดคล้องสมบัติต่อไปนี้

(ก) $\delta(0) = 0$ และ

(ข) แต่ละ $a,b \in R$ ถ้า $b \neq 0$ แล้วมี $q,r \in R$ ซึ่ง $a = bq + r$ โดย $r = 0$ หรือ $\delta(r) < \delta(b)$

และเรียกริงแบบยุคลิดที่เป็นอินทิกรัลโดเมนว่า *โดเมนแบบยุคลิด (Euclidean domain)*

เราเรียกเงื่อนไขข้อ (ข) ของบทนิยาม 5.3.1 ว่า *ขั้นตอนการหาร (division algorithm)* โดยเรียก q และ r ของขั้นตอนการหารว่า *ผลหาร (quotient)* และ *เศษเหลือ (remainder)* ตามลำดับ

5.3.2 **ตัวอย่าง**

1. ริง $\mathbb{Z}$ ของจำนวนเต็มเป็นโดเมนแบบยุคลิดโดย δ ซึ่งกำหนด $\delta(x) = |x|$ ทุกๆ $x \in \mathbb{Z}$

2. ทุกๆ ฟีลด์ F เป็นโดเมนแบบยุคลิดสำหรับทุกๆ δ ซึ่ง $\delta(0) = 0$ ตัวอย่างเช่น $\delta(a) = 0$ ทุกๆ $a \in F$ เพราะทุกๆ $a,b \in F$ ซึ่ง $b \neq 0$ จะมี $q = ab^{-1} \in F$ ที่ทำให้ $a = bq + 0$

3. ริงของจำนวนเต็มแบบเกาส์ $\mathbb{Z}[i]$ เป็นโดเมนแบบยุคลิดโดย δ ซึ่ง $\delta(a+bi) = a^2 + b^2$ ทุกๆ $a,b \in \mathbb{Z}$ เพราะ $\delta(0) = 0$ และสำหรับขั้นตอนการหารให้ $\alpha = a + bi$ และ $\beta = c + di \neq 0$ เป็นสมาชิกใน $\mathbb{Z}[i]$ แล้ว α และ β เป็นสมาชิกของฟีลด์ $\mathbb{Q}(i)$ จึงมีจำนวนตรรกยะ $r = \dfrac{ac+bd}{c^2+d^2}$ และ $s = \dfrac{bc-ad}{c^2+d^2}$ ซึ่ง $\dfrac{\alpha}{\beta} = r + si$ เลือก p และ q เป็นจำนวนเต็มซึ่ง $|r-p| \leq \frac{1}{2}$ และ $|s-q| \leq \frac{1}{2}$ ให้ $\theta = (r-p) + (s-q)i$ และเลือก $\gamma = \beta\theta$ แล้ว $\gamma = \alpha - (p+qi)\beta \in \mathbb{Z}[i]$ ซึ่งทำให้ได้ $\alpha = (p+qi)\beta + \gamma$ โดยที่ $\delta(\theta) = (r-p)^2 + (s-q)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ จะได้

$$\begin{aligned}\delta(\gamma)=\delta(\theta\beta)&=\delta\left[\left(c(r-p)-d(s-q)\right)+\left(d(r-p)+c(s-q)\right)i\right]\\&=\left(c(r-p)-d(s-q)\right)^2+\left(d(r-p)+c(s-q)\right)^2\\&=\left(c^2+d^2\right)\left((r-p)^2+(s-q)^2\right)=\delta(\theta)\delta(\beta)\le\frac{1}{2}\delta(\beta)<\delta(\beta)\end{aligned}$$ ❍

โดยทั่วไปผลหารและเศษเหลือในขั้นตอนการหารอาจมีได้หลายชุด ทฤษฎีบทต่อไปกล่าวเงื่อนไขจำเป็นและเพียงพอที่ทำให้ผลหารและเศษเหลือดังกล่าวมีได้เพียงชุดเดียว

5.3.3 **ทฤษฎีบท** ให้ R เป็นโดเมนแบบยุคลิดโดย δ ซึ่ง $\delta(ab)=\delta(a)\delta(b)$ ทุกๆ $a,b\in R$ แล้ว ผลหารและเศษเหลือในขั้นตอนการหารจะมีเพียงชุดเดียว ก็ต่อเมื่อ $\delta(a+b)\le\max\{\delta(a),\delta(b)\}$ ทุกๆ $a,b\in R$

บทพิสูจน์ สมมติมี $a,b\in R$ ซึ่ง $\delta(a+b)>\max\{\delta(a),\delta(b)\}$ แล้ว $b=0(a+b)+b$ โดยที่ $\delta(b)\le\max\{\delta(a),\delta(b)\}<\delta(a+b)$ และ $b=0(a+b)+b=1(a+b)-a$ โดยที่ $\delta(-a)=\delta(a)<\delta(a+b)$ ดังนั้นผลหารและเศษเหลือในขั้นตอนการหาร มีได้มากกว่าหนึ่งชุด

ในทางกลับกัน สมมติข้อความ "$\delta(a+b)\le\max\{\delta(a),\delta(b)\}$ ทุกๆ $a,b\in R$" เป็นจริง และให้ $q,q',r,r'\in R$ ซึ่ง $a=bq+r$ และ $a=bq'+r'$ โดยที่ $[r=0$ หรือ $\delta(r)<\delta(b)]$ และ $[r'=0$ หรือ $\delta(r')<\delta(b)]$ แล้ว

$$\delta(q-q')\delta(b)=\delta((q-q')b)=\delta(r-r')\le\max\{\delta(r),\delta(-r')\}<\delta(b)$$

ดังนั้น $\delta(q-q')<1$ ซึ่งทำให้ $\delta(q-q')=0$ นั่นคือ $q-q'=0$ และได้ $q=q'$ และเมื่อแทนค่า $q-q'=0$ ใน $0=b(q-q')+(r-r')$ จะได้ $r-r'=0$ และได้ $r=r'$ เพราะฉะนั้นผลหารและเศษเหลือในขั้นตอนการหารมีได้เพียงชุดเดียว ❐

5.3.4 **ข้อสังเกต** ค่าสัมบูรณ์ใน $\mathbb{Z}$ ไม่สอดคล้องเงื่อนไขของทฤษฎีบท 5.3.3 แม้ว่า $|ab|=|a||b|$ ทุกๆ จำนวนเต็ม a และ b ก็ตาม ตัวอย่างเช่น $|-1-1|=|-2|=2>1=\max\{|-1|,|-1|\}$ ซึ่งจะเห็นว่า $-7=4(-2)+1$ โดยที่ $|1|<|-2|$ และ $-7=3(-2)-1$ โดยที่ $|-1|<|-2|$ เป็นต้น นั่นคือผลหารและเศษเหลือในขั้นตอนการของ $\mathbb{Z}$ ไม่ได้มีเพียงชุดเดียว [แต่สำหรับ $0\le r<|b|$ ผลหารและเศษเหลือในขั้นตอนการของ $\mathbb{Z}$ มีเพียงชุดเดียว]

เราได้พิสูจน์แล้วว่า $\mathbb{Z}$ เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวโดยประยุกต์ขั้นตอนการหาร และขั้นตอนการหารใน $\mathbb{Z}$ เป็นกรณีเฉพาะของริงแบบยุคลิด ทฤษฎีบทต่อไปจะพิสูจน์ความจริงเช่นเดียวกันสำหรับกรณีทั่วไป

5.3.5 **ทฤษฎีบท** โดเมนแบบยุคลิดเป็นโดเมนของไอดีลมุขสำคัญ

บทพิสูจน์ ให้ R เป็นโดเมนแบบยุคลิดโดย δ และ J เป็นไอดีลของ R ถ้า $J=\{0\}=<0>$ แล้ว J เป็นไอดีลมุขสำคัญ จึงพิจารณากรณี $J\neq\{0\}$ แล้วมี $0\neq a\in J$ เรานิยาม $S:=\{\delta(c)|0\neq c\in J\}$ แล้ว $\phi\neq S\subseteq\mathbb{N}$ และเห็นชัดว่า S มีสมาชิกน้อยสุด (ถ้า $0\in S$ แล้ว 0 เป็นสมาชิกน้อยสุดและถ้า $0\notin S$ แล้ว S เป็นเซตย่อยของเซตของจำนวนเต็มบวกที่ไม่ใช่เซตว่าง จะได้โดยหลักการเป็นอันดับดี (well-ordering) ว่า S มีสมาชิกน้อยสุด) นั่นคือมี $0\neq b\in J$ ซึ่ง $\delta(b)$ เป็นสมาชิกน้อยสุดของ S

เพราะว่า $0\neq b\in J$ ดังนั้น $<b>\subseteq J$ ในทางกลับกันให้ $x\in J$ จะได้โดยขั้นตอนการหารว่ามี $q,r\in R$ ซึ่ง $x=bq+r$ โดยที่ $r=0$ หรือ $\delta(r)<\delta(b)$ แต่ถ้า $r\neq 0$ แล้ว $\delta(r)\in S$ โดยที่ $\delta(r)<\delta(b)$ จะขัดแย้งกับการเลือก $b\in J$ ซึ่ง $\delta(b)$ เป็นสมาชิกน้อยสุดใน S ดังนั้น $r=0$ เพราะฉะนั้น $x=bq\in<b>$ ทำให้ได้ $J\subseteq<b>$ เพราะฉะนั้น $J=<b>$ ❐

5.3.6 **บทแทรก** โดเมนแบบยุคลิดเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว

บทพิสูจน์ ให้ R เป็นโดเมนแบบยุคลิดแล้ว R เป็นโดเมนของไอดีลมุขสำคัญโดยทฤษฎีบท 5.3.6 ดังนั้น R เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวโดยทฤษฎีบท 5.2.12 ❐

สมบัติสำคัญมากประการหนึ่งของโดเมนแบบยุคลิดคือมีตัวหารร่วมมากของทุกๆ คู่สมาชิกในโดเมน และสามารถหาได้โดยกระบวนการที่มีชื่อเสียงที่สุดคือ "ขั้นตอนยุคลิด"

5.3.7 **ขั้นตอนยุคลิด** (Euclidean Algorithm) ให้ R เป็นโดเมนแบบยุคลิดโดย δ และ $a,b\in R$ ซึ่ง $b\neq 0$ แล้วประยุกต์ขั้นตอนการหารสำหรับ a และ b ได้ขั้นตอนต่อไปนี้

จะมี $q_0,r_1\in R$ ซึ่ง $a=bq_0+r_1$ โดยที่ $r_1=0$ หรือ $\delta(r_1)<\delta(b)$;

ถ้า $r_1\neq 0$ จะมี $q_1,r_2\in R$ ซึ่ง $b=r_1q_1+r_2$ โดยที่ $r_2=0$ หรือ $\delta(r_2)<\delta(r_1)$;

ถ้า $r_1\neq 0$ จะมี $q_1,r_2\in R$ ซึ่ง $r_1=r_2q_2+r_3$ โดยที่ $r_3=0$ หรือ $\delta(r_3)<\delta(r_2)$;

$$\vdots$$

ถ้า $r_k\neq 0$ จะมี $q_{k+1},r_{k+2}\in R$ ซึ่ง $r_k=r_{k+1}q_{k+1}+r_{k+2}$ โดยที่ $r_{k+2}=0$ หรือ $\delta(r_{k+2})<\delta(r_{k+1})$;

$$\vdots$$

แล้วมีจำนวนเต็มบวกน้อยสุด n ซึ่ง $r_{n+1}=0$ และ $r_n=(a,b)$

บทพิสูจน์ ให้ $a,b\in R$ เพราะว่า R เป็นโดเมนแบบยุคลิด จึงเป็นโดเมนของไอดีลมุขสำคัญ ดังนั้นมี $d\in R$ ซึ่ง $d=(a,b)$ ต่อไปจะแสดงการหา $d=(a,b)$ ด้วยการดำเนินตามขั้นตอนยุคลิดดังกล่าวในเงื่อนไขของทฤษฎีบท แล้วเพราะ $\{\delta(r_k)\}$ เป็นลำดับลดลงโดยแท้ของจำนวนเต็มบวก จึงมีจำนวนเต็มบวกน้อยสุด n ซึ่ง $r_n\neq 0$ แต่ $r_{n+1}=0$

ในการแสดงว่า r_n เป็นตัวหารร่วมของ a และ b จะตั้งต้นด้วยสมการขั้นที่ $n+1$ นั่นคือ $r_{n-1}=r_nq_n$ จึงเห็นชัดว่า $r_n|r_{n-1}$ และ $r_n|r_n$ แล้วดำเนินการแบบอุปนัยตามการลดลงของดรรชนีโดยสมมติว่า $r_n|r_{k+1}$ และ $r_n|r_k$ แล้วโดยสมการขั้นที่ $k+1$ นั่นคือ $r_{k-1}=r_kq_k+r_{k+1}$ ทำให้ได้ $r_n|r_{k-1}$ และเมื่อดำเนินการไปจนถึงขั้นที่ 2 จะได้ $r_n|b$ และโดยสมการขั้นที่ 1 จะได้ $r_n|a$

สุดท้ายจะแสดงว่า $r_n\in<a,b>$ ด้วยกระบวนการทำนองเดียวกันจากสมการขั้นที่ 1 ถึงสมการขั้นที่ $n+1$ ดังนี้ $r_1=a-bq_0\in<a,b>$ แล้วโดยสมการขั้นที่ 2 จะได้ $r_2\in<b,r_1>\subseteq<a,b>$ และโดยอุปนัยวิธีสมมติ $r_{k-1},r_k\in<a,b>$ แล้วสมการขั้นที่ $k+1$ ทำให้ได้ $r_{k+1}=r_{k-1}-r_kq_k\in<r_{k-1},r_k>\subseteq<a,b>$ ดังนั้น $r_n\in<a,b>$ $\square$

ตัวอย่างเช่น ในโดเมนแบบยุคลิด $\mathbb{Z}$ ถ้า $a=2210$ และ $b=1131$ โดยขั้นตอนยุคลิดจะได้

$$1131=(1)1079+52,\ 1079=(20(52)+39,\ 52=(1)(39)+13 \text{ และ } 39=(3)(13)$$

ดังนั้น $(a,b)=13$ และโดยทฤษฎีบทในหัวข้อ 5.1 จะมี $x,y\in\mathbb{Z}$ ซึ่ง $13=ax+by$ ส่วนการหา $x,y\in\mathbb{Z}$ ดังกล่าว เรากระทำกระบวนการย้อนกลับของขั้นตอนยุคลิดเช่นเดียวกัน โดยเริ่มจากสมการก่อนสุดท้ายจะได้

$$\begin{aligned}13 &= 52-(1)(39) = 52-(1)[1079-(20)(52) = (21)(52)-(1)(1079)\\ &= (21)[1131-(1)1079]-(1)1079 = (21)1131+(-22)(1079)\\ &= (21)1131+(-22)[2210-(1)1131] = (-22)(2210)+(43)(1131)\end{aligned}$$

สังเกตว่า $x,y\in\mathbb{Z}$ ในสมการ $(a,b)=ax+by$ ไม่ได้มีแค่เพียงชุดเดียว และโดยความเป็นจริง ถ้าให้ $x'=x+b$ และ $y'=y-a$ แล้ว $ax'+by'=a(x+b)+b(y-a)=ax+by=(a,b)$

ในตอนท้ายของหัวข้อนี้ จะแสดงการประยุกต์แนวคิดดังข้างต้นเพื่อหาเซตคำตอบทั้งหมดของ *สมการไดโอแฟนไทน์อันดับหนึ่ง (First Order Diophantine Equation)* $ax+by=N$ เมื่อ $a,b,N\in\mathbb{Z}$ โดยที่ $a\neq0$ และ $b\neq0$

เริ่มต้นด้วยการสมมติว่าสมการมีอย่างน้อยหนึ่งคำตอบ นั่นคือมี $(x_0,y_0)\in\mathbb{Z}\times\mathbb{Z}$ ซึ่ง $ax_0+by_0=N$ และให้ k เป็นจำนวนเต็มแล้ว

$$a\left(x_0+k\frac{b}{(a,b)}\right)+b\left(y_0-k\frac{a}{(a,b)}\right)=ax_0+by_0+k\frac{ab}{(a,b)}-k\frac{ab}{(a,b)}=ax_0+by_0=N$$

ซึ่งแสดงว่า $\left(x_0+k\frac{b}{(a,b)},y_0-k\frac{a}{(a,b)}\right)$ ก็เป็นคำตอบของ $ax+by=N$ ด้วย

ปัญหาต่อไปก็คือ เมื่อใดสมการ $ax+by=N$ มีคำตอบและจะหาคำตอบหนึ่งของสมการได้อย่างไร เมื่อสังเกตจากรูปแบบของสมการจะได้ว่า $N\in<a,b>$ และในโดเมนแบบยุคลิด $\mathbb{Z}$ ไอดีล $<a,b>$ เป็นไอดีลหลักก่อกำเนิดโดย $d=(a,b)$ นั่นคือ $N\in<d>$ ทำให้ได้ $d|N$ จึงสรุปว่า

"สมการ $ax+by=N$ มีคำตอบ x และ y เป็นจำนวนเต็ม ก็ต่อเมื่อ $(a,b)|N$"

และเพราะ (a,b) เป็นผลบวกเชิงเส้นของ a และ b นั่นคือมี $p,q\in\mathbb{Z}$ ซึ่ง $(a,b)=ap+bq$ และเพราะมี $r\in\mathbb{Z}$ ซึ่ง $N=r(a,b)$ จึงได้ว่า $x_0=rp$ และ $y_0=rq$ เป็นคำตอบหนึ่งของสมการ

เพื่อให้การแสดงว่า $\mathrm{A}=\left\{\left(x_0+k\frac{b}{(a,b)},y_0-k\frac{a}{(a,b)}\right)\middle| k\in\mathbb{Z}\right\}$ เป็นเซตคำตอบทั้งหมดของ $ax+by=N$ เราเหลือเพียงแสดงว่าทุกๆ คำตอบของสมการอยู่ในรูปแบบของสมาชิกในเซต A โดยให้ $(u,v)\in\mathbb{Z}\times\mathbb{Z}$ เป็นคำตอบใดๆ ของ $ax+by=N$ แล้ว $au+bv=N=ax_0+by_0$ ทำให้ได้ $a(u-x_0)=b(y_0-v)$ และเพราะ $d=(a,b)>0$ ดังนั้น $\frac{a}{d}(u-x_0)=\frac{b}{d}(y_0-v)$ นั่นคือ $\frac{b}{d}\,\Big|\,\frac{a}{d}(u-x_0)$ โดยที่ $\left(\frac{a}{d},\frac{b}{d}\right)=1$ จึงได้ $\frac{b}{d}\,\Big|\,(u-x_0)$ ดังนั้นมีจำนวนเต็ม k ที่ทำให้ $u-x_0=k\left(\frac{b}{d}\right)$ ซึ่งสมมูลกับ $u=x_0+k\left(\frac{b}{d}\right)$ และจะได้ $\frac{b}{d}(y_0-v)=\frac{a}{d}(u-x_0)=\left(\frac{a}{d}\right)\left(x_0+k\left(\frac{b}{d}\right)-x_0\right)=k\left(\frac{b}{d}\right)\left(\frac{a}{d}\right)$ ซึ่งสมมูลกับ $y_0-v=k\left(\frac{a}{d}\right)$ และสมมูลกับ $v=y_0-k\left(\frac{a}{d}\right)$ เพราะฉะนั้น (u,v) เป็นสมาชิกของเซต A (ซึ่งเห็นชัดว่าเป็นเซตอนันต์)

แบบฝึกหัด 5.3

1. จงพิสูจน์ว่าฟังก์ชัน δ ที่กำหนดบนโดเมน R ในแต่ละข้อต่อไปนี้ จะทำให้ R เป็นโดเมนแบบยุคลิดโดย δ หรือไม่
   1.1 $R=\mathbb{Z}$ และ $\delta(n)=n^2$ สำหรับทุกๆ $0\neq n\in\mathbb{Z}$
   1.2 $R=\mathbb{Q}$ และ $\delta(a)=a^2$ สำหรับทุกๆ $0\neq a\in\mathbb{Q}$
   1.3 $R=\mathbb{Q}$ และ $\delta(a)=50$ สำหรับทุกๆ $0\neq a\in\mathbb{Q}$
   1.4 $R=\mathbb{Z}[x]=$ เซตของพหุนามเหนือ $\mathbb{Z}$ และ $\delta(f(x))=\deg(f(x))$ เมื่อ $f(x)\neq 0$
   1.5 $R=\mathbb{Z}[x]$ และ $\delta(f(x))=$ ค่าสัมบูรณ์ของสัมประสิทธิ์นำของ $f(x)$ เมื่อ $f(x)\neq 0$
2. จงหาตัวหารร่วมมากของคู่จำนวนเต็ม a และ b ในแต่ละข้อต่อไปนี้ พร้อมทั้งแสดง (a,b) ในรูปผลบวกเชิงเส้นของ a และ b
   2.1 $a=11391$ และ $b=5673$ 2.2 $a=507885$ และ $b=60808$
   2.3 $a=91442056588823$ และ $b=779086434385541$
   2.4 $a=6003722857$ และ $b=77695236973$
   (สังเกตว่าข้อ 2.3 และข้อ 2.4 ประยุกต์ขั้นตอนยุคลิดเพียง 7 ขั้นและ 3 ขั้น ตามลำดับ)

3. ให้ R เป็นโดเมนแบบยุคลิดและ m เป็นจำนวนเต็มน้อยสุดของเซต $\{\delta(c) | 0 \neq c \in R\}$ จงพิสูจน์ว่าสำหรับทุกๆ $0 \neq u \in R$ ถ้า $\delta(u) = m$ แล้ว u เป็นหน่วย และถ้ามี $0 \neq v \in R$ ซึ่ง $\delta(v) = 0$ แล้ว v เป็นหน่วย

4. จงหาตัวก่อกำเนิดของไอดีล $<85, 1+13i>$ และ $<47-13i, 53+56i>$ ใน $\mathbb{Z}[i]$ [**ข้อแนะนำ**: หา $(85, 1+13i)$ และ $(47-13i, 53+56i)$ โดยขั้นตอนยุคลิด]

5. จงหาเซตคำตอบทั้งหมดของสมการไดโอแฟนไทน์อันดับหนึ่ง ในข้อต่อไปนี้

5.1 $2x+4y=5$	5.2 $17x+29y=31$	5.3 $99x+51y=112$
5.4 $164x+41y=99$	5.5 $21x+35y=91$	5.6 $85x+145y=505$
5.7 $56x+72y=8$	5.8 $158x-57y=7$	5.9 $123x+360y=99$

6. จะมีจำนวนเต็มบวก x และ y ที่สอดคล้องเงื่อนไข $x+y=100$, $7|x$ และ $11|y$ หรือไม่ ถ้ามี จงหาจำนวนเต็ม x และ y ทั้งหมดที่สอดคล้องเงื่อนไขดังกล่าว

7. ให้ a,b และ c เป็นจำนวนเต็มซึ่ง $a \neq 0$ และ $b \neq 0$ จงพิสูจน์ว่า

   7.1 $ax+by=a+c$ มีคำตอบ x และ y เป็นจำนวนเต็ม ก็ต่อเมื่อ $ax+by=c$ มีคำตอบ x และ y เป็นจำนวนเต็ม

   7.2 $ax+by=c$ มีคำตอบ x และ y เป็นจำนวนเต็ม ก็ต่อเมื่อ $(a,b)=(a,b,c)$

8. ให้ R เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวและ $0 \neq d \in R$ จงพิสูจน์ว่าจำนวนของไอดีลมุขสำคัญของ R ซึ่งบรรจุไอดีลหลัก $<d>$ มีอยู่เพียงจำนวนจำกัดเท่านั้น [**ข้อแนะนำ** : ถ้า $k \in R$ และ $<d> \subset <k>$ แล้ว $k|d$]

5.4 การวางนัยริงของจำนวนเต็มแบบเกาส์

ตัวอย่างสำคัญของโดเมนแบบยุคลิดคือริง $\mathbb{Z}[i]$ ของจำนวนเต็มแบบเกาส์ซึ่งได้แนะนำไว้แล้วในหัวข้อ 5.1 และโดยขั้นตอนการหารในริงของจำนวนเต็มแบบเกาส์ เราจึงสามารถพิสูจน์ทฤษฎีบทสำคัญในทฤษฎีจำนวน ทฤษฎีบทหนึ่งซึ่งค้นพบโดยนักคณิตศาสตร์ชาวฝรั่งเศสชื่อ แฟร์มาต์ (P. Fermat 1601 – 1665) ทฤษฎีบทนี้รู้จักกันในชื่อนี้ "ทฤษฎีบทของแฟร์มาต์" ซึ่งกล่าวว่า "*จำนวนเฉพาะที่เขียนได้ในรูป $4n+1$ เมื่อ n เป็นจำนวนเต็มบวก เขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็มสองจำนวน*" ในหัวข้อนี้ เราจะศึกษาการสร้างหมู่ของโดเมนแบบยุคลิดที่เป็นภาคขยายของ $\mathbb{Z}[i]$ (กล่าวคือมี $\mathbb{Z}[i]$ รวมอยู่ในหมู่นี้ด้วย)

ให้ D เป็นจำนวนตรรกยะที่ไม่เป็นกำลังสองของจำนวนตรรกยะใดๆ และนิยามเซตย่อย

$$\mathbb{Q}(\sqrt{D}) := \left\{a+b\sqrt{D} \,|\, a,b \in \mathbb{Q}\right\}$$

ของฟีลด์ $\mathbb{C}$ ของจำนวนเชิงซ้อน แล้วเห็นชัดว่าเซตนี้มีสมบัติปิดภายใต้ "การลบ" และ "การคูณ" โดยเอกลักษณ์ $\left(a+b\sqrt{D}\right)-\left(c+d\sqrt{D}\right)=(a-c)+(b-d)\sqrt{D}$ และ $\left(a+b\sqrt{D}\right)\left(c+d\sqrt{D}\right)$ $=(ac+bdD)+(ad+bc)\sqrt{D}$ ตามลำดับ ทำให้ได้ $\mathbb{Q}(\sqrt{D})$ เป็นริงย่อยของ $\mathbb{C}$ (เป็นริงสลับที่) ที่มีเอกลักษณ์และถ้า $D>0$ แล้ว $\mathbb{Q}(\sqrt{D})$ เป็นริงย่อยของ $\mathbb{R}$ แต่เพราะ D ไม่เป็นกำลังสองสมบูรณ์ ทำให้แต่ละสมาชิกใน $\mathbb{Q}(\sqrt{D})$ เขียนได้วิธีเดียวในรูป $a+b\sqrt{D}$ เมื่อ $a,b\in\mathbb{Q}$ นอกจากนี้ $\left(a+b\sqrt{D}\right)\left(a-b\sqrt{D}\right)=a^2-Db^2\neq 0$ สำหรับทุกๆ $a,b\in\mathbb{Q}$ ซึ่ง a และ b ไม่เป็นศูนย์พร้อมกัน แสดงว่าถ้า $a+b\sqrt{D}$ ไม่ใช่ศูนย์ ($a\neq 0$ หรือ $b\neq 0$) แล้ว $\dfrac{a-b\sqrt{D}}{a^2-Db^2}$ เป็นตัวผกผันของ $a+b\sqrt{D}$ ใน $\mathbb{Q}(\sqrt{D})$ เพราะฉะนั้น $\mathbb{Q}(\sqrt{D})$ เป็นฟีลด์ซึ่งเรียกว่า *ฟีลด์กำลังสอง (quadratic field)*)

จำนวน D ในย่อหน้าก่อน อาจเขียนในรูป $D=f^2D'$ เมื่อ f เป็นจำนวนตรรกยะและ D' ไม่เป็นพหุคูณของกำลังสองของจำนวนเต็มที่มากกว่า 1 นั่นคือ $D'=-1$ หรือ D' เป็น ± 1 เท่าของผลคูณของจำนวนเฉพาะที่ต่างกัน [ตัวอย่างเช่น $\frac{8}{5}=D=f^2D'=(\frac{2}{5})(10)$] เรียก D' ว่า *ภาคอิสระกำลังสอง (squarefree part)* ของ D และจาก $\sqrt{D}=f\sqrt{D'}$ จะขอละการพิสูจน์ว่า $\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{D'})$ ไว้เป็นแบบฝึกหัด เราจึงอาจกำหนดให้ D ในย่อหน้าก่อนเป็น *จำนวนเต็มกำลังสองอิสระ (squarefree integer)*

5.4.1 **ทฤษฎีบท** ถ้า D เป็นจำนวนเต็มกำลังสองอิสระแล้ว $\mathbb{Q}(\sqrt{D})$ เป็นฟีลด์ย่อยของฟีลด์ของจำนวนเชิงซ้อน $\mathbb{C}$ ❐

5.4.2 **ข้อสังเกต** เพราะ $-b\in\mathbb{Q}$ ทุกๆ $b\in\mathbb{Q}$ ดังนั้น $a+b\sqrt{D}$ และ $a-b\sqrt{D}$ ต่างเป็นสมาชิกของ $\mathbb{Q}(\sqrt{D})$ ทุกๆ $a,b\in\mathbb{Q}$ จึงเรียก $a-b\sqrt{D}$ ว่า *สังยุค (conjugate)* ของ $a+b\sqrt{D}$ และแทนด้วย $\overline{a+b\sqrt{D}}$ และสังเกตว่าในกรณี $D<0$ สังยุคในความหมายนี้ก็คือสังยุคของจำนวนเชิงซ้อนที่รู้จักกันดีนั่นเอง

นอกจากนี้เห็นชัดว่า $\alpha:\mathbb{Q}(\sqrt{D})\to\mathbb{Q}(\sqrt{D})$ ซึ่งนิยามโดย $\alpha(a+b\sqrt{D})=\overline{a+b\sqrt{D}}=a-b\sqrt{D}$ ทุกๆ $a,b\in\mathbb{Q}$ เป็นอัตสัณฐาน

5.4.3 **ทฤษฎีบท** ให้ D เป็นจำนวนเต็มกำลังสองอิสระ และนิยาม *ฟีลด์นอร์ม (field norm)* $N:\mathbb{Q}(\sqrt{D})\to\mathbb{Q}$ โดย $N(a+b\sqrt{D})=\left(a+b\sqrt{D}\right)\overline{\left(a+b\sqrt{D}\right)}=a^2-Db^2$ ทุกๆ $a,b\in\mathbb{Q}$ แล้ว

1. $N(\alpha)=0$ ก็ต่อเมื่อ $\alpha=0$ ทุกๆ $\alpha\in\mathbb{Q}(\sqrt{D})$
2. *สมบัติการคูณ(multiplicative property)*: $N(\alpha\beta)=N(\alpha)N(\beta)$ ทุกๆ $\alpha,\beta\in\mathbb{Q}(\sqrt{D})$
3. $N(1)=1$

บทพิสูจน์ ให้ $\alpha \in \mathbb{Q}(\sqrt{D})$ แล้วมี $a,b \in \mathbb{Q}$ ซึ่ง $a+b\sqrt{D}$

1. เพราะ $N(\alpha)=0$ ก็ต่อเมื่อ $a^2-Db^2=0$ จะได้ $a=0$ ก็ต่อเมื่อ $b=0$ สมมติ $a\neq 0$ แล้ว $b\neq 0$ ดังนั้น $D=(\frac{a}{b})^2$ ทำให้ D ไม่เป็นจำนวนเต็มหรือ $D=1$ หรือ D เป็นตัวคูณของกำลังสองของจำนวนเต็มที่ไม่ใช่ 1 ซึ่งไม่ว่ากรณีใด จะขัดแย้งกับสมมติฐานของ D จึงได้ $a=0=b$ นั่นคือ $\alpha=0$

2. ให้ $\alpha,\beta \in \mathbb{Q}(\sqrt{D})$ แล้ว $N(\alpha\beta)=\alpha\beta\overline{\alpha\beta}=\alpha\beta\overline{\alpha}\overline{\beta}=(\alpha\overline{\alpha})(\beta\overline{\beta})=N(\alpha)N(\beta)$

3. โดยข้อ 2 จะได้ $N(1)=N(1\cdot 1)=N(1)N(1)$ ดังนั้นโดยกฎการตัดออกใน $\mathbb{Q}$ จะได้ $N(1)=1$ ❐

ให้ $\mathbb{Q}(\sqrt{D})$ เป็นฟีลด์กำลังสองและนิยาม $\omega := \begin{cases} \sqrt{D}, & D\equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{D}}{2}, & D\equiv 1 \pmod 4 \end{cases}$ และ $\mathbb{Z}[\omega] := \{a+b\omega \mid a,b\in\mathbb{Z}\}$ นั่นคือ $\mathbb{Z}[\sqrt{D}] := \{a+b\sqrt{D} \mid a,b\in\mathbb{Z}\}$ เมื่อ $D\equiv 2,3 \pmod 4$ และ $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] := \{a+b\sqrt{D} \mid a,b\in\mathbb{Z}\}$ เมื่อ $D\equiv 1 \pmod 4$ แล้วเห็นชัดว่า $\mathbb{Z}[\omega]$ เป็นริงย่อย (สลับที่) ที่มีเอกลักษณ์ของ $\mathbb{Q}(\sqrt{D})$ และเรียก $\mathbb{Z}[\omega]$ ว่า*ริงของจำนวนเต็ม (ring of integer)* ในฟีลด์กำลังสอง $\mathbb{Q}(\sqrt{D})$

5.4.4 **ทฤษฎีบท** ให้ D เป็นจำนวนเต็มกำลังสองอิสระแล้ว $\mathbb{Z}[\omega]$ เป็นอินทิกรัลโดเมนที่ไม่ใช่ฟีลด์

บทพิสูจน์ เห็นชัดว่า $\mathbb{Z}[\omega]$ เป็นริงย่อยของฟีลด์ $\mathbb{Q}(\sqrt{D})$ และ $1\in\mathbb{Z}[\omega]$ ดังนั้น $\mathbb{Z}[\omega]$ เป็นอินทิกรัลโดเมน และ $1+\sqrt{D}\in\mathbb{Z}[\sqrt{D}]$ ซึ่งมีตัวผกผันในฟีลด์ $\mathbb{Q}(\sqrt{D})$ คือ

$$\frac{1}{1+\sqrt{D}}=\frac{1-\sqrt{D}}{(1+\sqrt{D})(1-\sqrt{D})}=\frac{1-\sqrt{D}}{1-D}=\frac{1}{1-D}-\frac{1}{1-D}\sqrt{D}$$

ถ้า $D\neq 2$ แล้ว $\frac{1}{1-D}\notin\mathbb{Z}$ ดังนั้น $1+\sqrt{D}$ ไม่มีตัวผกผันใน $\mathbb{Z}[\sqrt{n}]$ ส่วน $1+2\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ จะมีตัวผกผันในฟีลด์ $\mathbb{Q}(\sqrt{2})$ คือ $\frac{1}{1+2\sqrt{2}}=\frac{1-2\sqrt{2}}{(1+2\sqrt{2})(1-2\sqrt{2})}=-\frac{1}{7}+\frac{2}{7}\sqrt{2}\notin\mathbb{Z}[\sqrt{2}]$ ดังนั้น $1+2\sqrt{2}$ ไม่มีตัวผกผันใน $\mathbb{Z}[\sqrt{2}]$ เช่นกัน ❐

ถ้ากำหนดให้ $\mathbb{Z}$ คือ $\mathbb{Z}[\sqrt{0}]$ เป็นอินทิกรัลโดเมนที่มี $\mathbb{Q}=\mathbb{Q}(\sqrt{0})$ เป็นฟีลด์เศษส่วนและริงของจำนวนเต็มแบบเกาส์ $\mathbb{Z}[i]$ เป็นอินทิกรัลโดเมนในกลุ่ม $\mathbb{Z}[\sqrt{D}]$ เมื่อ $D=-1\equiv 3 \pmod 4$ นอกจากนี้ $\mathbb{Z}$ และ $\mathbb{Z}[i]$ ยังต่างเป็นโดเมนแบบยุคลิด จึงขอละไว้เป็นแบบฝึกหัดในการพิสูจน์ว่า $\mathbb{Q}(\sqrt{D})$ เป็นฟีลด์เศษส่วนของ $\mathbb{Z}[\sqrt{D}]$ ทุกๆ จำนวนเต็มกำลังสองอิสระ D และเราจะศึกษาต่อไปว่า $\mathbb{Z}[\sqrt{D}]$ เป็นโดเมนแบบยุคลิดสำหรับทุกๆ จำนวนเต็มกำลังสองอิสระ D หรือไม่

เพราะ $\mathbb{Z}[\omega]$ มีสมบัติปิดภายใต้การคูณระหว่างคู่สังยุคจึงเห็นชัดว่า $N:\mathbb{Z}[\omega]\to\mathbb{Z}$ นั่นคือ N เป็นฟังก์ชันกำกัดของฟีลด์นอร์ม N บน $\mathbb{Q}(\sqrt{D})$ ลงบน $\mathbb{Z}[\omega]$ ซึ่งกำหนดสำหรับแต่ละจำนวนเต็มกำลังสองอิสระ D ดังนี้

$$N(a+b\omega)=(a+b\omega)(a+b\overline{\omega}) = \begin{cases} a^2-Db^2, & D\equiv 2,3 \pmod 4 \\ a^2+ab+\frac{1-D}{4}b^2, & D\equiv 1 \pmod 4 \end{cases}$$

ทุกๆ $a,b\in\mathbb{Z}$ เมื่อ $\overline{\omega} = \begin{cases} -\sqrt{D}, & D\equiv 2,3 \pmod 4 \\ \frac{1-\sqrt{D}}{2}, & D\equiv 1 \pmod 4 \end{cases}$

ทฤษฎีบทต่อไปแสดงว่านอร์ม N บน $\mathbb{Z}[\omega]$ เป็นตัวช่วยในการพิจารณาว่าสมาชิกใดใน $\mathbb{Z}[\omega]$ เป็นหน่วยหรือสมาชิกลดทอนไม่ได้

5.4.5 **ทฤษฎีบท** ให้ D เป็นจำนวนเต็มกำลังสองอิสระ และ $\alpha\in\mathbb{Z}[\omega]$ แล้ว

1. $N(\alpha)=\pm 1$ ก็ต่อเมื่อ α เป็นหน่วยใน $\mathbb{Z}[\omega]$
2. ถ้า $N(\alpha)=\pm p$ เมื่อ p เป็นจำนวนเฉพาะแล้ว α เป็นสมาชิกลดทอนไม่ได้

บทพิสูจน์ 1. ให้ $\alpha\in\mathbb{Z}[\omega]$ ซึ่ง $N(\alpha)=\pm 1$ แล้วมี $\overline{\alpha}\in\mathbb{Z}[\omega]$ ซึ่ง $N(\alpha)=\alpha\overline{\alpha}=\pm 1$ จึงได้โดยนิยามว่า α เป็นหน่วยใน $\mathbb{Z}[\omega]$ และในทางกลับกันถ้า $\alpha\in\mathbb{Z}[\omega]$ เป็นหน่วย แล้วมี $\beta\in\mathbb{Z}[\omega]$ ซึ่ง $\alpha\beta=1$ ดังนั้น $N(\alpha)N(\beta)=N(\alpha\beta)=N(1)=1$ และเพราะ $N(\alpha)$ และ $N(\beta)$ ต่างเป็นจำนวนเต็ม จึงได้ $N(\alpha)=N(\beta)=\pm 1$

2. ให้ $\alpha\in\mathbb{Z}[\omega]$ ซึ่ง $N(\alpha)=\pm p$ เมื่อ p เป็นจำนวนเฉพาะแล้ว $N(\alpha)\notin\{0,\pm 1\}$ ดังนั้น $\alpha\neq 0$ และ α ไม่เป็นหน่วยใน $\alpha\in\mathbb{Z}[\omega]$ จึงให้ $\beta,\gamma\in\mathbb{Z}[\omega]$ ซึ่ง $\alpha=\beta\gamma$ แล้ว $N(\beta)N(\gamma)=N(\beta\gamma)=N(\alpha)=\pm p$ ทำให้ได้ $N(\beta)=\pm 1$ หรือ $N(\gamma)=\pm 1$ จึงได้โดยข้อ 1 ว่า β เป็นหน่วยหรือ γ เป็นหน่วย เพราะฉะนั้น α เป็นสมาชิกลดทอนไม่ได้ ❐

สำหรับคำถามว่า $\mathbb{Z}[\omega]$ เป็นโดเมนแบบยุคลิด (ซึ่งทำให้ $\mathbb{Z}[\omega]$ เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว) ทุกๆ จำนวนเต็มกำลังสองอิสระ D หรือไม่ เราจะแสดงก่อนว่ามีตัวอย่างจำนวนเต็มกำลังสองอิสระ D ซึ่ง $\mathbb{Z}[\omega]$ ไม่เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว ไม่เป็นโดเมนของไอดีลมุขสำคัญ และดังนั้น $\mathbb{Z}[\omega]$ ไม่เป็นโดเมนแบบยุคลิด

5.4.6 **ข้อสังเกต** จาก $n(n-1)=n^2-n=(n-\sqrt{n})(n+\sqrt{n})$ และเพราะ n หรือ $n-1$ ตัวใดตัวหนึ่งเป็นจำนวนคู่ทุกๆ จำนวนเต็ม n จึงได้ $2|n(n-1)$ และทำให้ $2|(n-\sqrt{n})(n+\sqrt{n})$ แต่ถ้า n เป็นจำนวนเต็มกำลังสองอิสระแล้ว 2 ไม่เป็นตัวหารทั้งของ $n-\sqrt{n}$ และของ $n+\sqrt{n}$ ทั้งนี้เพราะ

$n-\sqrt{n}=2(\frac{n}{2}-\frac{\sqrt{n}}{2})$ และ $n+\sqrt{n}=2(\frac{n}{2}+\frac{\sqrt{n}}{2})$ โดยที่ $\frac{n}{2}-\frac{\sqrt{n}}{2}$ และ $\frac{n}{2}+\frac{\sqrt{n}}{2}$ ไม่เป็นสมาชิกของ $\mathbb{Z}[\omega]$ สำหรับทุกๆ จำนวนเต็มกำลังสองอิสระ n ดังนั้น 2 ไม่เป็นสมาชิกเฉพาะใน $\mathbb{Z}[\omega]$

5.4.7 **ตัวอย่าง** จะแสดงก่อนว่ามีเพียง ± 1 เท่านั้นที่เป็นหน่วยในอินทิกรัลโดเมน $\mathbb{Z}[\sqrt{-5}]$ โดยสังเกตจาก $N(1)=1=N(-1)$ จึงได้ว่า ± 1 เป็นหน่วย ต่อไปให้ $a+b\sqrt{-5}$ เป็นหน่วยใน $\mathbb{Z}[\sqrt{-5}]$ แล้ว $\pm 1=N(a+b\sqrt{-5})=(a+b\sqrt{-5})(a-b\sqrt{-5})=a^2+5b^2\geq 0$ ดังนั้น $a^2+5b^2=1$ สมมติว่า $b^2>0$ แล้ว $a^2+5b^2\geq 0+5(1)=5>1$ จะเกิดข้อขัดแย้ง จึงได้ว่า $b^2=0$ ซึ่งทำให้ได้ $a^2=1$ นั่นคือ $a+b\sqrt{-5}=a=\pm 1$

ต่อไปจะแสดงว่า $\mathbb{Z}[\sqrt{-5}]$ ไม่เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว โดยสังเกตว่า 9 เขียนในรูปผลคูณของตัวประกอบใน $\mathbb{Z}[\sqrt{-5}]$ ได้อย่างน้อยสองแบบคือ $9=(3)(3)$ และ $9=(2+\sqrt{-5})(2-\sqrt{-5})$ จึงจะแสดงว่าสมาชิกทุกตัวใน $\{2+\sqrt{-5},2-\sqrt{-5},3\}$ ไม่เป็นสมาชิกลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$ และไม่มีคู่ใดสมทบกัน

ให้ $\alpha\in\{2+\sqrt{-5},2-\sqrt{-5},3\}$ และให้ $\beta,\gamma\in\mathbb{Q}(\sqrt{-5})$ ซึ่ง $\alpha=\beta\gamma$ แล้ว $9=N(\alpha)=N(\beta)N(\gamma)$ และเพราะ $N(\beta)$ และ $N(\gamma)$ เป็นจำนวนเต็มบวก จึงได้ $N(\beta)=N(\gamma)=3$ แต่สมการในรูปแบบ $a^2+5b^2=3$ ไม่มีคำตอบเป็นจำนวนเต็ม ดังนั้น $\beta,\gamma\notin\mathbb{Z}[\sqrt{-5}]$ ซึ่งแสดงว่าไม่มีสมาชิกตัวใดใน $\{2+\sqrt{-5},2-\sqrt{-5},3\}$ เป็นสมาชิกลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

สมมติมี $\alpha,\beta\in\{2+\sqrt{-5},2-\sqrt{-5},3\}$ ซึ่ง $\alpha|\beta$ และ $\beta|\alpha$ แล้วมี $\gamma=\pm 1$ เป็นหน่วยใน $\mathbb{Z}[\sqrt{-5}]$ โดยที่ $\alpha=\beta\gamma=\pm\beta$ ซึ่งจะเห็นว่าเป็นไปไม่ได้

สังเกตเพิ่มเติมได้อีกว่า ตัวหารร่วมทั้งหมดของ 9 และ $3(2+\sqrt{-5})$ ได้แก่ $1,3,\ 2+\sqrt{-5}$ โดยทั้ง 3 และ $2+\sqrt{-5}$ ไม่เป็นตัวหารของกันและกัน ดังนั้นจึงไม่มีตัวหารร่วมมากของ 9 และ $3(2+\sqrt{-5})$

เพราะฉะนั้น $\mathbb{Z}[\sqrt{-5}]$ เป็นตัวอย่างของอินทิกรัลโดเมนที่ไม่เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว (และดังนั้นไม่เป็นโดเมนแบบยุคลิด)

เราอาจแสดงว่า $\mathbb{Z}[\sqrt{-5}]$ ไม่เป็นโดเมนแบบยุคลิดได้อีกอย่างหนึ่งคือแสดงว่า $\mathbb{Z}[\sqrt{-5}]$ ไม่เป็นโดเมนของไอดีลมุขสำคัญ โดยสมมติว่ามี $a,b\in\mathbb{Z}$ ซึ่ง $J=<3,2+\sqrt{-5}>=<a+b\sqrt{-5}>$ แล้วจะมี $\alpha,\beta\in\mathbb{Z}[\sqrt{-5}]$ ซึ่ง $3=\alpha(a+b\sqrt{-5})$ และ $2+\sqrt{-5}=\beta(a+b\sqrt{-5})$ ทำให้ได้

$$9=N(3)=N(\alpha)(a^2+5b^2) \text{ และ } 9=N(2+\sqrt{-5})=N(\beta)(a^2+5b^2)$$

เพราะว่า $a^2+5b^2>0$ และ $a^2+5b^2=3$ ไม่มีคำตอบเป็นจำนวนเต็ม ดังนั้น $a^2+5b^2\in\{1,9\}$

ถ้า $a^2+5b^2=9$ แล้ว $N(\alpha)=1$ ทำให้ $\alpha=\pm1$ และได้ $a+b\sqrt{-5}=\pm3$ ซึ่งเป็นไปไม่ได้ ดังนั้น $a^2+5b^2=1$ ทำให้ได้ $a+b\sqrt{-5}=\pm1$ และได้ $1\in\mathbb{Z}[\sqrt{-5}]=J$ จึงมี $\gamma,\delta\in\mathbb{Z}[\sqrt{-5}]$ ที่ทำให้ $1=3\gamma+(2+\sqrt{-5})\delta$ ซึ่งสมมูลกับ $2-\sqrt{-5}=3(2-\sqrt{-5})\gamma+(2-\sqrt{-5})(2+\sqrt{-5})\delta$ $=3[(2-\sqrt{-5})\gamma+3\delta]$ แสดงว่า $2-\sqrt{-5}$ เป็นพหุคูณของ 3 ซึ่งเป็นไปไม่ได้

เพราะฉะนั้น J ไม่ใช่ไอดีลมุขสำคัญ ○

5.4.8 **ทฤษฎีบท** ถ้า $n\in\{-1,-2,2,3\}$ แล้ว $\mathbb{Z}[\sqrt{n}]$ เป็นโดเมนแบบยุคลิด (ดังนั้นเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว)

บทพิสูจน์ ให้ $n\in\{-1,-2,2,3\}$ และ $\delta:\mathbb{Z}[\sqrt{n}]\to\mathbb{N}$ นิยามโดย $\delta(\alpha)=|N(\alpha)|$ ทุกๆ $\alpha\in\mathbb{Z}[\sqrt{n}]$ โดยทฤษฎีบท 5.4.3 จะได้ $\delta(\alpha)=|N(\alpha)|=0$ ก็ต่อเมื่อ $N(\alpha)=0$ ซึ่งก็ต่อเมื่อ $\alpha=0$ และ $\delta(\alpha\beta)=|N(\alpha\beta)|=|N(\alpha)N(\beta)|=|N(\alpha)||N(\beta)|=\delta(\alpha)\delta(\beta)$ ทุกๆ $\alpha,\beta\in\mathbb{Z}(\sqrt{n})$ จึงเหลือเพียงแสดงข้อ (ข) ของบทนิยาม 5.3.1

ให้ $\alpha,\beta\in\mathbb{Z}[\sqrt{n}]$ โดยที่ $\beta\neq0$ แล้ว $\alpha\beta^{-1}\in\mathbb{Q}(\sqrt{n})$ ดังนั้นมี $a,b\in\mathbb{Q}$ ซึ่ง $\alpha=a+b\sqrt{n}$ แล้วเลือกจำนวนเต็ม x และ y ซึ่ง $|a-x|\le\frac{1}{2}$ และ $|b-y|\le\frac{1}{2}$ จะได้

$(a-x)^2\le\frac{1}{4}$ และ $-\frac{n}{4}\le-n(b-y)^2$ จะได้ $-\frac{n}{4}\le(a-x)^2-n(b-y)^2\le\frac{1}{4}$ ถ้า $n>0$ และ $(a-x)^2\le\frac{1}{4}$ และ $0\le-n(b-y)^2\le-\frac{n}{4}$ จะได้ $0\le(a-x)^2-n(b-y)^2\le\frac{1}{4}-\frac{n}{4}$ ถ้า $n<0$ ซึ่งทำให้ได้ $|(a-x)^2-n(b-y)^2|<1$ เมื่อ $n\in\{-1,-2,2,3\}$ ให้ $\sigma=x+y\sqrt{n}$ แล้ว $\sigma\in\mathbb{Z}(\sqrt{n})$ และ $\delta(\alpha\beta^{-1}-\sigma)=|N(\alpha\beta^{-1}-\sigma)|=|N((a-x)+(b-y)\sqrt{n})|=|(a-x)^2-n(b-y)^2|<1$ และให้ $\rho=\beta(\alpha\beta^{-1}-\sigma)$ แล้ว $\alpha=\beta\sigma+\rho$ และเพราะว่า α และ $\beta\sigma$ เป็นสมาชิกของ $\mathbb{Z}[\sqrt{n}]$ ดังนั้น $\rho\in\mathbb{Z}[\sqrt{n}]$ โดยที่ $\delta(\rho)=\delta(\beta(\alpha\beta^{-1}-\sigma))=\delta(\beta)\delta(\alpha\beta^{-1}-\sigma)<\delta(\beta)$ ทำให้ได้ว่ามี $\sigma,\rho\in\mathbb{Z}(\sqrt{n})$ ซึ่ง $\alpha=\beta\sigma+\rho$ โดยที่ $\delta(\rho)<\delta(\beta)$ จึงเป็นอันจบการพิสูจน์ □

5.4.9 **บทแทรก** $\mathbb{Z}[i]$ เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว □

5.4.10 **บทแทรก** ถ้า $n\in\{-1,-2,2,3\}$ แล้ว 2 เป็นสมาชิกลดทอนได้ใน $\mathbb{Z}(\sqrt{n})$ □

สังเกตจากทฤษฎีบท 5.3.3 ผลหารและเศษเหลือในขั้นตอนการหารสำหรับ $\mathbb{Z}(\sqrt{n})$ ซึ่ง $n\in\{-1,-2,2,3\}$ มีได้เพียงชุดเดียวสำหรับแต่ละ $\alpha,\beta\in\mathbb{Z}(\sqrt{n})$ ซึ่ง $\beta\neq0$

แบบฝึกหัด 5.4

1. จงแสดงว่าการพิสูจน์ $\alpha \in \mathbb{Z}[\omega]$ เป็นหน่วยใน $\mathbb{Z}[\omega]$ ก็ต่อเมื่อ $N(\alpha) = \pm 1$ สมมูลกับการหาคำตอบ x และ y ที่เป็นจำนวนเต็มทั้งหมดของสมการ $x^2 - Dy^2 = \pm 1$
2. จงแสดงว่าเมื่อ $D = -1$ $[\equiv 3 \pmod 4]$ กรุปของหน่วยทั้งหมดใน $\mathbb{Z}[i]$ [นั่นคือ $a + bi \in \mathbb{Z}[i]$ ซึ่ง $a^2 + b^2 = \pm 1$] คือกรุป $\{\pm 1, \pm i\}$ อันดับ 4 ส่วน $D = -3$ $[\equiv 1 \pmod 4]$ กรุปของหน่วยทั้งหมดใน $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ [ซึ่งกำหนดโดย $a, b \in \mathbb{Z}$ ทั้งหลายที่ $a^2 + ab + b^2 = \pm 1$ ซึ่งสมมูลกับ $(2a+b)^2 + 3b^2 = \pm 4$] คือกรุป $\{\pm 1, \pm \rho, \pm \rho^2\}$ อันดับ 6 ส่วน $D < 0$ อื่นๆ กรุปของหน่วยทั้งหมดคือ ± 1
3. จงแสดงว่าถ้า $D \in \{3, 5, 6, 7\}$ แล้วกรุปของหน่วยทั้งหมดใน $\mathbb{Z}[\sqrt{D}]$ เป็นกรุปอนันต์ [โดยการแสดงหน่วยที่มีอันดับอนันต์]
4. จงพิสูจน์ว่า $\{a + b(\frac{1+i\sqrt{19}}{2}) | a, b \in \mathbb{Z}\}$ เป็นริงย่อยของฟีลด์ของจำนวนเชิงซ้อนและเป็นโดเมนของไอดีลมุขสำคัญ แต่ไม่เป็นโดเมนแบบยุคลิด
5. ให้ $J_1 = <2, 1+\sqrt{-5}>$, $J_2 = <3, 2+\sqrt{-5}>$ และ $J_3 = <3, 2-\sqrt{-5}>$ เป็นไอดีลของริงของจำนวนเต็ม $\mathbb{Z}[\sqrt{-5}]$ จงพิสูจน์ว่า
   5.1 J_1, J_2 และ J_3 ไม่เป็นไอดีลมุขสำคัญของ $\mathbb{Z}[\sqrt{-5}]$
   5.2 ผลคูณของสองไอดีลที่ไม่ใช่ไอดีลมุขสำคัญอาจเป็นไอดีลมุขสำคัญ [$J_1^2 = <2>$]
   5.3 $J_1 J_2 = <1-\sqrt{-5}>$, $J_1 J_3 = <1+\sqrt{-5}>$ และ $J_1^2 J_2 J_3 = <6>$
6. ให้ D เป็นจำนวนเต็มกำลังสองอิสระและ f เป็นจำนวนเต็มบวก จงพิสูจน์ว่า
   6.1 $\mathbb{Z}[f\omega] := \{a + bf\omega | a, b \in \mathbb{Z}\}$ เป็นริงย่อยของ $\mathbb{Z}[\omega]$ ที่มีเอกลักษณ์
   6.2 ดรรชนีของกรุปการบวก $\mathbb{Z}[f\omega]$ ใน $\mathbb{Z}[\omega]$ คือ f (นั่นคือ $[\mathbb{Z}[\omega] : \mathbb{Z}[f\omega]] = f$)
   6.3 ถ้า H เป็นริงย่อยของ $\mathbb{Z}[\omega]$ ที่มีเอกลักษณ์และดรรชนีของกรุปการบวก $[\mathbb{Z}[\omega] : H] = f$ แล้ว $H = \mathbb{Z}[f\omega]$
7. ให้ K เป็นริงของจำนวนจริงควอเทอร์เนียนในตัวอย่าง 4.2.5 และนิยาม $N : K \to \mathbb{Z}$ โดย $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ ทุกๆ $a, b, c, d \in \mathbb{Z}$ และนิยามสัญลักษณ์ $\overline{a + bi + cj + dk} = a - bi - cj - dk$ จงพิสูจน์ว่า
   7.1 $N(\alpha) = \alpha\bar{\alpha}$ สำหรับทุกๆ $\alpha \in K$
   7.2 $N(\alpha\beta) = N(\alpha)N(\beta)$ สำหรับทุกๆ $\alpha, \beta \in K$
   7.3 $N(\alpha) = \pm 1$ ก็ต่อเมื่อ α เป็นหน่วย สำหรับทุกๆ $\alpha \in K$

7.4 กรุปของหน่วยทั้งหมดใน K สมสัณฐานกับกรุปควอเทอร์เนียนอันดับ 8 [ตัวผกผันในริงของตรรกยะควอเทอร์เนียนของสมาชิก $\alpha \neq 0$ คือ $\frac{\overline{\alpha}}{N(\alpha)}$]

5.5 ทฤษฎีบทของแฟร์มาต์

ให้ p เป็นจำนวนเฉพาะ แล้วโดยขั้นตอนการหารของจำนวนเต็ม จะมีจำนวนเต็ม q และ r ซึ่ง $p = 4q + r$ โดยที่ $r \in \{0,1,2,3\}$ แต่ถ้า $r \in \{0,2\}$ แล้ว $p = 4q$ หรือ $p = 2(2q+1)$ ซึ่งทำให้ p ไม่เป็นจำนวนเฉพาะหรือ $p = 2$ ดังนั้นถ้า p เป็นจำนวนเฉพาะซึ่ง $p \neq 2$ แล้ว p เขียนได้ในรูป $4n+1$ หรือ $4n+3$ เมื่อ n เป็นจำนวนเต็มบวก ในหัวข้อนี้ เราจะประยุกต์โดเมน $\mathbb{Z}[i]$ ของจำนวนเต็มแบบเกาส์ ในการพิสูจน์ว่า จำนวนเฉพาะในรูปแบบ $4n+1$ เมื่อ n เป็นจำนวนเต็มบวกเป็นผลบวกของกำลังสองของจำนวนเต็มสองจำนวน

5.5.1 **ทฤษฎีบท** ให้ p เป็นจำนวนเฉพาะและ c เป็นจำนวนเต็มซึ่ง $(p,c)=1$ ถ้ามีจำนวนเต็ม x และ y ที่ทำให้ $cp = x^2 + y^2$ แล้วมีจำนวนเต็ม a และ b ซึ่ง $p = a^2 + b^2$

บทพิสูจน์ จะพิสูจน์ก่อนว่าจำนวนเฉพาะตามสมมติฐานของทฤษฎีบทไม่ใช่สมาชิกเฉพาะของ $\mathbb{Z}[i]$ โดยสมมติในทางตรงกันข้ามว่า p เป็นจำนวนเฉพาะและเป็นสมาชิกเฉพาะใน $\mathbb{Z}[i]$ แล้ว เพราะ $cp = x^2 + y^2 = (x+yi)(x-yi)$ ดังนั้น $p|(x+yi)$ หรือ $p|(x-yi)$ ถ้า $p|(x+yi)$ แล้ว มี $u,v \in \mathbb{Z}$ ซึ่ง $x + yi = p(u+vi)$ ทำให้ได้ $x = pu$ และ $y = pv$ นั่นคือ $p|x$ และ $p|y$ ดังนั้น $p|(x-yi)$ และโดยการพิสูจน์ในทำนองเดียวกัน ถ้า $p|(x-yi)$ แล้ว $p|(x+yi)$ ดังนั้นไม่ว่ากรณีใดจะได้ $p|(x+yi)$ และ $p|(x-yi)$ จึงได้ว่า $p^2|(x+yi)(x-yi)$ ซึ่งแสดงว่า $p^2|cp$ ทำให้ได้ $p|c$ ซึ่งขัดแย้งกับ $(p,c)=1$

เพราะว่า p ไม่ใช่สมาชิกเฉพาะใน $\mathbb{Z}[i]$ จึงมี $a,b,d,e \in \mathbb{Z}$ ซึ่ง $p = (a+bi)(d+ei)$ โดยที่ $a+bi$ และ $d+ei$ ไม่เป็นหน่วยใน $\mathbb{Z}[i]$ ทำให้ได้ $N(a+bi) = a^2 + b^2 \neq 1$ และ $N(d+ei) = d^2 + e^2 \neq 1$ แต่ $p = (a+bi)(d+ei) = (a-bi)(d-ei)$ จึงได้

$$p^2 = (a+bi)(d+ei)(a-bi)(d-ei) = (a^2+b^2)\ (d^2+e^2)$$

ซึ่งแสดงว่า $(a^2+b^2)|p^2$ ดังนั้น $(a^2+b^2) \in \{1, p, p^2\}$ แต่ $d^2 + e^2 \neq 1$ แสดงว่า $a^2 + b^2 \neq p^2$ และ $a^2 + b^2 \neq 1$ ทำให้ได้ $a^2 + b^2 = p$ จึงเป็นอันจบการพิสูจน์ ❐

5.5.2 **ทฤษฎีบท** ถ้า p เป็นจำนวนเฉพาะในรูปแบบ $4n+1$ เมื่อ n เป็นจำนวนเต็มบวก แล้วมีจำนวนเต็ม x ซึ่ง $p|(x^2+1)$ [นั่นคือ $x^2 \equiv -1 \pmod{p}$]

บทพิสูจน์ ให้ p เป็นจำนวนเฉพาะที่มีจำนวนเต็มบวก n ซึ่ง $p=4n+1$ แต่เพราะ $p-1=4n$ จึงได้ $\frac{p-1}{2}=2n$ ให้ $x=1\cdot 2\cdot 3\cdots\frac{p-1}{2}$ แล้ว x เป็นจำนวนเต็มซึ่งเป็นผลคูณของจำนวนเต็มทั้งหมด $2n$ ตัวซึ่งเป็นจำนวนคู่ จึงได้ว่า

$$x=1\cdot 2\cdot 3\cdots\frac{p-1}{2}=(-1)(-2)(-3)\cdots(-\frac{p-1}{2})$$

และจากความจริงที่ว่า $a\equiv a \pmod p$ ทุกๆ จำนวนเต็ม a ทำให้ได้

$$x^2\equiv\left(1\cdot 2\cdot 3\cdots\frac{p-1}{2}\right)\left((-1)(-2)(-3)\cdots(-\frac{p-1}{2})\right) \pmod p$$

และเนื่องจาก $k\equiv p+k \pmod p$ ทุกๆ จำนวนเต็ม k จะได้ $-1\equiv p-1 \pmod p$, $-2\equiv p-2 \pmod p$, ..., $-\frac{p-1}{2}\equiv p-\frac{p-1}{2}=\frac{p+1}{2} \pmod p$ ทำให้ได้

$$x^2\equiv 1\cdot 2\cdot 3\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) \pmod p$$

แต่ $1\cdot 2\cdot 3\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1)=(p-1)!$ จะได้โดยทฤษฎีบทของวิลสัน (แบบฝึกหัด 5.5 ข้อ 1) ว่า $x^2\equiv(p-1)!\equiv -1 \pmod p$ ❐

5.5.3 ทฤษฎีบทของแฟร์มาต์ (Fermat's Theorem)

ถ้า p เป็นจำนวนเฉพาะในรูปแบบ $4n+1$ เมื่อ n เป็นจำนวนเต็มบวก แล้วมีจำนวนเต็ม a และ b ซึ่ง $p=a^2+b^2$

บทพิสูจน์ ให้ p เป็นจำนวนเฉพาะที่มีจำนวนเต็มบวก n ซึ่ง $p=4n+1$ แล้วโดยทฤษฎีบท 5.5.2 มีจำนวนเต็ม x ซึ่ง $x^2\equiv -1 \pmod p$ และโดยขั้นตอนการหารของจำนวนเต็มจะมีจำนวนเต็ม q และ r ซึ่ง $x=pq+r$ โดยที่ $0\le r<p$ ทำให้ได้ $x\equiv r \pmod p$ และได้ $r^2\equiv x^2\equiv -1$ ดังนั้นมีจำนวนเต็ม r ซึ่ง $0\le r<p$ และ $r^2\equiv -1 \pmod p$

ถ้า $\frac{p}{2}<r<p$ เราให้ $y=p-r$ แล้ว y เป็นจำนวนเต็มซึ่ง $0\le y\le\frac{p}{2}$ และเพราะ $y^2=(p-r)^2=p^2-2pr+r^2$ ดังนั้น $y^2\equiv r^2\equiv -1 \pmod p$ จึงกล่าวได้ว่า

จะมีจำนวนเต็ม r ซึ่ง $0\le r\le\frac{p}{2}$ และ $r^2\equiv -1 \pmod p$

นั่นคือมีจำนวนเต็ม c ซึ่ง $pc=r^2+1$ โดยที่ $pc=r^2+1\le\frac{p^2}{4}+1=\frac{p^2}{4}+\frac{p^2}{p^2}<p^2(\frac{1}{4}+\frac{1}{p^2})<p^2(\frac{1}{4}+\frac{1}{4})$ $[\because p\ge 2\Rightarrow\frac{1}{p^2}<\frac{1}{4}]=\frac{p^2}{2}<p^2$ $[\because\frac{1}{2}<1]$ ทำให้ได้ $1\le c<p$ ดังนั้น $(p,c)=1$ แล้วโดยทฤษฎีบท 5.5.1 จะมีจำนวนเต็ม a และ b ซึ่ง $p=a^2+b^2$ ❐

แบบฝึกหัด 5.5

1. **ทฤษฎีบทของวิลสัน** (Wilson's Theorem)

   ในอินทิกรัลโดเมนถ้า $x^2 = 1$ แล้ว $0 = (x-1)(x+1)$ นั่นคือ $x = \pm 1$ ซึ่งแสดงว่ามีเพียง ± 1 เท่านั้นที่เป็นตัวผกผันของตัวเองภายใต้การคูณ ดังนั้นสมาชิก $2,3,\ldots,p-1$ ในฟีลด์ $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะจะจับคู่กันเป็นตัวผกผันของกันและกัน จงพิสูจน์ว่าถ้า p เป็นจำนวนเฉพาะแล้ว

   1.1 $(2)(3)\ldots(p-1) = 1$ ใน $\mathbb{Z}_p$

   1.2 $(p-2)! = 1 (\bmod p)$ และ $(p-1)!+1 = 0 (\bmod p)$

2. มีจำนวนเฉพาะในรูปแบบ $4n+3$ เมื่อ n เป็นจำนวนเต็มบวก อยู่เป็นจำนวนอนันต์

3. จงพิสูจน์ว่าถ้า p เป็นจำนวนเฉพาะในรูปแบบ $4n+3$ เมื่อ n เป็นจำนวนเต็มบวก แล้วจะไม่มีจำนวนเต็ม x จำนวนใดซึ่ง $x^2 \equiv -1 \pmod p$

4. จงพิสูจน์ว่าไม่มีจำนวนเฉพาะในรูปแบบ $4n+3$ เมื่อ n เป็นจำนวนเต็มบวก ที่เป็นผลบวกของกำลังสองของจำนวนเต็มสองจำนวน

5. ให้ p และ q เป็นจำนวนเฉพาะที่ต่างกัน จงพิสูจน์ว่า

   5.1 $p^{q-1} + q^{p-1} \equiv 1 (\bmod pq)$

   5.2 ถ้า $(p-1)|m$ และ $(p-1)|m$ แล้ว $a^m \equiv 1 (\bmod pq)$ ทุกๆ a ที่ไม่ใช่ตัวคูณของ p และ q และ $a^{m+1} \equiv a (\bmod pq)$ ทุกๆ จำนวนเต็ม a

6. จงวางนัยทั่วไปผลของข้อ 5.2 สำหรับจำนวนเฉพาะ $p_1,\ldots,p_n$ ที่ต่างกันทั้งหมด (โดยไม่ต้องพิสูจน์)

บทที่ 6
ริงพหุนาม

เมื่อกล่าวถึง "พหุนาม" เราจะนึกถึงกลุ่มของฟังก์ชันที่มีรูปแบบเรียบง่ายแต่มีสมบัติพิเศษหลายอย่าง พหุนามจึงมีบทบาทในคณิตศาสตร์เกือบทุกแขนง ตัวอย่างเช่นในเชิงแคลคูลัส พหุนามเป็นฟังก์ชันที่มีความต่อเนื่องและหาอนุพันธ์ได้บนเซตของจำนวนจริงและหาปริพันธ์ได้บนทุกช่วงจำกัด เราได้ศึกษาพหุนามกันมาตั้งแต่ระดับชั้นมัธยมซึ่งเป็นระดับชั้นที่ศึกษาพหุนามในลักษณะการหาค่าผลบวก ผลคูณและการแยกตัวประกอบ ส่วนในระดับสูงขึ้นเราศึกษาพหุนามในลักษณะการเป็นตัวอย่างที่ดีในเชิงแคลคูลัสและการประยุกต์ดังกล่าวแล้ว สำหรับในบทนี้ จะขอแนะนำพหุนามในอีกลักษณะหนึ่งซึ่งแตกต่างจากที่เคยได้รู้จักกันมา กล่าวคือจะศึกษาพหุนามเชิงนามธรรมโดยกำหนดพหุนามเป็นสมาชิกของริง และปรากฏว่าการศึกษาในแนวทางนี้ ทำให้ได้รู้จักสมบัติพิเศษต่างๆ ของพหุนามอีกมากมาย โดยเฉพาะการตอบคำถามที่มีมาช้านานเกี่ยวกับการมีรากของพหุนาม พหุนามลดทอนได้หรือไม่ และการแยกตัวประกอบของพหุนาม เป็นต้น

6.1 กำเนิดและพัฒนาการของพหุนาม

ในหัวข้อนี้ เราจะให้บทนิยามของ "พหุนาม" และกล่าวถึงรูปลักษณ์ของพหุนามในรูปแบบของตัวยังไม่กำหนดหนึ่งตัว พร้อมทั้งศึกษาสมบัติเบื้องต้นของพหุนาม

ให้ R เป็นริง เรียกฟังก์ชันจากเซตของจำนวนเต็มที่ไม่เป็นลบไปยัง R ว่า *ลำดับเหนือ* R *(a sequence over* R*)* และเขียนแทนด้วย $(a_0, a_1, \ldots, a_n, \ldots)$ โดยเรียก $a_k = f(k) \in R$ ทุกๆ จำนวนเต็มที่ไม่เป็นลบ k ว่า *พจน์ที่* k *(the* k^{th} *term)* ของลำดับ ดังนั้นถ้า $f = (a_0, a_1, \ldots)$ และ $g = (b_0, b_1, \ldots)$ เป็นลำดับเหนือ R แล้ว $f = g$ ก็ต่อเมื่อ $a_k = b_k$ ทุกๆ $k = 0, 1, 2, \ldots$

6.1.1 ทฤษฎีบท ให้ R เป็นริงและ $\Im$ แทนเซตของลำดับเหนือ R ทั้งหมดและนิยามการดำเนินการบวก + และการคูณบน $\Im$ สำหรับแต่ละ $f = (a_0, a_1, \ldots) \in \Im$ และ $g = (b_0, b_1, \ldots) \in \Im$ ตามลำดับดังนี้

$$f + g = (a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

และ $\quad fg = (c_0, c_1, \ldots)$ โดยที่ $c_n = \sum_{i=0}^{n} a_{n-i} b_i = a_n b_0 + a_{n-1} b_1 + \cdots a_1 b_{n-1} + a_0 b_n = \sum_{k+j=n} a_k b_j$

แล้ว $(\Im; +, \cdot)$ เป็นริง ยิ่งไปกว่านั้นถ้า R เป็นริงสลับที่หรือริงมีเอกลักษณ์ แล้ว $\Im$ เป็นริงที่มีสมบัติดังกล่าวด้วย ตามลำดับ

บทพิสูจน์ ให้ $f=(a_0,a_1,\ldots)\in\Im$ และ $g=(b_0,b_1,\ldots)\in\Im$ สำหรับทุกๆ จำนวนเต็มที่ไม่เป็นลบ k และ j เพราะ $a_k,b_k,b_j\in R$ ดังนั้น $a_k+b_k\in R$ และ $a_kb_j\in R$ ทำให้ได้ $f+g\in\Im$ และ $fg\in\Im$ และเห็นได้ชัดว่า + สอดคล้องสมบัติการสลับที่และการเปลี่ยนหมู่โดยมี $\overline{0}=(0,0,\ \ldots,0)$ เป็นเอกลักษณ์การบวกและ $-f=(-a_0,-a_1,\ldots)\in\Im$ เป็นสมาชิกลบของ f

ให้ $h=(d_0,d_1,\ldots)\in\Im$ แล้ว $f(gh)=(a_0,a_1,\ldots)(e_0,e_1,\ldots)=(q_0,q_1,\ldots)$ โดยที่ $e_n=\sum_{k+j=n}b_kd_j$ และ $q_m=\sum_{k+j=m}a_ke_j$ ทุกๆ จำนวนเต็มที่ไม่เป็นลบ m และ n และ $(fg)h=(c_0,c_1,\ldots)(d_0,d_1,\ldots)=(p_0,p_1,\ldots)$ โดยที่ $c_n=\sum_{k+j=n}a_kb_j$ และ $p_m=\sum_{k+j=m}c_kd_j$ ทุกๆ จำนวนเต็มที่ไม่เป็นลบ m และ n และเมื่อพิจารณาพจน์ที่ r ใดๆ ของ $f(gh)$ และ $(fg)h$ จะเห็นชัดว่า

$$q_y=\sum_{k+j=y}a_ke_j=\sum_{k+j=y}a_k\left(\sum_{s+t=j}b_sd_t\right)=\sum_{k+s+t=y}a_k(b_sd_t)=\sum_{k+s+t=y}(a_kb_s)d_t$$
$$=\sum_{u+j=y}\left(\sum_{k+s=u}a_kb_s\right)d_j\ =p_y$$

ซึ่งแสดงว่า $f(gh)=(fg)h$ และโดยการจัดรูปในทำนองเดียวกัน ก็จะได้ $f(g+h)=fg+fh$

เห็นชัดว่าถ้า R เป็นริงสลับที่และมีเอกลักษณ์ 1 แล้ว $fg=gh$ ทุกๆ $f,g\in\Im$ และ $(1,0,0,\ldots)$ เป็นเอกลักษณ์การคูณบน $\Im$ ❐

6.1.2 **บทนิยาม** ให้ R เป็นริง จะเรียก $f\in\Im$ ว่า *พหุนามเหนือ* R *(polynomial over* R*)* ถ้ามีจำนวนเต็มที่ไม่เป็นลบ n ซึ่ง $a_k=0$ ทุกๆ จำนวนเต็ม $k>n$ (นั่นคือพจน์ของ f เกือบทั้งหมดเป็นศูนย์ยกเว้นจำนวนจำกัดพจน์เท่านั้น)

ตัวอย่างเช่น $(0,2,3,0,\ldots,0,\ldots)$ เป็นพหุนามเหนือริงของจำนวนเต็มและ $(1,\frac{1}{3},0,-0.2,\ 0\ldots,0,\ldots)$ เป็นพหุนามเหนือริงของจำนวนจริง เป็นต้น

6.1.3 **บทนิยาม** ให้ $f=(a_0,a_1,\ldots,a_n,0,\ldots)$ เป็นพหุนามเหนือริง R สำหรับบางจำนวนเต็มที่ไม่เป็นลบ n จะเรียก a_k ว่า *สัมประสิทธิ์ของพจน์ที่* k *(*k^{th} *coefficient)* ทุกๆ $0\le k\ \le n$ เรียก a_0 ว่า *พจน์คงตัว (constant term)* และถ้า $a_n\neq 0$ จะเรียก a_n ว่า *สัมประสิทธิ์นำของ* f *(leading coefficient of* f*)* และเรียก n ว่า *กำลัง (degree)* ของ f ซึ่งแทนด้วยสัญลักษณ์ $\deg f$

ถ้า $a_n=1$ จะเรียก f ว่า *พหุนามโมนิก (monic polynomial)* และถ้า $a_k=0$ ทุกๆ k นั่นคือ $f=(0,0,\ldots)$ จะเรียก f ว่า *พหุนามศูนย์ (zero polynomial)* และไม่นิยามกำลังของพหุนาม

ศูนย์ ถ้า $a_0 \neq 0$ และ $a_k = 0$ ทุกๆ $k > 0$ จะเรียก f ว่า *พหุนามคงตัว (constant polynomial)* ซึ่งมีกำลังเป็นศูนย์

ตัวอย่างเช่น $(2,0,\ldots,0,\ldots)$ เป็นพหุนามคงตัวและ $(0,-2,0,3,1,0\ldots,0,\ldots)$ เป็นพหุนามโมนิกมีกำลังเป็น 4 เป็นต้น

6.1.4 **ทฤษฎีบท** ให้ f และ g เป็นพหุนามเหนือริงสลับที่ R

1. ถ้า f และ g ต่างไม่ใช่พหุนามศูนย์แล้ว $\deg(f+g) \leq \max\{\deg f, \deg g\}$
2. ถ้า fg ไม่ใช่พหุนามศูนย์แล้ว $\deg(fg) \leq \deg f + \deg g$

บทพิสูจน์ ให้ R เป็นริงสลับที่ f และ g เป็นพหุนามเหนือ R

1. ให้ f และ g ต่างไม่ใช่พหุนามศูนย์ แล้วมีจำนวนเต็ม $n \geq m \geq 0$ ซึ่ง $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$ และ $g = (b_0, b_1, \ldots, b_m, 0, \ldots)$ โดยที่ $a_n \neq 0$ และ $b_m \neq 0$

ถ้า $n > m$ แล้ว $f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_m + b_m, a_{m+1}, \ldots, a_n, 0, \ldots)$ โดยที่ $a_n \neq 0$ ทำให้ได้ $\deg(f+g) = n = \max\{\deg f, \deg g\}$ และถ้า $n = m$ แล้ว $f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, 0, \ldots)$ โดยที่ $a_n + b_n$ อาจเป็นศูนย์ ทำให้ได้ $\deg(f+g) \leq n = \max\{\deg f, \deg g\}$ ดังนั้นไม่ว่ากรณีใด $\deg(f+g) \leq \max\{\deg f, \deg g\}$

2. ให้ fg ไม่ใช่พหุนามศูนย์แล้ว f และ g ต่างไม่ใช่พหุนามศูนย์ จึงมีจำนวนเต็มบวก m และ n ซึ่ง $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$ และ $g = (b_0, b_1, \ldots, b_m, 0, \ldots)$ โดยที่ $a_n \neq 0$ และ $b_m \neq 0$ ทำให้ได้ $fg = (c_0, c_1, \ldots)$ โดยที่ $c_k = a_k b_0 + a_{k-1} b_1 + \cdots a_1 b_{k-1} + a_0 b_k = \sum_{k+j=n} a_k b_j$

ถ้า $i + j = k > n + m$ แล้ว $i > n$ หรือ $j > m$ จะได้ $a_i = 0$ หรือ $b_j = 0$ ซึ่งไม่ว่ากรณีใด $a_i b_j = 0$ ดังนั้น $c_k = 0$ ทุกๆ $k > n + m$ เพราะฉะนั้น $\deg(fg) \leq n + m = \max\{\deg f, \deg g\}$ ❐

6.1.5 **ข้อสังเกต** ถ้า $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$ และ $g = (b_0, b_1, \ldots, b_m, 0, \ldots)$ เป็นพหุนามเหนือริงสลับที่ R โดยที่ $a_n \neq 0$ และ $b_m \neq 0$ เมื่อ $n \geq m$ แล้ว $f - g = f + (-g) = (a_0 - b_0, a_1 - b_1, \ldots, a_m - b_m, a_{m+1}, \ldots, a_n, 0, \ldots)$ โดยที่ $a_k - b_k \in R$ ทุกๆ $0 \leq k \leq n$ ทำให้ได้ $f - g$ เป็นพหุนามเหนือ R นอกจากนี้ $\deg(fg) \leq n + m$ ทำให้ได้ fg เป็นพหุนามเหนือ R ดังนั้นเซตของพหุนามเหนือ R ทั้งหมดเป็นริงย่อยของ $\mathfrak{I}$

6.1.6 **ทฤษฎีบท** ให้ R เป็นอินทิกรัลโดเมนแล้ว

1. เซตของพหุนามเหนือ R ทั้งหมดเป็นอินทิกรัลโดเมน
2. ถ้า f และ g เป็นพหุนามเหนือ R แล้ว $fg = 0$ หรือ $\deg(fg) = \deg f + \deg g$

บทพิสูจน์ ให้ R เป็นอินทิกรัลโดเมน

1. โดยทฤษฎีบท 6.1.1 เราเหลือเพียงแสดงว่าเซตของพหุนามเหนือ R ทั้งหมดไม่มีตัวหาร ขอบท 6.1.4 ข้อ 2 จะได้ว่า $c_k = 0$ ทุกๆ $k > n+m$ สำหรับ $k = n+m$ จะได้

$$c_k = c_{m+n} = a_{n+m}b_0 + a_{n+m-1}b_1 + \cdots a_1 b_{n+m-1} + a_0 b_{n+m} = a_n b_m$$

เพราะ $a_n \neq 0, b_m \neq 0$ และ R ไม่มีตัวหารของศูนย์ ดังนั้น $a_n b_m \neq 0$ จึงได้ $c_{m+n} \neq 0$ ซึ่งแสดงว่า $fg \neq 0$

2. ถ้า $fg \neq 0$ แล้ว f และ g ต่างไม่ใช่พหุนามศูนย์และโดยบทพิสูจน์ข้อ 1 ทำให้ได้ $c_{m+n} \neq 0$ และ $c_k = 0$ ทุกๆ $k > n+m$ ซึ่งแสดงว่า $\deg(fg) = n+m = \deg f + \deg g$ ❐

การพิสูจน์ทฤษฎีบทต่อไป กระทำได้โดยตรงจากบทนิยาม จึงขอละไว้เป็นแบบฝึกหัด

6.1.7 **ทฤษฎีบท** ให้ R เป็นริงสลับที่และ $\wp$ แทนเซตของพหุนามเหนือ R ทั้งหมดแล้ว $\theta : R \to \wp$ ซึ่งนิยามโดย $\theta(a) = (a,0,\ldots,0,\ldots)$ ทุกๆ $a \in R$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง ❐

6.1.8 **ข้อสังเกต** โดยทฤษฎีบท 6.1.7 จะมีริงย่อย $\overline{R} := \{(a,0,\ldots,0,\ldots) | a \in R\}$ ของ $\wp$ ซึ่ง $\overline{R} \cong R$ ดังนั้นสมาชิกของริงทั้งสองมีโครงสร้างเหมือนกัน ริงทั้งสองจึงต่างกันเพียงสัญลักษณ์ที่ใช้แทนสมาชิกของริงเท่านั้น ซึ่งอาจกล่าวว่าสมาชิกที่สมนัยกันของริงทั้งสองใช้แทนกันได้ จึงนิยมแทนพหุนาม $(a,0,\ldots,0,\ldots)$ ด้วย a สำหรับทุกๆ $a \in R$

6.1.9 **ทฤษฎีบท** ให้ R เป็นริงมีเอกลักษณ์ 1 ให้ $x := (0,1,0,\ldots,0,\ldots)$ และสำหรับจำนวนเต็ม $n > 1$ ให้ $x^n := \underbrace{x \cdots x}_{n \text{ times}}$ แล้ว $x^n = (\underbrace{0,\cdots,0}_{n \text{ times}},1,0,\ldots)$ ทุกๆ จำนวนเต็มบวก n

บทพิสูจน์ ให้ R เป็นริงมีเอกลักษณ์ 1 เราจะพิสูจน์โดยอุปนัยเชิงคณิตศาสตร์บน n ซึ่งโดยสมมติฐาน จะได้ทฤษฎีบทเป็นจริงสำหรับ $n = 1$ จึงให้ k เป็นจำนวนเต็มบวกซึ่ง $x^k = (\underbrace{0,\cdots,0}_{k \text{ times}},1,0,\ldots)$ แล้วโดยการคำนวณแบบตรงไปตรงมา จะได้

$$x^{k+1} = x^k x = (\underbrace{0,\cdots,0}_{k \text{ times}},1,0,\ldots)\,(0,1,0,\ldots,0,\ldots) = (\underbrace{0,\cdots,0}_{k+1 \text{ times}},1,0,\ldots)$$

ดังนั้นทฤษฎีบทเป็นจริงสำหรับ $k+1$ แล้วโดยอุปนัยเชิงคณิตศาสตร์จะได้ว่าทฤษฎีบทเป็นจริง ❐

ให้ R เป็นริงมีเอกลักษณ์ 1 และ $f = (a_0,a_1,\ldots,a_n,0,\ldots)$ เป็นพหุนามเหนือ R เมื่อ n เป็นจำนวนเต็มที่ไม่เป็นลบ แล้ว

$$\begin{aligned} f = (a_0,a_1,\ldots,a_n,0,\ldots) &= (a_0,0,\ldots) + (0,a_1,0,\ldots) + \cdots + (\underbrace{0,\ldots,0}_{n},a_n,0,\ldots) \\ &= (a_0,0,\ldots)(1,0,\ldots) + (a_1,0,\ldots)(0,1,0,\ldots) + \cdots + (a_n,0,\ldots)(\underbrace{0,\ldots,0}_{n},1,0,\ldots) \end{aligned}$$

$$= (a_0,0,\ldots)(1,0,\ldots)+(a_1,0,\ldots)x+\cdots+(a_n,0,\ldots)x^n$$

และโดยข้อสังเกต 6.1.8 จะแทน $(1,0,0,\ldots)$ ด้วย 1 และ $(a_k,0,0,\ldots)$ ด้วย $a_k \in R$ ทุกๆ $k = 0,1,2,\ldots,n$ ดังนั้นพหุนามจึงอาจเขียนได้ในรูป $f = a_0 + a_1x + \ldots + a_nx^n$

ในกรณี R เป็นริงที่ไม่มีเอกลักษณ์ แล้วลำดับ $x = (0,1,0,\ldots,0,\ldots)$ ไม่ใช่พหุนามเหนือ R อย่างไรก็ตาม R จะถูกฝังในริง S ที่มีเอกลักษณ์ 1 นั่นคืออาจกล่าวว่า R เป็นริงย่อยของ S และในกรณีเช่นนี้ $x = (0,1,0,\ldots,0,\ldots)$ เป็นพหุนามเหนือ S และทำให้ได้ว่าทุกๆ พหุนามเหนือ R เป็นพหุนามเหนือ S ดังนั้นแต่ละพหุนามเหนือ R จึงยังคงเขียนได้ในรูป

$$f = a_0 + a_1x + \ldots + a_nx^n = \sum_{k=0}^{n} a_kx^k$$

เมื่อ $a_k \in R$ ทุกๆ $k = 0,1,2,\ldots,n$ โดยแทน $x^0 = 1$ และ $a_01 = a_0$ จึงกล่าวในกรณีทั่วไปว่า $x = (0,1,0,\ldots,0,\ldots)$ เป็น *รูปแบบยังไม่กำหนด (indeterminate form)*

เพื่อไม่ให้เกิดความสับสน ต่อไปจะเขียนแทนเซต $\wp$ ของพหุนามเหนือ R ทั้งหมดดังนี้

$$R[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid a_0, a_1, \ldots, a_n \in R\}$$

และแต่ละ $f \in R[x]$ อาจแทนด้วย $f(x)$

แบบฝึกหัด 6.1

1. กำหนดให้ $f(x) = 2x^2 + 3x + 1$ และ $g(x) = 2x^2 + 3x + 1$ จงคำนวณ $f(x) + g(x)$, $f(x) - g(x)$ และ $f(x)g(x)$ ใน $\mathbb{Z}[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_6[x]$ และ $\mathbb{Z}_7[x]$
2. จงหาตัวหารของศูนย์ที่มีกำลัง 0,1 และ 2 ใน $\mathbb{Z}_4[x]$ พร้อมทั้งหาตัวอย่าง $f(x)$ และ $g(x)$ ใน $\mathbb{Z}_4[x]$, $\mathbb{Z}_6[x]$ และ $\mathbb{Z}_9[x]$ ซึ่ง $\deg(fg) < \deg f + \deg g$
3. จงเขียนและบอกจำนวนพหุนามกำลังสองและกำลังสามทั้งหมดใน $\mathbb{Z}_5[x]$ พร้อมทั้งวางนัยกรณีทั่วไป
4. จงหาพหุนาม $f(x)$ ทั้งหมดที่ไม่ใช่พหุนามศูนย์และสอดคล้องสมบัติตามแต่ละข้อต่อไปนี้

   4.1 $f(x) = f(-x)$ 4.2 $f(x) = -f(-x)$ 4.3 $f(x^2) = (f(x))^2$
5. จงพิสูจน์ว่า

   5.1 ถ้า R ไม่เป็นอินทิกรัลโดเมนแล้ว $R[x]$ ไม่เป็นอินทิกรัลโดเมน

   5.2 ถ้า $charR = p$ แล้ว $charR[x] = p$

   5.3 ถ้า S เป็นริงย่อย (ไอดีล) ของริง R แล้ว $S[x]$ เป็นริงย่อย (ไอดีล) ของ $R[x]$

6. ให้ $h: R \to S$ เป็นสาทิสสัณฐานของริง และนิยาม $\overline{h}: R[x] \to S[x]$ โดย

$\overline{h}(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} h(a_k)x^k$ ซึ่งจะเรียก $\overline{h}$ ว่า ฟังก์ชันที่ *ชักนำ (induce)* โดย h

6.1 จงพิสูจน์ว่า $\overline{h}$ เป็นสาทิสสัณฐานซึ่ง $\overline{h}$ เป็นชนิดหนึ่งต่อหนึ่ง (ทั่วถึง) ก็ต่อเมื่อ h เป็นชนิดหนึ่งต่อหนึ่ง (ทั่วถึง) พร้อมทั้งบรรยาย $\ker h$

6.2 ในกรณีเฉพาะเมื่อ $R = \mathbb{Z}$ และ $S = \mathbb{Z}_n$ จงพิสูจน์ว่า $\overline{h}(a(x)) = 0$ ก็ต่อเมื่อ n เป็นตัวหารของทุกๆ สัมประสิทธิ์ของ $a(x)$

7. ให้ $h: R \to S$ เป็นสาทิสสัณฐานของริงและนิยาม $\varphi: R[x] \to S$ โดย $\varphi(f) = h(f(s))$ จงพิสูจน์ว่าถ้า R และ S เป็นริงสลับที่แล้ว φ เป็นสาทิสสัณฐาน

8. ให้ R เป็นริงของเมทริกซ์เหนือ $\mathbb{Z}$ ขนาด 2×2 ทั้งหมด จงพิสูจน์ว่า

8.1 $x^2 - A^2 = (x + A)(x - A) \in R[x]$ สำหรับทุกๆ $A \in R$

8.2 มี $C, A \in R$ ซึ่ง $C^2 - A^2 \neq (C + A)(C - A)$ [ซึ่งแสดงว่าเงื่อนไข " R และ S เป็นริงสลับที่" ในข้อ 7 ละทิ้งไม่ได้

9. ให้ R เป็นริงสลับที่มีเอกลักษณ์และ $f = a_0 + a_1x + \ldots + a_nx^n$ เป็นตัวหารของศูนย์ใน $R[x]$ จงพิสูจน์ว่ามี $0 \neq b \in R$ ซึ่ง $ba_n = ba_{n-1} = \cdots = ba_0 = 0$

10. ให้ G เป็นกรุป (ภายใต้การคูณ) และ R เป็นริงแล้ว $R(G) := \sum_{g \in G} R$ เป็นกรุปผลบวกตรงของกรุปอาบีเลียน R ซึ่งดรรชนีโดย G จงพิสูจน์ว่าถ้า $G = < x >$ เป็นกรุปวัฏจักรขนาดอนันต์แล้ว $R(G) \cong R[x]$

6.2 ขั้นตอนการหารในริงพหุนาม

หัวข้อ 6.1 เรานิยามเซต $R[x] = \{a_0 + a_1x + \ldots + a_nx^n | a_0, a_1, \ldots, a_n \in R\}$ ของพหุนามทั้งหมดเหนือริง R และพิสูจน์ว่าถ้า R เป็นอินทิกรัลโดเมนแล้ว $R[x]$ เป็นอินทิกรัลโดเมน (ทฤษฎีบท 6.1.6) แต่ถ้า R เป็นฟีลด์แล้ว $0 \neq x \in R[x]$ โดยที่ไม่มี $y \in R[x]$ ตัวใดที่ทำให้ $xy = 1$ ซึ่งแสดงว่า $R[x]$ ไม่เป็นฟีลด์ จึงไม่สามารถนิยามการหารใน $R[x]$ อย่างไรก็ตามถ้า R เป็นฟีลด์แล้ว $R[x]$ จะเป็นอินทิกรัลโดเมนที่มีสมบัติพิเศษหลายอย่างเช่นเดียวกับระบบจำนวนเต็ม ตัวอย่างเช่นเมื่อหาร $f \in R[x]$ ด้วย $0 \neq g \in R[x]$ จะได้ผลหารและเศษเหลือเช่นเดียวกับในโดเมนแบบยุคลิด ตัวอย่างเฉพาะเช่นเมื่อหาร x^2 ด้วย $x - 2$ จะได้ผลหารเป็น $x + 2$ โดยมีเศษเท่ากับ 4 (เพราะ $x^2 = (x - 2)(x + 2) + 4$) เป็นต้น ในหัวข้อนี้เราสนใจศึกษาขั้นตอนการหารสำหรับพหุนาม การมีตัวหารร่วมมาก และการเป็นโดเมนชนิดต่างๆ ของ $R[x]$ โดยเฉพาะเมื่อ R เป็นฟีลด์

6.2.1 ขั้นตอนการหารสำหรับพหุนาม (Division Algorithm for Polynomials)

ให้ R เป็นฟีลด์แล้วสำหรับแต่ละ $f, g \in R[x]$ ที่ไม่ใช่พหุนามศูนย์จะมี $q, r \in R[x]$ และมีเพียงคู่เดียวซึ่ง $f = qg + r$ โดยที่ $r = 0$ หรือ $\deg r < \deg g$

บทพิสูจน์ ถ้า $\deg f < \deg g$ แล้ว $q = 0$ และ $r = f$ เป็นพหุนามที่ต้องการ จึงพิจารณากรณี $\deg f \geq \deg g$ แล้วมีจำนวนเต็ม $0 \leq m \leq n$ ซึ่ง $f = \sum_{k=0}^{n} a_k x^k$ และ $g = \sum_{k=0}^{m} b_k x^k$ โดยที่ $a_n \neq 0$ และ $b_m \neq 0$ จะพิสูจน์โดยอุปนัยเชิงคณิตศาสตร์บน $n = \deg f$ ถ้า $n = 0$ แล้ว $m = 0$ ทำให้ $f = a_0$ และ $g = b_0$ และให้ $q = a_0 b_0^{-1}$ และ $r = 0$ แล้ว $f = a_0 = (a_0 b_0^{-1}) b_0 = qg + r$

สมมติทฤษฎีบทเป็นจริงสำหรับทุกๆ พหุนาม f ที่มีกำลังน้อยกว่า n แล้ว $(a_n b_m^{-1} x^{n-m}) g$ เป็นพหุนามกำลัง n ที่มี a_n เป็นสัมประสิทธิ์นำ ทำให้ได้

$$f - (a_n b_m^{-1} x^{n-m}) g = (a_n x^n + \ldots + a_0) - (a_n x^n + \ldots + a_n b_m^{-1} b_0 x^{n-m})$$

เป็นพหุนามที่มีกำลังน้อยกว่า n ดังนั้นโดยสมมติฐานของอุปนัยจะมี $q', r \in R[x]$ ซึ่ง

$$f - (a_n b_m^{-1} x^{n-m}) g = q'g + r$$

โดยที่ $r = 0$ หรือ $\deg r < \deg g$ ดังนั้นมี $q = q' + a_n b_m^{-1} x^{n-m} \in R[x]$ ซึ่ง $f = qg + r$

ต่อไปสมมติว่า $f = q_1 g + r_1$ โดยที่ ($r_1 = 0$ หรือ $\deg r_1 < \deg g$) และ $f = q_2 g + r_2$ โดยที่ ($r_2 = 0$ หรือ $\deg r_2 < \deg g$) แล้ว $(q_1 - q_2) g = r_2 - r_1$ แต่ถ้า $q_1 \neq q_2$ แล้ว

$$\deg g < \deg(q_1 - q_2) + \deg g = \deg(q_1 - q_2) g = \deg(r_2 - r_1) < \deg g$$

ซึ่งเป็นไปไม่ได้ ดังนั้น $q_1 = q_2$ และทำให้ได้ $r_1 = r_2$ ❐

เช่นเดียวกับขั้นตอนการหารในโดเมนแบบยุคลิด เราเรียก f ว่า *ตัวตั้งหาร(dividend)* เรียก g ว่า *ตัวหาร (divisor)* เรียก q ว่า *ผลหาร (quotient)* และเรียก r ว่า *เศษเหลือ (remainder)* และถ้า $r = 0$ แล้ว $f = qg$ ในกรณีเช่นนี้จะกล่าวว่า *g หาร f (g divide f)* หรือ g เป็น *ตัวประกอบ (factor)* ของ f และแทนความหมายนี้ด้วยสัญลักษณ์ $g \mid f$

6.2.2 บทนิยาม

ให้ R เป็นอินทิกรัลโดเมน สำหรับ $c \in R$ และ $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ เราอาจใช้สัญลักษณ์ $f(x)$ แทน $\sum_{k=0}^{n} a_k x^k$ และแทนสมาชิก $\sum_{k=0}^{n} a_k c^k \in R$ ด้วย $f(c)$ โดยเรียกว่า *ค่าของ $f(x)$ ที่ c (the value of $f(x)$ at c)*

6.2.3 ตัวอย่าง

ในการหาเศษจากการหาร $f = 1 + x + x^{11} + x^{111} + x^{1111}$ ด้วย $g = x^2 + 1$ เหนือฟีลด์ $\mathbb{C}$ ของจำนวนเชิงซ้อนทั้งหมด เราประยุกต์ขั้นตอนการหารสำหรับพหุนามว่ามี $q, r \in$

$\mathbb{C}[x]$ ซึ่ง $f = q(x^2+1)+r$ โดยที่ $r = 0$ หรือ $\deg r < \deg g = 2$ ดังนั้น r เป็นพหุนามศูนย์ หรือเป็นพหุนามเชิงเส้นในรูปแบบ $r = ax+b$ โดยที่ $a,b \in \mathbb{C}$ (ที่จะต้องหาต่อไป)

เพราะว่า $i \in \mathbb{C}$ และ $1-2i = 1+i+i^{11}+i^{111}+i^{1111} = q(i^2+1)+(ai+b)$ ทำให้ได้ $a = -2$ และ $b = 1$ ดังนั้น $r = -2x+1$ เป็นเศษเหลือที่ต้องการ ○

6.2.4 **ตัวอย่าง** ให้ $f(x)$ เป็นพหุนามเหนือฟีลด์ $\mathbb{R}$ ของจำนวนจริงทั้งหมดซึ่งเมื่อหารด้วย $x-1$ จะเหลือเศษ 1 เมื่อหารด้วย $x-2$ จะเหลือเศษ 4 เมื่อหารด้วย $x-3$ จะเหลือเศษ 9 และต้องการหาเศษเมื่อหาร $f(x)$ ด้วย $(x-1)(x-2)(x-3)$

วิธีทำ เพราะ $f(x)$ และ $g(x) = (x-1)(x-2)(x-3)$ เป็นพหุนามเหนือ $\mathbb{R}$ ดังนั้นโดยขั้นตอนการหารจะมี $q(x), r(x) \in \mathbb{R}[x]$ ซึ่ง $f(x) = g(x)q(x)+r(x)$ โดยที่ $r = 0$ หรือ $\deg r(x) < 3$ และถ้า $\deg r(x) < 3$ จะเขียน $r(x)$ ได้ในรูปแบบ ax^2+bx+c เมื่อ $a,b,c \in \mathbb{R}$ (ซึ่งจะต้องหาต่อไป) แต่จาก

$$f(x) = (x-1)(x-2)(x-3)q(x)+(ax^2+bx+c)$$

และข้อกำหนด $f(1) = 1,\ f(2) = 4$ และ $f(3) = 9$ จะได้ความสัมพันธ์ต่อไปนี้

$$1 = a+b+c,\quad 4 = 4a+2b+c \quad \text{และ} \quad 9 = 9a+3b+c$$

ทำให้ได้ $a = 1$ และ $b = c = 0$ ดังนั้น $r(x) = x^2$ เป็นเศษที่ต้องการ ○

ดังกล่าวแล้วว่า $R[x]$ จะไม่เป็นฟีลด์แม้ในกรณีที่ R เป็นฟีลด์ก็ตาม แต่ทฤษฎีบท 6.1.6 แสดงว่าถ้า R เป็นฟีลด์แล้ว $R[x]$ เป็นอินทิกรัลโดเมน ดังนั้นโดยทฤษฎีบท 4.6.4 จะมีฟีลด์เศษส่วนของ $R[x]$ ที่เรียกว่า *ฟีลด์ของฟังก์ชันตรรกยะ (field of rational functions)* ซึ่งสมาชิกของฟีลด์เขียนได้ในรูปเศษส่วน $\frac{p(x)}{q(x)}$ ของพหุนามสองพหุนามใน $R[x]$ โดยที่ $q(x) \neq 0$ นอกจากนี้ทฤษฎีบท 6.1.4 ทฤษฎีบท 6.1.6 และขั้นตอนการหารยังแสดงว่า ฟังก์ชันซึ่งนิยาม $\delta : f(x) \to \deg f(x)$ จาก $R[x]$ ไปยังเซต $\mathbb{N}^*$ ของจำนวนเต็มไม่เป็นลบยังแสดงว่า $R[x]$ เป็นโดเมนแบบยุคลิดโดย δ ซึ่งทำให้ $R[x]$ เป็นโดเมนของไอดีลมุขสำคัญและเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว

6.2.5 **ทฤษฎีบท** ถ้า R เป็นฟีลด์ แล้ว

1. $R[x]$ เป็นโดเมนแบบยุคลิด เป็นโดเมนของไอดีลมุขสำคัญและเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว
2. $u \in R[x]$ เป็นหน่วย ก็ต่อเมื่อ $0 \neq u \in R$ (นั่นคือพหุนามคงตัวที่ไม่ใช่ศูนย์)

บทพิสูจน์ ให้ R เป็นฟีลด์แล้ว $R[x]$ เป็นอินทิกรัลโดเมน

1. นิยาม $\delta : R[x] \to \mathbb{N}^*$ โดย $\delta(0) = 0$ และ $\delta(f) = \deg f$ ถ้า $f \neq 0$ แล้วโดยนิยามของ δ ทฤษฎีบท 6.1.6 และทฤษฎีบท 6.2.1 เห็นได้ชัดว่า δ สอดคล้องบทนิยาม 5.3.1 ดังนั้น $R[x]$ เป็นโดเมนแบบยุคลิด ทำให้ได้โดยทฤษฎีบท 5.3.6 และบทแทรก 5.3.7 ว่า $R[x]$ เป็นโดเมนของไอดีลมุขสำคัญและโดเมนของการแยกตัวประกอบได้แบบเดียว

2. เพราะ $u \in R[x]$ เป็นหน่วย ก็ต่อเมื่อ $u \neq 0$ และมี $0 \neq q \in R[x]$ ซึ่ง $uq = 1$ โดยที่ 1 เป็นพหุนามคงตัว จึงมีกำลังเป็นศูนย์ดังนั้น u เป็นหน่วย ก็ต่อเมื่อ $0 = \deg 1 = \deg u + \deg q$ ซึ่งก็ต่อเมื่อ $\deg u = \deg q = 0$ และก็ต่อเมื่อ $0 \neq u \in R$ ❐

6.2.6 **ข้อสังเกต** ถ้า R เป็นฟีลด์แล้ว

1. ถ้า $\{0\} \neq J \subset R[x]$ เป็นไอดีลแท้แล้วมี $0 \neq c(x) \in J$ ซึ่งไม่ใช่หน่วยใน $R[x]$ และกำลังของ $c(x)$ เป็นจำนวนเต็มบวก โดยหลักการเป็นอันดับอย่างดีจะมี $b(x) \in J$ ที่มี**กำลังน้อยสุด**ซึ่ง $< b(x) > \subseteq J$ และถ้า $a(x) \in J$ แล้วโดยขั้นตอนการหารจะมี $q(x), r(x) \in R[x]$ ซึ่ง $a(x) = q(x)b(x) + r(x)$ โดยที่ $r = 0$ หรือ $\deg r(x) < \deg b(x)$ แต่ $a(x), b(x) \in J$ และ J เป็นไอดีลดังนั้น $r(x) \in J$ ถ้า $r \neq 0$ ซึ่งจะขัดแย้งกับการเลือก $b(x)$ จึงได้ว่า $r = 0$ และได้ $a(x) = q(x)b(x) \in < b(x) >$ ดังนั้น $J =< b(x) >$ เป็นไอดีลมุขสำคัญ

2. ให้ $a(x)$ สมทบกับ $b(x)$ ใน $R[x]$ แล้ว $a(x) | b(x)$ และ $b(x) | a(x)$ นั่นคือมี $c(x)$, $d(x) \in R[x]$ ซึ่ง $a(x) = b(x)c(x)$ และ $b(x) = a(x)d(x)$ ทำให้ได้ $c(x)d(x) = 1$ ซึ่งแสดงว่า $c(x)$ และ $d(x)$ เป็นหน่วยใน $R[x]$ ดังนั้น $c(x)$ และ $d(x)$ เป็นพหุนามคงตัว นั่นคือเป็นสมาชิกของฟีลด์ R ทำให้ได้ $a(x) = cb(x)$ และ $b(x) = c^{-1}a(x) = \frac{1}{c}a(x)$

ถ้า $a(x) = a_0 + a_1x + \cdots + a_nx^n$ โดย $a_n \neq 0$ เป็นสัมประสิทธิ์นำแล้วมีพหุนามโมนิก $\frac{a_0}{a_n} + \frac{a_1}{a_n}x + \cdots + x^n = \frac{1}{a_n}a(x)$ เพียงหนึ่งเดียวซึ่งสมทบกับ $a(x)$

ถ้า F เป็นฟีลด์แล้ว $F[x]$ เป็นโดเมนของไอดีลมุขสำคัญ ดังนั้นสำหรับ $a(x), b(x) \in F[x] - \{0\}$ จะได้โดยทฤษฎีบท 5.1.6 ว่ามี $d(x) \in F[x]$ เป็นตัวหารร่วมมากของ $a(x)$ และ $b(x)$ นั่นคือ $d(x) = (a(x), b(x))$ และโดยข้อสังเกต 6.2.6 ข้อ 2 อาจเลือก $d(x)$ ที่เป็นพหุนามโมนิก จึงเป็นข้อตกลงกันว่า $d(x)$ เป็น *ตัวหารร่วมมาก (greatest common divisor)* ของ $a(x)$ และ $b(x)$ ก็ต่อเมื่อ

1. $d(x)$ เป็นพหุนามโมนิกซึ่ง $d(x) | a(x)$ และ $d(x) | b(x)$

และ 2. ถ้า $c(x) \in F[x]$ ซึ่ง $c(x) | a(x)$ และ $c(x) | b(x)$ แล้ว $c(x) | d(x)$

ในกรณีที่ $d(x)$ เป็นหน่วย จะกล่าวว่า $a(x)$ และ $b(x)$ เป็น *พหุนามเฉพาะสัมพัทธ์ (relatively prime polynomial)*

โดยทฤษฎีบท 5.1.6 ถ้า $d(x) = (a(x), b(x))$ แล้ว $d(x)$ เขียนได้ในรูป *ผลบวกเชิงเส้น (linear combination)* ของ $a(x)$ และ $b(x)$ ยุคลิดได้แสดงขั้นตอนการหา $d(x)$ และ $u(x)$, $v(x) \in F[x]$ ที่ทำให้ $d(x) = u(x)a(x) + v(x)b(x)$ ซึ่งขอกล่าวไว้ในขั้นตอนยุคลิดต่อไปนี้

6.2.7 **ขั้นตอนยุคลิด** (Euclidean Algorithm) ให้ F เป็นฟีลด์ และ $a(x), b(x) \in F[x]$ ซึ่ง $a(x) \neq 0$ และ $b(x) \neq 0$ โดยขั้นตอนการหารสำหรับพหุนาม จะมี $q_1(x), r_1(x) \in F[x]$ ซึ่ง

$$a(x) = b(x)q_1(x) + r_1(x) \text{ โดยที่ } r_1 = 0 \text{ หรือ } \deg r_1(x) < \deg b(x)$$

ถ้า $r_1 \neq 0$ โดยขั้นตอนการหารสำหรับพหุนาม จะมี $q_2(x), r_2(x) \in F[x]$ ซึ่ง

$$b(x) = r_1(x)q_2(x) + r_2(x) \text{ โดยที่ } r_2 = 0 \text{ หรือ } \deg r_2(x) < \deg r_1(x)$$

ถ้า $r_2 \neq 0$ โดยขั้นตอนการหารสำหรับพหุนาม จะมี $q_3(x), r_3(x) \in F[x]$ ซึ่ง

$$r_1(x) = r_2(x)q_3(x) + r_3(x) \text{ โดยที่ } r_2 = 0 \text{ หรือ } \deg r_2(x) < \deg r_1(x)$$

$$\vdots$$

และสำหรับ $k \geq 1$ ถ้า $r_k \neq 0$ โดยขั้นตอนการหารสำหรับพหุนาม จะมี $q_3(x), r_3(x) \in F[x]$ ซึ่ง

$$r_{k-1}(x) = r_k(x)q_{k+1}(x) + r_{k+1}(x) \text{ โดยที่ } r_{k+1} = 0 \text{ หรือ } \deg r_{k+1}(x) < \deg r_k(x)$$

เพราะว่า $\deg b(x)$ เป็นจำนวนเต็มที่ไม่เป็นลบ ดังนั้นจะมีลำดับลดลงของจำนวนเต็มบวกที่มีขอบเขตล่างดังนี้

$$\deg b(x) > \deg r_1(x) > \deg r_2(x) > \cdots > \deg r_k(x) > \cdots$$

ทำให้ลำดับนี้ลู่เข้าสู่ลิมิต 0 นั่นคือมีจำนวนเต็มบวก n ซึ่ง

$$r_{n-1}(x) = r_n(x)q_{n+1}(x) \text{ โดยที่ } r_{n+1} = 0$$

แล้วจะแสดงว่า $r_n(x) = (a(x), b(x))$ โดยกระบวนการย้อนกลับของขั้นตอนยุคลิด ดังนี้

จาก $r_{n-1}(x) = r_n(x)q_{n+1}(x)$ จะได้ $r_n(x) | r_{n-1}(x)$

และจาก $r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$ โดยที่ $r_n | r_n$ และ $r_n | r_{n-1}$ จะได้ $r_n | r_{n-2}$

$$\vdots$$

สำหรับ $k \geq 1$ สมมติให้ $r_n | r_{n-t}$ ทุกๆ $0 \leq t < k$ แล้วโดยสมมติฐานขั้นอุปนัยและจาก $r_{n-k}(x) = r_{n-k+1}(x)q_{n-k+2}(x) + r_{n-k+2}(x)$ จะได้ $r_n | r_{n-k+1}$ และ $r_n | r_{n-k+2}$ ทำให้ได้ $r_n | r_{n-k}$

โดยอุปนัยเชิงคณิตศาสตร์อย่างเข้ม จะได้ $r_n | r_k$ ทุกๆ $0 \leq k \leq n-1$ เมื่อให้ $r_0 := b(x)$ เพราะฉะนั้น $r_n(x) | b(x)$ และด้วยเหตุผลเดียวกัน $r_n(x) | a(x)$

ต่อไปสมมติว่า $c(x) \in F[x]$ ซึ่ง $c(x)|a(x)$ และ $c(x)|b(x)$ แล้วจากทุกๆ สมการในขั้นตอนยุคลิด จะเห็นชัดว่า $c(x)|r_k(x)$ ทุกๆ $0 \le k \le n$ ดังนั้น $c(x)|r_x(x)$ ❐

ในการหา $u(x), v(x) \in F[x]$ ซึ่ง $d(x) = u(x)a(x) + v(x)b(x)$ เราดำเนินกระบวนการย้อนกลับขั้นตอนยุคลิดซึ่งจะแสดงให้เห็นในตัวอย่างต่อไปนี้

6.2.8 **ตัวอย่าง** สำหรับพหุนาม $a(x) = x^4 - x^2 + x - 1$ และ $b(x) = x^3 - x^2 + x - 1$ เหนือฟีลด์ $\mathbb{Q}$ ของจำนวนตรรกยะทั้งหมด เราจะดำเนินการตามขั้นตอนยุคลิดดังนี้

$$a(x) = x^4 - x^2 + x - 1 = (x^3 - x^2 + x - 1)(x+1) + (-x^2 + x),$$
$$b(x) = x^3 - x^2 + x - 1 = (-x^2 + x)(-x) + (x-1),$$
$$r_1(x) = (-x^2 + x) = (x-1)(-x) + 0$$

ดังนั้น $(x-1) = (x^4 - x^2 + x - 1,\ x^3 - x^2 + x - 1)$

โดยกระบวนการย้อนกลับขั้นตอนยุคลิด จะได้

$$\begin{aligned}(x-1) &= 1(x^3 - x^2 + x - 1) + (x)(-x^2 + x)\\ &= 1(x^3 - x^2 + x - 1) + x[(x^4 - x^2 + x - 1) - (x^3 - x^2 + x - 1)(x+1)]\\ &= x[(x^4 - x^2 + x - 1)\\ &= x[(x^4 - x^2 + x - 1) + (1 - x - x^2)(x^3 - x^2 + x - 1)\end{aligned}$$ ❍

แบบฝึกหัด 6.2

1. จงพิสูจน์ความจริงของข้อความในข้อต่อไปนี้
   1.1 ถ้า R เป็นริงที่มีตัวหารของศูนย์แล้ว $R[x]$ เป็นริงที่มีตัวหารของศูนย์
   1.2 ถ้า R เป็นริงและ $a(x), b(x) \in R[x]$ มีกำลัง 3 และ 4 ตามลำดับแล้ว $a(x)b(x)$ อาจมีกำลัง 8
   1.3 ถ้า R เป็นริงแล้ว x ไม่ใช่ตัวหารของศูนย์ใน $R[x]$
   1.4 ถ้า R เป็นอินทิกรัลโดเมน แล้วทุกๆ หน่วยใน $R[x]$ เป็นหน่วยใน R
   1.5 $\mathbb{Z}[x]$ เป็นโดเมนแบบยุคลิดหรือเป็นโดเมนของการแยกตัวประกอบได้แบบเดียว
2. จงแสดงว่า $\{a + xf(x) | a \in 2\mathbb{Z}$ และ $f(x) \in \mathbb{Z}[x]\}$ เป็นไอดีลของ $\mathbb{Z}[x]$ แต่ไม่เป็นไอดีลมุขสำคัญ
3. จงหาตัวหารร่วมมากของคู่พหุนามในข้อต่อไปนี้
   3.1 $x^3 - 6x^2 + x + 4$ และ $x^5 - 6x + 1$
   3.2 $x^2 + 1$ และ $x^6 + x^3 + x + 1$

4. จงหาผลหารและเศษเหลือเมื่อหาร x^3+2 ด้วย $2x^2+3x+4$ ใน $\mathbb{Z}[x]$, ใน $\mathbb{Z}_3[x]$ และใน $\mathbb{Z}_5[x]$
5. จงหาพหุนาม $f(x)$ ที่มีกำลังน้อยสุดที่จะเป็นไปได้ซึ่งเมื่อหาร $f(x)$ ด้วย $(x-1)^2$ และด้วย $(x-2)^3$ แล้วเหลือเศษ $2x$ และ $3x$ ตามลำดับ
6. จงพิสูจน์ว่าถ้า $m>1$ เป็นจำนวนเต็มแล้ว $x+2$ ไม่เป็นตัวหารของ x^m+2 ใน $\mathbb{Z}[x]$ แต่ $x+(n-1)$ เป็นตัวหารของ $x^m+(n-1)$ ใน $\mathbb{Z}_n[x]$ ทุกๆ จำนวนเต็มบวก n และ m
7. ให้ $\overline{h}$ เป็นดังในแบบฝึกหัด 6.1 ข้อ 6 จงพิสูจน์ว่าถ้า $f(x)$ เป็นตัวหารของ $g(x)$ แล้ว $\overline{h}(f(x))$ เป็นตัวหารของ $\overline{h}(g(x))$
8. ในกระบวนการของขั้นตอนยุคลิด จงพิสูจน์ว่า $(a(x),b(x)) = (b(x),r_1(x)) = \cdots = (r_{n-1}(x),r_n(x)) = r_n(x)$
9. ให้ F และ K เป็นฟีลด์ซึ่ง $F \subseteq K$ จงพิสูจน์ว่าถ้า $f(x),g(x) \in F[x]$ เป็นพหุนามเฉพาะสัมพัทธ์ แล้ว $f(x)$ และ $g(x)$ เป็นพหุนามเฉพาะสัมพัทธ์ใน $K[x]$
10. ให้ R เป็นอินทิกรัลโดเมนซึ่งมี F เป็นฟีลด์เศษส่วน จงพิสูจน์ว่าแต่ละ $f(x)$ ใน $F[x]$ เขียนได้ในรูป $\dfrac{f_0(x)}{a}$ เมื่อ $f_0(x) \in R[x]$ และ $a \in R$

6.3 รากและการมีรากของพหุนาม

การศึกษาพหุนามเหนือฟีลด์ สิ่งสำคัญอย่างหนึ่งคือการหารากทั้งหมดของพหุนามในฟีลด์นั้นๆ เพราะทำให้สามารถหาตัวประกอบเชิงเส้นของพหุนามได้ทั้งหมด ในหัวข้อนี้ จะศึกษาสมบัติที่เกี่ยวกับรากของพหุนามและเงื่อนไขซึ่งทำให้พหุนามเหนือฟีลด์มีตัวประกอบเชิงเส้น

ถ้า R เป็นริงมีเอกลักษณ์ $c \in R$ และ $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$ เป็นพหุนามกำลัง n ขอทบทวนว่าสัญลักษณ์ $f(c)$ หมายถึงสมาชิก $\sum_{k=0}^{n} a_k c^k \in R$ โดยเรียกว่า "ค่าของ $f(x)$ ที่ c" หรือ "การแทนค่า $f(x)$ ด้วย c" เราเริ่มต้นด้วยผลพลอยได้ของขั้นตอนการหารที่ทำให้ได้ทฤษฎีบทที่สำคัญต่อไปนี้

6.3.1 **ทฤษฎีบทเศษเหลือ** (Remainder Theorem) ให้ R เป็นอินทิกรัลโดเมนและ $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$ แล้วสำหรับแต่ละ $c \in R$ จะมี $q(x) \in R[x]$ เพียงหนึ่งเดียวซึ่ง $f(x) = (x-c)q(x) + f(c)$ [นั่นคือ $f(c)$ คือเศษเหลือจากการหาร $f(x)$ ด้วย $x-c$]

บทพิสูจน์ ให้ R เป็นอินทิกรัลโดเมน $f(x)=\sum_{k=0}^{n} a_k x^k \in R[x]$ และ $c \in R$ ถ้า $f=0$ เลือก $q=0$ แล้ว $f(c)=0$ เป็นเศษเหลือจากการหาร $f(x)$ ด้วย $x-c$ จึงพิจารณากรณีที่มีจำนวนเต็มไม่เป็นลบ n ซึ่ง $f(x)=\sum_{k=0}^{n} a_k x^k$ โดยที่ $a_n \neq 0$ แล้วโดยขั้นตอนการหารจะมี $q(x), r(x) \in R[x]$ ซึ่ง $f(x)=(x-c)q(x)+r(x)$ โดยที่ $r(x)=0$ หรือ $\deg r(x)<1$ นั่นคือ $r(x)$ เป็นพหุนามคงตัวและ $\deg q(x)=n-1$

ให้ $q(x)=\sum_{k=0}^{n-1} q_k x^k \in R[x]$ แล้ว $\sum_{k=0}^{n} a_k x^k = (x-c)\sum_{k=0}^{n-1} q_k x^k + r$ และเมื่อกระจายผลคูณทางขวาของสมการและเปรียบเทียบสัมประสิทธิ์ที่สมนัยกันของพหุนามเดียวกันจะได้

$$
\begin{array}{lll}
q_{n-1}=a_n, & & \\
q_{n-2}-cq_{n-1}=a_{n-1} & \text{ซึ่งสมมูลกับ} & q_{n-2}=cq_{n-1}+a_{n-1}, \\
q_{n-3}-cq_{n-2}=a_{n-2} & \text{ซึ่งสมมูลกับ} & q_{n-3}=cq_{n-2}+a_{n-2}, \\
\vdots & & \vdots \\
q_1-cq_2=a_2 & \text{ซึ่งสมมูลกับ} & q_1=cq_2+a_2, \\
q_0-cq_1=a_1 & \text{ซึ่งสมมูลกับ} & q_0=cq_1+a_1 \\
\text{และ}\quad r-cq_0=a_0 & \text{ซึ่งสมมูลกับ} & r=cq_0+a_0
\end{array}
$$

และเมื่อแทนค่าย้อนกลับ จะได้

$$
\begin{aligned}
r &= cq_0+a_0 = c(cq_1+a_1)+a_0 = c^2q_1+ca_1+a_0 = \cdots = \\
&= c^n a_n + c^{n-1}a_{n-1}+\cdots+ca_1+a_0 = f(c)
\end{aligned}
$$

□

ตัวอย่างเช่นเศษเหลือเมื่อหาร $f(x)=4x^2-2x+7 \in \mathbb{Q}[x]$ ด้วย $(x-3) \in \mathbb{Q}[x]$ คือ $f(3)=4(3)^2-2(3)+7=37$ และเมื่อหาร $f(x)$ ด้วย $(2x+1) \in \mathbb{Q}[x]$ จะได้เศษคือ $f(-\frac{1}{2})=4(-\frac{1}{2})^2-2(-\frac{1}{2})+7=9$ เป็นต้น

6.3.2 **บทนิยาม** ถ้า $f(c)$ ในทฤษฎีบทเศษเหลือเป็นศูนย์ (นั่นคือ $f(c)=0$ เมื่อ $c \in R$) จะเรียก c ว่า *ราก (root)* ของพหุนาม $f(x)$ และกล่าวว่า $f(x)$ มีรากใน R

สังเกตว่าถ้า $f(c)$ ในทฤษฎีบทเศษเหลือเป็นศูนย์แล้ว $x-c$ เป็นตัวประกอบของ $f(x)$ เราจึงได้ทฤษฎีบทตัวประกอบต่อไปนี้

6.3.3 **ทฤษฎีบทตัวประกอบ** (Factor Theorem) ให้ R เป็นอินทิกรัลโดเมนและ $c \in R$ แล้ว c เป็นรากของ $f(x) \in R[x]$ ก็ต่อเมื่อ $f(c)=0$ ซึ่งก็ต่อเมื่อ $x-c$ เป็นตัวประกอบของ $f(x)$

บทพิสูจน์ โดยทฤษฎีบทเศษเหลือจะได้ $f(c)=0$ ก็ต่อเมื่อ $x-c$ เป็นตัวประกอบของ $f(x)$ และโดยนิยามของรากของ $f(x)$ จะได้ว่าถ้า c เป็นรากของ $f(x)$ แล้ว $f(c)=0$ ซึ่งทำให้ได้ $x-c$ เป็นตัวประกอบของ $f(x)$ ในทางกลับกันให้ $x-c$ เป็นตัวประกอบของ $f(x)$ แล้วจะมี $h(x)\in R[x]$ ซึ่ง $f(x)=(x-c)h(x)=(x-c)q(x)+f(c)$ โดยที่ $f(c)$ เป็นค่าคงตัวจึงได้ $(x-c)[h(x)-q(x)]$ มีกำลังเป็นศูนย์ ในขณะที่ $x-c$ มีกำลัง 1 จึงเป็นไปได้กรณีเดียวคือ $h(x)-q(x)$ เป็นพหุนามศูนย์ซึ่งทำให้ได้ $f(c)=0$ ❐

ตัวอย่างเช่น พิจารณา $f(x)=x^2+1$ เป็นพหุนามเหนือฟีลด์ $\mathbb{Z}_5$ ของจำนวนเต็มมดูโล 5 จะได้ $f(2)=2^2+1=0\in\mathbb{Z}_5$ ดังนั้น 2 เป็นรากของ x^2+1 ใน $\mathbb{Z}_5$ เป็นต้น

6.3.4 **ตัวอย่าง** จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้พหุนาม $(x+1)(x+2)\cdots(x+n)+n!$ มีรากเป็นจำนวนเต็มอย่างน้อยหนึ่งรากในฟีลด์ $\mathbb{R}$

วิธีทำ ให้ n เป็นจำนวนเต็มบวกและ $f(x)=(x+1)(x+2)\cdots(x+n)+n!\in\mathbb{R}[x]$ สังเกตว่าถ้า n เป็นจำนวนคี่แล้ว

$$\begin{aligned}f(-(n+1))&=(-(n+1)+1)(-(n+1)+2)\cdots(-(n+1)+n)+n!\\&=(-n)(-(n-1))\cdots(-2)(-1)+n!=(-1)^n(n-1)\cdots(2)(1)+n!\\&=(-1)^n n!+n!=0\end{aligned}$$

ซึ่งแสดงว่า $-n-1$ เป็นรากที่เป็นจำนวนเต็มตัวหนึ่งของ $f(x)$ จึงให้ n เป็นจำนวนคู่และ c เป็นจำนวนเต็มถ้า $c\geq 0$ แล้ว

$$f(c)=(c+1)(c+2)\cdots(c+n)+n!\geq 2n!>0$$

ดังนั้น c ไม่เป็นรากของ $f(x)$ และถ้า $-n\leq c\leq -1$ แล้ว $1\leq -c\leq n$ จึงได้ $c-c=0$ เป็นตัวประกอบหนึ่งในผลคูณ $(c+1)(c+2)\cdots(c+n)$ ทำให้ได้ $f(c)=0+n!\neq 0$ ซึ่งแสดงว่า c ไม่เป็นรากของ $f(x)$ และสุดท้ายถ้า $c<-n$ แล้ว $c+k<0$ ทุกๆ $k\in\{1,2,\ldots,n\}$ ทำให้ได้ $(c+1)(c+2)\cdots(c+n)=(-1)^n|c+1||c+2|\cdots|c+n|>0$ จึงได้ว่า $f(c)>n!>0$ ซึ่งแสดงว่า c ไม่เป็นรากของ $f(x)$ อีกเช่นกัน ดังนั้นไม่ว่ากรณีใด ถ้า n เป็นจำนวนคู่แล้ว c ไม่เป็นรากของ $f(x)$ เพราะฉะนั้น $f(x)$ ไม่มีรากเมื่อ n เป็นจำนวนคู่

เพราะฉะนั้นจำนวนเต็มบวก n ทั้งหมดที่ต้องการคือ n ที่เป็นจำนวนคี่ ❍

6.3.5 **ทฤษฎีบท** ให้ D เป็นอินทิกรัลโดเมนซึ่งเป็นโดเมนย่อยของอินทิกรัลโดเมน E และ $f(x)\in D[x]$ มีกำลังเป็นจำนวนเต็มบวก n แล้ว f มีรากที่แตกต่างกันทั้งหมดไม่เกิน n รากใน E

บทพิสูจน์ ให้ m เป็นจำนวนเต็มบวกและ $c_1, c_2, \ldots, c_m \in E$ เป็นรากที่แตกต่างกันทั้งหมดของ $f(x)$ แล้วโดยทฤษฎีบทตัวประกอบ $x - c_1$ เป็นตัวประกอบของ $f(x)$ ดังนั้นมี $q_1(x) \in E[x]$ ซึ่ง $f(x) = q_1(x)(x - c_1)$ แต่ c_2 เป็นรากของ $f(x)$ ดังนั้น $f(c_2) = 0$ และโดยการแทนค่าจะได้ $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$ โดยที่ $(c_2 - c_1) \neq 0$ และ E เป็นอินทิกรัลโดเมน ดังนั้น $q_1(c_2) = 0$ ซึ่งแสดงว่า c_2 เป็นรากของ $q_1(x)$ และในทำนองเดียวกันจะมี $q_2(x) \in E[x]$ ซึ่ง $f(x) = q_2(x)(x - c_2)(x - c_1)$ เมื่อดำเนินกระบวนการเช่นนี้ไป m ครั้ง ผลคูณ $(x - c_m)\cdots$ $\cdots(x - c_1)$ จะเป็นตัวหารของ $f(x)$ โดยที่ $\deg(x - c_m)\cdots(x - c_1) = m$ ดังนั้น $m \leq n$ ❐

ทฤษฎีบทต่อไป แนะนำวิธีการตรวจสอบว่าสมาชิกตัวใดในฟีลด์เศษส่วนของโดเมนของการแยกตัวประกอบได้แบบเดียว D เป็นรากของ $f(x) \in D[x]$

6.3.6 **ทฤษฎีบทการมีรากเศษส่วน** (Rational Root Test) ให้ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวและ F เป็นฟีลด์เศษส่วนของ D และให้ $f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$ ถ้า $u = \frac{c}{d} \in F$ โดยที่ $(c, d) = 1$ และ u เป็นรากของ $f(x)$ แล้ว $c | a_0$ และ $d | a_n$

บทพิสูจน์ ให้ u เป็นรากของ $f(x)$ แล้ว $f(u) = 0$ ทำให้ได้

$$0 = a_0 + a_1(\frac{c}{d}) + a_2(\frac{c}{d})^2 + \cdots + a_n(\frac{c}{d})^n$$

ซึ่งสมมูลกับ $0 = a_0 d^n + a_1 c d^{n-1} + a_2 c^2 d^{n-1} + \cdots + a_n c^n$ ทำให้ได้

$$a_0 d^n = c\left(\sum_{k=1}^{n} (-a_k) c^{k-1} d^{n-k}\right) \quad \text{และ} \quad -a_n c^n = d\left(\sum_{k=0}^{n-1} c^k a^{n-k-1}\right)$$

แต่ $(c, d) = 1$ ดังนั้น $c | a_0$ จากสมการแรกและ $d | a_n$ จากสมการที่สอง ❐

6.3.7 **ตัวอย่าง** เมื่อจะหารากตรรกยะของ $f(x) = x^4 - 2x^3 - 7x^2 - \frac{11}{3}x - \frac{4}{3} \in \mathbb{Q}[x]$ เราสังเกตว่า $f \in \mathbb{Q}[x]$ และ $3f = 3x^4 - 6x^3 - 21x^2 - 11x - 4 \in \mathbb{Z}[x]$ มีรากตรรกยะชุดเดียวกัน จึงประยุกต์ทฤษฎีบท 6.3.6 กับ $3f$ ได้ว่าจำนวนตรรกยะทั้งหมดที่อาจเป็นรากของ $3f$ ได้แก่ $\pm 1, \pm 2, \pm 4, \pm \frac{1}{3}, \pm \frac{2}{3}$ และ $\pm \frac{4}{3}$ แล้วโดยการแทนค่าจะได้ 4 เท่านั้นที่เป็นรากตรรกยะของ $3f$ ○

6.3.8 **ทฤษฎีบท** ให้ $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ และ $\frac{r}{s}$ เป็นรากตรรกยะของ f โดยที่ $(r, s) = 1$ แล้ว $(r - sk) | f(k)$ ทุกๆ จำนวนเต็ม k

บทพิสูจน์ ให้ $q(x) = s^n f(\frac{x}{s})$ แล้ว $q(x) = a_n x^n + a_{n-1} s x^{n-1} + \cdots + a_1 s^{n-1} x + a_0 s^n \in \mathbb{Z}[x]$ โดยเฉพาะอย่างยิ่ง $q(r) = s^n f(\frac{r}{s}) = 0$ และ $q(ks) = s^n f(k)$ ทุกๆ จำนวนเต็ม k

ให้ k เป็นจำนวนเต็มและ $m = |r - sk|$ ถ้า $r - sk = 0$ แล้ว $k = \frac{r}{s}$ จะได้ $r - sk$ เป็นตัวประกอบของ $f(k) = 0$ จึงสมมติให้ $r - sk \neq 0$ แล้ว m เป็นจำนวนเต็มบวกและจาก $sk \equiv r \pmod{m}$ จะได้ $q(ks) \equiv q(r) = 0$ นั่นคือ $m | q(ks)$ ดังนั้น $m | s^n f(k)$ แต่ $(m,s) = 1$ จะได้ว่า $m | f(k)$ และได้ว่า $(r - sk) | f(k)$ ตามต้องการ ❐

6.3.9 **ตัวอย่าง** จงหารากตรรกยะทั้งหมดของพหุนาม $3x^4 + 5x^3 + x^2 + 5x - 2$

วิธีทำ ให้ $\frac{r}{s}$ เป็นรากตรรกยะของ $f(x) = 3x^4 + 5x^3 + x^2 + 5x - 2$ โดยเลือก r และ s ซึ่ง $(r,s) = 1$ และ $s > 0$ แล้วโดยทฤษฎีบทการมีรากเศษส่วนจะได้ $\frac{r}{s} \in \{\pm 1, \pm\frac{1}{3}, \pm 2, \pm\frac{2}{3}\}$

ต่อไปประยุกต์ทฤษฎีบท 6.3.8 เพื่อตรวจสอบว่า $\frac{r}{s}$ ตัวใดในย่อหน้าก่อนเป็นรากของ $f(x)$ โดยเริ่มตรวจสอบว่าจำนวนเต็ม ± 1 เป็นรากหรือไม่ (ทั้งนี้เพราะ ± 1 เป็นจำนวนเต็มที่สะดวกต่อการคำนวณ) เพราะว่า $f(1) = 12$ และ $f(-1) = 8$ ดังนั้น ± 1 ไม่ใช่รากของ $f(x)$ ต่อไปสร้างตารางค่าของ $\frac{r}{s}$, $r - s$ และ $r + s$ เพื่อตรวจสอบว่า $\pm\frac{1}{3}, \pm 2$ หรือ $\pm\frac{2}{3}$ ตัวใดเป็นรากของ $f(x)$ โดยอาศัย $f(1) = 12$ และ $f(-1) = 8$ ดังนี้

$\frac{r}{s}$	$\frac{1}{3}$	$-\frac{1}{3}$	2	-2	$\frac{2}{3}$	$-\frac{2}{3}$	
$r-s$	-2	-4	1	-3	-1	-5	$f(1) = 12$
$r+s$	4	2	3	-1	5	1	$f(-1) = 8$

เพราะ ± 5 ไม่เป็นตัวประกอบของ 8 และ 12 ส่วน 3 ไม่เป็นตัวประกอบของ 8 จึงเหลือเพียง $\frac{r}{s} \in \{\pm\frac{1}{3}, -2\}$ ที่ต้องตรวจสอบว่าเป็นรากของ $f(x)$ หรือไม่ และพบว่า $f(-\frac{1}{3}) = -\frac{100}{27}$ แต่ $f(\frac{1}{3}) = f(-2) = 0$ ดังนั้นรากตรรกยะทั้งหมดของ $f(x)$ คือ $\frac{1}{3}$ กับ -2 ❍

ให้ D เป็นอินทิกรัลโดเมนและ $f \in D[x]$ ถ้า $c \in D$ เป็นรากของ f แล้วโดยทฤษฎีบทตัวประกอบจะมี $h(x) \in D[x]$ ซึ่ง $f(x) = (x - c)h(x)$ และทฤษฎีบท 6.3.5 แสดงให้เห็นว่ามีจำนวนเต็มบวก m มากสุดและ $g(x) \in D[x]$ ซึ่ง $f(x) = (x - c)^m g(x)$ โดยที่ $x - c$ ไม่เป็นตัวหารของ $g(x)$ นั่นคือ $g(c) \neq 0$ ถ้า $m > 1$ จะกล่าวว่า $f(x)$ มี *ตัวประกอบเชิงเส้นซ้ำ (linear repeated factor)* ใน $D[x]$ และกล่าวว่า c เป็น *รากซ้ำ (multiple root)* ของ f ใน D สำหรับ $m = 1$ เราเรียก c ว่า *รากเชิงเดียว (simple root)* ของ f ใน D และเรียก m ว่า *ภาวะรากซ้ำ (multiplicity)* ของราก c

ตัวอย่างเช่นพหุนาม $(x^2 + 1)(x + 1)^2$ เหนือฟีลด์ $\mathbb{R}$ มี -1 เป็นรากซ้ำใน $\mathbb{R}$ เป็นต้น

6.3.10 **ตัวอย่าง** จงหาจำนวนจริง a และ b และจำนวนเต็มบวก n ทั้งหมดที่ทำให้ 1 เป็นรากซ้ำอย่างน้อยสองครั้งของพหุนาม $f(x) = x^n - ax^{n-1} + bx - 1$

วิธีทำ สังเกตว่า $f(x)$ มี 1 เป็นรากก็ต่อเมื่อ $0 = f(1) = 1^n - a1^{n-1} + b - 1 = -a + b$ ซึ่งก็ต่อเมื่อ $a = b$ นอกจากนี้ 1 เป็นรากซ้ำอย่างน้อยสองครั้ง ทำให้ได้ $n \geq 2$

ถ้า $n = 2$ แล้ว $f(x) = x^2 - (a-b)x - 1 = x^2 - 1 = (x-1)(x+1)$ แต่ 1 ไม่เป็นรากซ้ำของ $x^2 - 1$ จึงได้ว่า $n \geq 3$ และเพราะว่า

$$f(x) = x^n - ax^{n-1} + ax - 1 = (x^n - 1) - ax(x^{n-2} - 1)$$
$$= (x-1)[x^{n-1} + \cdots + x + 1 - ax(x^{n-3} + \cdots + x + 1)]$$

ดังนั้นถ้า 1 เป็นรากซ้ำอย่างน้อยสองครั้งของ $f(x)$ แล้ว 1 จะเป็นรากของพหุนาม $x^{n-1} + \cdots + x + 1 - ax(x^{n-3} + \cdots + x + 1)$ จึงได้ว่า

$$0 = (1^{n-1} + \cdots + 1 + 1) - a(1^{n-3} + \cdots + 1 + 1) = n - a(n-2)$$

ซึ่งทำให้ได้ $a = \dfrac{n}{n-2}$ ดังนั้นคำตอบของโจทย์คือ $a = b = \dfrac{n}{n-2}$ ทุกๆ $n \geq 3$

ตัวอย่างเช่นถ้า $n = 3$ แล้ว $a = b = 3$ ดังนั้น 1 เป็นรากซ้ำอย่างน้อยสองครั้งของ $f(x) = x^3 - 3x^2 + 3x - 1 = (x-1)^3$ หรือถ้า $n = 4$ แล้ว $a = b = 2$ ดังนั้น 1 เป็นรากซ้ำอย่างน้อยสองครั้งของ $f(x) = x^4 - 2x^3 + 2x - 1 = (x^4 - 1) - 2x(x^2 - 1) = (x^2 - 1)(x^2 - 2x + 1)$ $= (x-1)^3(x+1)$ เป็นต้น ○

ในการตรวจสอบว่าพหุนามใดมีรากซ้ำหรือไม่ เราต้องการมโนคติของอนุพันธ์รูปนัย

6.3.11 **บทนิยาม** ให้ D เป็นอินทิกรัลโดเมนและ $f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$ เรียกพหุนาม $\sum_{k=1}^{n} k a_k x^{k-1} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in D[x]$ ว่า *อนุพันธ์รูปนัย (formal derivative)* ของ f และแทนด้วยสัญลักษณ์ f' [**หมายเหตุ** เราใช้ชื่อ "อนุพันธ์รูปนัย" เพราะว่าไม่ได้นิยาม f' ในรูปของลิมิต]

ทฤษฎีบทต่อไป พิสูจน์ได้โดยตรงจากบทนิยาม จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

6.3.12 **ทฤษฎีบท** ให้ D เป็นอินทิกรัลโดเมน $c \in D$ และ $f, g \in D[x]$ แล้ว

$(cf)' = cf'$, $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$ และ $(g^n)' = ng^{n-1}g'$ สำหรับทุกๆ จำนวนเต็มบวก n □

6.3.13 **ทฤษฎีบท** ให้ D เป็นอินทิกรัลโดเมนซึ่งเป็นโดเมนย่อยของอินทิกรัลโดเมน E และ $f(x) \in D[x]$ แล้ว

1. $c \in E$ เป็นรากซ้ำของ f ก็ต่อเมื่อ $f(c) = 0$ และ $f'(c) = 0$

2. ถ้า D เป็นฟีลด์และ f และ f' เป็นสมาชิกเฉพาะสัมพัทธ์ แล้ว f ไม่มีรากซ้ำใน E

บทพิสูจน์ 1. ให้ $m \geq 0$ เป็นภาวะรากซ้ำของ c ซึ่งเป็นรากของ $f(x) \in D[x]$ แล้ว $f(x) = (x-c)^m g(x)$ โดยที่ $g(c) \neq 0$ แล้วโดยทฤษฎีบท 6.3.12 จะได้

$$f'(x) = m(x-c)^{m-1} g(x) + (x-c)^m g'(x)$$

ถ้า c เป็นรากซ้ำของ f แล้ว $m > 1$ ทำให้ได้ $f'(c) = 0$

ในการพิสูจน์บทกลับให้ $f(c) = 0$ และ $f'(c) = 0$ และเพราะ $f(c) = 0$ จะได้ $m \geq 1$ และถ้า $m = 1$ แล้ว $f'(x) = g(x)$ ทำให้ได้ $0 = f'(c) = g(c)$ ซึ่งขัดแย้งกับ $g(c) \neq 0$ ดังนั้น $m > 1$ นั่นคือ c เป็นรากซ้ำของ f

2. ให้ D เป็นฟีลด์แล้ว $0 \neq 1 \in D \subseteq E$ และให้ f และ f' เป็นสมาชิกเฉพาะสัมพัทธ์กันแล้วโดยทฤษฎีบท 5.1.6 จะมี $u, v \in D[x]$ ซึ่ง $uf + vf' = 1$ สมมติว่า f มีรากซ้ำใน E นั่นคือมี $c \in E$ ซึ่งเป็นรากซ้ำของ f แล้วโดยข้อ 1 จะได้ $f(c) = 0$ และ $f'(c) = 0$ ทำให้ได้ $1 = u(c)f(c) + v(c)f'(c) = 0$ เกิดข้อขัดแย้งกันเอง ดังนั้น f ไม่มีรากซ้ำใน E ❐

แบบฝึกหัด 6.3

1. ให้ D เป็นอินทิกรัลโดเมนและ $f(x), a(x), b(x) \in D[x]$ จงพิสูจน์ว่าถ้า $f(x) = a(x)b(x)$ แล้วรากทุกๆ รากของ $a(x)$ และ $b(x)$ เป็นรากของ $f(x)$
2. จงหาจำนวนจริง a และ b ทั้งหมดที่ทำให้ $x-2$ เป็นตัวประกอบร่วมของ $x^2 + ax - ab$ และ $x^3 - ax^2 + \frac{a}{4}x + 2b$ เหนือฟีลด์ของจำนวนจริงทั้งหมด $\mathbb{R}$
3. ให้ $f(x) \in \mathbb{R}[x]$ จงพิสูจน์ว่า
   3.1 ถ้า $z \in \mathbb{C}$ เป็นรากของ $f(x)$ แล้วสังยุค $\overline{z}$ เป็นรากของ $f(x)$
   3.2 ถ้า $f(x)$ ไม่ใช่พหุนามศูนย์และ $z \in \mathbb{C}$ เป็นรากซ้ำ m ครั้งของ $f(x)$ แล้ว $\overline{z}$ เป็นรากซ้ำ m ครั้งของ $f(x)$
   3.3 ถ้า $\deg f$ เป็นจำนวนคี่แล้ว $f(x)$ มีรากเป็นจำนวนจริง
4. จงพิสูจน์ว่าถ้า D เป็นอินทิกรัลโดเมนแล้ว $D[x]$ ไม่เป็นโดเมนของไอดีลหลัก
   [ข้อแนะนำ: พิจารณาไอดีล $< x, c >$ เมื่อ $c \in D$ เป็นสมาชิกลดทอนไม่ได้]
5. ให้ F เป็นฟีลด์และ $f, g \in F[x]$ จงพิสูจน์ว่าถ้า $\deg g \geq 1$ แล้วมีพหุนาม $f_0, f_1, \ldots, f_r \in F[x]$ เพียงชุดเดียวซึ่ง $f = f_0 + f_1 g + f_2 g^2 + \ldots + f_r g^r$ โดยที่ $\deg f_i < \deg g$ ทุกๆ $0 \leq i \leq r$

6. ให้ D เป็นอินทิกรัลโดเมนและ $f \in D[x]$ โดยที่ $\deg f > 0$ จงพิสูจน์ว่า

6.1 ถ้า $char(D) = 0$ แล้ว $f' \neq 0$

6.2 ถ้า $char(D) = p$ แล้ว $f' \neq 0$ ก็ต่อเมื่อ $f \in D[x^p]$ (นั่นคือ f เขียนได้ในรูป $f = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{jp} x^{jp}$)

7. ให้ F เป็นฟีลด์ $a_0, a_1, \ldots, a_n$ เป็นสมาชิกที่ต่างกันใน F และ $c_0, c_1, \ldots, c_n \in F$ จงพิสูจน์ว่า $f(x) = \sum_{i=0}^{n} \frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n} c_i$ เป็นพหุนามหนึ่งเดียวใน $F[x]$ ซึ่ง $f(a_i) = c_i$ ทุกๆ $0 \leq i \leq n$ [ข้อแนะนำ: แสดงก่อนว่ามีพหุนาม $f(x) \in F[x]$ กำลัง $n+1$ อย่างมากพหุนามเดียวซึ่ง $f(a_i) = c_i$ ทุกๆ $0 \leq i \leq n$]

8. ให้ $f(x) = a_n x^n + \cdots + a_0$ เป็นพหุนามเหนือ $\mathbb{R}$ ของจำนวนจริงทั้งหมด จงพิสูจน์ว่า

8.1 แต่ละ $a, c \in \mathbb{R}$ ซึ่ง $c > 0$ จะมี $M > 0$ ซึ่ง $|f(a+h) - f(a)| \leq M|h|$ ทุกๆ $h \in \mathbb{R}$ ที่ $|h| \leq c$

8.2 **ทฤษฎีบทค่ากลาง** (Intermed iate Value Theorem) ถ้า $a, b, d \in \mathbb{R}$ ซึ่ง $a < b$ และ $f(a) < d < f(b)$ แล้วมี $c \in \mathbb{R}$ ซึ่ง $a < c < b$ และ $f(c) = d$ [ข้อแนะนำ: เลือก c เป็นขอบเขตบนน้อยสุดของ $\{x \mid a < x < b$ และ $f(x) \leq d\}$ แล้วประยุกต์ข้อ 8.1]

8.3 ถ้า $g \in \mathbb{R}[x]$ มีกำลังเป็นจำนวนคี่แล้ว g มีรากจริง [ข้อแนะนำ: เลือก $a, b \in \mathbb{R}$ ที่เหมาะสมซึ่ง $g(a) < 0$ และ $g(b) > 0$ แล้วประยุกต์ข้อ 8.2]

6.4 การลดทอนได้ของพหุนาม

เราทราบจากหัวข้อ 6.2 แล้วว่า ริงของพหุนามเหนือฟีลด์เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว และในบทที่ 5 เราได้แสดงว่า แต่ละสมาชิกที่ไม่ใช่ศูนย์และไม่ใช่หน่วยในโดเมนของการแยกตัวประกอบได้แบบเดียว เขียนได้แบบเดียวในรูปผลคูณของสมาชิกลดทอนไม่ได้ของโดเมนนั้น ในหัวข้อนี้ เราศึกษาหาเงื่อนไขของพหุนามที่จะเป็นพหุนามลดทอนไม่ได้ อย่างไรก็ตามหัวข้อก่อนๆ ได้มีการจำแนกพหุนามที่เป็นหน่วยในริงพหุนาม และได้แสดงหมู่ของพหุนามที่แยกตัวประกอบต่ออีกไม่ได้ไปบ้างแล้ว จึงขอเริ่มต้นด้วยการเขียนสรุปไว้ในทฤษฎีบทต่อไปนี้

6.4.1 ทฤษฎีบท ให้ D เป็นอินทิกรัลโดเมน

1. $u \in D[x]$ เป็นหน่วย ก็ต่อเมื่อ u เป็นพหุนามคงตัวซึ่งเป็นหน่วยใน D โดยเฉพาะพหุนาม u เหนือฟีลด์เป็นหน่วย ก็ต่อเมื่อ u เป็นพหุนามคงตัวที่ไม่ใช่ศูนย์

2. ถ้า $c \in D$ เป็นสมาชิกลดทอนไม่ได้แล้วพหุนาม c เป็นสมาชิกลดทอนไม่ได้ใน $D[x]$

3. ทุกๆ พหุนามเชิงเส้นที่มีสัมประสิทธิ์นำเป็นหน่วยใน D เป็นสมาชิกลดทอนไม่ได้ใน $D[x]$ โดยเฉพาะทุกๆ พหุนามเชิงเส้นเหนือฟีลด์เป็นสมาชิกลดทอนไม่ได้

บทพิสูจน์ 1. ใช้การพิสูจน์ทฤษฎีบท 6.2.5 ข้อ 2 จะได้ $u \in D[x]$ เป็นหน่วย ก็ต่อเมื่อมี $0 \neq q \in D[x]$ ซึ่ง $uq = 1$ ซึ่งก็ต่อเมื่อ $\deg u = \deg q = 0$ และก็ต่อเมื่อ $u, q \in D$ โดยที่ $uq = 1$ ดังนั้น ก็ต่อเมื่อ u เป็นพหุนามคงตัวซึ่งเป็นหน่วยใน D

2. ให้ $u, v \in D[x]$ ซึ่ง $0 \neq c = uv$ แล้วเพราะ D เป็นอินทิกรัลโดเมน ดังนั้น $u \neq 0$, $v \neq 0$ และ $0 = \deg c = \deg u + \deg v$ ทำให้ได้ $\deg u = \deg v = 0$ นั่นคือ $u, v \in D$ แล้ว โดยทฤษฎีบท 6.4.1 ข้อ 1 จะได้ว่า u และ v เป็นหน่วยใน $D[x]$

3. ให้ $ax + b \in D[x]$ โดยที่ $a \neq 0$ เป็นหน่วยใน D และให้ $u, v \in D[x]$ ซึ่ง $ax + b = uv$ เพราะว่า a เป็นหน่วยใน D ดังนั้น $u \neq 0$, $v \neq 0$ และ $\deg u + \deg v = 1$ จึงได้ $\deg u = 0$ (และ $\deg v = 1$) หรือ $\deg v = 0$ (และ $\deg u = 1$) นั่นคือ u หรือ v เป็นหน่วยใน $D[x]$

$\square$

6.4.2 **ข้อสังเกต** ถ้า D เป็นโดเมนย่อยของอินทิกรัลโดเมน E แล้ว**อาจ**มี $f \in D[x] \subset E[x]$ ซึ่ง f เป็นสมาชิกลดทอนไม่ได้ใน $E[x]$ แต่ f ลดทอนได้ใน $D[x]$ ตัวอย่างเช่น $2x + 2 = 2(x+1)$ เป็นสมาชิกลดทอนได้ใน $\mathbb{Q}[x]$ เพราะทุกสมาชิกในฟีลด์ $\mathbb{Q}$ เป็นหน่วยใน $\mathbb{Q}[x]$ แต่ทั้ง 2 และ $x+1$ ไม่เป็นหน่วยใน $\mathbb{Z}[x]$ โดยทฤษฎีบท 6.4.1 ข้อ 1 (2 ไม่ใช่หน่วยใน $\mathbb{Z}$ และ $(x+1) \notin \mathbb{Z}$)

โดยกลับกันก็**อาจ**มี $f \in D[x] \subset E[x]$ ซึ่ง f เป็นสมาชิกลดทอนไม่ได้ใน $D[x]$ แต่ f ลดทอนได้ใน $E[x]$ ตัวอย่างเช่น $x^2 + 1$ เป็นสมาชิกลดทอนไม่ได้ใน $\mathbb{R}[x]$ แต่ $x^2 + 1 = (x-i)(x+i)$ โดยที่ $(x-i), (x+i) \in \mathbb{C}[x]$ ต่างไม่ใช่สมาชิกหน่วยใน $\mathbb{C}[x]$

ต่อไป จะเรียกพหุนามเหนือริงสลับที่ซึ่งเป็นสมาชิกลดทอนไม่ได้ว่า *พหุนามลดทอนไม่ได้ (irreducible polynomial)*

6.4.3 **ทฤษฎีบท** ให้ F เป็นฟีลด์และ $f(x) \in F[x]$

1. ถ้า $\deg f(x) \geq 2$ และ $f(x)$ เป็นพหุนามลดทอนไม่ได้แล้ว $f(x)$ ไม่มีรากใน F
2. ถ้า $\deg f(x) \in \{2, 3\}$ แล้ว $f(x)$ เป็นพหุนามลดทอนไม่ได้ ก็ต่อเมื่อ $f(x)$ ไม่มีรากใน F

บทพิสูจน์ 1. สมมติ $f(x)$ มีรากใน F แล้วโดยทฤษฎีบทตัวประกอบจะมี $c \in F$ และ $g(x) \in F[x]$ ซึ่ง $f(x) = (x-c)g(x)$ แต่ $\deg f(x) \geq 2$ และ $\deg(x-c) = 1$ ทำให้ $\deg g(x) \geq 1$ นั่นคือทั้ง $x - c$ และ $g(x)$ ไม่ใช่หน่วยใน $F[x]$ ดังนั้น $f(x)$ เป็นพหุนามลดทอนได้

2. ให้ $\deg f(x) \in \{2,3\}$ ถ้า $f(x)$ เป็นพหุนามลดทอนไม่ได้แล้ว $f(x)$ ไม่มีรากใน F โดยข้อ 1 จึงพิสูจน์บทกลับโดยให้ $f(x)$ เป็นพหุนามลดทอนได้เหนือ F แล้วจะมี $g,h \in F[x] \setminus F$ ซึ่ง $f(x) = g(x)h(x)$ และเพราะ $\deg f(x) = \deg g(x) + \deg h(x)$ ดังนั้น $1 \le \deg g(x) < \deg f(x)$ และ $1 \le \deg h(x) < \deg f(x)$ แต่เพราะ $\deg f(x) \in \{2,3\}$ ดังนั้น $\deg g(x) = 1$ หรือ $\deg h(x) = 1$ และไม่ว่ากรณีใด จะมีพหุนามเชิงเส้นที่เป็นตัวประกอบของ $f(x)$ ดังนั้น $f(x)$ มีรากใน F □

6.4.4 **ตัวอย่าง** ให้ $f(x) = x^3 + 3x^2 + x + 2 \in \mathbb{Z}_5[x]$ แล้วเพราะ $f(0) = f(1) = 2$, $f(2) = f(3) = 4$ และ $f(4) = 3$ ซึ่งแสดงว่า $f(x)$ ไม่มีรากใน $\mathbb{Z}_5$ ดังนั้น $f(x)$ เป็นพหุนามลดทอนไม่ได้เหนือฟีลด์ $\mathbb{Z}_5$ โดยทฤษฎีบท 6.4.3 ข้อ 2 ○

6.4.5 **ตัวอย่าง** จงแยกตัวประกอบของพหุนาม $2x^4 + x^3 + 3x^2 + 2x + 4$ เหนือ $\mathbb{Z}_5$

วิธีทำ ให้ $f(x) = 2x^4 + x^3 + 3x^2 + 2x + 4 \in \mathbb{Z}_5[x]$ เพราะ $f(0) = 4$, $f(1) = 2$, $f(2) = 0$ และ $f(3) = 1 = f(4)$ ดังนั้น 2 เป็นรากของ $f(x)$ ใน $\mathbb{Z}_5$ เพียงรากเดียว ทำให้ได้โดยทฤษฎีบทตัวประกอบว่า $x - 2$ เป็นตัวประกอบเชิงเส้นของ $f(x)$ จึงได้

$$f(x) = (x-2)(2x^3 + 3x + 3) \in \mathbb{Z}_5[x]$$

ต่อไปให้ $g(x) = 2x^3 + 3x + 3$ แล้ว $g(0) = 3 = g(1)$, $g(2) = 0$, $g(3) = 1$ และ $g(4) = 3$ ทำให้ได้ว่า 2 เป็นรากของ $g(x)$ ใน $\mathbb{Z}_5$ เพียงรากเดียว ดังนั้น $g(x) = (x-2)(2x^2 + 4x + 1) \in \mathbb{Z}_5$ ทำให้ได้ $f(x) = (x-2)^2(2x^2 + 4x + 1)$ และสังเกตว่า $2x^2 + 4x + 1$ ไม่มีรากใน $\mathbb{Z}_5$ และเพราะ

$$\begin{aligned}(x-2)^2(2x^2 + 4x + 1) &= (x-2)^2(2x^2 + 4x + 2(3)) \\ &= 2(x-2)^2(x^2 + 2x + 3)\end{aligned}$$

แต่ 2 เป็นหน่วยใน $\mathbb{Z}_5$ จึงได้ว่า $(x-2)^2(2x^2 + 4x + 1)$ และ $2(x-2)^2(2x^2 + 4x + 3)$ เป็นรูปแบบเดียวกันของการแยกตัวประกอบของ $x^4 + x^3 + 3x^2 + 2x + 4$ เหนือ $\mathbb{Z}_5$ ○

เพื่อให้ได้เกณฑ์ตรวจสอบการเป็นพหุนามลดทอนไม่ได้สำหรับกรณีพหุนามกำลังสูงขึ้น จึงต้องการมโนคติของพหุนามปฐมฐาน นอกจากนี้ยังต้องการเห็นการแยกตัวประกอบได้แบบดีเยี่ยวของพหุนามลดทอนได้ เราจึงพิจารณาพหุนามเหนือโดเมนของการแยกตัวประกอบได้แบบเดียว

6.4.6 **บทนิยาม** ให้ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว $0 \ne f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$ จะแทนตัวหารร่วมมากของสัมประสิทธิ์ $a_0, a_1, \ldots, a_n$ ทุกตัวด้วยสัญลักษณ์ $C(f)$ นั่น

คือ $C(f) = (a_0, a_1, \ldots, a_n)$ และถ้า $C(f)$ เป็นหน่วยใน D จะเรียก $f(x)$ ว่า *พหุนามปฐมฐาน (primitive polynomial)*

สังเกตว่าถ้า $f \in D[x]$ แล้วจะมีพหุนามปฐมฐาน $f_1 \in D[x]$ ซึ่ง $f = C(f)f_1$ ยิ่งไปกว่านั้น เห็นได้ชัดว่าทุกๆ พหุนามโมนิกเป็นพหุนามปฐมฐาน เกาส์ได้พิสูจน์ทฤษฎีบทต่อไปนี้

6.4.7 **ทฤษฎีบทประกอบของเกาส์** (Gauss's Lemma) ให้ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว และ $f, g \in D[x]$ แล้ว

1. ถ้า $a \in D$ แล้ว $C(af) = aC(f)$
2. $C(fg) = C(f)C(g)$

โดยเฉพาะผลคูณของพหุนามปฐมฐานเป็นพหุนามปฐมฐาน

บทพิสูจน์ จาก $(aa_0, aa_1, \ldots, aa_n) = a(a_0, a_1, \ldots, a_n)$ ทุกๆ $a, a_0, a_1, \ldots, a_n \in D$ จะได้ว่าข้อ 1 เป็นจริง ในการพิสูจน์ข้อ 2 ให้ $f, g \in D[x]$ แล้วมีพหุนามปฐมฐาน $f_1, g_1 \in D[x]$ ซึ่ง $f = C(f)f_1$ และ $g = C(g)g_1$ แต่เพราะ $C(f), C(g) \in D$ จึงได้โดยข้อ 1 ว่า $C(fg) = C\left(C(f)f_1C(g)g_1\right) = C(f)C(g)C\left(f_1g_1\right)$ จึงเหลือเพียงแสดงว่า ผลคูณของพหุนามปฐมฐานเป็นพหุนามปฐมฐาน

ให้ $f_1 = \sum_{i=0}^{n} a_i x^i$ และ $g_1 = \sum_{j=0}^{m} b_j x^j$ แล้ว $f_1 g_1 = \sum_{k=0}^{m+n} c_k x^k$ โดยที่ $c_k = \sum_{i+j=k} a_i b_j$ สมมติ $f_1 g_1$ ไม่ใช่พหุนามปฐมฐาน เพราะ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวและ $(c_0, c_1, \ldots, c_{m+n})$ ไม่ใช่หน่วย จึงมีสมาชิกลดทอนไม่ได้ $p \in D$ ซึ่ง $p | c_k$ ทุกๆ $k \in \{0, \ldots, m+n\}$ เนื่องจาก $C(f_1)$ เป็นหน่วย ดังนั้น p ไม่เป็นตัวหารของ $C(f_1)$ แสดงว่ามี $i \in \{0, \ldots, n\}$ ซึ่ง p ไม่เป็นตัวหารของ a_i ทำให้มี $s \in \{0, \ldots, n\}$ ตัวน้อยสุดซึ่ง $p | a_i$ ทุกๆ $i < s$ แต่ p ไม่เป็นตัวหารของ a_s และในทำนองเดียวกันมี $t \in \{0, \ldots, m\}$ ตัวน้อยสุดซึ่ง $p | b_j$ ทุกๆ $j < t$ แต่ p ไม่เป็นตัวหารของ b_t โดยที่ p เป็นตัวหารของ

$$c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots + a_{s+t} b_0$$

และ p เป็นตัวหารของทุกๆ สมาชิกในเซต $\{a_0 b_{s+t}, \ldots, a_{s-1} b_{t+1}, a_{s+1} b_{t-1}, \ldots, a_{s+t} b_0\}$ ดังนั้น $p | a_s b_t$ แต่ p เป็นสมาชิกลดทอนไม่ได้ในโดเมนของการแยกตัวประกอบได้แบบเดียว ดังนั้น p เป็นสมาชิกเฉพาะ ทำให้ได้ $p | a_s$ หรือ $p | b_t$ ซึ่งขัดแย้งกับการเลือก a_s และ b_t เพราะฉะนั้น $f_1 g_1$ เป็นพหุนามปฐมฐาน ❐

6.4.8 **ทฤษฎีบท** ให้ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวที่มี F เป็นฟิลด์เศษส่วน และให้ $f, g \in D[x]$ เป็นพหุนามปฐมฐานแล้ว f และ g สมทบกันใน $D[x]$ ก็ต่อเมื่อ f และ g สมทบกันใน $F[x]$

บทพิสูจน์ ถ้า f และ g สมทบกันใน $D[x] \subseteq F[x]$ เห็นชัดว่า f และ g สมทบกันใน $F[x]$ จึงให้ f และ g สมทบกันใน $F[x]$ แล้วมีหน่วย $u \in F[x]$ ซึ่ง $f = gu$ และโดยทฤษฎีบท 6.4.1 จะได้ $u \in F$ แต่เพราะ F เป็นฟีลด์เศษส่วนของ D จึงมี $b, c \in D$ ซึ่ง $c \neq 0$ และ $u = \frac{b}{c}$ ทำให้ได้ $cf = bg$ และเพราะ $C(f)$ เป็นหน่วยใน D ดังนั้น c สมทบกับ $cC(f)$ แต่ $cC(f) = C(cf) = C(bg) = bC(g)$ และ $bC(g)$ สมทบกับ b ดังนั้น c สมทบกับ b จึงมี v เป็นหน่วยใน D ซึ่ง $b = cv$ ทำให้ได้ $cf = bg = cvg$ และได้ $f = vg$ ซึ่งแสดงว่า f และ g สมทบกันใน $D[x]$ ❐

6.4.9 **ทฤษฎีบท** ให้ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวที่มี F เป็นฟีลด์เศษส่วน และให้ $f \in D[x]$ เป็นพหุนามปฐมฐานที่มีกำลังเป็นจำนวนเต็มบวกแล้ว f เป็นพหุนามลดทอนไม่ได้ใน $D[x]$ ก็ต่อเมื่อ f เป็นพหุนามลดทอนไม่ได้ใน $F[x]$

บทพิสูจน์ ให้ f เป็นพหุนามลดทอนได้ใน $F[x]$ แล้วมี $g, h \in F[x]$ ซึ่ง $f = gh$, $\deg g \geq 1$ และ $\deg h \geq 1$ ดังนั้นมี $a_i, b_i, c_j, d_j \in D$ โดยที่ $b_i \neq 0$ และ $d_j \neq 0$ สำหรับ $i \in \{0, \ldots, n\}$ และ $j \in \{0, \ldots, m\}$ ซึ่ง $g = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i$ และ $h = \sum_{j=0}^{m} \frac{c_j}{d_j} x^j$

ให้ $b = b_0 b_1 \cdots b_n$ แล้วสำหรับแต่ละ $i \in \{0, \ldots, n\}$ ให้ $b_i^* = b_0 \cdots b_{i-1} b_{i+1} \cdots b_n$ และให้ $g_1 = \sum_{i=0}^{n} a_i b_i^* x^i \in D[x]$ แล้ว $g_1 = ag_2$ เมื่อ $a = C(g_1)$ และ $g_2 \in D[x]$ เป็นพหุนามปฐมฐาน ดังนั้น $g = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i = \sum_{i=0}^{n} \frac{a_i b_i^*}{b} x^i = \frac{1}{b} g_1 = \frac{a}{b} g_2$ และ $\deg g = \deg g_2$ ในทำนองเดียวกันมี $c, d \in D$ และ $h_2 \in D[x]$ เป็นพหุนามปฐมฐานซึ่ง $h = \frac{c}{d} h_2$ และ $\deg h = \deg h_2$ ทำให้ $f = gh = (\frac{a}{b})(\frac{c}{d}) g_2 h_2$ และได้ $bdf = acg_2h_2$

เนื่องจาก f เป็นพหุนามปฐมฐาน (โดยสมมติฐาน) และ g_2h_2 เป็นพหุนามปฐมฐาน (โดยทฤษฎีบท 6.4.7) ดังนั้น bd สมทบกับ $bdC(f)$ และ ac สมทบกับ $acC(g_2h_2)$ แต่ $bdC(f) = C(bdf) = C(acg_2h_2) = acC(g_2h_2)$ ทำให้ bd สมทบกับ ac ใน D แล้วโดยบทพิสูจน์ของทฤษฎีบท 6.4.8 จะได้ bd สมทบกับ ac ใน D ทำให้ได้ f สมทบกับ g_2h_2 ใน $D[x]$ เพราะฉะนั้น f เป็นพหุนามลดทอนได้ใน $D[x]$

การพิสูจน์บทกลับให้ f เป็นพหุนามลดทอนไม่ได้ใน $F[x]$ และให้ $g, h \in D[x] \subseteq F[x]$ ซึ่ง $f = gh$ แล้ว g หรือ h เป็นหน่วยใน $F[x]$ และโดยทฤษฎีบท 6.2.5 จะได้ g หรือ h เป็นพหุนามคงตัวใน F และโดยไม่เสียนัยทั่วไปให้ g เป็นพหุนามคงตัว ดังนั้น $C(f) = gC(h)$ แต่ f เป็นพหุนามปฐมฐาน ทำให้ g ต้องเป็นหน่วยใน D และดังนั้นเป็นหน่วยใน $D[x]$ ซึ่งแสดงว่า f เป็นพหุนามลดทอนไม่ได้ใน $D[x]$ ❐

เนื่องจากฟีลด์ $\mathbb{Q}$ ของจำนวนตรรกยะเป็นฟีลด์เศษส่วนของโดเมนของการแยกตัวประกอบได้แบบเดียว $\mathbb{Z}$ เราได้บทแทรกต่อไปนี้

6.4.10 บทแทรก พหุนามโมนิก f เหนือ $\mathbb{Z}$ ลดทอนไม่ได้เหนือ $\mathbb{Q}$ ก็ต่อเมื่อ f ลดทอนไม่ได้เหนือ $\mathbb{Z}$ ❐

6.4.11 ตัวอย่าง จงแสดงว่า $x^5 + 2x^2 + 1$ เป็นพหุนามลดทอนไม่ได้เหนือ $\mathbb{Q}$

วิธีทำ พิจารณาก่อนว่า $f(x) = x^5 + 2x^2 + 1$ มีรากตรรกยะหรือไม่ ซึ่งโดยทฤษฎีบท 6.3.6 ถ้า $\frac{c}{d} \in \mathbb{Q}$ เป็นรากของ $f(x)$ แล้ว $c|1$ และ $d|1$ ทำให้ $\frac{c}{d}$ ที่เป็นไปได้ทั้งหมดได้แก่ ± 1 แต่ $f(1) \neq 0$ และ $f(-1) \neq 0$ ดังนั้น $f(x)$ ไม่มีรากใน $\mathbb{Q}$ (และดังนั้นไม่มีรากใน $\mathbb{Z}$) ซึ่งแสดงว่า $f(x)$ ไม่มีตัวประกอบเป็นพหุนามเชิงเส้น

จาก $f(x)$ เป็นพหุนามโมนิกเหนือ $\mathbb{Z}$ จึงสมมติว่า $f(x)$ ลดทอนได้เหนือ $\mathbb{Z}$ แล้ว $f(x)$ เป็นผลคูณของพหุนามกำลังสองและกำลังสามนั่นคือมี $g(x), h(x) \in \mathbb{Z}[x]$ ซึ่ง $\deg g(x) = 2$, $\deg h(x) = 3$ และ $f(x) = g(x)h(x)$ ดังนั้น $g(x)$ และ $h(x)$ เป็นพหุนามโมนิกจึงมีรูปแบบทั่วไปเป็น $g(x) = x^2 + ax + b$ และ $h(x) = x^3 + cx^2 + dx + e$ เมื่อ $a, b, c, d, e \in \mathbb{Z}$ ทำให้ได้ $f(x) = x^5 + 2x^2 + 1 = (x^2 + ax + b)\,(x^3 + cx^2 + dx + e)$

$$= x^5 + (a+c)x^4 + (d + ac + b)x^3 + (e + ad + bc)x^2 + (ae + bd)x + be$$

และจากความสัมพันธ์ $be = 1$ จะได้ $b = e \in \{\pm 1\}$

ถ้า $b = e = 1$ แล้วจาก $0 = ae + bd = a + d$ และ $a + c = 0$ จะได้ $d = -a = c$ และจาก $0 = d + ac + b$ จะได้ $a^2 + a - 1 = 0$ ซึ่งแสดงว่า a เป็นรากใน $\mathbb{Z}$ ของ $x^2 + x - 1$ แต่ $x^2 + x - 1$ ไม่มีรากใน $\mathbb{Z}$ จึงเกิดเป็นข้อขัดแย้งกันเอง และถ้า $b = e = -1$ แล้ว $0 = ae + bd = -(a + d)$ ทำให้ได้ $d = -a = c$ ซึ่งจะนำไปสู่ข้อขัดแย้งเดียวกัน ดังนั้นข้อสมมติจึงไม่เป็นจริง นั่นคือ $f(x) = x^5 + 2x^2 + 1$ ลดทอนไม่ได้เหนือ $\mathbb{Z}$ และดังนั้นลดทอนไม่ได้เหนือ $\mathbb{Q}$ โดยบทแทรก 6.4.10 ❍

จากตัวอย่างข้างต้นจะเห็นว่าโดยทั่วไป ก็ยังยากที่จะตัดสินว่าพหุนามเหนือ $\mathbb{Z}$ เป็นพหุนามลดทอนได้หรือไม่ อย่างไรก็ตามก็ยังพอมีเกณฑ์ในการตัดสินพหุนามลดทอนไม่ได้เหนือโดเมนของการแยกตัวประกอบได้แบบเดียว และเกณฑ์ที่สำคัญซึ่งรู้จักกันดีเกณฑ์หนึ่งก็คือ "เกณฑ์พหุนามลดทอนไม่ได้ของไอเซนสไตน์" (F. M. Eisenstein 1823 – 1852 เป็นนักคณิตศาสตร์ชาวเยอรมัน)

6.4.12 เกณฑ์พหุนามลดทอนไม่ได้ของไอเซนสไตน์

(Eisenstein's Criterion on Irreducible Polynomials)

ให้ D เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวที่มี F เป็นฟีลด์เศษส่วนและให้ $f = \sum_{i=0}^{n} a_i x^i \in D[x]$ โดยที่ $\deg f \geq 1$ ถ้า p เป็นสมาชิกลดทอนไม่ได้ใน D ซึ่งสอดคล้องเงื่อนไขต่อไปนี้

(ก) p ไม่เป็นตัวหารของสัมประสิทธิ์นำ a_n และ p^2 ไม่เป็นตัวหารของพจน์คงตัว a_0

และ (ข) p เป็นตัวหารของสัมประสิทธิ์ตัวอื่นๆ $a_{n-1},\dots,a_0$ ทุกตัว

แล้ว f เป็นสมาชิกลดทอนไม่ได้ใน $F[x]$

ถ้า f เป็นพหุนามปฐมฐาน แล้ว f เป็นสมาชิกลดทอนไม่ได้ใน $D[x]$

บทพิสูจน์ ให้ $f = C(f)f_1$ โดยที่ f_1 เป็นพหุนามปฐมฐานใน $D[x]$ และ $C(f) \in D \subseteq F$ (โดยเฉพาะ $f = f_1$ ถ้า f เป็นพหุนามปฐมฐาน) เนื่องจาก $C(f)$ เป็นหน่วยใน F จึงเหลือเพียงแสดงว่า f_1 เป็นสมาชิกลดทอนไม่ได้ใน $F[x]$ ด้วยการสมมติในทางตรงข้ามว่า $f_1 = gh$ โดยที่ $f_1 = \sum_{i=0}^{n} a_i^* x^i \in D[x]$, $g = \sum_{k=0}^{r} b_k x^k \in D[x]$, $h = \sum_{j=0}^{s} c_j x^j \in D[x]$, $r \geq 1$ และ $s \geq 1$ แต่ $a_n = C(f)a_n^*$ และ p ไม่เป็นตัวหารของ a_n ดังนั้น p ไม่เป็นตัวหารของ a_n^* และของ $C(f)$ ยิ่งไปกว่านั้น p^2 ไม่เป็นตัวหารของพจน์คงตัว a_0^* ของ f_1 และจาก p ไม่เป็นตัวหารของ $C(f)$ แต่ p เป็นตัวหารของ $a_i = C(f)a_i^*$ ทุกๆ $i \in \{0,1,\dots,n-1\}$ จะได้ p เป็นตัวหารของ a_i^* ทุกๆ $i \in \{0,1,\dots,n-1\}$ นั่นคือ f_1 ก็สอดคล้องเงื่อนไขเกี่ยวกับการหารสัมประสิทธิ์ด้วย p เช่นเดียวกับ f

เนื่องจาก p ไม่เป็นตัวหารของ $a_0^* = b_0c_0$ และทุกๆ สมาชิกลดทอนไม่ได้ใน D เป็นสมาชิกเฉพาะ ดังนั้น $p|b_0$ หรือ $p|c_0$ และโดยไม่เสียนัยทั่วไปสมมติว่า $p|b_0$ แล้วเพราะ p^2 ไม่เป็นตัวหารของ a_0^* จะได้ p ไม่เป็นตัวหารของ c_0 จึงมีสัมประสิทธิ์ b_k ของ g ซึ่งไม่เป็นตัวหารของ p (หรือมิเช่นนั้น p เป็นตัวหารของสัมประสิทธิ์ทุกตัวของ $gh = f_1$ จะเกิดข้อขัดแย้งกันเอง) ให้ k เป็นจำนวนเต็มบวกตัวน้อยสุดซึ่ง $p|b_i$ ทุกๆ $i < k$ แต่ p ไม่เป็นตัวหารของ b_k แล้ว $1 \leq k \leq r < n$ แต่เพราะ $a_k^* = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$ และ $p|a_k^*$ ดังนั้น $p|b_kc_0$ ทำให้ได้ $p|b_k$ หรือ $p|c_0$ ซึ่งจะเกิดข้อขัดแย้งกันเองไม่ว่ากรณีใด ❐

6.4.13 **ตัวอย่าง** พหุนาม $25x^5 - 9x^4 + 3x^2 - 12$ ลดทอนไม่ได้เหนือโดเมนของไอดีลหลัก $\mathbb{Z}$ เพราะโดยเกณฑ์ของไอเซนสไตน์และจำนวนเฉพาะ 3 จะได้ว่า 3 ไม่เป็นตัวหารของ 25 และ $3^2 = 9$ ไม่เป็นตัวหารของ -12 แต่ 3 เป็นตัวหารของ $-9, 0$ และ 3 ❍

6.4.14 **ตัวอย่าง** จงหาพหุนามเหนือ $\mathbb{Q}$ กำลังน้อยสุดที่มี $\sqrt[2012]{2}$ เป็นราก

วิธีทำ เห็นชัดว่า $\sqrt[2012]{2}$ เป็นรากของ $x^{2012}-2$ และให้ $f(x)$ เป็นพหุนามเหนือ $\mathbb{Q}$ กำลังน้อยสุดที่มี $\sqrt[2012]{2}$ เป็นราก แล้วโดยขั้นตอนการหาร จะมี $q(x), r(x) \in \mathbb{Q}[x]$ ที่ทำให้

$$x^{2012}-2 = f(x)q(x)+r(x) \text{ ซึ่งสมมูลกับ } r(x) = (x^{2012}-2) - f(x)q(x)$$

โดยที่ $r(x)=0$ หรือ $\deg r(x) < \deg f(x)$ แต่ถ้า $r(x) \neq 0$ แล้ว $r(x)$ จะเป็นพหุนามเหนือ $\mathbb{Q}$ ซึ่งมีกำลังน้อยกว่ากำลังของ $f(x)$ และมี $\sqrt[2012]{2}$ เป็นราก จะขัดแย้งกับการเลือกพหุนาม $f(x)$ ดังนั้น $r(x)=0$ จึงได้ว่า $x^{2012}-2 = f(x)q(x)$

แต่ $x^{2012}-2$ เป็นพหุนามลดทอนไม่ได้โดยเกณฑ์ของไอเซนสไตน์ ด้วยจำนวนเฉพาะ 2 ดังนั้น $q(x)$ เป็นพหุนามคงตัว เพราะฉะนั้น $f(x) = c(x^{2012}-2)$ เมื่อ $c \in \mathbb{Q}$ ❍

6.4.15 **ทฤษฎีบท** ให้ D เป็นโดเมนของไอดีลหลักแล้ว $f(x)$ เป็นพหุนามลดทอนไม่ได้ในเหนือ D ก็ต่อเมื่อ $f(x+c)$ เป็นพหุนามลดทอนไม่ได้เหนือ D ทุกๆ $c \in D$

บทพิสูจน์ ให้ $c \in D$ แล้วเพราะ $\deg g(x+c) = \deg g(x) = \deg g(x-c)$ ทุกๆ $g(x) \in D[x]$ และ $f(x+c) = g(x+c)h(x+c)$ ก็ต่อเมื่อ $f(x) = g(x)h(x)$ ซึ่งก็ต่อเมื่อ $f(x) = f((x-c)+c) = g(x-c)h(x-c)$ สำหรับบาง $g(x), h(x) \in D[x]$ จึงเห็นได้ชัดว่า $f(x)$ เป็นพหุนามลดทอนไม่ได้เหนือ D ก็ต่อเมื่อ $f(x+c)$ เป็นพหุนามลดทอนไม่ได้เหนือ D ❐

6.4.16 **ตัวอย่าง** จงแสดงว่าถ้า p เป็นจำนวนเฉพาะ แล้วพหุนาม $x^{p-1}+x^{p-2}+\cdots+x+1$ ลดทอนไม่ได้เหนือ $\mathbb{Z}$

วิธีทำ ให้ p จำนวนเฉพาะและให้ $f(x) = x^{p-1}+x^{p-2}+\cdots+x+1$ แล้ว

$$(x-1)f(x) = (x-1)(x^{p-1}+x^{p-2}+\cdots+x+1) = x^p-1$$

และเมื่อแทน x ด้วย $x+1$ จะได้ $xf(x+1) = (x+1)^p-1$ ทำให้ได้โดยทฤษฎีบททวินามว่า

$$xf(x+1) = x^p + \binom{p}{1}x^{p-1} + \ldots + \binom{p}{p-1}x$$

และสำหรับ $x \neq 0$ จะได้

$$f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + p$$

เพราะ $p \mid \binom{p}{k}$ ทุกๆ $1 \le k < p$ ดังนั้น $f(x)$ เป็นพหุนามลดทอนไม่ได้เหนือ $\mathbb{Z}$ โดยเกณฑ์ของไอเซนสไตน์และทฤษฎีบท 6.4.15 ❍

แบบฝึกหัด 6.4

1. ให้ $p \in \mathbb{Z}$ เป็นจำนวนเฉพาะ F เป็นฟีลด์ จงพิสูจน์ว่า

   1.1 พหุนาม $x^p - c$ ลดทอนไม่ได้ใน $F[x]$ ก็ต่อเมื่อ $x^p - c$ ไม่มีรากใน F ทุกๆ $c \in F$

   1.2 ถ้า $char(F) = p$ แล้วพหุนาม $x^p - x - c$ ลดทอนไม่ได้ใน $F[x]$ ก็ต่อเมื่อ $x^p - x - c$ ไม่มีรากใน F

2. ให้ $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ โดยที่ $a_n \neq 0$ จงพิสูจน์ว่าถ้ามีจำนวนเฉพาะ p และ $0 < k < n$ ซึ่ง (ก) p ไม่เป็นตัวหารของ a_n และ a_k และ p^2 ไม่เป็นตัวหารของ a_0 และ

   (ข) $p | a_i$ ทุกๆ $0 \leq i < k$

   แล้วมีพหุนามลดทอนไม่ได้ $g \in \mathbb{Z}[x]$ ซึ่ง $\deg g \geq k$ และ g เป็นตัวประกอบของ f

3. ให้ $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ และ $p \in \mathbb{Z}$ เป็นจำนวนเฉพาะ และให้ $\overline{f} = \sum_{k=0}^{n} \overline{a}_k x^k \in \mathbb{Z}_p[x]$ เมื่อ $\overline{a}$ เป็นภาพของ a ภายใต้สาทิสสัณฐานธรรมชาติจาก $\mathbb{Z}$ ไปทั่วถึง $\mathbb{Z}_p$

   3.1 จงพิสูจน์ว่าถ้า f เป็นพหุนามโมนิกและ $\overline{f}$ เป็นพหุนามลดทอนไม่ได้ใน $\mathbb{Z}_p[x]$ แล้ว f เป็นพหุนามลดทอนไม่ได้ใน $\mathbb{Z}[x]$

   3.2 จงหาตัวอย่างที่แสดงว่า 3.1 อาจไม่เป็นจริงถ้า f ไม่เป็นพหุนามโมนิก

   3.3 จงขยายผลของ 3.1 ไปในโดเมนของการแยกตัวประกอบได้แบบเดียว

4. จงพิสูจน์ว่า $f(x) = c_{2m+1}x^{2m+1} + c_{2m}x^{2m} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ ซึ่งมีกำลังเป็นจำนวนคี่ $2m+1 \geq 3$ เป็นพหุนามลดทอนไม่ได้ใน $\mathbb{Z}[x]$ ถ้ามีจำนวนเฉพาะ p ซึ่งสอดคล้องสมบัติต่อไปนี้

   (ก) p ไม่เป็นตัวหารของ c_{2m+1} และ p^2 ไม่เป็นตัวหารของ c_0 และ

   (ข) p เป็นตัวหารของ c_i ถ้า $m+1 \leq i \leq 2m$ และ p^2 เป็นตัวหารของ c_i ถ้า $1 \leq i \leq m$

5. จงหาจำนวนเต็มบวก n น้อยสุดสามจำนวนซึ่ง $x^{n-1} + \cdots + x + 1$ เป็นพหุนามลดทอนได้

6. จงแสดงว่าทุกๆ พหุนามลดทอนไม่ได้เหนือ $\mathbb{C}$ เป็นพหุนามลดทอนไม่ได้เหนือ $\mathbb{R}$ และทุกๆ พหุนามลดทอนไม่ได้เหนือ $\mathbb{R}$ เป็นพหุนามลดทอนไม่ได้เหนือ $\mathbb{Q}$

7. ให้ c เป็นจำนวนเต็ม จงแสดงว่า

   7.1 ถ้า c เป็นจำนวนบวกแล้วพหุนาม $x^2 + c$ ลดทอนไม่ได้เหนือ $\mathbb{R}, \mathbb{Q}$ และ $\mathbb{Z}$ แต่ $x^2 + c$ ลดทอนได้เหนือ $\mathbb{C}$

   7.2 ถ้ามีจำนวนเต็มบวก d ซึ่ง $c = -d^2$ แล้ว $x^2 + c$ ลดทอนได้เหนือ $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ และ $\mathbb{Z}$

   7.3 ถ้า c เป็นจำนวนลบอื่นๆ นอกจากในข้อ 7.2 แล้ว $x^2 + c$ ลดทอนไม่ได้เหนือ $\mathbb{Q}$ และ

$\mathbb{Z}$ แต่ลดทอนได้เหนือ $\mathbb{C}$ และ $\mathbb{R}$

8. จงพิสูจน์ว่าพหุนาม $a_n x^n + \cdots + a_1 x + a_0$ ลดทอนไม่ได้เหนือฟีลด์ F ก็ต่อเมื่อพหุนาม $a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ ลดทอนไม่ได้เหนือฟีลด์ F

9. จงประยุกต์เกณฑ์ของไอเซนสไตน์ และ/หรือ ผลในข้อ 8 แสดงว่าพหุนามในข้อต่อไปนี้ลดทอนได้หรือไม่เหนือ $\mathbb{Z}$

9.1 $2x^3 - 6x^2 + 9x - 3$ 9.2 $x^4 + 15$

9.3 $x^4 - 2x^3 + 100x^2 + 4x - 1$ 9.4 $6x^4 + 4x^3 - 6x^2 - 8x + 5$

9.5 $x^4 - \frac{1}{2}x^2 + \frac{3}{2}x - \frac{4}{3}$ 9.6 $x^3 + \frac{1}{2}x^2 - \frac{3}{2}x + \frac{6}{5}$

6.5 พหุนามหลายตัวแปร

ถ้า R เป็นริงสลับที่มีเอกลักษณ์ ในหัวข้อ 6.1 ได้แสดงให้เห็นแล้วว่าริง $R[x]$ ของพหุนามเหนือ R เป็นริงสลับที่มีเอกลักษณ์เช่นเดียวกัน โดยเรียก x ว่ารูปแบบยังไม่กำหนดและ $R[x]$ เป็นริงของพหุนามที่มีตัวยังไม่กำหนดตัวเดียวหรือริงของพหุนามตัวแปรเดียวและถ้าพิจารณา $S = R[x]$ เป็นริงสลับที่มีเอกลักษณ์แล้ว $S[y] = R[x][y]$ จะเป็นริงของพหุนามเหนือ S โดยมี y เป็นรูปแบบยังไม่กำหนดซึ่งเห็นชัดว่า $x \neq y$ โดยนิยมแทน $S[y] = R[x][y]$ ด้วยสัญลักษณ์ $R[x, y]$ และเรียกว่าริงของพหุนามสองตัวแปร

โดยอุปนัยวิธีถ้า R เป็นริงสลับที่มีเอกลักษณ์แล้ว $x_1, x_2, \ldots, x_n \in R[x_1, x_2, \ldots, x_n]$ เป็นรูปแบบยังไม่กำหนด n ตัว $(n \geq 2)$ ของริงสลับที่มีเอกลักษณ์ $R[x_1, x_2, \ldots, x_n]$ ซึ่งเรียกว่าริงของพหุนาม n ตัวแปรหรือริงของพหุนามหลายตัวแปร และโดยวิธีการสร้างจะเห็นว่า สมบัติใดที่เป็นจริงสำหรับริงของพหุนามตัวแปรเดียว จะเป็นจริงสำหรับริงของพหุนามหลายตัวแปร โดยเฉพาะถ้า R เป็นฟีลด์ (หรืออินทิกรัลโดเมน) แล้ว $R[x_1, x_2, \ldots, x_n]$ เป็นอินทิกรัลโดเมน ทำให้มีฟีลด์ของฟังก์ชันตรรกยะ (ที่บรรจุ $R[x_1, x_2, \ldots, x_n]$) ใน n ตัวแปรซึ่งสมาชิกเป็นฟังก์ชันตรรกยะในรูปแบบ $\frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)}$ โดยที่ $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ และ $q(x_1, \ldots, x_n) \neq 0$

ทฤษฎีบทต่อไปนี้ เป็นผลโดยตรงจากริงพหุนามตัวแปรเดียว

6.5.1 **ทฤษฎีบท** ถ้า R เป็นโดเมนของการแยกตัวประกอบได้แบบเดียวหรือเป็นฟีลด์ แล้ว $R[x_1, \ldots, x_n]$ เป็นโดเมนของการแยกตัวประกอบได้แบบเดียว ❐

ให้ R เป็นฟีลด์ สังเกตว่าสมาชิก f ใน $R[x_1, x_2, \dots, x_n]$ เป็นผลบวกของพจน์ในรูปแบบ $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ นั่นคือ $f = \sum_{i=0}^{m} a_i x_1^{k_{i_1}} x_2^{k_{i_2}} \cdots x_n^{k_{i_n}}$ โดยเป็นที่นิยมกันว่าจะละไม่เขียนตัวแปร x_i ในพจน์ $a_i x_1^{k_{i_1}} x_2^{k_{i_2}} \cdots x_n^{k_{i_n}}$ ถ้า $k_{i_j} = 0$ เช่นพหุนาม $a_0 x_1^0 x_2^0 x_3^0 + a_1 x_1^2 x_2^0 x_3^1 + a_2 x_1^1 x_2^2 x_3^0$ จะเขียนเป็น $a_0 + a_1 x_1^2 x_3 + a_2 x_1 x_2^2$ เป็นต้น และเช่นเดียวกับในริงของพหุนามตัวแปรเดียว เราเรียก $a_0, a_1, \dots, a_m$ ว่า *สัมประสิทธิ์ (coefficient)* ของ f และ *กำลัง (degree)* ของ f คือ $\deg f = \max\{k_{i_1} + \cdots + k_{i_n} \mid 0 \le i \le m\}$

ถ้า R เป็นริงสลับที่ไม่มีเอกลักษณ์แล้ว R จะถูกฝังในริงสลับที่มีเอกลักษณ์ S และในกรณีเช่นนี้ $x_1, x_2, \dots, x_n$ และ $x_1^{k_{i_1}} x_2^{k_{i_2}} \cdots x_n^{k_{i_n}}$ ไม่เป็นสมาชิกของ $R[x_1, x_2, \dots, x_n]$ ซึ่งเป็นริงย่อยของ $S[x_1, x_2, \dots, x_n]$

ถ้า R เป็นริง การคำนวณโดยตรงแสดงให้เห็นว่าการส่ง $R[x_1] \to R[x_1, x_2, \dots, x_n]$ โดย $\sum_{i=0}^{m} a_i x_1^i \to \sum_{i=0}^{m} a_i x_1^{k_{i_1}} x_2^0 \cdots x_n^0 = \sum_{i=0}^{m} a_i x_1^i \in R[x_1, x_2, \dots, x_n]$ เป็นสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง และในกรณีทั่วไปถ้า $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ แล้วจะมีสาทิสสัณฐานชนิดหนึ่งต่อหนึ่ง $R[x_{i_1}, \dots, x_{i_k}] \to R[x_1, \dots, x_n]$ นั่นคือ $R[x_{i_1}, \dots, x_{i_k}]$ ถูกฝังในลักษณะเป็นริงย่อยของ $R[x_1, \dots, x_n]$

นอกจากนี้ถ้า R และ S เป็นริงสลับที่ $\varphi : R \to S$ เป็นสาทิสสัณฐานและ $s_1, s_2, \dots, s_n \in S$ แล้ว $\overline{\varphi} : R[x_1, \dots, x_n] \to S$ นิยามโดย $\overline{\varphi}(\sum_{i=0}^{m} a_i x_1^{k_{i_1}} \cdots x_n^{k_{i_n}}) = \sum_{i=0}^{m} \varphi(a_i) s_1^{k_{i_1}} \cdots s_n^{k_{i_n}}$ เป็นสาทิสสัณฐานซึ่ง $\overline{\varphi}|_R = \varphi$ ซึ่งทำให้ได้ว่า

$$R[x_1, \dots, x_k][x_{k+1}, \dots, x_n] \cong R[x_1, x_2, \dots, x_n] \cong R[x_{k+1}, \dots, x_n][x_1, \dots, x_k]$$

ตัวอย่างกรณีเฉพาะเช่น $R[x][y] \cong R[x, y] \cong R[y][x]$ (เป็นเหตุผลที่เราใช้ $R[x, y]$ แทน $R[x][y]$ ดังกล่าวข้างต้น) โดยเฉพาะ

$$f = x^2 y + x^3 y + x^4 + xy + y^2 + 5 \in R[x, y],$$

$$f = y^2 + (x^2 + x^3 + x)y + x^4 + 5 \in R[x][y]$$

และ $$f = x^4 + yx^3 + yx^2 + yx + (y^2 + 5) \in R[y][x]$$

แบบฝึกหัด 6.5

1. ให้ R เป็นอินทิกรัลโดเมน

   1.1 จงให้บทนิยามที่สมเหตุสมผลของ "กำลังของพหุนามใน $R[x, y]$" พร้อมทั้ง

บรรยายพหุนามกำลังน้อยกว่าหรือเท่ากับสามทั้งหมดใน $\mathbb{Z}_3[x,y]$

1.2 จงให้นิยาม "การบวก" และ "การคูณ" ของพหุนามใน $R[x,y]$ ในลักษณะขยายบทนิยามของ "การบวก" และ "การคูณ" ของพหุนามใน $R[x]$

1.3 จงพิสูจน์ว่า $\deg a(x,y)b(x,y) = \deg a(x,y) + \deg b(x,y)$

2. จงเขียน $(3x^3+2x)y^3 + (x^2-6x+1)y^2 + (x^4-2x)y + (x^4-3x^2+2) \in R[x][y]$ ในรูปที่แสดงการเป็นสมาชิกของ $R[y][x]$

3. จงพิสูจน์ทฤษฎีบท 6.5.1

4. ให้ R เป็นริงสลับที่ จงพิสูจน์ว่า

$$R[x_1,\dots,x_k][x_{k+1},\dots,x_n] \cong R[x_1,x_2,\dots,x_n] \cong R[x_{k+1},\dots,x_n][x_1,\dots,x_k]$$

บรรณานุกรม

1. ฉวีวรรณ รัตนประเสริฐ *พีชคณิตแผนใหม่* ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร 2527
2. ฉวีวรรณ รัตนประเสริฐ *ทฤษฎีกรุปเบื้องต้น* โครงการตำรา คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร 2553
3. Burton, D.M., *Abstract Algebra and Linear Algebra*, Addison Wesley Series In Mathematics, Reading, Mass., 1971.
4. Dummit, D.S., *Abstract Algebra*, New Jersey : Prentice-Hall, Inc., 1991.
5. Durbin J. R., *Modern Algebra*, John Wiley & Son, New York, 1979.
6. Hall, M., *The Theory of Group*, New York : The Macmillan Company, 1959.
7. Hungerford, T.W., *Abstract Algebra : An Introduction*, Sauders College Publishing, 1990.
8. Kochendorffer, R., *Group*, London : Mcgraw-Hill Publishing Company Limited, 1970
9. Malik, D.S., *Fundamentals of Abstract Algebra*, New York : The McGraw-Hill Companies, Inc., 1997.
10. Zassenhans, H.J., *The Theory of Groups*, New York : Dover Publications, Inc.,1999.

บัญชีศัพท์

ก

ข

ค

จ

ช

ซ

ฐ

ด

ต

ถ

ท

น

บ

ผ

พ

ฟ

ภ

ม

ย

ร

ล

ว

ศ

ส

ห

อ