บทที่ 7
ริงและสมบัติเบื้องต้นของริง

สำหรับ 6 บทที่ผ่านมาได้ศึกษาโครงสร้างทางพีชคณิตที่ประกอบด้วยเซตกับการดำเนินการทวิภาคบนเซตนั้นเพียงการดำเนินการทวิภาคเดียว ในบทนี้จะศึกษาโครงสร้างทางพีชคณิตที่ซับซ้อนกว่าเดิม คือ ประกอบด้วยเซตที่มีการดำเนินการทวิภาคบนเซตนั้นสองการดำเนินการทวิภาคที่แตกต่างกันซึ่งถูกเรียกว่าริง (ring) โดยแบ่งเนื้อหาออกเป็น 3 ส่วน ในส่วนแรกจะกล่าวถึงสมบัติเบื้องต้นของริงและริงผลหาร ในส่วนที่สองจะกล่าวถึงความสัมพันธ์ระหว่างริงสองริงโดยใช้ฟังก์ชันเป็นตัวพิจารณา นั่นคือ โฮโมมอร์ฟิซึมและไอโซมอร์ฟิซึม และส่วนสุดท้ายจะกล่าวถึงริงพหุนาม ดังนี้

บทนิยามและตัวอย่างของริง

บทนิยาม 7.1 กำหนดให้ R เป็นเซตที่ไม่ใช่เซตว่างและกำหนด $+$ (การบวก) และ $\cdot$ (การคูณ) เป็นการดำเนินการทวิภาคบน R จะเรียกระบบคณิตศาสตร์ $(R, +, \cdot)$ ว่าริง (ring) ก็ต่อเมื่อ

1. $(R, +)$ เป็นอาบีเลียนกรุป
2. $(R, \cdot)$ เป็นกึ่งกรุป และ
3. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ และ $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

สำหรับทุก a, b, $c \in R$ (เราเรียกสมบัติการแจกแจง (distributive property))

จากบทนิยาม 7.1 จะได้ว่า ถ้า $(R, +, \cdot)$ เป็นริง แล้ว $(R, +)$ เป็นอาบีเลียนกรุป ดังนั้น R จะมีสมาชิกเอกลักษณ์สำหรับการบวกเสมอ และเราจะเขียนแทนสมาชิกเอกลักษณ์ของกรุป $(R, +)$ ด้วยสัญลักษณ์ 0 ซึ่งเรียกสมาชิกเอกลักษณ์สำหรับการบวก (additive identity element) หรือสมาชิกศูนย์ (zero element) ของริง $(R, +, \cdot)$ นอกจากนี้ จะได้ว่า ถ้า $(R, +, \cdot)$ เป็นริง แล้ว $(R, +)$ เป็นอาบีเลียนกรุป ดังนั้น R สมบัติต่าง ๆ เกี่ยวกับกรุปที่เราได้ศึกษามาแล้วสามารถนำมาใช้ได้ แต่สำหรับ $(R, \cdot)$ เป็นเพียงกึ่งกรุปเท่านั้น ดังนั้น อาจไม่มีสมบัติการสลับที่ และอาจจะไม่มีสมาชิกเอกลักษณ์สำหรับการคูณ สัญลักษณ์การดำการทวิภาค $+$ (การบวก) และ $\cdot$ (การคูณ) เป็นสัญลักษณ์ที่แทนการดำเนินการใด ๆ ก็ได้โดยไม่จำเป็นต้องเป็นการดำเนินการการบวกและการคูณในเรื่องของระบบจำนวนจริง ซึ่งเรามักเรียกการดำเนินการแรกของริงว่าการบวก และเรียกการดำเนินการหลังของริงว่าการคูณ

เห็นได้ชัดว่าเซตของจำนวนเต็ม $\mathbb{Z}$ เซตของจำนวนตรรกยะ $\mathbb{Q}$ และเซตของจำนวนจริง $\mathbb{R}$ กับการบวก และการคูณปกติเป็นริง เซตของจำนวนเต็มมอดุโล n $(\mathbb{Z}_n)$ กับการบวกในมอดุโล n $(+_n)$ และการคูณในมอดุโล n $(\cdot_n)$ เป็นริง นอกจากนี้ยังมีตัวอย่างอื่น ๆ ดังนี้

ตัวอย่างที่ 7.1 กำหนดให้ $R = \{f \mid f : \mathbb{R} \longrightarrow \mathbb{R}\}$ และสำหรับ $f, \mathrm{g} \in \mathbb{R}$ กำหนดการบวก และการคูณบนเซต R ดังนี้

$$(f + \mathrm{g})(x) = f(x) + \mathrm{g}(x)$$

และ $$(f \cdot \mathrm{g})(x) = f(x)\mathrm{g}(x) \qquad \text{สำหรับทุก } x \in \mathbb{R}$$

จงพิจารณาว่า $(R,+,\cdot)$ เป็นริงหรือไม่ อย่างไร

วิธีทำ จะแสดงว่า $(R,+)$ เป็นอาบีเลียนกรุป

(1) ให้ $f,g\in R$
จาก $(f+g)(x)=f(x)+\mathrm{g}(x)\in\mathbb{R}$ สำหรับทุก $x\in\mathbb{R}$ จึงได้ว่า $f+g:\mathbb{R}\longrightarrow\mathbb{R}$
ดังนั้น $f+g\in R$ นั่นคือ $(R,+)$ มีสมบัติปิด

(2) สำหรับ $f,g,h\in R$ พิจารณา

$$\begin{aligned}((f+g)+h)(x)&=(f+g)(x)+h(x)\\&=(f(x)+g(x))+h(x)\\&=f(x)+(g(x)+h(x))\\&=f(x)+(g+h)(x)\\&=(f+(g+h))(x)\end{aligned}$$

สำหรับทุก $x\in\mathbb{R}$ ดังนั้น $(f+g)+h=f+(g+h)$
นั่นคือ $(R,+)$ มีสมบัติการเปลี่ยนหมู่

(3) มีฟังก์ชันศูนย์ เป็นสมาชิกเอกลักษณ์
นั่นคือ $(R,+)$ มีสมบัติการมีเอกลักษณ์

(4) ให้ $f\in R$ ดังนั้น $f(x)\in R$
นิยามฟังก์ชัน g โดย $g(x)=-f(x)$ สำหรับทุก $x\in\mathbb{R}$
จะได้ว่า $g\in R$ และ

$$(f+g)(x)=f(x)+g(x)=f(x)-f(x)=0$$
$$(g+f)(x)=g(x)+f(x)=-f(x)+f(x)=0$$

ดังนั้น $f+g$ และ $g+f$ เป็นฟังก์ชันศูนย์
นั่นคือ $(R,+)$ มีสมบัติการมีอินเวอร์ส

(5) จากจำนวนจริงมีสมบัติการสลับที่ภายใต้การบวก ดังนั้น $(R,+)$ มีสมบัติการสลับที่
จาก (1), (2), (3), (4) และ (5) จะได้ว่า $(R,+)$ เป็นอาบีเลียนกรุป
ต่อไปจะแสดงว่า $(R,\cdot)$ เป็นกึ่งกรุป

(6) ให้ $f, g \in R$
จาก $(f \cdot g)(x) = f(x) \cdot \mathrm{g}(x) \in \mathbb{R}$ สำหรับทุก $x \in \mathbb{R}$
จึงได้ว่า $f \cdot g : \mathbb{R} \longrightarrow \mathbb{R}$
ดังนั้น $f \cdot g \in R$ นั่นคือ $(R, \cdot)$ มีสมบัติปิด

(7) สำหรับ $f, g, h \in R$ พิจารณา

$$\begin{aligned} ((f \cdot g) \cdot h)(x) &= (f \cdot g)(x) \cdot h(x) \\ &= (f(x) \cdot g(x)) \cdot h(x) \\ &= f(x) \cdot (g(x) \cdot h(x)) \\ &= f(x) \cdot (g \cdot h)(x) \\ &= (f \cdot (g \cdot h))(x) \end{aligned}$$

สำหรับทุก $x \in \mathbb{R}$ ดังนั้น $(f \cdot g) \cdot h = f \cdot (g \cdot h)$
นั่นคือ $(R, \cdot)$ มีสมบัติการเปลี่ยนหมู่
จาก (6) และ (7) จะได้ว่า $(R, \cdot)$ เป็นกึ่งกรุป

(8) สำหรับ $f, g, h \in R$ และ $x \in \mathbb{R}$ พิจารณา

$$\begin{aligned} (f \cdot (g + h))(x) &= f(x) \cdot (g + h)(x) \\ &= f(x) \cdot (g(x) + h(x)) \\ &= f(x) \cdot g(x) + f(x) \cdot h(x)) \\ &= (f \cdot g)(x) + (f \cdot h)(x) \\ &= ((f \cdot g) + (f \cdot h))(x) \end{aligned}$$

ดังนั้น $f \cdot (g + h) = f \cdot g + f \cdot h$ สำหรับทุก $x \in \mathbb{R}$
ในทำนองเดียวกัน จะได้ว่า $(g + h) \cdot f = g \cdot f + h \cdot f$ สำหรับทุก $x \in \mathbb{R}$
นั่นคือ $(R, +, \cdot)$ มีสมบัติการแจกแจง
เพราะฉะนั้น $(R, +, \cdot)$ เป็นริง

สมบัติเบื้องต้นของริง

บทนิยาม 7.2 กำหนดให้ $(R, +, \cdot)$ เป็นริง จะเรียก $(R, +, \cdot)$ ว่าริงสลับที่ (commutative ring) ก็ต่อเมื่อ $a \cdot b = b \cdot a$ สำหรับทุก $a, b \in R$ และเรียก $(R, +, \cdot)$ ว่าริงที่มีสมาชิกเอกลักษณ์ (ring with identity or ring with unit element) ก็ต่อเมื่อ มี $1 \in R$ ที่ทำให้ $1 \cdot a$ = $a \cdot 1 = a$ สำหรับทุก $a \in R$

จากบทนิยาม 7.2 จะได้ว่า ถ้า $(R, +, \cdot)$ เป็นริงที่มีสมาชิกเอกลักษณ์ แล้ว R จะมีสมาชิกเอกลักษณ์สำหรับการคูณ ซึ่งเราจะเขียนแทนด้วยสัญลักษณ์ 1 ซึ่งเรียกว่าสมาชิกเอกลักษณ์สำหรับการคูณ (multiplicative identity element) หรือสมาชิกเอกลักษณ์ (unit element) ของ $(R, +, \cdot)$ พิจารณา $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ และ $(\mathbb{R}, +, \cdot)$ ต่างก็เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์เนื่องจากมี

1 ทำหน้าที่เป็นสมาชิกเอกลักษณ์ รวมถึง $(\mathbb{Z}_n, +_n, \cdot_n)$ เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ เพราะว่ามี $[1]$ ทำหน้าที่เป็นสมาชิกเอกลักษณ์ สมบัติของริง $(Z, +, \cdot)$ อันหนึ่ง คือ ถ้า $a \cdot b = 0$ แล้ว $a = 0$ หรือ $b = 0$ สำหรับทุก $a, b \in \mathbb{Z}$ แต่สำหรับริง $(R, +_8, \cdot_8)$ เมื่อ $R = \{[0], [2], [4], [6]\} \subset \mathbb{Z}_8$ จะได้ว่า $[2] \cdot [4] = [0]$ โดยที่ $[2] \neq [0]$ และ $[4] \neq [0]$ ซึ่งในที่นี้ จะเรียก $[2], [4] \in R$ ว่าตัวหารของศูนย์ ดังบทนิยาม ต่อไปนี้

บทนิยาม 7.3 กำหนดให้ $(R, +, \cdot)$ เป็นริง และกำหนดให้ $a \in R$ โดยที่ $a \neq 0$ จะเรียก a ว่าตัวหารของศูนย์ (zero divisor or divisor of zero) ก็ต่อเมื่อ มี $b \in R$ โดยที่ $b \neq 0$ ที่ทำให้

$$a \cdot b = b \cdot a = 0$$

และเรียก $(R, +, \cdot)$ ว่าริงที่มีตัวหารของศูนย์ (zero with zero divisor) ก็ต่อเมื่อ ริง $(R, +, \cdot)$ มีสมาชิกที่เป็นตัวหารของศูนย์

พิจารณาริงสลับที่ $(\mathbb{Z}, +_n, \cdot_n)$ เมื่อ n ไม่เป็นจำนวนเฉพาะ จะได้ว่า $n = a \cdot b$ โดยที่ $1 < a < n$ และ $1 < b < n$ ดังนั้น

$$[0] = [n] = [a \cdot b] = [a] \cdot [b]$$

โดยที่ $[a] \neq [0]$ และ $[b] \neq [0]$ นั่นคือ $[a]$ และ $[b]$ เป็นตัวหารของศูนย์ของ $\mathbb{Z}_n$

พิจารณาริง $(M_2(\mathbb{Z}), +, \cdot)$ เมื่อ $M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{Z} \right\}$ จะเห็นว่า

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

ดังนั้น $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ และ $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ ต่างก็เป็นตัวหารของศูนย์ของ $M_2(\mathbb{Z})$

บทนิยาม 7.4 กำหนดให้ $(R, +, \cdot)$ เป็นริงสลับที่และเป็นริงที่มีสมาชิกเอกลักษณ์ 1 จะเรียกริง $(R, +, \cdot)$ ว่าอินทิกรัลโดเมน (integral domain) ก็ต่อเมื่อ $(R, +, \cdot)$ ไม่มีตัวหารของศูนย์

ริง $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ และ $(\mathbb{R}, +, \cdot)$ ต่างก็เป็นอินทิกรัลโดเมน สำหรับริง $(\mathbb{Z}_6, +_6, \cdot_6)$ เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ แต่ไม่เป็นอินทิกรัลโดเมน เพราะว่ามี $[2], [3] \in \mathbb{Z}_6$ ที่ทำให้ $[2] \cdot_n [3] = [0]$ นั่นคือ มี $[2]$ และ $[3]$ เป็นตัวหารของศูนย์

บทนิยาม 7.5 กำหนดให้ $(R, +, \cdot)$ เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ 1 จะเรียกริง $(R, +, \cdot)$ ว่าริงการหาร (divisiion ring) ก็ต่อเมื่อ $(R \setminus \{0\}, \cdot)$ เป็นกรุป

บทนิยาม 7.6 กำหนดให้ $(R,+,\cdot)$ เป็นริง และ $S \subseteq R$ จะเรียก S ว่าริงย่อย (subring) ก็ต่อเมื่อ $(S,+,\cdot)$ เป็นริง

สำหรับริง $(R,+,\cdot)$ ใด ๆ จะมี $(\{0\},+,\cdot)$ และ $(R,+,\cdot)$ เป็นริงย่อยเสมอ และเรียกริงย่อยทั้งสองว่าริงย่อยทริเวียล หรือ ริงย่อยชัด (trivial subring) ของ $(R,+,\cdot)$ ก่อนที่จะกล่าวถึงสมบัติของริง จะให้ข้อตกลงว่า สำหรับริง $(R,+,\cdot)$ ใด ๆ ถ้า $a,b \in R$ แล้วสัญลักษณ์ $-a$ แทนตัวผกผันภายใต้การบวกของ a และ a^{-1} แทนตัวผกผันภายใต้การคูณของ a (ในกรณีที่ a มีตัวผกผันภายใต้การคูณ) ในบางครั้งเมื่อไม่จำเป็นต้องบ่งบอกการดำเนินการทวิภาคบนเซต R เราจะเขียนว่า R เป็นริง แทน $(R,+,\cdot)$ เป็นริง ab แทน $a \cdot b$ และ $a-b$ แทน $a+(-b)$

ทฤษฎีบท 7.7 กำหนดให้ R เป็นริง และ $a,b \in R$ จะได้ว่า

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

การพิสูจน์ กำหนดให้ R เป็นริง และ $a,b \in R$

(1) พิจารณา $0 + a0 = a0 = a(0+0) = a0 + a0$
เนื่องจาก $(R,+)$ เป็นกรุป ดังนั้น กฎการตัดออกจึงเป็นจริง
จึงทำให้ $a0 = 0$ ในทำนองเดียวกัน จะได้ว่า $0a = 0$

(2) เนื่องจาก $ab + a(-b) = a(b+(-b)) = a0 = 0$
และ $ab + (-a)b = (a+(-a))b = 0b = 0$
ดังนั้น $a(-b)$ และ $(-a)b$ ต่างก็เป็นตัวผกผันภายใต้การบวกของ ab
เพราะว่า $(R,+)$ เป็นกรุป
ดังนั้น $-(ab)$ เป็นตัวผกผันภายใต้การบวกของ ab เช่นกัน
ดังนั้น $a(-b) = (-a)b = -(ab)$

(3) โดยข้อ (2) จะได้ว่า $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$

เนื่องจากริงทุกริงมีสมาชิกเอกลักษณ์ภายใต้การบวก (0) ดังนั้น สำหรับริงที่มีสมาชิกเพียงตัวเดียว จะได้ว่าสมาชิกนั้นคือ 0 และ $0+0=0=(0)(0)$ ซึ่งเรียกริงเช่นนี้ว่าริงทริเวียลหรือริงชัด (trivial ring) นั่นคือ $R=\{0\}$ คือ ริงทริเวียล ในกรณีที่ R เป็นริงที่มีสมาชิกเอกลักษณ์ 1 และ R ไม่เป็นริงทริเวียล จะได้ว่า 0 และ 1 แตกต่างกัน ดังบทแทรกต่อไปนี้

บทแทรก 7.8 กำหนดให้ R เป็นริงที่มีสมาชิกเอกลักษณ์ 1 และ R ไม่เป็นริงทริเวียล จะได้ว่า $0 \neq 1$ เมื่อ 0 คือ สมาชิกเอกลักษณ์ภายใต้การบวกของ R

การพิสูจน์ กำหนดให้ R เป็นริงที่มีสมาชิกเอกลักษณ์ 1 และ R ไม่เป็นริงทริเวียล
สมมติให้ $0 = 1$ จะได้ว่า
ถ้า $a \in R$ แล้ว $a = 1a = 0a = 0$
ดังนั้น $R = \{0\}$ เป็นริงทริเวียล
นั่นคือ $0 \neq 1$

ในกรณีที่ R เป็นริงที่มีสมาชิกเอกลักษณ์ จะได้ว่า

ทฤษฎีบท 7.9 กำหนดให้ R เป็นริงที่มีสมาชิกเอกลักษณ์ 1 จะได้ว่า

1. $(-1)a = -a$ สำหรับทุก $a \in R$
2. $(-1)(-1) = 1$

การพิสูจน์ กำหนดให้ R เป็นริงที่มีเอกลักษณ์ 1

(1) สมมติให้ $a \in R$ เนื่องจาก

$$a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$$

ดังนั้น $(-1)a$ เป็นตัวผกผันภายใต้การบวกของ a
แต่เนื่องจาก $-a$ เป็นตัวผกผันภายใต้การบวกของ a
จึงทำให้ $(-1)a = -a$

(2) จากข้อ (1) ถ้าให้ $a = -1$ จะได้ว่า $(-1)(-1) = -(-1) = 1$

ทฤษฎีบท 7.10 กำหนดให้ R เป็นริง และ $S \subseteq R$ โดยที่ $S \neq \varnothing$ จะได้ว่า S เป็นริงย่อยของ R ก็ต่อเมื่อ

1. $a - b \in S$ สำหรับทุก $a, b \in S$ และ
2. $ab \in S$ สำหรับทุก $a, b \in S$

การพิสูจน์ กำหนดให้ R เป็นริง และ $S \subseteq R$ โดยที่ $S \neq \varnothing$
ถ้า S เป็นริงย่อยของ R แล้วจะเห็นได้ชัดว่าสมบัติข้อ 1. และ 2. เป็นจริง
ในทางกลับกัน สมมติให้สมบัติข้อ 1. และ 2. เป็นจริง
กำหนดให้ $a, b \in S$
โดยข้อ 1. จะได้ว่า $a - a = 0 \in S$ และ $0 - b = -b \in S$
อาศัยทฤษฎีบท 5.3 จึงได้ว่า $(S, +)$ เป็นกรุปย่อยของ $(R, +)$
เนื่องจาก $S \subseteq R$ ฉะนั้น $a, b \in R$
แต่เพราะว่า $(R, +)$ เป็นอาบีเลียนกรุป จึงได้ว่า $a + b = b + a$
ดังนั้น $(S, +)$ เป็นอาบีเลียนกรุป
เนื่องจาก $S \subseteq R$ และ R มีสมบัติการเปลี่ยนหมู่สำหรับการคูณ
จึงทำให้ S มีสมบัติดังกล่าวด้วย
โดยสมบัติข้อ 2. จะได้ $(S, \cdot)$ เป็นกึ่งกรุป
เนื่องจาก R มีคุณสมบัติการแจกแจง จึงได้ว่า S มีสมบัติการกระจายด้วย
นั่นคือ S เป็นริงย่อยของ R

ตัวอย่างที่ 7.2 กำหนดให้ R เป็นริงใด ๆ และกำหนดเซต

$$Z(R) = \{r \in R \mid rx = xr \text{ สำหรับทุก } x \in R\}$$

จงแสดงว่า $Z(R)$ เป็นริงย่อยของ R

วิธีทำ เนื่องจากมี $0 \in R$ ที่ซึ่ง $0x = 0 = x0$ สำหรับทุก $x \in R$
ดังนั้น $0 \in Z(R)$ นั่นคือ $Z(R) \neq \varnothing$
สำหรับ $r, s \in Z(R)$ จะได้ว่า $r, s \in R$
เนื่องจาก R เป็นจริง จะได้ว่า $r - s, rs \in R$ และได้ว่า

$$(r - s)x = rx - sx = xr - xs = x(r - s) \quad \text{สำหรับทุก } x \in R$$

และ $(rs)x = r(sx) = r(xs) = (rx)s = (xr)s = x(rs)$ สำหรับทุก $x \in R$

ดังนั้น $r - s, rs \in Z(R)$
โดยทฤษฎีบท 7.10 จึงสรุปได้ว่า $Z(R)$ เป็นริงย่อยของ R
จะเรียกเซต $Z(R)$ ว่าศูนย์กลาง (center) ของ R

บทนิยาม 7.11 กำหนดให้ R เป็นริงใด ๆ จะเรียก $a \in R$ ว่าสมาชิกนิรพล (nilpotent element) ก็ต่อเมื่อ มีจำนวนเต็มบวก n ที่ทำให้

$$a^n = \underbrace{aaa \cdots a}_{\text{n ตัว}} = 0$$

ถ้า a เป็นสมาชิกนิรพล โดยที่ k เป็นจำนวนเต็มบวกที่น้อยที่สุดซึ่ง $a^k = 0$ แล้วจะเรียก a ว่าสมาชิกนิรพลขนาด k และเขียนแทนเซตของสมาชิกนิรพลทั้งหมดของ R ด้วยสัญลักษณ์ $N(R)$

ในริง $(\mathbb{Z}_4, +_4, \cdot_4)$ จะได้ว่า $[0], [2] \in \mathbb{Z}_4$ เป็นสมาชิกนิรพล ทั้งนี้เพราะว่า $[0]^1 = [0]$ และ $[2]^2 = [0]$ นั่นคือ $N(R) = \{[0], [2]\}$ เนื่องจาก $0^1 = 0$ ดังนั้น 0 เป็นสมาชิกนิรพลขนาด 1 นั่นคือ $0 \in N(R)$ และจะได้ว่า $N(R) \neq \phi$

ทฤษฎีบท 7.12 ถ้า R เป็นริงสลับที่ แล้ว $N(R)$ เป็นริงย่อยของ R

การพิสูจน์ กำหนดให้ R เป็นริงสลับที่
จะเห็นว่า $0 \in N(R)$ ดังนั้น $N(R) \neq \phi$
ให้ $a, b \in N(R)$ โดยที่ a และ b เป็นสมาชิกนิรพลขนาด k และ m ตามลำดับ
เนื่องจาก $ab = ba$ และ $a^k = b^m = 0$ เพราะฉะนั้น

$$\begin{aligned}
(a-b)^{k+m} &= \binom{k+m}{0} a^{k+m} + \binom{k+m}{1} a^{k+m-1}(-b)^1 + \cdots \\
&\quad + \binom{k+m}{m} a^k(-b)^m + \binom{k+m}{m+1} a^{k-1}(-b)^{m+1} \\
&\quad + \cdots + (-b)^{k+m} \\
&= 0
\end{aligned}$$

และ

$$\begin{aligned}
(ab)^{km} &= \underbrace{(ab)(ab)\cdots(ab)}_{\text{nk ตัว}} \\
&= \underbrace{aa\cdots a}_{\text{nk ตัว}}\underbrace{bb\cdots b}_{\text{nk ตัว}} \\
&= a^{km}b^{km} \\
&= (a^k)^m(b^m)^k \\
&= (0)^m(0)^k = 0
\end{aligned}$$

นั่นคือ $a - b, ab \in N(R)$
โดยทฤษฎีบท 7.10 จึงสรุปได้ว่า $N(R)$ เป็นริงย่อยของ R

บทนิยาม 7.13 กำหนดให้ R เป็นริงใด ๆ จะเรียกจำนวนเต็มบวก n ว่าแคแรกเทอริสติก (characteristic) ของ R ก็ต่อเมื่อ n เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้

$$na = \underbrace{a + a \cdots + a}_{n \text{ ตัว}} = 0 \text{ สำหรับทุก } a \in R$$

ถ้า k เป็นจำนวนเต็มบวกที่น้อยที่สุดซึ่ง $ka = 0$ แล้วจะเรียก a ว่าสมาชิกนิรพลขนาด k และเขียนแทนเซตของสมาชิกนิรพลทั้งหมดของ R ด้วยสัญลักษณ์ $N(R)$

การพิสูจน์ กำหนดให้ R เป็นอินทิกรัลโดเมนจำกัดที่มีสมาชิก q ตัว และ $a \in R$ จะได้ว่า

$$qa = \underbrace{a + a \cdots + a}_{q \text{ ตัว}} = 0 \text{ สำหรับทุก } a \in R$$

สมมติให้ $M = \{m \in \mathbb{N} | ma = 0$ สำหรับ $a \in R\}$
จะเห็นว่า $q \in M \subseteq \mathbb{N}$ ดังนั้น $M \neq \varnothing$
จึงทำให้ได้ว่า M มีสมาชิกตัวที่น้อยที่สุด สมมติว่าคือ m
เพราะฉะนั้น m เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $ma = 0$ สำหรับทุก $a \in R$ นั่นคือ R มีแคแรกเทอริสติก m

พิจารณา $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ จะได้ว่า $\mathbb{Z}_p$ เป็นอินทิกรัลโดเมนที่มีแคแรกเทอริสติก p ทั้งนี้เพราะว่า สำหรับทุก $[a] \in \mathbb{Z}_p$

นอกจากนี้ $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ และ $(\mathbb{C}, +, \cdot)$ เป็นอินทิกรัลโดเมนที่มีแคแรคเทอริสติกเป็นศูนย์ เพราะว่าสำหรับสมาชิก a ใด ๆ โดยที่ $a \neq 0$ และ $n \in \mathbb{Z}$ จะได้ว่า ถ้า $na = 0$ แล้ว $n = 0$

ทฤษฎีบท 7.14 กำหนดให้ R เป็นริงที่มีสมาชิกเอกลักษณ์ 1 จะได้ว่า R มีแคแรกเทอริสติก n ก็ต่อเมื่อ n เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $n1 = 0$

การพิสูจน์ ($\Rightarrow$) กำหนดให้ R เป็นริงที่มีสมาชิกเอกลักษณ์ 1
ถ้า R มีแคแรกเทอริสติก n
จะได้ว่า n เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $na = 0$ สำหรับทุก $a \in R$
และเนื่องจาก $1 \in R$
ดังนั้น n จึงเป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $n1 = 0$

($\Leftarrow$) ให้ n เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $n1 = 0$
สมมติให้ $a \in R$ จะได้ว่า

$$\begin{aligned} na &= \underbrace{a + a + \cdots + a}_{\text{n ตัว}} \\ &= a\,\underbrace{(1 + 1 + \cdots + 1)}_{\text{n ตัว}} \\ &= a(n1) \\ &= a0 \\ &= 0 \end{aligned}$$

นั่นคือ n เป็นแคแรกเทอริสติกของ R

ทฤษฎีบท 7.15 ถ้า D เป็นอินทิกรัลโดเมน แล้ว Char$(D) = 0$ หรือ Char$(D) = p$ อย่างใดอย่างหนึ่ง เมื่อ p เป็นจำนวนเฉพาะ

การพิสูจน์ กำหนดให้ D เป็นอินทิกรัลโดเมน และสมมติให้ Char$(D) \neq 0$
ดังนั้น จะมี p เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ $pa = 0$ สำหรับทุก $a \in D$
ต่อไปสมมติให้ n เป็นจำนวนเต็มบวกที่ $n|p$
ดังนั้น $n \leq p$ และ $p = nk$ สำหรับบาง $k \in \mathbb{N}$ โดยที่ $1 \leq k \leq p$
พิจารณา $0 = pa$ = $(nk)a = n(ka)$ สำหรับทุก $a \in D$
ถ้า $ka = 0$ สำหรับทุก $a \in D$
จะได้ว่า $k \geq p$ ทำให้ $k = p$
นั่นคือ $n = 1$
แต่ถ้า $ka \neq 0$ สำหรับบาง $a \in D$ และสมมติให้ $b \in D$
เนื่องจาก $(nk)a = 0$
ดังนั้น $((nk)a)b = (nd)(ka) = 0$
เนื่องจาก $ka \neq 0$ จึงได้ว่า $nb = 0$
ดังนั้น $nb = 0$ สำหรับทุก $b \in D$
เพราะฉะนั้น $n \geq p$ เป็นผลให้ $n = p$
จึงสรุปได้ว่า p เป็นจำนวนเฉพาะ

ในกรณีที่ D เป็นอินทิกรัลโดเมนจำกัด โดยทฤษฎีบท 7.15 จะได้บทแทรกดังต่อไปนี้

บทแทรก 7.16 ถ้า D เป็นอินทิกรัลโดเมนจำกัด แล้ว Char$(D) = p$ เมื่อ p เป็นจำนวนเฉพาะ

การพิสูจน์ กำหนดให้ D เป็นอินทิกรัลโดเมนจำกัด เนื่องจาก $(D, +)$ เป็นกรุปจำกัด
ดังนั้น ให้ $|D| = d$ จะได้ว่า

$$da = \underbrace{a + a + \cdots a +}_{\text{d ตัว}} = 0 \quad \text{สำหรับทุก } a \in D$$

นั่นคือ มีจำนวนเต็มบวก d ที่ทำให้ $da = 0$ สำหรับทุก $a \in D$
เพราะฉะนั้น Char$(D) \neq 0$
โดยทฤษฎีบท 7.15 จึงได้ว่า Char$(D) = p$ เป็นจำนวนเฉพาะ

สรุปท้ายบท